

СИЛА

 ThinOS 8.6

РУКОВОДСТВО АДМИНИСТРАТОРА

СОДЕРЖАНИЕ

ГЛАВА 1. ВВЕДЕНИЕ	3
ГЛАВА 2. ПЕРЕД НАЧАЛОМ РАБОТЫ С THINOS.....	4
ГЛАВА 3. НАЧАЛО РАБОТЫ	10
ГЛАВА 6. НАСТРОЙКА СОЕДИНЕНИЙ БРОКЕРОВ	64
ГЛАВА 7. НАСТРОЙКА ЛОКАЛЬНЫХ ПАРАМЕТРОВ	108
ГЛАВА 8. МОДУЛЬ ТСХ.....	118
ГЛАВА 9. ВЫПОЛНЕНИЕ ДИАГНОСТИКИ	120
ГЛАВА 10. УПРАВЛЕНИЕ BIOS НА THINOS.....	145
ГЛАВА 10. БЕЗОПАСНОСТЬ СИСТЕМЫ	154
ГЛАВА 11. УСТРАНЕНИЕ НЕПОЛАДOK В РАБОТЕ	157
ПРИЛОЖЕНИЕ А	158
ПРИЛОЖЕНИЕ Б. ВАЖНЫЕ ПРИМЕЧАНИЯ	167
ПРИЛОЖЕНИЕ В. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ	168
КОНТАКТНАЯ ИНФОРМАЦИЯ	169

ГЛАВА 1. ВВЕДЕНИЕ

Тонкие клиенты под управлением микропрограммного обеспечения СИЛА ThinOS отвечают исключительным требованиям безопасности и оптимальной производительности. Эти эффективные тонкие клиенты устойчивы к вирусам и вредоносному ПО, обеспечивая при этом сверхбыстрый доступ к приложениям, файлам и сетевым ресурсам, находящимся в среде Citrix, Dell vWorkspace, Microsoft VMware и других. Тонкие клиенты на базе ThinOS самоуправляемы, способны загружаться в течение нескольких секунд с момента включения и не обладают ни опубликованным API, ни локально доступной файловой системой, ни браузером, благодаря чему не требуют локальной установки антивирусного ПО или брандмауэра для защиты от вирусов и иного вредоносного ПО.

ОБ ЭТОМ РУКОВОДСТВЕ

Настоящее руководство предназначено для администраторов тонких клиентов под управлением ThinOS. В нем содержатся сведения и подробные конфигурации системы, которые призваны помочь Вам спроектировать среду ThinOS и управлять ею.

ГЛАВА 2. ПЕРЕД НАЧАЛОМ РАБОТЫ С THINOS

АВТОМАТИЗАЦИЯ ОБНОВЛЕНИЙ И ИЗМЕНЕНИЯ ПАРАМЕТРОВ С ПОМОЩЬЮ ЦЕНТРАЛИЗОВАННОЙ НАСТРОЙКИ КОНФИГУРАЦИИ

ThinOS управляется централизованно и настраивается с помощью INI-файлов так, что обновления и любые нужные конфигурации по умолчанию автоматически рассылаются по тонким клиентам в вашей среде. В настоящем разделе описано, как в три простых шага настроить среду на автоматическую рассылку обновлений и конфигураций по тонким клиентам под управлением ThinOS. Если INI-файлы не обнаружены, Вы можете задать нужные параметры в локальных диалоговых окнах на каждом тонком клиенте. Многие из этих параметров локальных конфигураций, такие как разрешение экрана, настройки мыши и клавиатуры, сохраняются в ThinOS во избежание сброса после перезагрузки. Однако, как только будут найдены INI-файлы, клиент с ThinOS после перезагрузки будет игнорировать локально-настроенные параметры и станет использовать те, что содержатся в INI-файле.

ПРИМЕЧАНИЕ: тонким клиентам СИЛА не требуется ПО для управления устройствами. Они настроены на получение IP-адреса, микропрограммного обеспечения и инструкций по конфигурации с сервера DHCP. Для более удобного управления тонким клиентом Вы можете использовать WDM или WMS.

АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ И НАСТРОЙКИ

Для того чтобы тонкий клиент под управлением ThinOS мог успешно обратиться к файлам INI и обновиться с сервера, Вам необходимо настроить на сервере правильную структуру папок, в которых расположены файлы INI и другие файлы обновления, дать тонкому клиенту инструкции по местонахождению сервера и затем перезагрузить или включить тонкий клиент.

Если DHCP и сервер настроены и доступны, тонкий клиент проверяет (при каждой загрузке) наличие обновлений по жестко закрепленным параметрам сервера DHCP (см. таблицу 1): №161 задает URL сервера, а параметр №162 – корневой путь к серверу. При наличии обновлений они устанавливаются автоматически.

ИСПОЛЬЗОВАНИЕ ПАРАМЕТРОВ DHCP

В таблице ниже содержатся доступные параметры DHCP.

Таблица 1. Параметры DHCP.

Параметр	Описание	Примечания
1	Маска подсети	Обязателен, если тонкий клиент должен взаимодействовать с серверами в другой подсети. MS DHCP требует наличия маски подсети и всегда отправляет ее.
2	Смещение вре-	Необязателен

Параметр	Описание	Примечания
	мени	
3	Шлюз по умолчанию	Необязателен, но рекомендуется Обязателен, если тонкий клиент должен взаимодействовать с серверами в другой подсети
6	Сервер имен доменов (DNS)	Необязателен, но рекомендуется
15	Имя домена	Необязателен, но рекомендуется. См. параметр 6.
28	Широковещательный адрес	Необязателен
44	IP-адрес сервера WINS	Необязателен
51	Время аренды адреса (Lease Time)	Необязателен, но рекомендуется
52	Перегрузка параметров (Option Overload)	Необязателен
53	Тип сообщения DHCP	Рекомендуется
54	IP-адрес сервера DHCP	Рекомендуется
55	Список запроса параметров	Передается тонким клиентом
57	Максимальный размер сообщения DHCP	Необязателен (всегда передается тонким клиентом)

Параметр	Описание	Примечания
58	Время T1 (воз- обновления)	Необязателен, но рекомендуется
59	Время T2 (пере- привязки)	Необязателен, но рекомендуется
61	Идентификатор клиента	Всегда передается
161	Файловый сер- вер (ftp/http/https)	Необязательная строка. Для этого параметра задается имя или IP-адрес файлового сервера. Если указано имя, оно должно быть преобразуемым серверами DNS, указанными в параметре б. Если сервер выдает пустую строку или не выдает значения для этого поля, файловым сервером по умолчанию считается машина, на которой расположен сервер DHCP.
162	Корневой путь к файловому сер- веру (ftp/http/https)	<p>Необязательная строка. Если сервер выдает пустую строку или не выдает значения для этого поля, используется строка null.</p> <p>К пути поиска автоматически добавляется \wyse\wnos. Например, если Вы указали pub\serversoftware, поиск будет осуществляться по пути pub\serversoftware\wyse\wnos.</p> <p>ПРИМЕЧАНИЕ: автодобавление компонента \wyse можно отключить, дописав к введенной строке знак доллара (\$). Например, если Вы указали pub\serversoftware\$, поиск будет осуществляться по пути pub\serversoftware\wnos.</p> <p>ПРИМЕЧАНИЕ: наличие или отсутствие ведущего слэша (\) в строке пути для некоторых серверов может быть важным. Некоторые серверы ограничивают доступ к корневому пути пользователя, указанного при входе в систему. Для этих серверов наличие ведущего слэша необязательно. Некоторые серверы *NIX можно настроить так, чтобы пользователь файла имел доступ ко всей файловой системе. Для таких серверов указание ведущего слэша означает, что доступ начинается с корневой файловой системы. Необходимо обеспечить точное соответствие спецификации файла файловому</p>

Параметр	Описание	Примечания
		серверу. На безопасных серверах Windows слэш необходимо указывать для штатного доступа.
165	Сервер WMS	Необязательная строка. Содержит IP-адрес сервера WMS
166	Сервер WMS MQTT	Необязательная строка. Содержит IP-адрес сервера MQTT
167	Проверка WMS CA	Необязательная строка
181	Список серверов PNAgent/PNLite	Необязательная строка. Тонкий клиент использует этот сервер для аутентификации учетных данных пользователя Windows и получения списка опубликованных в ICA приложений, которые валидны для проверенных учетных данных. Пользователь вводит эти учетные данные при входе в систему на тонком клиенте.
182	Список доменов NT для PNAgent/PNLite	<p>Необязательная строка. Тонкий клиент создает прокручиваемый список доменов на основе информации из данного пункта.</p> <p>Этот список выводится при входе в систему тонкого клиента в порядке, заданном в этом (182) параметре DHCP (например, первый указанный домен становится доменом по умолчанию). Пользователь выбирает домен, в котором он затем пройдет аутентификацию по ID и паролю. Для аутентификации используется только выбранный домен. Если список доменов неполон и учетные данные пользователя должны проверяться в домене, которого нет в списке (при условии, что сервер из параметра 181 способен выполнить аутентификацию в домене, отсутствующем в списке), пользователь может не выбирать домены, перечисленные в этом (182) параметре, а просто ввести при входе в систему нужное доменное имя.</p>

Параметр	Описание	Примечания
184	Имя пользователя для файлового сервера	Необязательная строка. Имя пользователя, которое будет использоваться для аутентификации на сервере, указанном в параметре 161.
185	Пароль для файлового сервера	Необязательная строка. Пароль, который будет использоваться для аутентификации на сервере, указанном в параметре 161.
186	Список серверов WDM	Необязательные двоичные IP-адреса WDM. В этом параметре можно указать до двух серверов WDM. Если указано два сервера, то при загрузке тонкий клиент попытается подключиться к первому из них. Если к первому подключиться не удастся, он попытается подключиться ко второму.
187	Порт сервера WDM	<p>Необязательное число. Формат: Byte, Word или массив из двух значений типа Byte.</p> <p>ПРИМЕЧАНИЕ: значение этого параметра, если не встроено в параметр информации о классе вендора (Vendor Class Specific Information), интерпретируется в обратном порядке, когда передается в виде двухбайтовой последовательности: например, переданное значение 0x0050 превратится в 0x5000. Этот параметр используется старыми версиями ThinOS. В новых версиях ThinOS он присутствует для обратной совместимости.</p>
188	Сервер Virtual Desktop Broker	Необязательная строка
190	Безопасный порт WDM	Необязательный параметр. Формат: Word или массив из двух значений типа Byte. Предписывает использовать для взаимодействия с WDM протокол HTTPS вместо HTTP.

Параметр	Описание	Примечания
192	Порт сервера WDM	<p>Необязательный параметр. Формат: Word или массив из двух значений типа Byte.</p> <p>ПРИМЕЧАНИЕ: значение этого параметра содержит ту же информацию, что в параметре 187. Разница в том, что значение этого параметра интерпретируется ThinOS в правильном порядке (т.е., например, 0x0050 так и останется 0x0050). Если сервер DHCP выдает значения и для параметра 192, и для 187, параметр 192 имеет преимущественную силу.</p>
194	WDM FQDN	Необязательный параметр: полное доменное имя для WDM
199	Групповой ключ WMS	<p>Необязательная строка. Может содержать групповой регистрационный ключ WMS для агента WMS. Вступает в силу в ситуации, когда WMS отключен и групповой ключ WMS равен null. Эта необязательная строка используется WMS в качестве группового регистрационного ключа. Если сервер WMS или сервер MQTT имеет значение null, то агент WMS устанавливает для них стандартные значения серверов.</p>

ГЛАВА 3. НАЧАЛО РАБОТЫ

Эта глава поможет Вам быстро усвоить основы и начать работу с Вашим тонким клиентом.

НАСТРОЙКА THINOS С ПОМОЩЬЮ МАСТЕРА ПЕРВОГО ЗАПУСКА

First Boot Wizard (Мастер первого запуска) активируется, когда вВы впервые загружаете новый тонкий клиент под управлением ThinOS. Тонкий клиент запускает приложение First Boot Wizard до того, как Вы оказываетесь на системном рабочем столе ThinOS, и позволяет Вам выполнить набор задач, таких как: настройка системных предпочтений, настройка подключения к Интернету, загрузка конфигураций с USB, настройка управляющего ПО и настройка брокерных соединений.

Если Вы уже являетесь пользователем тонкого клиента и обновили ThinOS до версии 8.5 или более поздней, то для запуска мастера первого запуска Вы можете сбросить тонкий клиент в заводские настройки.

Диаграмма работы мастера первого запуска показана на рисунках 1 и 2.

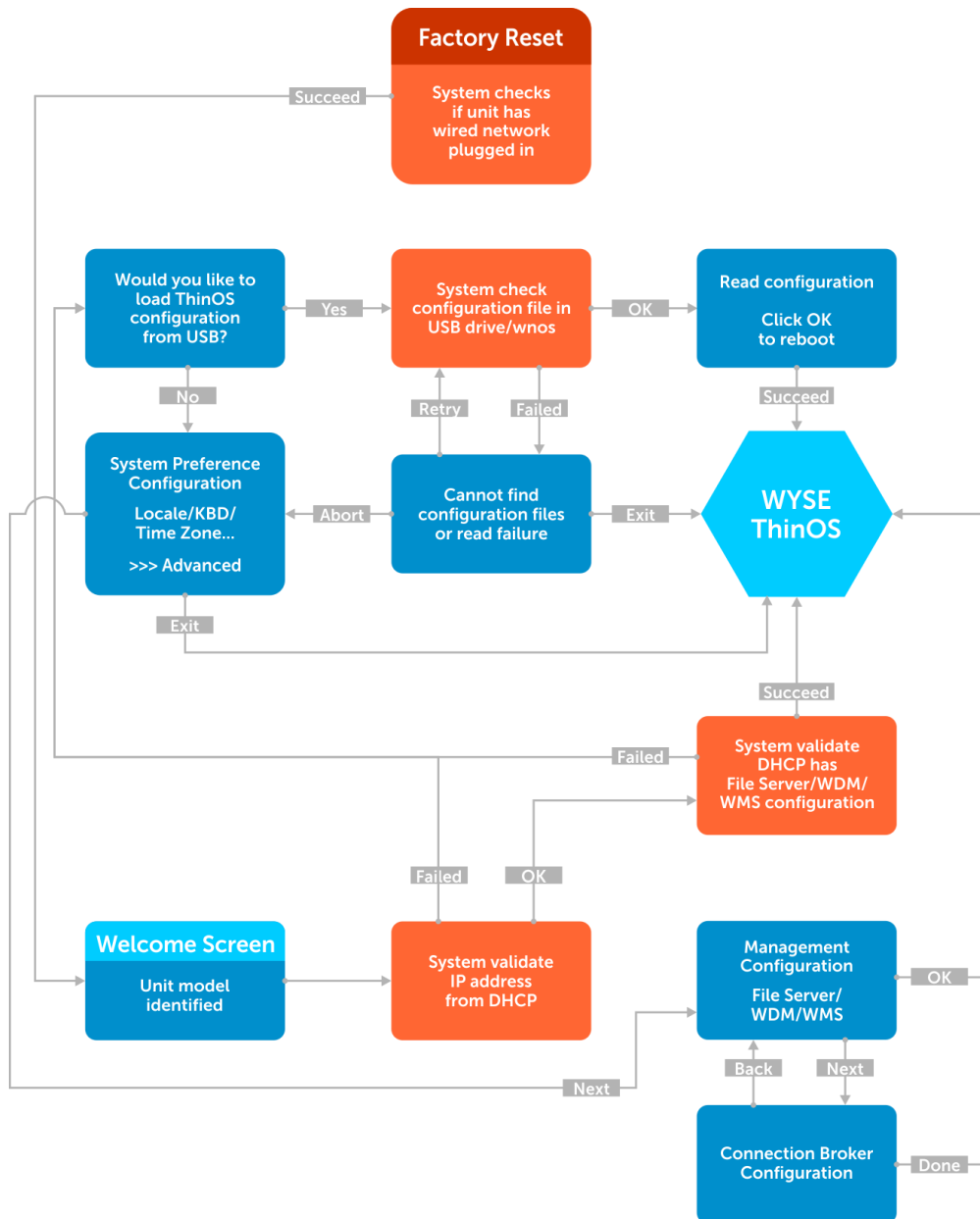


Рис. 1. Мастер первого запуска – сеть успешно обнаружена.

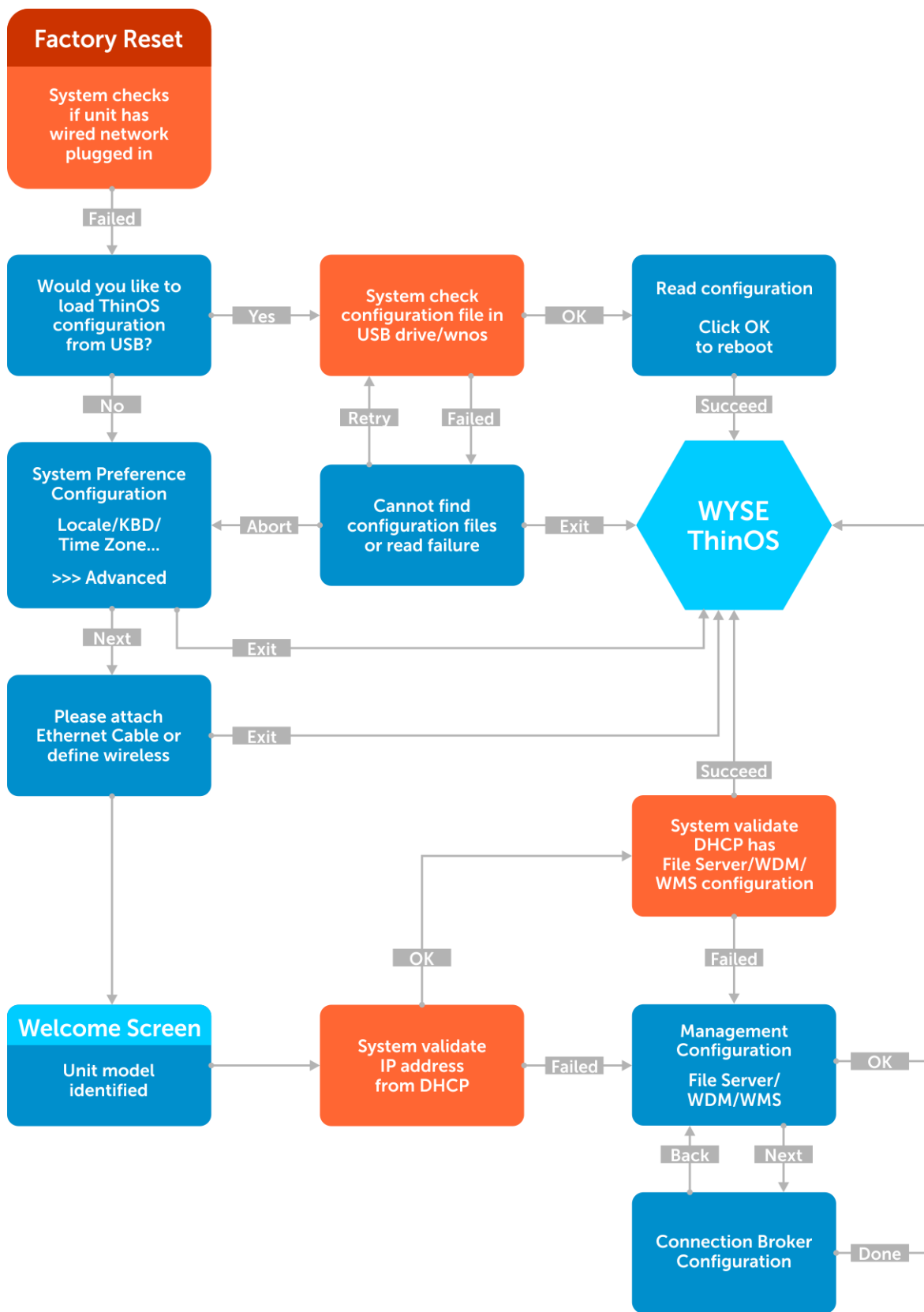


Рис. 2. Мастер первого запуска – сеть не обнаружена.

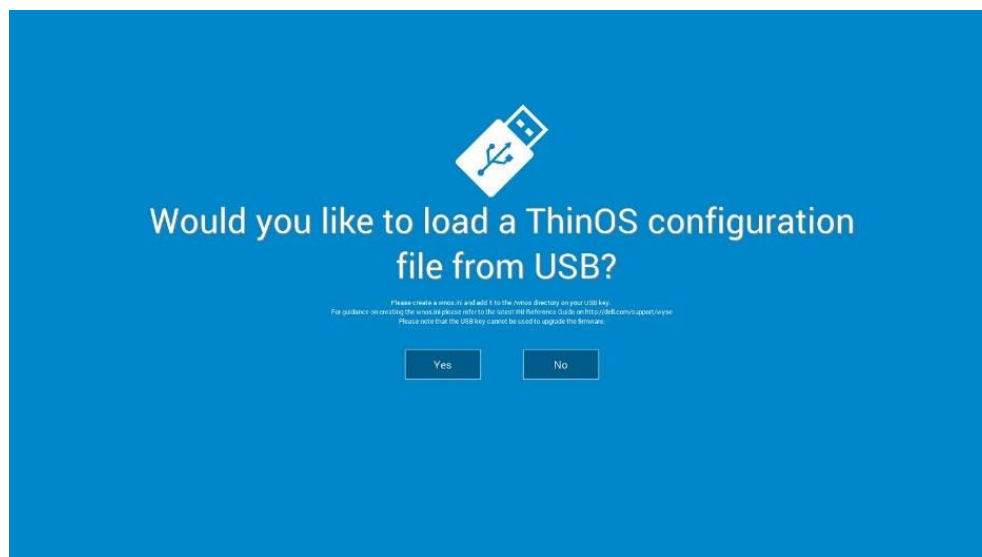
Первичная настройка через мастер первого запуска (First Boot Wizard):

1. Подключите новый или существующий тонкий клиент к Ethernet с помощью проводного подключения. Для запуска First Boot Wizard на существующем тонком клиенте необходимо восстановить на нем заводские настройки по умолчанию.
2. Включите тонкий клиент.

Тонкий клиент проверяет наличие подключения к проводной сети. Если сеть успешно обнаружена, появляется приветственный экран, на котором указано название модели Вашего тонкого клиента.

Тонкий клиент проверяет IP-адрес, полученный от DHCP. Если DHCP содержит конфигурации файлового сервера и WMS, то сразу загружается рабочий стол ThinOS, а мастер первого запуска не активируется. Если проверка DHCP проходит неудачно или если подключение к Ethernet отсутствует, переходите к следующему шагу.

ПРИМЕЧАНИЕ: чтобы закрыть мастер первого запуска во время проверки состояния сети на приветственном экране, нажмите Ctrl + Esc.



На экране **Would you like to load a ThinOS configuration file from USB?** (Загрузить файл конфигурации ThinOS с USB-накопителя?). Выберите **Yes** (Да) или **No** (Нет).

Чтобы загрузить файл конфигурации ThinOS с USB-флеш-накопителя, убедитесь в том, что Вы создали файл wnos.ini и добавили его в каталог /wnos на USB-накопителе. Таким образом, Вы можете загружать пакеты и обои рабочего стола, прописанные в INI-файле. Вставьте USB-накопитель в разъем тонкого клиента и нажмите на кнопку **Yes** (Да).

ПРИМЕЧАНИЕ: поддерживаются только USB- накопители с файловыми системами FAT, FAT32 и ExFAT. USB-накопители с файловой системой NTFS не поддерживаются.

Тонкий клиент проверяет файл конфигурации, считанный с USB -накопителя.

Если файл конфигурации ThinOS, найденный на USB-накопителе, правилен, то появляется сообщение: «Read configuration success» (Конфигурация прочитана успешно). Нажмите на кнопку **OK**, чтобы закрыть мастер первого запуска и загрузить рабочий стол ThinOS.

Если файл конфигурации ThinOS wnos.ini не найден или повреждён, то появляется сообщение: «Cannot find configuration files, or read configuration failure» (Невозможно найти файлы конфигурации или ошибка чтения конфигурации). Запишите на USB-накопитель нужный файл, вставьте

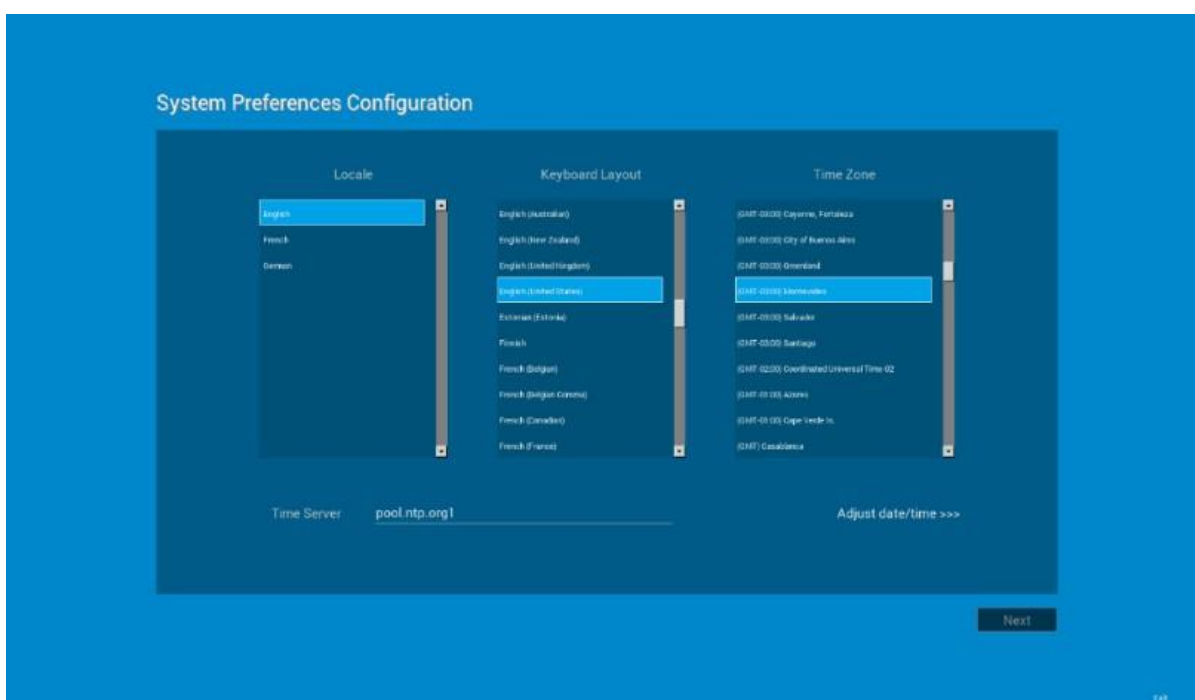
USB-накопитель в тонкий клиент и нажмите на кнопку **Retry** (Повторить). Если файл правильный, появится сообщение: «Read configuration success» (Конфигурация прочитана успешно). Нажмите на кнопку **OK**, чтобы закрыть мастер первого запуска и загрузить рабочий стол ThinOS.

Если Вы не хотите загружаться с USB-накопителя, то вместо **Retry (Повторить)** нажмите на кнопку **Abort (Прервать)**, чтобы открыть интерфейс конфигурации системных предпочтений.

ПРИМЕЧАНИЕ: чтобы закрыть экран сообщения: «Cannot find configuration files, or read configuration failure (Невозможно найти файлы конфигурации или ошибка чтения конфигурации)» и загрузить рабочий стол ThinOS, нажмите на кнопку Exit (Выход).

При выборе **No (Нет)** откроется интерфейс конфигурации системных предпочтений.

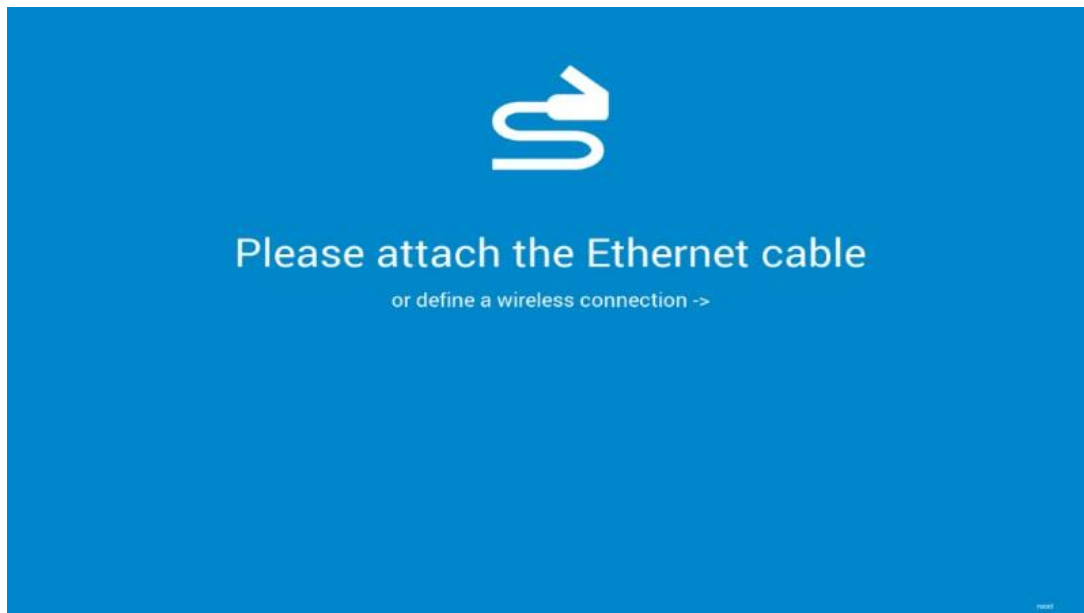
3. На экране **System Preferences Configuration** (Настройка системных предпочтений) настройте следующие параметры:



- **Locale** (Язык и региональные стандарты) – выберите язык, на котором будет загружаться ThinOS;
- **Keyboard Layout** (Раскладка клавиатуры) – выберите нужную раскладку клавиатуры;
- **Time Zone** (Часовой пояс) – выберите часовой пояс;
- **Time Server** (Сервер времени) – здесь перечислены IP-адреса или имена хостов серверов времени, порт указывать не обязательно;
- **Advanced** (Дополнительно) – нажмите на кнопку **Advanced** (Дополнительно), чтобы настроить такие параметры, как переход на летнее/зимнее время, формат даты и времени, сервер времени и т.п.

ПРИМЕЧАНИЕ: чтобы закрыть экран настройки системных предпочтений и загрузить рабочий стол ThinOS, нажмите на кнопку **Exit** (Выход).

Если нет подключения к Ethernet, то появится сообщение о необходимости подключить сетевой кабель.



Выполните одно из следующих действий:

- подключите кабель Ethernet к тонкому клиенту;
- нажмите на кнопку **Define a wireless connection** (Определить беспроводное подключение). Из списка выберите беспроводную сеть и нажмите на кнопку **Connect** (Подключиться).

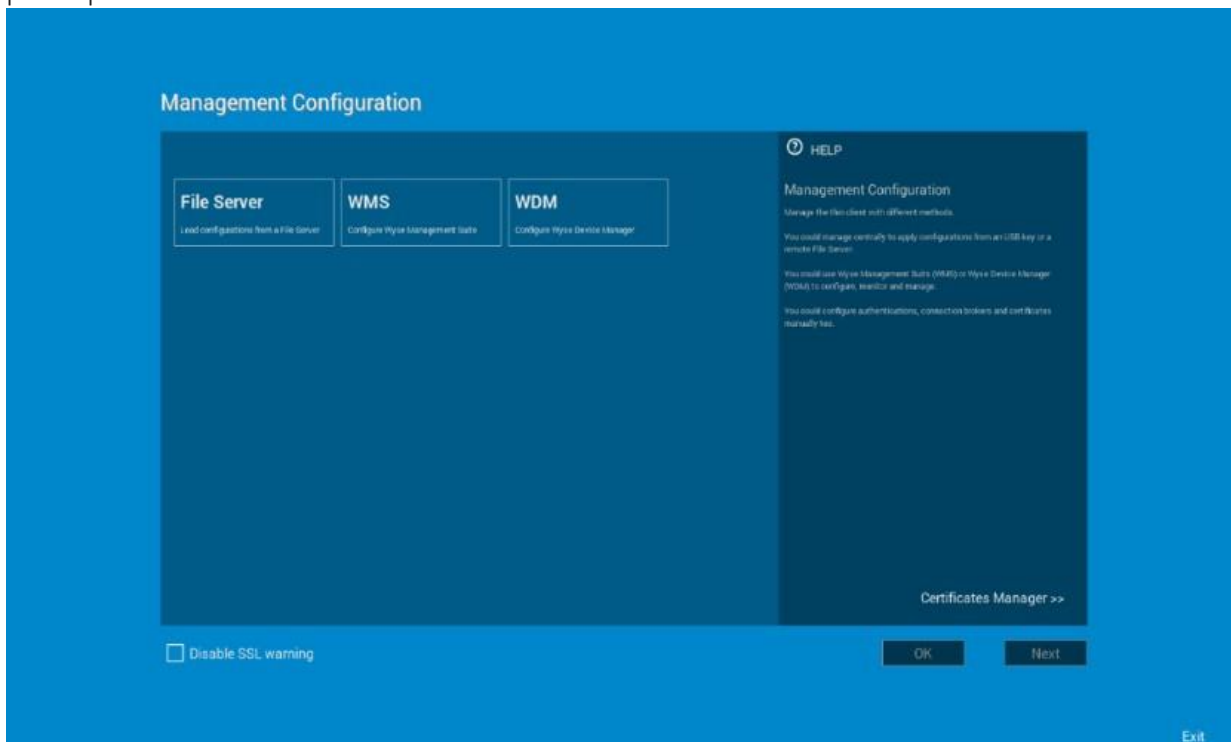
ПРИМЕЧАНИЕ:

- на тонких клиентах без модуля WLAN задать беспроводную сеть нельзя;
- чтобы закрыть экран **Attach the Ethernet cable** (Подключите кабель Ethernet) и загрузить рабочий стол ThinOS, нажмите на кнопку **Exit** (Выход).

После установки соединения тонкий клиент проверяет IP-адрес, полученный от DHCP. Если DHCP содержит конфигурации файлового сервера, WMS, то загрузится рабочий стол ThinOS. Если проверка DHCP проходит неудачно или не удастся установить подключение к сети, появится экран *Management Configuration* (Конфигурация управления). Переходите к шагам 6–9.

4. Нажмите на кнопку **Next** (Далее), чтобы открыть экран *Management Configuration* (Конфигурация управления).

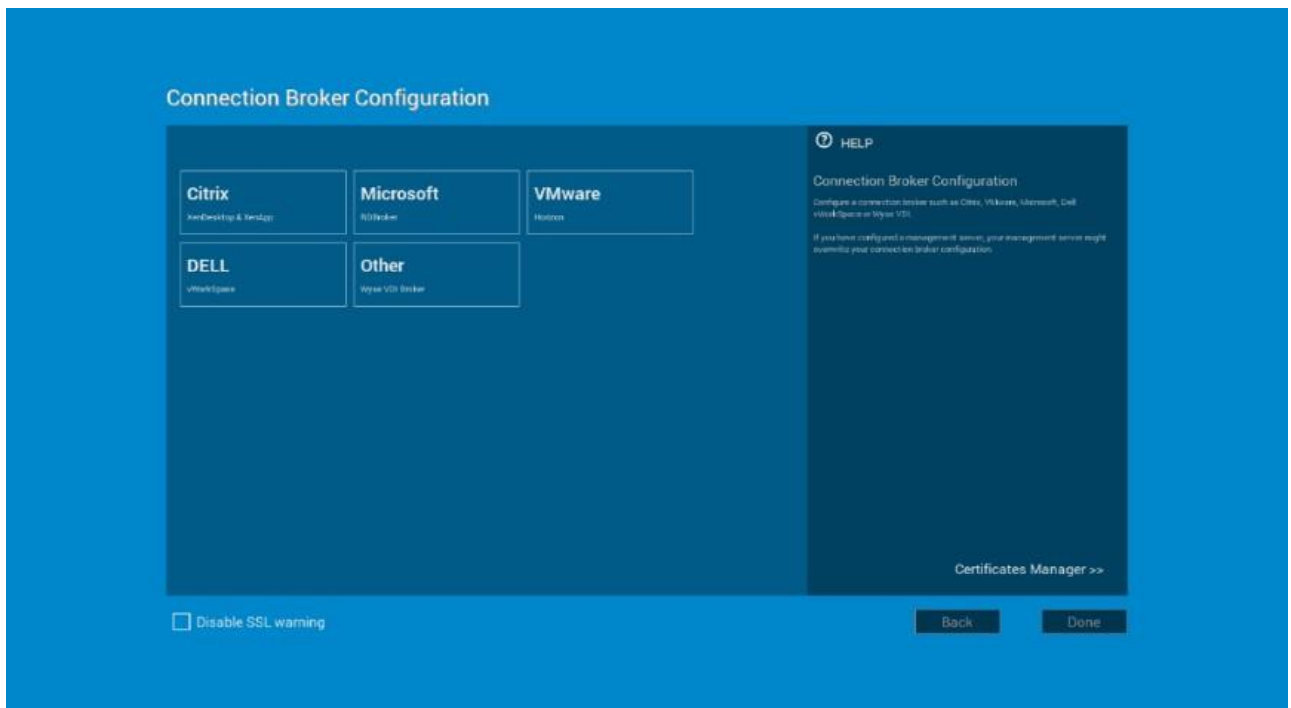
5. На экране **Management Configuration** (Конфигурация управления) настройте следующие параметры:



- **File Server** (Файловый сервер) – введите данные файлового сервера, чтобы получать с него конфигурации, в том числе файлы INI, микропрограммное обеспечение и пакеты обновлений.
- **WMS** – введите групповой регистрационный ключ и URL сервера WMS, чтобы зарегистрировать тонкий клиент в WMS.
- **WDM** – введите IP-адреса или имена хостов серверов WDM.
- **Disable SSL warning** (Отключить предупреждение SSL) – установите этот флажок, чтобы отключить вывод предупреждений SSL (Secure Sockets Layer).
- **Certificates Manager** (Диспетчер сертификатов) – нажмите на кнопку **Certificates Manager**, чтобы импортировать или запросить сертификат.

ПРИМЕЧАНИЕ: чтобы закрыть экран **Management Configuration** (Конфигурация управления) и загрузить рабочий стол ThinOS, нажмите на кнопку **Exit** (Выход).

6. Нажмите на кнопку **Done** (Готово) для выхода из мастера первого запуска или кнопку **Next** (Далее) для перехода к настройке брокера подключений.
7. На экране **Connection Broker Configuration** (Конфигурация брокера подключений) настройте следующие параметры:



- **Citrix:** этот брокер позволяет подключаться к полным рабочим столам с помощью Citrix Virtual Apps and Desktops (ранее Citrix XenDesktop) или к отдельным приложениям с помощью Citrix Virtual Apps (ранее Citrix XenApp) с централизованного хоста посредством Citrix Receiver Client;
 - **Server Address** (Адрес сервера): введите имя или IP-адрес брокера подключений;
 - **Enable theme: ThinOS Lite** (Разрешить тему: ThinOS Lite): установите этот флажок для загрузки тонкого клиента в режиме ThinOS Lite;
 - **StoreFront style** (Стиль StoreFront): установите этот флажок, чтобы включить на тонком клиенте макет опубликованных приложений и рабочих столов на основе Citrix StoreFront;
- **Microsoft:** этот брокер позволяет подключаться к виртуальным рабочим столам с помощью подключений RemoteApp и Remote Desktop Connection. Введите имя или IP-адрес брокера подключений;
- **VMware:** этот брокер позволяет Вам подключаться к удаленным рабочим столам с помощью клиента VMware Horizon;
 - **Server Address** (Адрес сервера): введите имя или IP-адрес брокера подключений;
 - **Enable theme: VMware View** (Разрешить тему: VMware View): установите этот флажок, чтобы выбрать для рабочего стола ThinOS тему VMware View;
- **DELL:** этот брокер позволяет подключаться к виртуальным рабочим столам или приложениям с помощью Dell vWorkspace. Введите имя или IP-адрес брокера подключений;
- **Amazon WorkSpaces:** этот брокер позволяет клиентам PCoIP подключаться к виртуальным рабочим столам под управлением AWS. Введите имя хоста, IP-адрес или полное доменное имя брокерного подключения;

ПРИМЕЧАНИЕ: вариант Amazon WorkSpaces доступен только для клиентов PCoIP.

- **Other** (Другое): этот вариант позволяет Вам подключаться к виртуальным рабочим столам или приложениям с помощью других поддерживаемых протоколов. Введите имя или IP-адрес брокера подключений;
- **Certificates Manager** (Диспетчер сертификатов): нажмите на кнопку **Certificates Manager**, чтобы импортировать или запросить сертификат;
- **Disable SSL warning** (Отключить предупреждение SSL): установите этот флажок, чтобы отключить вывод предупреждений для подключения SSL (Secure Sockets Layer);

8. Нажмите на кнопку **Done** (Готово).

ПРИМЕЧАНИЕ: чтобы выполнить настройку конфигурации управления еще раз, нажмите на кнопку **Back** (Назад) и выполните шаги 6 и 7.

Работа мастера первого запуска завершается, и на экране появляется рабочий стол ThinOS.

РАБОТА С ВАШИМ РАБОЧИМ СТОЛОМ

То, что Вы видите после входа в систему на сервере, зависит от конфигурации.

Пользователи с классическим рабочим столом увидят классический рабочий стол ThinOS с полной панелью задач, рабочим столом и диспетчером подключений Connect Manager, хорошо знакомыми пользователям ThinOS. Этот вариант установлен на заводе по умолчанию и рекомендуется для сред сервера терминалов с опубликованными приложениями, а также для обратной совместимости с версиями ThinOS 6.x. Более подробно мы поговорим о классическом рабочем столе в разделе [Характеристики классического рабочего стола](#).

Пользователи рабочего стола Zero увидят рабочий стол Zero с панелью инструментов Zero и назначенным списком подключений на выбор. Этот вариант рекомендуется для VDI и любых подключений, эксплуатируемых только в полноэкранном режиме. Более подробно мы поговорим о рабочем столе Zero в разделе [Характеристики рабочего стола Zero](#).

В любом случае, Вы можете выбрать тот рабочий стол, который Вам нужен (классический или Zero), и создать нужные подключения на панели **Visual Experience** (Визуальный облик) диалогового окна **Remote Connections** (Удаленные подключения). Чтобы открыть диалоговое окно **Remote Connections**, выполните одну из следующих задач:

Классический рабочий стол: щелкните по имени пользователя и затем выберите System Setup (Настройка системы) > Remote Connections (Удаленные подключения).

ПРИМЕЧАНИЕ: имеется в виду имя пользователя, вошедшего в систему. Оно отображено в нижней левой части панели задач.

Рабочий стол Zero: щелкните по значку System Settings (Параметры системы) на панели инструментов Zero и затем выберите Remote Connections (Удаленные подключения).

БЛОКИРОВКА ТОНКОГО КЛИЕНТА

Чтобы никто не смог получить доступ к информации без разрешения, в ThinOS есть возможность заблокировать тонкий клиент. После этого для дальнейшей работы требуется указать учетные данные. Для блокировки выполните любое из следующих действий:

Отсоедините смарт-карту входа в систему: если администратор установил параметр SCRemovalBehavior=1 в INI-файлах, то тонкий клиент будет блокироваться, стоит Вам вынуть

смарт-карту, с помощью которой Вы входили в систему на этом тонком клиенте. Чтобы разблокировать тонкий клиент, Вам потребуется та же самая смарт-карта и правильный PIN-код. Обратите внимание, что при отсоединении смарт-карты Вы можете выйти из системы, если администратор настроил такое поведение в INI-файлах. В таком случае Вам придется потом войти в систему как обычно.

Используйте команду Lock Terminal (Заблокировать терминал) в контекстном меню и диалоговом окне выключения питания (Shutdown): на классическом рабочем столе можно щелкнуть правой кнопкой на пустом месте экрана и выбрать из контекстного меню Lock Terminal, или же воспользоваться диалоговым окном Shutdown. На рабочем столе Zero используйте диалоговое окно Shutdown. Чтобы разблокировать тонкий клиент, Вам потребуется указать свой пароль.

Используйте экранную заставку: если администратор указал значение LockTerminal=2 для параметра ScreenSaver, то при активации экранной заставки тонкий клиент блокируется. Чтобы разблокировать тонкий клиент, введите свой пароль входа в систему в диалоговом окне разблокировки. Обратите внимание, что при работе с диалоговым окном разблокировки Вы не сможете видеть обои.

ВЫХОД ИЗ СИСТЕМЫ И ВЫКЛЮЧЕНИЕ

В диалоговом окне **Shutdown** (Выключение) выберите соответствующий вариант:

Классический рабочий стол: нажмите на **Shutdown** (Выключение) в меню диспетчера подключений Connect Manager или в меню рабочего стола.

Рабочий стол Zero: щелкните по значку **Shutdown** (Выключение) на панели инструментов Zero.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ДЛЯ НАЧАЛА РАБОТЫ

В этом разделе мы вкратце поговорим о рабочем столе Zero, классическом рабочем столе, диалоговом окне входа в систему и системной информации.

КАК РАБОТАТЬ С ИНТЕРАКТИВНЫМ РАБОЧИМ СТОЛОМ ZERO

У рабочего стола Zero установлен фон по умолчанию, а в левой части экрана расположена панель инструментов Zero. В таблице перечислены клавиши быстрого доступа для рабочего стола Zero:

Таблица 2. Клавиши быстрого доступа для рабочего стола Zero.

Действие	Клавиши
Открыть панель инструментов Zero	Ctrl+Alt+стрелка вверх
Открыть окно выбора для переключения между рабочим столом и активными в данный момент подключениями	Ctrl+Alt+стрелка вниз
Заблокировать тонкий клиент	Ctrl+Alt+стрелка влево или Ctrl+Alt+стрелка вправо
Клавиши быстрого доступа для команд меню	Левый Alt + подчеркнутая буква или правый Alt + подчеркнутая буква
Сделать скриншот полного рабочего стола и поместить в буфер обмена	Print Screen
Сделать скриншот активного окна и поместить в буфер обмена	Alt+PrintScreen

ПРИМЕЧАНИЕ: функция копирования и вставки работает между различными сеансами приложений, а также между сеансами приложений и рабочим столом. Однако ее работа зависит от конфигурации серверных сеансов.

ПРИМЕЧАНИЕ: кроме стандартной двухкнопочной мыши, тонкий клиент поддерживает мышь Microsoft Wheel Mouse с колесом для прокрутки. Другие сходные типы мыши с колесом могут не работать.

Чтобы поменять местами левую и правую кнопки, используйте диалоговое окно **Peripherals (Периферия)**, см. раздел Настройка параметров периферии.

ПАНЕЛЬ ИНСТРУМЕНТОВ ZERO

Панель инструментов Zero обычно находится в левой части рабочего стола Zero. Однако администратор может настроить рабочий стол так, чтобы панель инструментов была убрана или спрятана. Она появляется только тогда, когда пользователь наводит указатель мыши на левый край экрана рабочего стола.

Администратор может настроить параметры панели инструментов в диалоговом окне или же с помощью параметра SysMode в файле wnos.ini.

Таблица 3. Значки на панели инструментов.

Значок	Описание
Home (Главная)	Открывает список доступных подключений
System Information (Системная информация)	Отображает системную информацию о тонком клиенте
System Settings (Параметры системы)	Открывает меню параметров системы, в котором можно настраивать параметры системы тонкого клиента и выполнять диагностику
Shutdown Terminal (Выключить терминал)	Щелкните по значку Shutdown Terminal (Выключить терминал) для выбора вариантов выключения, доступных на тонком клиенте
	ПРИМЕЧАНИЕ: значок «Выключить терминал» не отображается на панели инструментов при настройке системных параметров с помощью кнопки Admin Mode (Режим администратора).

ПРИМЕЧАНИЕ: на панели инструментов Zero отображаются текущая дата и время, если их отображение настроено администратором. Тонкий клиент может синхронизировать системные часы с сигналами времени, передаваемыми сервером SNTP (Simple Network Time Protocol).

СПИСОК ПОДКЛЮЧЕНИЙ

На панели инструментов Zero щелкните по значку **Home** (Главная), чтобы открыть список назначенных подключений. Иногда он содержит только подключения по умолчанию.

Используйте следующие параметры. В зависимости от уровня привилегий пользователя, некоторые параметры могут быть недоступны для использования:

Таблица 4. Параметры подключений.

Параметр	Описание
Имя подключения	Открывает подключение, которое Вы хотите использовать. ПРИМЕЧАНИЕ: слева от каждого открытого подключения в списке отображается синий значок.
Кнопка Reset (Сброс)	Сброс подключения. ПРИМЕЧАНИЕ: полезно в случае, если подключение работает неправильно

	или его необходимо перезапустить.
Кнопка Close (Закрыть)	Закрывает подключение. ПРИМЕЧАНИЕ: если подключение не открыто, кнопка Close становится серой.
Кнопка Edit (Правка)	Открывает диалоговое окно Connection Settings (Настройки подключения), где можно изменить параметры подключения. ПРИМЕЧАНИЕ: функции правки могут быть недоступны для низкого уровня привилегий.
Add Connection (Добавить подключение)	Позволяет настраивать и добавлять новые подключения.
Global Connection Settings (Глобальные параметры подключений)	Если Вы не используете файлы INI для задания глобальных параметров подключений, можно щелкнуть Global Connection Settings (Глобальные параметры подключений) и открыть одноименное диалоговое окно, в котором задаются параметры, влияющие на все подключения в списке.

РАБОТА С ТЕМОЙ ZERO

Используйте тему Zero, чтобы настроить по своему вкусу ThinOS в режиме Citrix, VMware, классическом или VDI. Чтобы активировать ту или иную тему Zero, задайте параметры INI соответственно вашим предпочтениям для темы Zero и перезапустите тонкий клиент. Появится сообщение «Visual experience settings are changed» (Настройки визуального облика изменены), и тонкий клиент загрузит выбранную тему Zero.

```
ZeroTheme={Classic,VDI,Citrix,VMware} SysMode={Classic,VDI,Citrix,VMware}
```

Параметры INI задаются в файле wnos.ini. Также можно управлять конфигурацией с помощью WMS.

Режим Citrix Zero: при настройке ThinOS в режиме Citrix Zero устройство ищет файл xen.ini и загружает режим Citrix Zero. Если файл xen.ini не удастся найти, то во время конфигурации используется файл wnos.ini. Если потребуется выйти из режима Citrix Zero, то во время конфигурации необходимо использовать wnos.ini.

Режим VMware Zero: при настройке ThinOS в режиме VMware Zero устройство загружает режим VMware Zero.

ПРИМЕЧАНИЕ: в режиме VMware Zero на экране отображаются обои VMware.

ХАРАКТЕРИСТИКИ КЛАССИЧЕСКОГО РАБОЧЕГО СТОЛА

В этом разделе содержатся сведения о классическом интерактивном рабочем столе, контекстном меню, меню рабочего стола и диспетчере подключений Connect Manager.

КАК РАБОТАТЬ С КЛАССИЧЕСКИМ ИНТЕРАКТИВНЫМ РАБОЧИМ СТОЛОМ

Для классического рабочего стола по умолчанию установлен фон с горизонтальной панелью задач в нижней части экрана.

На фоне рабочего стола расположены значки, представляющие доступные серверные подключения и опубликованные приложения. Если навести указатель мыши на такой значок и задержать его на нем, появится информация о подключении. Щелчок правой кнопкой открывает диалоговое окно **Connection Settings (Настройки подключения)**, где можно просмотреть дополнительные сведения о подключении. Количество значков, которые можно отобразить на рабочем столе, зависит от разрешения экрана и административной конфигурации.

Чтобы открыть серверное подключение или опубликованное приложение, дважды нажмите на его значке на рабочем столе или же выберите значок клавишей Tab, нажав клавишу нужное количество раз, и нажмите **Enter** для запуска подключения.

По щелчку правой кнопкой на рабочем столе открывается контекстное меню, см. раздел [Использование контекстного меню](#).

По щелчку на имени пользователя или на рабочем столе открывается меню рабочего стола, см. раздел [Использование меню рабочего стола](#).

ПРИМЕЧАНИЕ:

- имеется в виду имя пользователя, вошедшего в систему. Оно отображено в нижней левой части панели задач;
- регулятор громкости, если администратор разрешил его отображение, показан в правом углу панели задач, а при наведении указателя мыши на индикатор времени появляются текущие дата и время; тонкий клиент может синхронизировать системные часы с сигналами времени, передаваемыми сервером SNTP (Simple Network Time Protocol).

ИСПОЛЬЗОВАНИЕ КОНТЕКСТНОГО МЕНЮ

Как пользоваться контекстным меню:

1. Войдите в систему как администратор.
2. Нажмите правой кнопкой мыши по рабочему столу. Появится **контекстное** меню.
3. В **контекстном** меню для просмотра и использования доступны следующие опции:
 - **Administrator Mode** (Режим администратора): позволяет администратору настраивать различные параметры локально на тонком клиенте.
 - **Hide all windows** (Скрыть все окна): вывести весь рабочий стол на передний план.
 - **Copy to clipboard** (Копировать в буфер обмена): копировать в буфер обмена скриншот всего экрана, текущего окна или журнала событий. Затем содержимое буфера обмена можно вставить в сеанс ICA или RDP. Можно скопировать в буфер изображение всего экрана или текущего окна и затем экспортировать скриншоты с помощью пункта **Export Screenshot** (Экспортировать скриншот) меню Troubleshooting (Отладка).
 - **Purge clipboard** (Очистить буфер обмена): очистить содержимое буфера обмена для освобождения памяти.

- **Lock Terminal** (Заблокировать терминал): перевести тонкий клиент в состояние блокировки, если пользователь вошел в систему с паролем. Разблокировать тонкий клиент можно только тем же самым паролем.
- **Group Sessions** (Групповые сеансы): позволяет открыть больше трех сеансов ICA, RDP, PCoIP, Blast или ICA Seamless. Сеансы будут отображаться на панели задач в виде группы.

ИСПОЛЬЗОВАНИЕ МЕНЮ РАБОЧЕГО СТОЛА

Как пользоваться меню рабочего стола:

1. Нажмите по рабочему столу или по вашему имени пользователя.

ПРИМЕЧАНИЕ

Имеется в виду имя пользователя, вошедшего в систему. Оно отображено в нижней левой части панели задач. Появится меню рабочего стола.

2. В меню рабочего стола для просмотра и использования доступны следующие опции:
 - 2.1. **System Setup** (Настройка системы): предоставляет доступ к следующим диалоговым окнам настройки локальной системы:
 - 2.1.1. **Network Setup** (Настройка сети): позволяет выбрать настройки DHCP или задать сетевые параметры вручную, а также указать расположение серверов, необходимых для функционирования тонкого клиента. Для пользователей с низким уровнем привилегий этот пункт меню недоступен;
 - 2.1.2. **Remote Connections** (Удаленные подключения): позволяет настроить брокерные подключения тонкого клиента, включая брокерные серверные подключения Microsoft, Citrix Xen, Dell vWorkspace, VMware View, Amazon WorkSpaces или иные;
 - 2.1.3. **Central Configuration** (Централизованная конфигурация): позволяет настроить параметры подключения тонкого клиента к серверам централизованной настройки, таким как файловый сервер и дополнительные настройки сервера WDA;
 - 2.1.4. **VPN Manager** (Менеджер VPN): позволяет настроить менеджер VPN на тонком клиенте;
 - 2.1.5. **System Preference** (Системные предпочтения): позволяет выбрать по своему вкусу параметры тонкого клиента, являющиеся предметом личных предпочтений;
 - 2.1.6. **Display** (Экран): позволяет настроить разрешение и частоту обновления экрана;
 - 2.1.7. **Peripherals** (Периферийные устройства): позволяет выбрать настройки периферийных устройств, в том числе звука, клавиатуры, мыши, последовательного порта, камеры, Bluetooth и сенсорного экрана;
 - 2.1.8. **Printer** (Принтер): позволяет настроить сетевые принтеры и локальные принтеры, подключенные к тонкому клиенту.
 - 2.2. **System Information** (Системная информация): выдает системную информацию о тонком клиенте;
 - 2.3. **System Tools** (Системные инструменты): выдает информацию об устройствах, сертификатах, пакетах, глобальных INI, пользовательских INI, wdm или ccm.ini;
 - 2.4. **Troubleshooting options** (Параметры отладки): отображает графики быстродействия (Performance Monitor), дает информацию о распределении ресурсов CPU, памяти и сетевых ресурсов, настройки трассировки и журнала событий, параметры извлечения и восстановления для управления CMOS и прочие параметры, полезные для отладки ThinOS;

- 2.5. **Applications** (Приложения): содержит подменю из всех локально сконфигурированных приложений и заполняется опубликованными приложениями, когда пользователь входит в систему с помощью PNLite или PNAgent;
- 2.6. **Shutdown** (Выключение): открывает диалоговое окно Sign-off (Выйти из системы) / LockTerminal (Заблокировать терминал) / Shutdown (Выключение) / Restart the System (Перезагрузка).

РАБОТА С ДИСПЕТЧЕРОМ ПОДКЛЮЧЕНИЙ

Как пользоваться диспетчером подключений:

1. Нажмите на Connect Manager (Диспетчер подключений) на панели задач.
 - у диспетчера подключений Connect Manager имеется список записей для конкретных подключений и набор кнопок управления этими подключениями;
 - пользователи с низким уровнем привилегий не смогут увидеть диспетчер подключений Connect Manager. Им будет показано диалоговое окно Connection Manager.
2. В диалоговом окне Connection Manager настройте параметры с помощью следующих кнопок:
 - нажмите на **Connect (Подключиться)**, чтобы выбрать подключение из списка и подключиться.
 - нажмите на **New (Создать)**, чтобы открыть диалоговое окно Connection Settings (Настройки подключения) напрямую или через пункт меню Connection Protocol (Протокол подключения) для создания определения нового подключения.

Локально определенные подключения добавляются в список подключений. Имейте в виду следующее:

- **для привилегированных пользователей:** все локально заданные определения подключений, как правило, временные и уничтожаются при выходе пользователя из системы либо при выключении или перезапуске тонкого клиента. Однако администратор (задав enablelocal=yes) может сохранить определение локального подключения, сделав его постоянным;
- **для автономных пользователей:** локально определенные подключения не уничтожаются при перезагрузке или выключении тонкого клиента, а отдельный вход в систему отсутствует. В таком случае параметры конфигурации сети должны задаваться локально.
- нажмите на **Properties (Свойства)**, чтобы открыть диалоговое окно Connection Settings (Настройки подключения) для выбранного подключения. Имейте в виду следующее:
 - **привилегированные пользователи** могут просматривать и править определения для выбранного в настоящий момент подключения. При выходе пользователя из системы правки теряются.
 - **непривилегированные пользователи** не могут создавать или править подключения, но могут просматривать их определения. Однако можно дать непривилегированному пользователю право создавать подключения с помощью параметров INI.
 - **автономные пользователи** могут вносить постоянные правки в существующие подключения, за исключением использования сервисов PNAgent/PNLite.

- для выхода из системы на тонком клиенте нажмите на **Sign-off (Выйти из системы)**;
- чтобы удалить подключение, выберите его из списка и нажмите на **delete (Удалить)**;
- для сброса виртуального подключения выберите его из списка и нажмите на **Reset VM (Сбросить VM)**;
- для настройки параметров, влияющих на все подключения в списке, нажмите на **Global Connection Settings (Глобальные параметры подключений)**. Откроется одноименное диалоговое окно.

ДИАЛОГОВОЕ ОКНО LOGIN (ВХОД В СИСТЕМУ)

С помощью диалогового окна Login можно не только войти на сервер, но и выполнить следующее:

- просмотреть системную информацию;
- запустить режим администратора для настройки параметров тонкого клиента;
- изменить или сбросить собственный пароль и разблокировать Вашу учетную запись;
- открыть диалоговое окно Shutdown (Выключение) комбинацией клавиш CTRL+ALT+DELETE.

Возможности диалогового окна Login:

- **System Information (Системная информация)**: нажмите на кнопку **Sys Info**, чтобы открыть диалоговое окно System Information (Системная информация). Здесь можно просмотреть такую информацию о тонком клиенте, как версия системы, IP-адрес, подключенные устройства, журналы событий и т.д.;
- **Admin Mode (Режим администратора)**: нажмите на кнопку **Admin Mode**, чтобы настроить локально на тонком клиенте различные параметры, кроме конфигураций брокера. Например, здесь можно вручную настроить URL сервера Citrix XenBroker или переопределить URL, централизованно определенный на файловых серверах в диалоговом окне Remote Connections, как описано в разделе **Remote Connections (Удаленные подключения)**.
- классический рабочий стол: используйте пункт Leave Administrator Mode (Выйти из режима администратора) в диалоговом окне Shutdown (Выключение);
- рабочий стол Zero: используйте пункт Leave Administrator Mode (Выйти из режима администратора) в диалоговом окне Shutdown (Выключение) или значок Leave Administrator Mode (Выйти из режима администратора) (X) на правой верхней панели меню System Settings (Параметры системы);

ПРИМЕЧАНИЕ: по умолчанию кнопка Admin Mode отсутствует в диалоговом окне входа в систему. Чтобы отобразить ее, установите флажок Show local admin button (Показать локальную кнопку администратора) в диалоговом окне Shutdown (Выключение).

ПРИМЕЧАНИЕ: по умолчанию кнопка Admin Mode не защищена паролем. Чтобы защитить ее паролем, используйте параметр AdminMode в файле wnos.ini.

- **Shutdown (Выключение)**: нажмите на кнопку **Shutdown (Выключение)**, чтобы открыть диалоговое окно **Shutdown**. В нем можно выйти из системы или же вы-

ключить тонкий клиент, перезапустить его, сбросить в заводские настройки и т.д.;

- **Account Self-Service (Самообслуживание учетной записи):** щелкните по значку **Account Self-Service (Самообслуживание учетной записи)**, который отображается, если настроена опция AccountSelfService INI-параметра PasswordServer. Появится диалоговое окно Account Self-Service (Самообслуживание учетной записи), в котором можно изменить или сбросить Ваш собственный пароль и разблокировать Вашу учетную запись.

Для описанного процесса необходимо, чтобы пользователь заранее зарегистрировал свои секретные вопросы и ответы на них в среде Windows. Для сервера самообслуживания учетной записи необходимо задать на вкладке **Broker Setup (Настройка брокера)** протокол HTTPS (не HTTP), в виде `https://ip-адрес`. После того как даны правильные ответы на секретные вопросы, пароль будет изменен или учетная запись разблокирована.

ДОСТУП К СИСТЕМНОЙ ИНФОРМАЦИИ

Для просмотра системной информации откройте диалоговое окно System Information (Системная информация).

- Классический рабочий стол: выберите **System Information (Системная информация)** из меню рабочего стола.
- Рабочий стол Zero: щелкните по значку **System Information (Системная информация)** на панели инструментов Zero.

В диалоговом окне **System Information (Системная информация)** доступны следующие параметры:

- Вкладка **General (Общее):** здесь отображается общая информация, такая как: версия системы, серийный номер, размер RAM (полный и свободный), тактовая частота CPU, размер ROM, монитор, параллельные порты, имя терминала, источник загрузки, скорость чтения и записи в память, размер SSD, разрешение дисплея, последовательные порты.
- Вкладка **Copyright (Авторские права):** здесь приведены уведомления об авторских правах и патентах на ПО.

Кнопка **Acknowledgments (Благодарности)** на вкладке **Copyright** диалогового окна **System Information**, относится к ПО третьих сторон.

- **Вкладка Event Log (Журнал событий):** здесь приведены этапы загрузки тонкого клиента, как правило, начиная с версии системы и до проверки микропрограммного обеспечения, а также сообщения об ошибках, которые бывают полезны в диагностике неисправностей. Здесь также указаны данные о подключенных к тонкому клиенту мониторах и USB-устройствах и данные об инициализации Bluetooth.

При установке пакетов и перезапуске устройства ThinOS клиент ThinOS проверяет версию установленного пакета. Если новейшая версия пакета не установлена, то здесь будут показаны данные о текущей версии пакета и рекомендуемой версии, до которой следует обновиться.

- **Вкладка Status (Состояние):** здесь показана информация о параметрах быстрого действия TCP, параметрах быстрого действия UDP, занятости CPU, времени активности системы, состоянии WMS, свободной памяти, активных сеансах и состоянии WDM.

- **Вкладка IPv6:** здесь показана информация об IPv6, такая как: адрес Link-local Address, адрес IPv6 и шлюз IPv6 по умолчанию.

ПРИМЕЧАНИЕ: эта вкладка присутствует, если IPv6 активирован на вкладке General (Общее) диалогового окна Network Setup (Настройка сети).

- **Вкладка ENET:** здесь отображаются сведения о проводных сетевых подключениях.
- **Вкладка WLAN:** здесь отображаются сведения о беспроводных сетевых подключениях.
- **Вкладка About (О программе):** здесь отображаются данные об операционной системе ThinOS:
 - наименование платформы;
 - тип операционной системы;
 - имя сборки ThinOS;
 - версия сборки ThinOS;
 - имя BIOS;
 - версия BIOS;
 - версия Citrix Broker или Receiver – отражает ревизии ICA между версиями ThinOS;
 - версия Dell vWorkspace;
 - версия VMware Horizon – отражает ревизии Horizon между версиями ThinOS;
 - версия Microsoft Broker или RDP;
 - версия Teradici PCoIP – отражает ревизии PCoIP между версиями ThinOS, только для устройств PCoIP;
 - версия Imprivata;
 - версия Caradigm;
 - версия SECUREMATRIX;
 - версия HealthCast.

ПРИМЕЧАНИЕ:

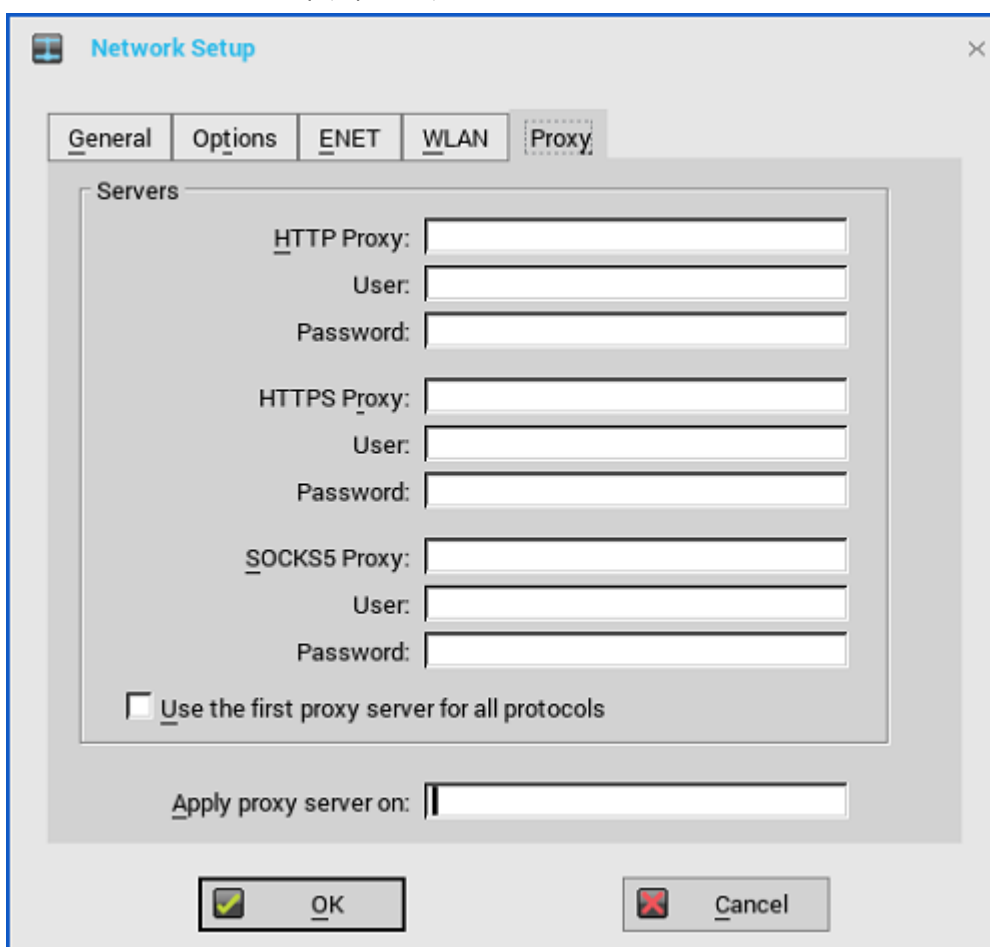
- Kernel mode (Режим ядра) – компоненты реализованы в ядре согласно спецификации. Номер версии указывается как [max].[min] и представляет собой базовую версию протокола, сервера или клиента для компонента. Например, версия протокола Microsoft RDP равна 10.0, версия Imprivata – 5.2.
- User mode (Режим пользователя) – компоненты взяты из исходного кода либо представляют собой двоичные файлы третьих сторон, скомпилированные или интегрированные в ThinOS. Номер версии указывается как [max].[min].[svn_revision]. Здесь [max] и [min] – базовая версия компонента третьей стороны, а [svn_revision] – субверсия контроля исходного кода ThinOS. По версии ThinOS можно идентифицировать изменения между различными субверсиями. Например, у Citrix Receiver версия равна 14.0.44705, у VMware Horizon – 4.8.x. Компоненты соответствуют установленным пакетам. При удалении пакета соответствующее поле на вкладке About остается пустым.

НАСТРОЙКА ПАРАМЕТРОВ ПРОКСИ

На вкладке **Proxy (Прокси)** окна настройки сети поддерживаются WMS, HDX Flash Redirection и RealTime Multimedia Engine (RTME). Поддерживаемые протоколы: HDX FR, WMS и RTME:

- Для **HDX FR**: поддерживаются протоколы HTTP и HTTPS.
- Если настроены и HTTP, и HTTPS, HDX FR работает с прокси HTTPS.
- Передача учетных данных пользователя возможна посредством \$UN/\$PW.
- Для **WMS**: поддерживаются протоколы HTTP, HTTPS и Socks5 (рекомендуется).
- Для **RTME**: поддерживаются протоколы HTTP и HTTPS.

1. Из меню рабочего стола выберите **System Setup (Настройка системы)**, а затем **Network Setup (Настройка сети)**. Появится диалоговое окно Network Setup (Настройка сети).
2. Откройте вкладку **Proxy (Прокси)** и выполните следующие действия:



- 2.1. Укажите в соответствующих полях номер порта **HTTP proxy** (HTTP-прокси) или **HTTPS proxy** (HTTPS-прокси), имя пользователя – **User** (Пользователь) и пароль – **Password** (Пароль). Передача учетных данных посредством (\$UN/\$PW) не рекомендуется, так как она начинается до входа пользователя в систему.

В WMS для обмена данными с сервером WMS/MQTT используются протоколы HTTP/HTTPS и MQTT. Однако HTTP-прокси не может перенаправлять пакеты TCP на сервер MQTT, для этого необходим прокси-сервер SOCKS5. Если доступен только сервер HTTP, то команда реального времени, требующая MQTT, не будет работать.

По умолчанию для **HTTP/HTTPS-прокси** выбран порт 808, а для **SOCKS5-прокси** – порт 1080.

- 2.2. Установите флажок **Use the first proxy server for all protocols** (Использовать первый прокси-сервер для всех протоколов), чтобы все протоколы могли использовать общий сер-

вер, который прописан в поле **HTTP Proxy** (HTTP-прокси). И HTTP-прокси, и HTTPS-прокси используют один и тот же хост и порт, а прокси-агент SOCKS5 использует хост HTTP с портом Socks5 по умолчанию (1080).

Если настроен **SOCKS5-прокси**, то WMS-прокси использует только SOCKS5. Если SOCKS5 не настроен, то WMS-прокси ищет в конфигурации альтернативные протоколы, например HTTP.

2.3. В поле **Apply proxy server on** (Применять прокси-сервер к) Укажите для поддерживаемых приложений WMS, FR и RTME, разделяя их точками с запятой.

3. Нажмите на кнопку **OK**, чтобы сохранить настройки.

Пользовательский сценарий

1. Настройте правильный хост и порт прокси-сервера.
2. Настройте учетные данные пользователя соответственно настройкам прокси-сервера.

После перезапуска системы клиент подключается к серверу WMS через прокси-сервер SOCKS5. Через прокси-сервер SOCKS5 устанавливается MQTT-подключение. Команды реального времени работают через прокси-сервер SOCKS5.

3. Подключитесь к рабочему столу Citrix, настройте прокси в параметрах Интернета в браузере. HDX FR должен корректно работать через HTTP/ HTTPS прокси.

НЕСКОЛЬКО ВХОДОВ В СИСТЕМУ ДЛЯ CITRIX И VMWARE HORIZON

ThinOS поддерживает функцию нескольких входов в систему PNA. Имеется возможность выполнить вход в нескольких экземплярах Citrix StoreFront или PNAgent под разными учетными данными. Начиная с этого выпуска, можно одновременно подключаться к Citrix StoreFront/PNAgent и к серверу VDM.

Для настройки функции нескольких входов в систему выполните следующие действия:

1. Настройте сервер Pnlite и брокер VDI в INI-файле следующим образом:

```
SelectServerList=vdm; \
description="description" host=<полное доменное имя сервера Horizon>
SelectServerList=pna; \
description="description" host=<полное доменное имя сервера StoreFront>
```

или

```
multilogon=yes
pnliteserver=<полное доменное имя сервера StoreFront> VDIBroker=<полное доменное имя сервера Horizon>
```

или

```
multilogon=yes SelectServerList=vdm; \
description="description" host=<полное доменное имя сервера Horizon>
SelectServerList=pna; \
description="description" host=<полное доменное имя сервера StoreFront>
```

2. В окне входа в систему (Login) выберите брокер Citrix или VMware для подключения либо подключитесь к обоим брокерам Citrix и VMware под разными учетными данными.

Ограничения

ThinOS поддерживает лишь один вход в систему VDM, даже если параметр MultiLogon установлен в значение **yes**. При первом успешном подключении к брокеру VDI последующие брокеры VDI игнорируются.

Например:

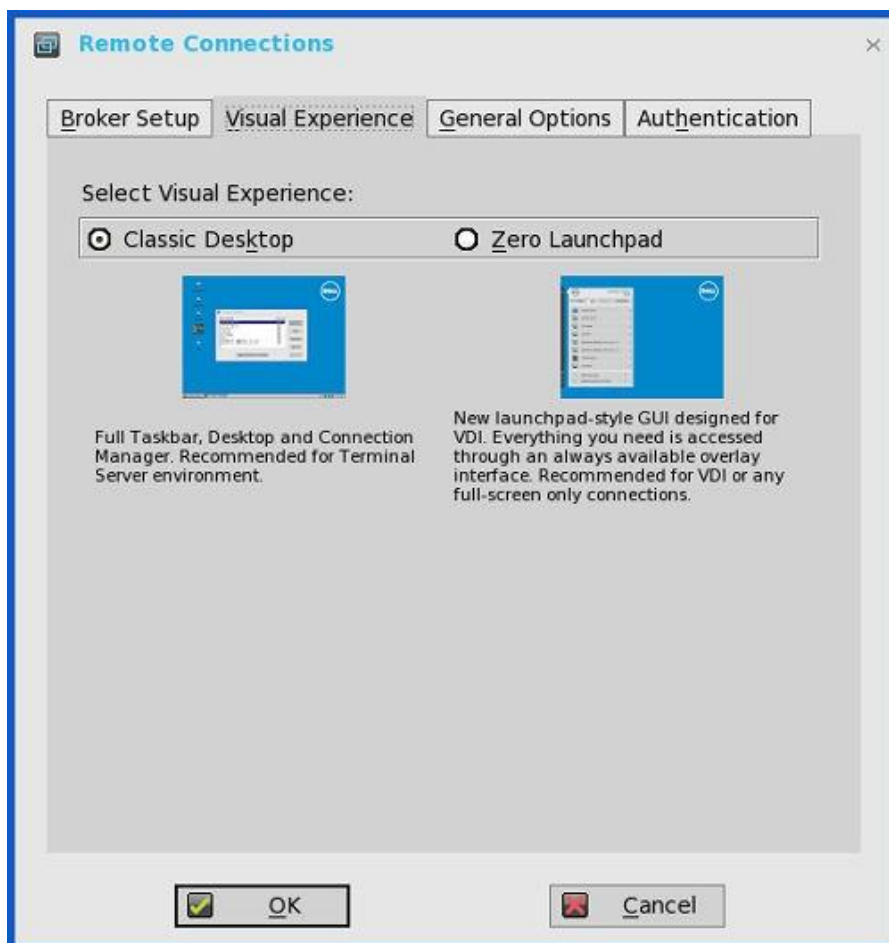
```
multilogon=yes  
VDIBroker=<полное доменное имя сервера Horizon 1>;  
VDIBroker=<полное доменное имя сервера Horizon 2>
```

Если подключение к первому брокеру VDI произошло успешно, второй брокер VDI игнорируется. Если подключиться к первому брокеру VDI не удалось, используется второй брокер VDI.

НАСТРОЙКА ВИЗУАЛЬНОГО ПРЕДСТАВЛЕНИЯ

Для настройки параметров экрана выполните следующие действия:

1. Из меню рабочего стола выберите System Setup (Настройка системы), а затем Remote Connections (Удаленные подключения). Будет открыта вкладка Remote Connections (Удаленные подключения).
2. Откройте вкладку Visual Experience (Визуальное представление):



ПРИМЕЧАНИЕ: вкладка **Visual Experience** (Визуальное представление) выделена серым цветом и недоступна, если установлен флажок **Storefront Style** для сервера брокера Citrix, выбранного на вкладке **Broker Setup** (Настройка брокера).

- 2.1. **Классический рабочий стол:** отображаются полная панель задач, рабочий стол и диспетчер подключений Connect Manager. Этот вариант рекомендуется для сред сервера терминалов, а также для обратной совместимости с версиями ThinOS 6.x.
- 2.2. **Панель запуска Zero Launchpad:** отображается новый стиль GUI, разработанный для VDI. Этот вариант рекомендуется для VDI и любых подключений, эксплуатируемых только в полноэкранном режиме. Для конфигурации также имеются панель инструментов, клавиши быстрого доступа и значки подключений.

На панели запуска Zero Launchpad доступны следующие настройки:

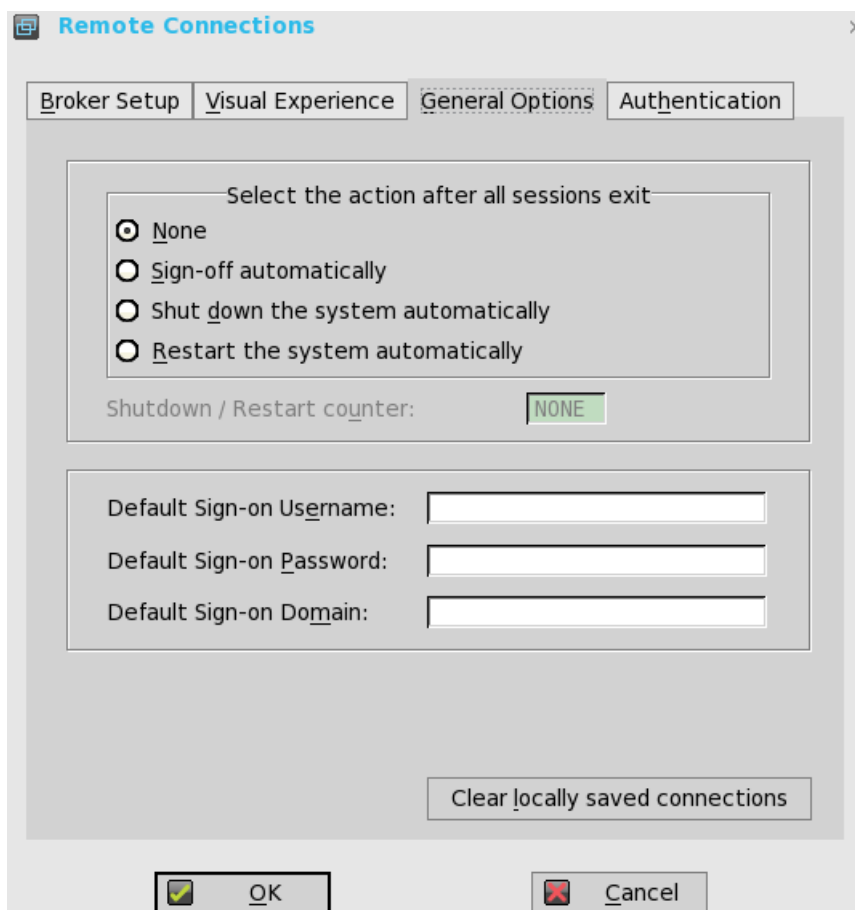
- активация панели инструментов Zero в левой части экрана:
 - активация панели инструментов Zero при остановке указателя мыши на экране. Необходимо выбрать время простоя мыши (0, 0,5 или 1 с) после которого появляется панель инструментов Zero;
 - активация панели инструментов Zero в левой части экрана по щелчку.
- отключение клавиши быстрого доступа, которая выводит панель инструментов на экран;
- скрытие панели инструментов, если доступен один сеанс;
- скрытие значка **Home** (Главная).

3. Нажмите на кнопку **OK**, чтобы сохранить настройки.

НАСТРОЙКА ОБЩИХ ПАРАМЕТРОВ

Для настройки общих параметров выполните следующие действия:

1. Из меню рабочего стола выберите **System Setup** (Настройка системы), а затем **Remote Connections** (Удаленные подключения). Откроется диалоговое окно **Remote Connections** (Удаленные подключения).



2. Откройте вкладку **General Options** (Общие параметры):
 - 2.1. Установите нужный переключатель, чтобы выбрать действие после закрытия всех открытых рабочих столов. Доступны следующие варианты: **None** (Ничего не делать), **Sign-off automatically** (Автоматически выйти из системы), **Shut down the system automatically** (Автоматически выключить систему) и **Restart the system automatically** (Автоматически перезагрузить систему).

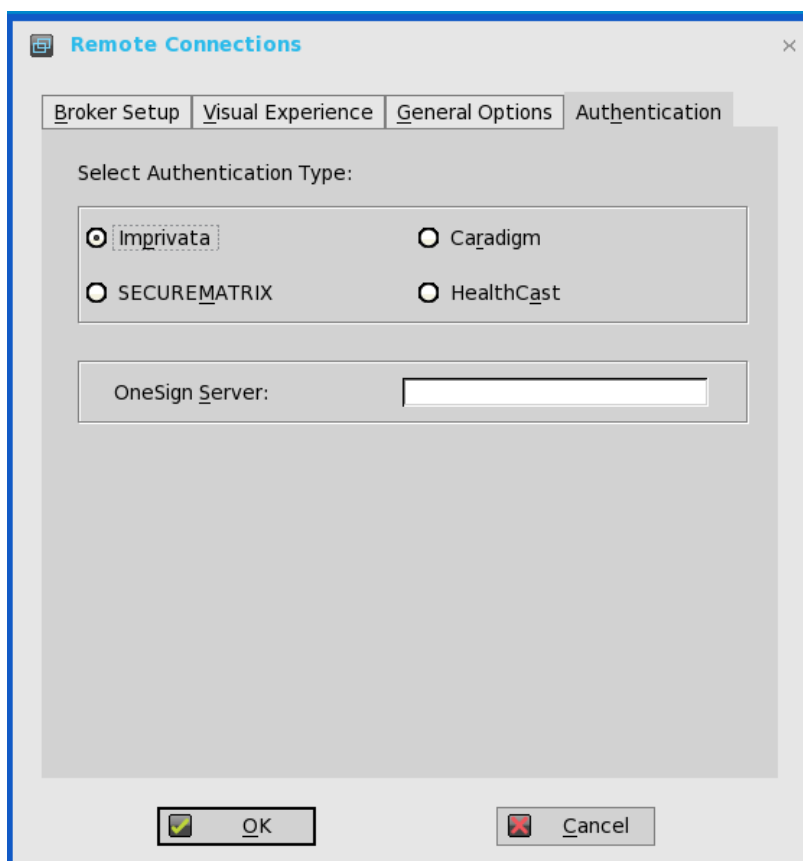
ПРИМЕЧАНИЕ: по умолчанию выбрано **None** (Ничего не делать), тонкий клиент автоматически выполняет возврат на рабочий стол терминала.
 - 2.2. **Default Sign-on Username** (Имя пользователя по умолчанию для входа): введите имя пользователя по умолчанию.
 - 2.3. **Default Sign-on Password** (Пароль по умолчанию для входа): введите пароль по умолчанию.
 - 2.4. **Default Sign-on Domain** (Домен по умолчанию для входа): введите домен по умолчанию.
 - 2.5. Чтобы очистить локально сохраненные подключения, нажмите на кнопку **Clear locally saved connections** (Очистить локально сохраненные подключения).

ПРИМЕЧАНИЕ: если были указаны все три компонента учетных данных по умолчанию для входа (имя пользователя, пароль и домен), то после запуска тонкого клиента происходит автоматический вход в систему и открывается рабочий стол.

НАСТРОЙКА ПАРАМЕТРОВ АУТЕНТИФИКАЦИИ

Для настройки параметров аутентификации выполните следующие действия:

1. Из меню рабочего стола выберите **System Setup** (Настройка системы), а затем Remote Connections (Удаленные подключения). Откроется диалоговое окно Remote Connections (Удаленные подключения).
2. Откройте вкладку **Authentication (Аутентификация)** и выберите тип аутентификации. Доступны следующие варианты:
 - Imprivata: [настройка сервера Imprivata OneSign](#);
 - Caradigm: [настройка сервера Caradigm](#);
 - SECUREMATRIX: [настройка SECUREMATRIX](#);
 - HealthCast: [введение в HealthCast](#).



3. Настроив предпочтительный способ аутентификации, нажмите на кнопку **OK**, чтобы сохранить настройки.

Настройка сервера Imprivata OneSign

OneSign Virtual Desktop Access обеспечивает бесшовную аутентификацию и может сочетаться с единым входом в систему для «доступа без кликов» к рабочим столам и приложениям в среде виртуального рабочего стола.

Для настройки сервера OneSign: откройте параметры сервера OneSign, введя либо `https://ip-адрес`, либо `https://полное-доменное-имя-сервера`; перезагрузите клиент, чтобы появилось диалоговое окно входа в систему; затем введите свои учетные данные, чтобы открыть диалоговое окно брокера VDI для входа. Кроме того, можно задать эту же функцию в файле INI. Поддерживаются следующие функции и действия OneSign:

- аутентификация клиента и брокера:
 - Citrix Virtual Apps (ранее Citrix XenApp);
 - Citrix Virtual Apps and Desktops (ранее Citrix XenDesktop);
 - VMware View.
- режим киоска;
- быстрое переключение пользователей;
- доступ пользователя к VDI без OneSign;
- отключение по клавишам быстрого доступа;
- перенаправление на устройство считывания бесконтактных карт;
- вход в систему посредством вопросов и ответов;
- аутентификация по паролю;
- аутентификация по паролю + смена пароля;
- аутентификация по паролю + смена пароля;
- аутентификация по бесконтактной карте и паролю;
- аутентификация по бесконтактной карте и PIN-коду;
- аутентификация по бесконтактной карте и PIN-коду;
- аутентификация только по бесконтактной карте | восстановление пароля;
- восстановление пароля пользователя;
- сброс пароля пользователя;
- обновление пароля пользователя;
- добавление бесконтактной карты;
- блокировка/разблокировка терминала бесконтактной картой;
- ThinOS поддерживает новейшую версию Imprivata WebAPI 5. В нее входят OneSign Objects (WebAPI v4) и Fingerprint Authentication (WebAPI v5).

Настройка объектов на сервере Imprivata

Imprivata WebAPI обновлен с версии 4 до версии 5. Начиная с предыдущей версии, поддерживаются объекты конфигурации, с помощью которых можно контролировать различные аспекты поведения клиента. Imprivata WebAPI доступен на сервере OneSign 4.9 и более поздних версиях. Объекты конфигурации контролируют различные аспекты поведения клиента.

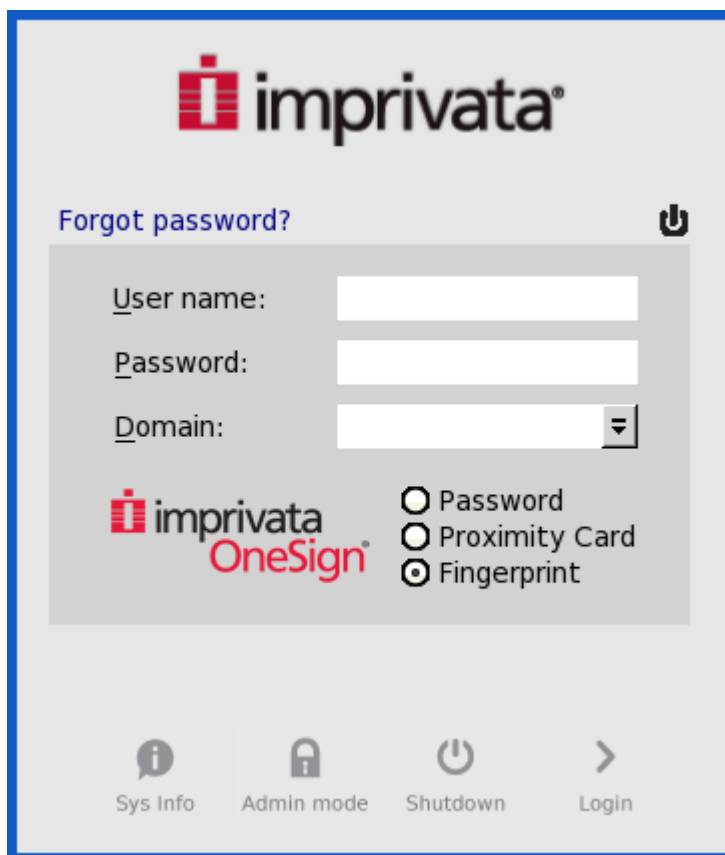
Настройка объектов на сервере Imprivata происходит следующим образом:

1. Настройка общего объекта конфигурации.
 - 1.1. На сервере Imprivata нажмите на **Computer policy** (Политика компьютера), а затем откройте вкладку **General** (Общее).
 - 1.2. Установите соответствующий флажок, чтобы пользователь мог выключать и перезапускать рабочую станцию с экрана блокировки.

ПРИМЕЧАНИЕ: отображение кнопки выключения и команд перезапуска пользователю OneSign GINA.

На сервере Imprivata поддерживаются следующие объекты конфигурации:

- **Shutdown Allow** (Разрешить выключение):
 - если установить этот флажок, то на экранах входа в систему и блокировки в ThinOS будут отображаться значки выключения и перезапуска;



- если снять этот флажок, то значки выключения и перезапуска будут серыми;
 - **FailedOneSignAuth Allow** (Разрешить авторизацию при неудаче OneSign): возможны только варианты **Yes** (Да) и **No** (Нет). Пользователь без поддержки OneSign сможет подключиться к брокеру, если выбрать переключатель **No** (Нет).
- **Logging Allow** (Разрешить журнал):
 - этот параметр позволяет выводить журналы OneSign в ThinOS, необходима соответствующая конфигурация INI;
 - Loglevel=0/1/2/3. По умолчанию используется значение 0. Если установлено в 0, журналы не отображаются.
- **Display name format** (Формат отображения имени): можно настроить правильное отображение имени учетной записи в разных форматах во всплывающих уведомлениях.

2. Настройка объекта конфигурации Walkway.

На сервере Imprivata нажмите на **Computer policy** (Политика компьютера), а затем откройте вкладку **Walk Away** (Пользователь отошел):

- **Key mouse inactivity enabled and behavior** (Настройка по отсутствию активности клавиатуры и мыши): флажок **In addition to keyboard and mouse inactivity** (В дополнение к неактивности клавиатуры и мыши) не поддерживается;
- **Passive proximity cards** (Пассивные бесконтактные карты):

- установите флажок **Tap to lock** (Прикоснуться для блокировки), чтобы иметь возможность блокировать компьютер бесконтактной картой;
- для того чтобы заблокировать компьютер и затем войти в систему как другой пользователь, установите флажок **Switch users** (Сменить пользователя);
- Параметр INI: TapToLock=0/1/2.
- **Lock warning enabled and type** (Наличие и тип предупреждения о блокировке) для выбора одного из типов предупреждения:
 - **None** (Нет): предупреждение не выдается;
 - **Notification balloon** (Уведомление в окне): ThinOS выводит окно с уведомлением;
 - **Screensaver** (Заставка): скрыть содержимое экрана перед блокировкой рабочей станции.
- **Warning message** (Текст предупреждения) для настройки текста предупреждения:
- **Lock Screen type** (Тип блокировки экрана): поддерживается только тип **Obscure**;
- **Hot key to lock workstation or log off user** (Клавиша быстрого доступа для блокировки или выхода из системы): в ThinOS поддерживаются следующие клавиши:
 - "F1 ~ F12", "BKSP", "DEL", "DOWN", "END", "ENTER", "ESC", "HOME", "INS", "LALT", "LEFT", "LCONTROL", "NUMLOCK", "PGDN", "PGUP", "RCONTROL", "RIGHT", "RTALT", "SPACE", "TAB", "UP", "a~z", "A~Z", "0~9" и модификаторы "+", "%", "^";
 - (Shift, Alt и Ctrl).
- **Suspend action** (Действие при приостановке): эта функция в ThinOS контролируется конфигурацией сервера. Поэтому добавлен новый INI:

SuspendAction=0/1; 0 означает блокировку, 1 – выход из системы.

3. Настройка объекта конфигурации SSPR.

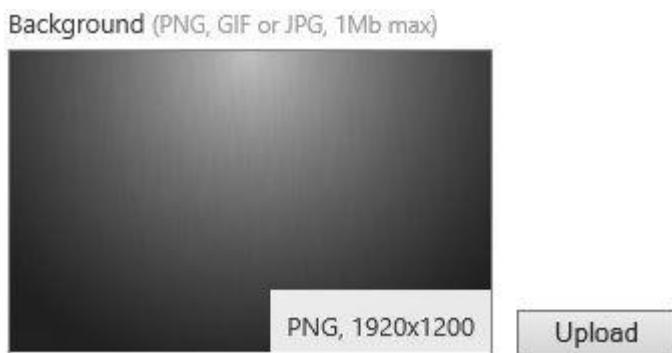
Объект конфигурации SSPR контролирует поведение функции самостоятельного сброса пароля пользователем. Атрибут `enabled` указывает, может ли пользователь сам сбросить свой пароль для восстановления доступа в нештатной ситуации. Атрибут `mandatory` указывает, обязан ли пользователь сбросить свой пароль для восстановления доступа в нештатной ситуации.

4. Настройка объекта конфигурации RFIDeas.

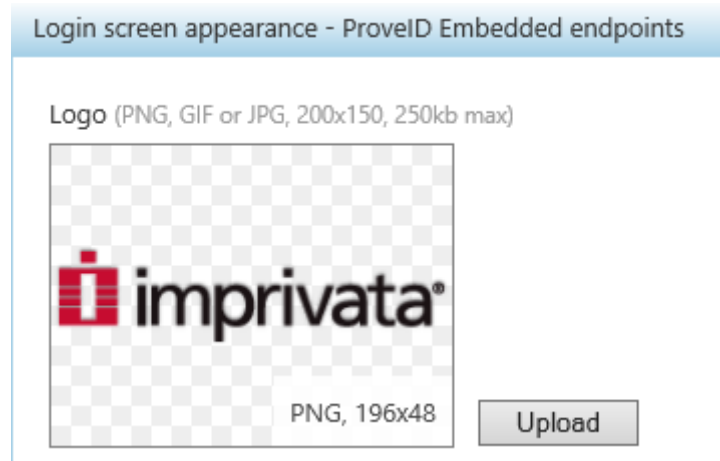
Объект конфигурации RFIDeas контролирует поведение считывателей RFIDeas. Эту конфигурацию можно задать двумя способами: либо с помощью политики компьютера на сервере OneSign, либо в INI-файлах ThinOS.

5. Настройка объекта конфигурации Custom background (Нестандартный фон).

На сервере Imprivata нажмите **Computer policy** (Политика компьютера), а затем откройте вкладку **Customization** (Индивидуальная настройка). Загрузите изображение для заднего фона.



6. Настройка объекта конфигурации Co-Branding (Кобрендинг).



Вернитесь в **Computer policy** (Политика компьютера) к вкладке **Customization** (Индивидуальная настройка).

Изображение логотипа влияет на все диалоговые окна в ThinOS с «сырым» логотипом.

7. Настройка объекта конфигурации SSPR Customization (Индивидуальная настройка SSPR):
- текст, отображаемый в окнах входа в систему и блокировки, можно модифицировать;
 - ThinOS поддерживает собственный текст до 17 знаков. Стандартный UI ThinOS:

8. Password Self-Services force enrollment feature (Принудительное задание секретных вопросов).

Если установить этот флажок, то основной пароль аутентификации может быть сброшен.

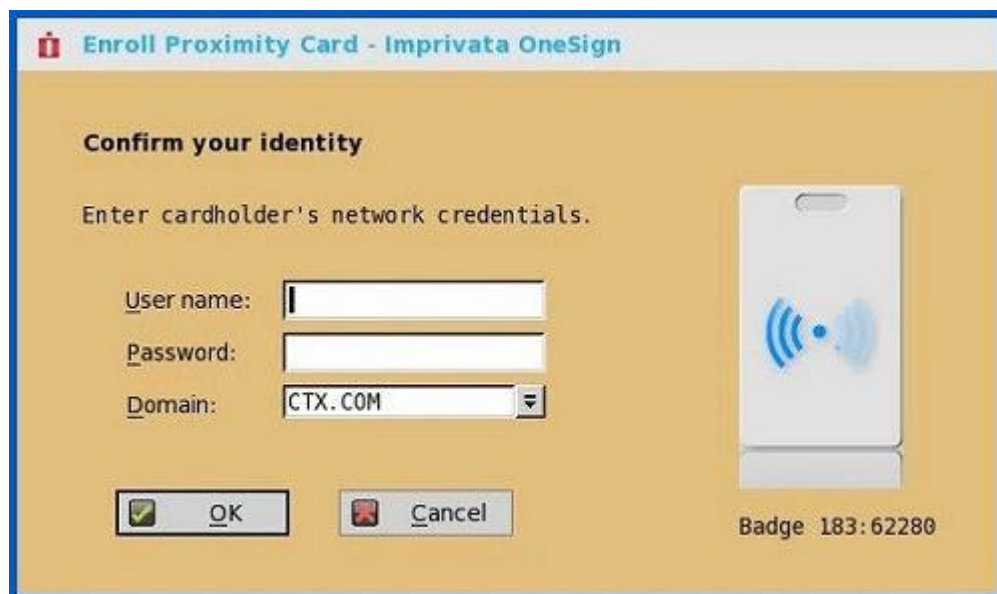
Конфигурация INI для сервера Imprivata OneSign

Добавлен новый параметр INI: AutoAccess=command. Новое значение: AutoAccess=Local. Если значение AutoAccess установлено в local, ThinOS игнорирует брокеры, настроенные на устройстве Imprivata OneSign, и запускает брокеры/подключения, определенные в файле wnos.ini или локально на клиенте. Допускается запускать подключения vWorkspace, Microsoft и другие подключения ThinOS, поддерживая аутентификацию пользователя Imprivata.

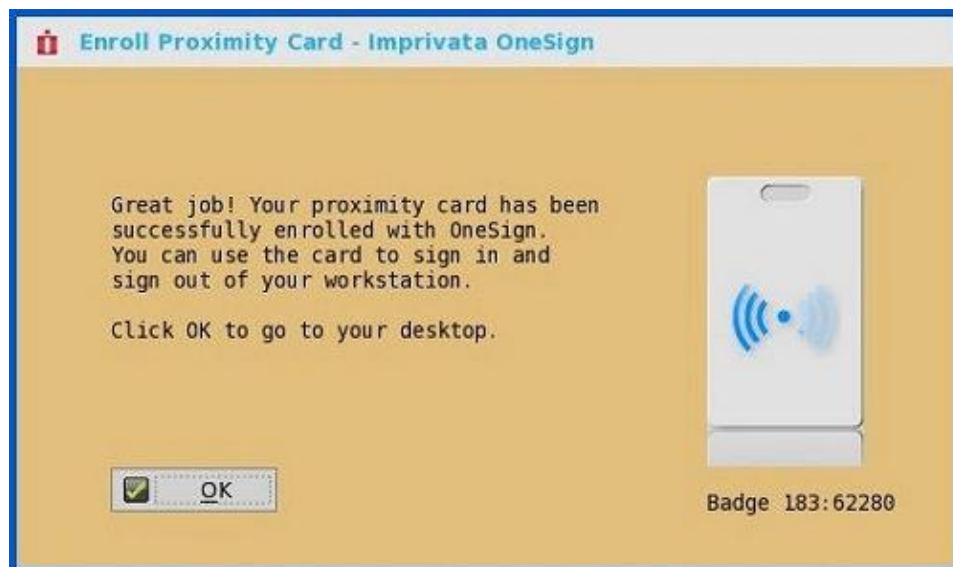
Регистрация бесконтактных карт



1. Прикоснитесь бесконтактной картой к считывателю. Появится страница регистрации карты.
2. Введите учетные данные владельца карты и нажмите на кнопку **OK**.



Процесс регистрации бесконтактной карты завершен.



Биометрический единый вход в систему Imprivata

Функция идентификации пользователя по отпечаткам пальцев отличается высокой надежностью: ее очень трудно воспроизвести, изменить или злоупотребить ею. Для ее реализации на сервере OneSign требуется следующее:

- версия устройства Imprivata v4.9 или более поздняя, поддерживающая WebAPI v5 и более поздних версий;
- обязательна лицензия на идентификацию по отпечаткам пальцев.

ПРИМЕЧАНИЕ:

- поддерживаются следующие протоколы: Microsoft RDP, Citrix ICA, PCoIP и VMware Blast;
- необходимые сканеры отпечатков пальцев:
 - ET710 (PID 147e VID 2016);
 - ET700 (PID 147e VID 3001).

Поддерживаемые сценарии

1. Вход в систему или разблокировка устройств под управлением ThinOS с аутентификацией по отпечаткам пальцев:
 - настройте сервер OneSign на ThinOS и затем подключите сканер отпечатков пальцев;
 - после инициализации сервера OneSign автоматически появится окно ThinOS Fingerprint:



- аутентификация по отпечаткам пальцев работает в окне разблокировки ThinOS.



2. Разблокировка виртуального рабочего стола по отпечатку пальца:

- включите Imprivata Virtual Channel в глобальных настройках подключений ThinOS;
- если заблокировать виртуальный рабочий стол во время сеанса, автоматически появится окно запроса отпечатка пальца.

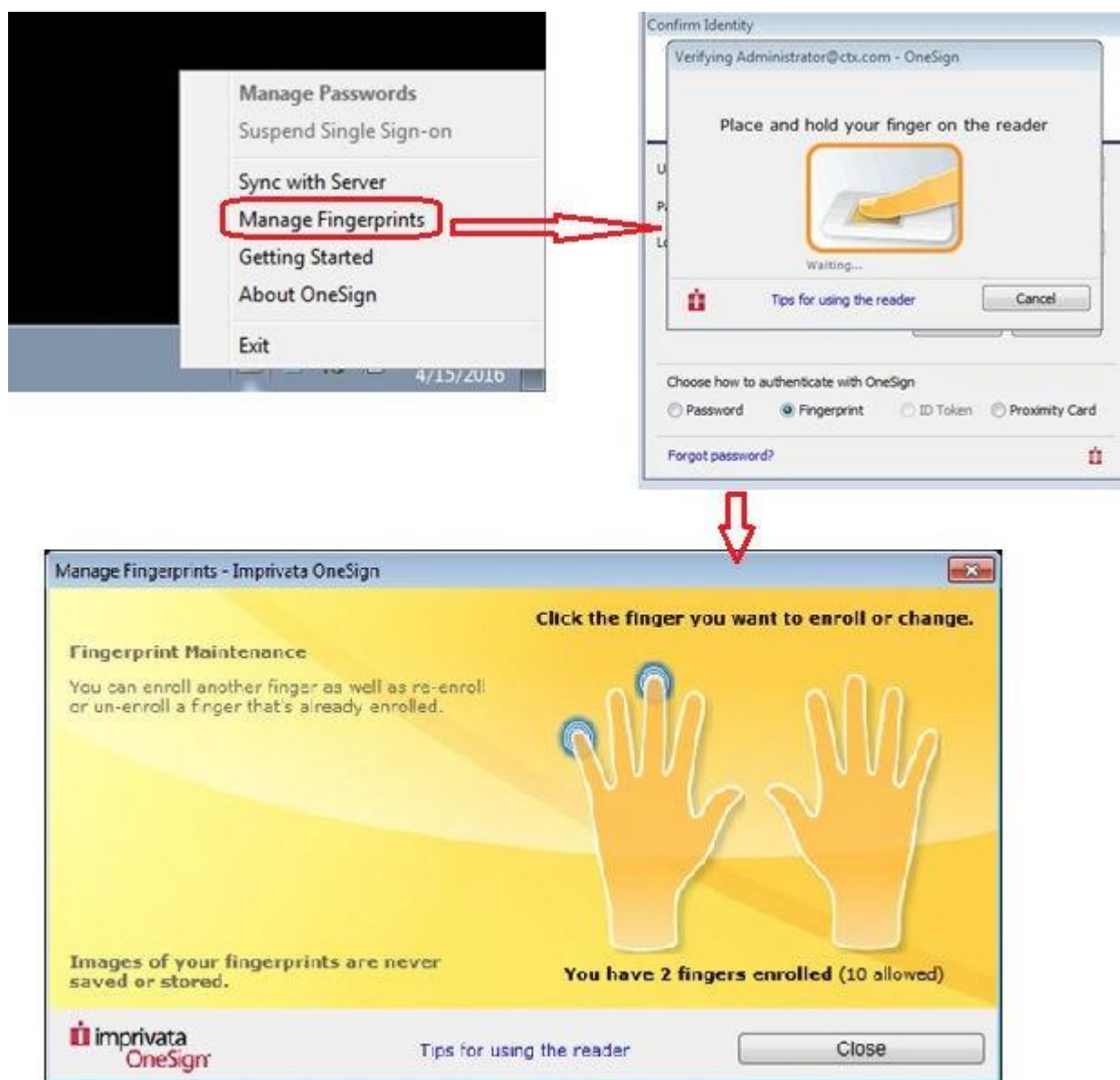


3. Управление отпечатками пальцев на виртуальном рабочем столе:

- поддерживается Legend Fingerprint Management;
- управление отпечатками пальцев с помощью Imprivata Confirm ID не поддерживается. Для завершения регистрации требуется присутствие и пользователя, и супервайзера, этот процесс рекомендуется проводить на платформе Windows.

Для управления отпечатками пальцев выполните следующие действия:

- нажмите правой кнопкой мыши на значке агента OneSign в системном трее;
- нажмите на **Manage Fingerprints** (Управление отпечатками пальцев) и введите правильные учетные данные в появившемся окне.

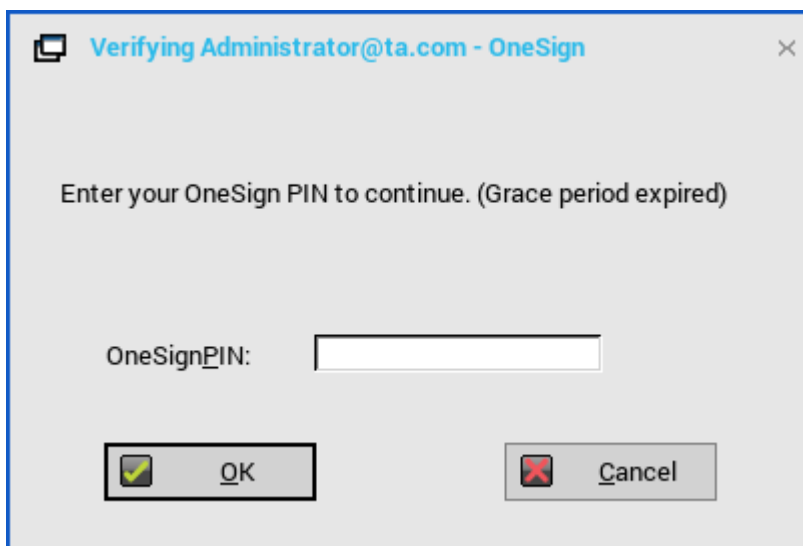


Льготный период для пропуска второго фактора аутентификации

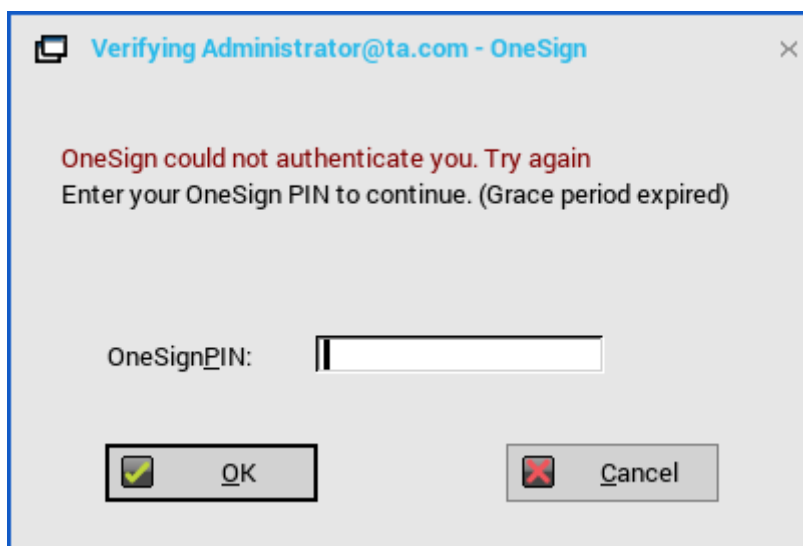
Льготный период (Grace period) позволяет задать лимит времени на сервере OneSign для входа в систему без второго фактора аутентификации после первого сеанса входа в систему.

ПРИМЕЧАНИЕ: после указания льготного периода необходимо сначала выполнить первоначальный вход в систему по бесконтактному бейджу, а затем ввести пароль или PIN-код OneSign.

Если бесконтактная карта используется после завершения льготного периода, то появится окно второго фактора аутентификации с сообщением *Grace period expired* (Льготный период прошел).



Если введен неправильный пароль или PIN-код, то появляется окно второго фактора аутентификации с предупреждением «OneSign could not authenticate you. Try again». (OneSign не удалось идентифицировать Вас. Повторите попытку.)



Использование смарт-карт как бесконтактных карт:

Смарт-карта может быть использована в качестве бесконтактной карты для аутентификации пользователя. Когда пользователь прикасается смарт-картой к считывателю смарт-карт, агент Imprivata использует уникальный серийный номер карты в качестве уникального ID (UID) бесконтактной карты.

Для использования смарт-карт в качестве бесконтактных карт выполните следующие действия:

1. Войдите в консоль администратора OneSign.
2. Откройте страницу Policies (Политики) и нажмите на **Computer Policy** (Политика компьютера).
3. В разделе Smart card readers (Считыватели смарт-карт) установите флажок Treat smart card authentications as proximity card authentications (Считать аутентификацию по смарт-карте аутентификацией по бесконтактной карте).

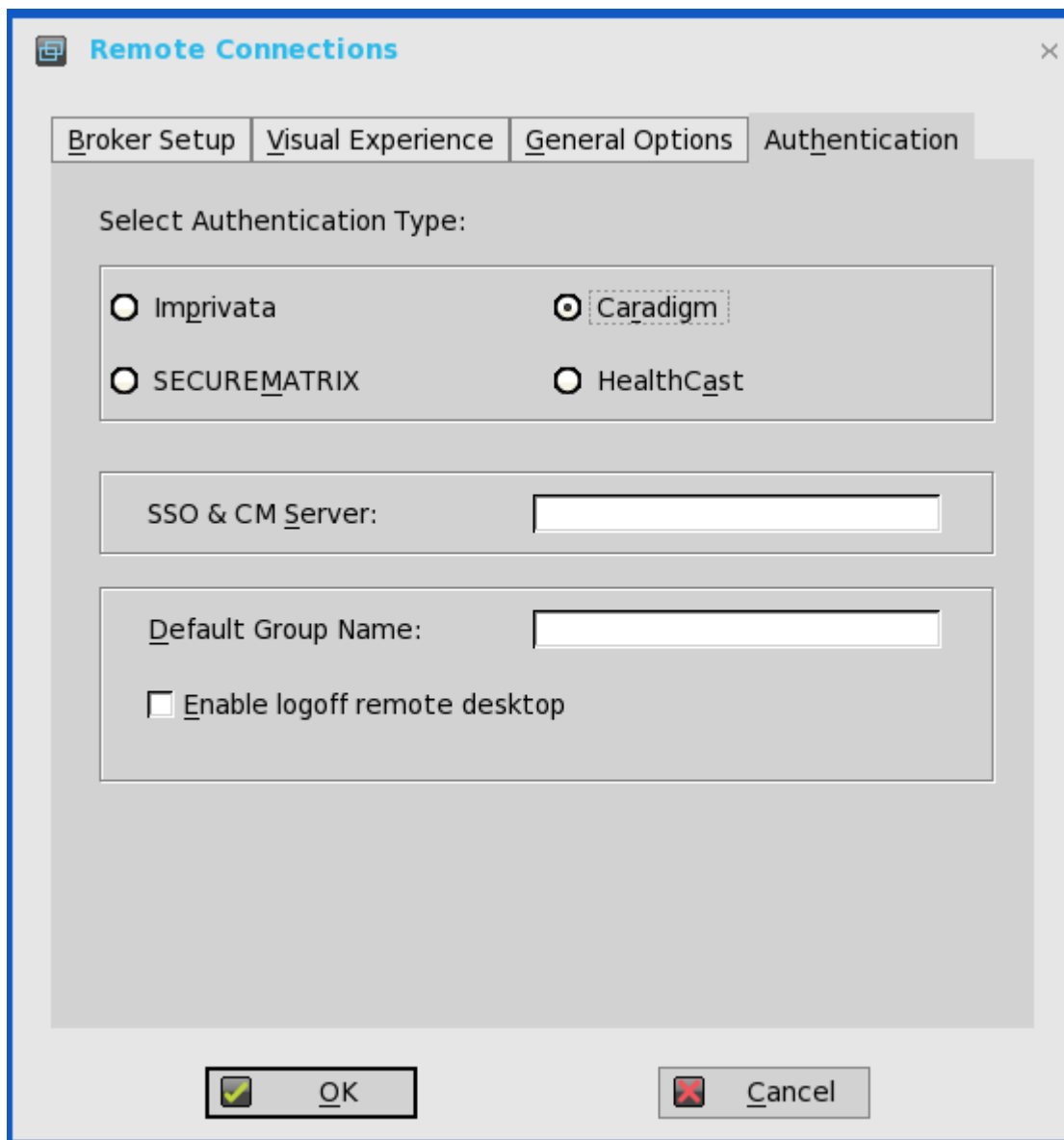
Для аутентификации пользователя по бесконтактной карте подключите к тонкому клиенту поддерживаемый считыватель карт. Перед тем как прикоснуться картой к считывателю, убедитесь, что она уже зарегистрирована на пользователя. При прикосновении картой к считывателю, тонкий клиент выполнит аутентификацию пользователя и запустит подключение VDI.

Настройка сервера Caradigm

Caradigm Single Sign-on and Context Management (SSO & CM) разработан компанией Caradigm, которая оказывает услуги управления единым входом в систему и контекстного управления. Решение Caradigm интегрировано в ThinOS, начиная с версии ThinOS 8.1.

Для настройки интеграции Caradigm в ThinOS выполните следующие действия:

1. В меню рабочего стола выберите **System Setup** (Настройка системы), а затем **Remote Connections** (Удаленные подключения). Откроется диалоговое окно **Remote Connections** (Удаленные подключения).



2. Откройте вкладку Authentication (Аутентификация) и выберите Caradigm:
 - SSO & CM Server (Сервер SSO и CM): введите IP-адрес сервера;
 - Single Sign-On (SSO) и Context Management (CM);
 - Default Group Name (Имя группы по умолчанию): введите имя группы по умолчанию в поле Default Group Name (Имя группы по умолчанию);
 - флажок Enable logoff remote desktop (Разрешить выход из системы на удаленном рабочем столе):

- установите этот флажок, чтобы закрыть сеанс текущего пользователя до выхода из системы;
- сбросьте флажок, чтобы выполнить отключение от сеанса.

3. Нажмите на кнопку **ОК**, чтобы сохранить настройки.

Настройка сервера Caradigm Vault

Для настройки сервера Caradigm Vault в операционной системе ThinOS выполните следующие действия:

1. Из меню рабочего стола выберите System Setup (Настройка системы), а затем Remote Connections (Удаленные подключения). Откроется диалоговое окно Remote Connections (Удаленные подключения).
2. Откройте вкладку **Authentication (Аутентификация)**, нажмите на кнопку **Caradigm**, введите в поле **SSO & CM Server** IP-адрес указанного сервера и нажмите на кнопку **ОК**.
3. На сервере Caradigm Vault выполните следующие действия:
 - убедитесь, что флажок Enroll unenrolled badges (Регистрировать незарегистрированные бейджи) установлен;
 - убедитесь, что все записи привязки ID бейджей удалены.

Tap Server

Way2Care Parameters	
Default Group Name	EGPGroup
Default Grace Period (min)	480
Badge Tap Processing Parameters	
Enroll Unenrolled Badges?	<input checked="" type="checkbox"/>
Badge Enrollment Timeout (sec)	300
Remote Desktop Tap Synchronization Timeout (sec)	120
Client Certificate Validation Parameters	
Reject Expired Certificates?	<input type="checkbox"/>
Reject Self-Signed Certificates?	<input type="checkbox"/>
Revoked Client Certificates	Revoke a Certificate
<< Click Revoke a Certificate to specify a Thin Client certificate that should be rejected >>	
Client Certificate Filters	Add New Filter
<< Click Add New Filter to specify a filter for acceptable Thin Client certificates >>	
Badge ID Mapping Parameters	Add New Badge ID Mapping
<< Click Add New Badge ID Mapping to specify a mapping for Thin Client badge IDs >>	
Apply	

4. Выберите **SSO&CM > Advanced Configurations** (Дополнительная конфигурация) и выполните следующие действия:

Fast Quiesce Criteria Evaluation Script		
<input checked="" type="checkbox"/> Enable Proximity Support		
Proximity Grace Period (XP Workstations)	30 (sec)	Proximity Key Timeout
		30 (sec)
<input checked="" type="checkbox"/> Enable Way2Care	<input type="checkbox"/> Force all Way2Care users to reauthenticate	

- 4.1. Убедитесь, что флажок **Enable Proximity Support** (Разрешить поддержку бесконтактных карт) установлен.
- 4.2. Убедитесь, что флажок **Enable way2care** (Разрешить way2care) установлен.

5. Для подготовки сертификата для сервера Caradigm Vault Server выполните следующие действия:

Сервер Caradigm Vault использует сертификат для проверки подключения между сервером-«раздатчиком» (Tap Server) и тонким клиентом.

5.1. Чтобы подать запрос на сертификат:

- сертификат должен быть выдан вашим сертификационным органом;
- подготовьте сертификат в двух форматах:
 - формат PFX с закрытым ключом;
 - формат PEM: текстовый файл DER, зашифрованный по Base64. Пусть, например, это будут файлы с именами Caradigm.cer и Caradigm.pfx.

5.2. Для импорта сертификата на тонкий клиент используйте любой из следующих двух вариантов:

- нажмите на **System Setup > System tools > Certificates** (Настройка системы > Системные инструменты > Сертификаты) для импорта сертификатов с USB-устройства или файлового сервера;
- импортируйте сертификат с помощью INI-файла.

```
AddCertificate=client_cert.pfx password=passpass
```

5.3. Для добавления сертификата на сервер Vault выполните следующие действия:

Thin Client Certificates

Client Certificates				Import a Certificate
Owner Name	Issuer Name	Valid From	Valid Until	Delete
CN=CaradigmClient,OU=bj,O=bj,L=bj,ST=bj,C=US	CN=SSO-SSODC-CA,DC=SSO,DC=COM	04/07/2015 08:15 UTC	04/06/2017 08:15 UTC	<input type="checkbox"/>
CN=Test client,O=Caradigm,L=Andover,ST=Massachusetts,C=US	CN=Test client,O=Caradigm,L=Andover,ST=Massachusetts,C=US	02/19/2014 19:30 UTC	02/14/2034 19:30 UTC	<input type="checkbox"/>
CN=sqwireless2,CN=Users,DC=sqwireless,DC=com	CN=sqwireless.com,DC=sqwireless,DC=com	09/17/2013 09:30 UTC	09/17/2014 09:30 UTC	<input type="checkbox"/>

Select All Select Expired Reset Apply

На странице **Thin Client Certificates** (Сертификаты тонких клиентов) добавьте сертификаты для устройств-тонких клиентов. Сертификаты должны быть в текстовом формате или в формате PEM, т.е. в виде текстового файла DER, зашифрованного по Base64. Для добавления сертификата выполните следующие действия:

- откройте файл сертификата DER в Блокноте;
- войдите в консоль Vault Server Admin Console и нажмите на Appliance (Устройство) > Thin Client Certificates (Сертификаты тонких клиентов);
- скопируйте текст из Блокнота на сервер Vault.

Конфигурация на серверах VDI и рабочих столах

Решение Caradigm для ThinOS поддерживает несколько типов серверов VDI, в т.ч. VMware View Horizon 6, Citrix Virtual Apps 6.5, Citrix Virtual Apps and Desktops 5.6 и Citrix Virtual Apps and Desktops 7.6.

Для настройки сервера VDI и рабочего стола выполните следующие действия:

- установите компоненты рабочего стола Caradigm на серверы и рабочие столы;
- укажите IP-адрес сервера Vault и укажите действительный токен безопасности;
- добавьте следующие строки в раздел Service файла конфигурации \programdata\sentillion\vergence\Authenticator.ini.

```
TapServerIdentification=True RemotePromptForPassword=Badge
```

ПРИМЕЧАНИЕ: в настоящий момент Caradigm SSO поверх PCoIP поддерживают следующие тонкие клиенты СИЛА с поддержкой PCoIP:

- PC4-1263 с PCoIP;
- PC4-1210 с PCoIP;
- PC4-1240 с PCoIP (D10DP);
- MK2-1240 AIO с PCoIP (5213);
- PC4-1242 с PCoIP.

Клиент SSO и CM, установленный на вашем сервере VDI и рабочих столах, необходимо обновить до новейшей версии 6.2.5, чтобы эта функция поддерживалась.

Caradigm Way2Care

Way2Care входит в состав портфеля Caradigm Identity and Access Management (IAM) и предназначен для безопасного доступа нескольких медицинских приложений к информации о пациентах.

- в ThinOS версии 8.6 для поддержки Way2Care добавлен новый параметр INI:

```
CaradigmServer=xxx UseWay2Care=yes
```

- вместе с параметром CaradigmServer также можно задать:

```
DisableManualLogon=yes EGPGroup=xxx
```

Эта функция использует Way2Care API, отличный от TapServer API. Way2Care работает с UID в десятичном формате.

Настройка SECUREMATRIX

SECUREMATRIX укрепляет безопасность корпоративных и облачных приложений. Решение обеспечивает конечным пользователям удобный вход в систему по одноразовому паролю, который может использоваться для доступа к рабочим столам, ОС Windows, VPN, интрасетям, экстрасетям, веб-серверам, электронной коммерции и другим сетевым ресурсам.

Для настройки **сервера SECUREMATRIX** введите либо `https://ip-адрес`, либо `https://полное-доменное-имя-сервера`, перезагрузите клиент, чтобы появилось диалоговое окно **входа в систему**, а затем введите свои учетные данные, чтобы открыть диалоговое окно **брокера VDI** для входа. Для получения дополнительных сведений см. документацию по SECUREMATRIX.

Введение в HealthCast

Решение HealthCast Single Sign-On (SSO) предназначено для повышения пользовательского комфорта, упрощения потока операций и укрепления безопасности в требовательных средах. Те же самые бесконтактные карты, которые используются для физического доступа, используются для открытия и закрытия уникальных пользовательских сеансов и перекрытия любых сеансов, ненамеренно оставленных открытыми на устройствах ThinOS. Как правило, пользователю приходится вводить свой пароль только раз в день, а бесконтактная карта позволяет упростить процедуры и сэкономить время при безопасном переходе с одного общего компьютера на другой. Кроме того, бесконтактные карты можно защитить PIN-кодом, если организация сочтет это нужным. Решение HealthCast SSO также поддерживает самостоятельный сброс пароля пользователем, поэтому возможно восстанавливать свои пароли, не обращаясь в поддержку.

ПРИМЕЧАНИЕ: решение HealthCast SSO под управлением ThinOS является клиент-серверным. ThinOS реализует его клиентский функционал, но для правильной работы решения необходимо также установить и настроить компоненты сервера HealthCast на серверной системе. Обратитесь в HealthCast через веб-сайт компании, чтобы получить один или несколько исполняемых файлов установки сервера, ознакомиться с требованиями к серверу и информацией о конфигурации.

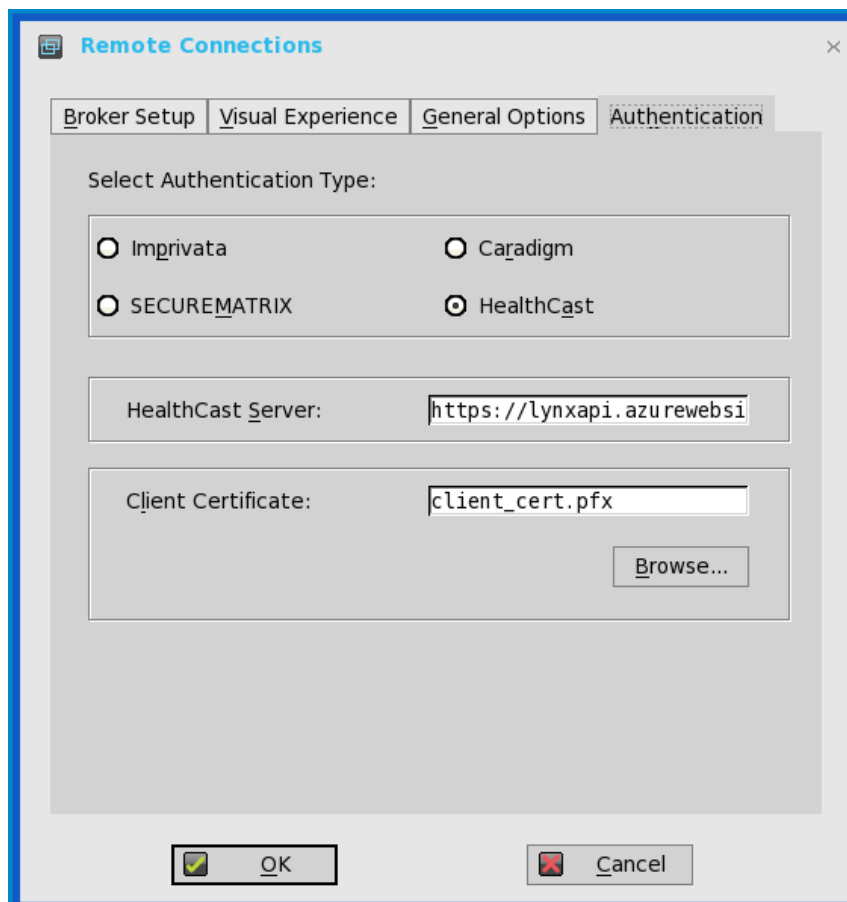
Настройка HealthCast в ThinOS

HealthCast Web API Server интегрирован в версию ThinOS, позволяя реализовать решение HealthCast SSO. Для использования решения HealthCast SSO необходимо настроить ThinOS на работу с сервером HealthCast Web API Server. Это можно сделать посредством INI-файла (wnos.ini) или через пользовательский интерфейс ThinOS. Для крупных инсталляций рекомендуется использовать файл INI.

Настройка через пользовательский интерфейс ThinOS

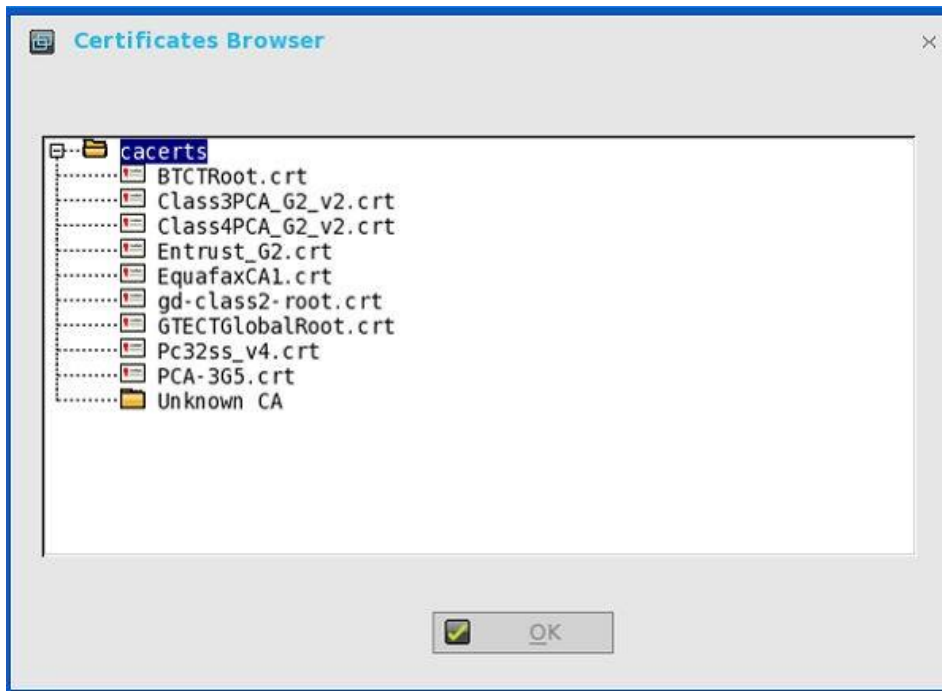
Для работы с HealthCast Web API настройте параметры HealthCast на стороне тонкого клиента. Для этого выполните следующие действия:

1. Из меню рабочего стола выберите **System Setup** (Настройка системы), а затем **Remote Connections** (Удаленные подключения). Откроется диалоговое окно Remote Connections (Удаленные подключения).



2. Откройте вкладку Authentication (Аутентификация) и выберите HealthCast.
3. В появившемся окне введите данные сервера HealthCast.

4. Для импорта клиентского сертификата нажмите на **Browse** (Обзор) и выберите нужный сертификат.



5. Нажмите на кнопку **OK**, чтобы сохранить настройки.

Настройка с помощью файла INI

Для настройки с помощью параметров INI добавьте в файл wnos.ini следующие параметры INI:

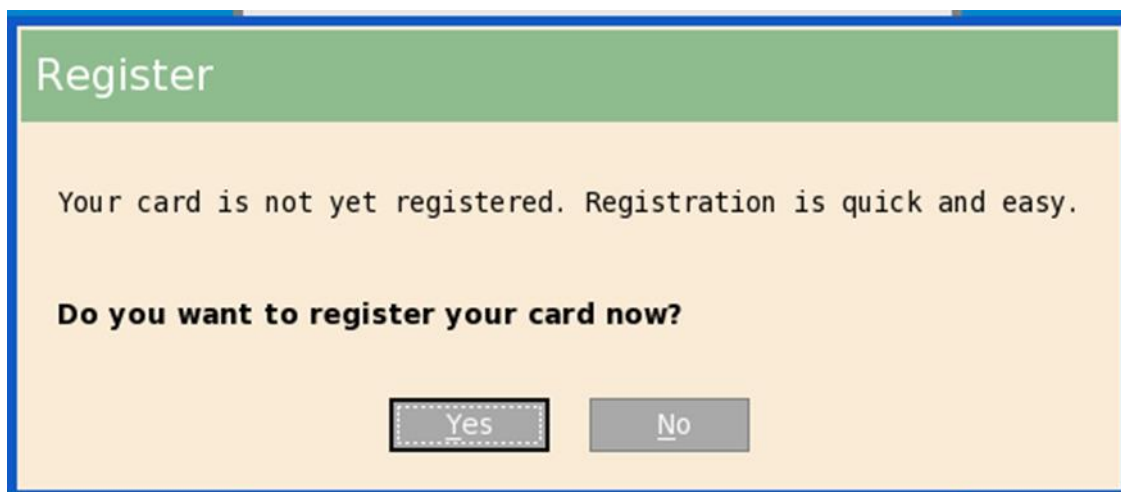
HealthCastServer— адрес сервера и параметры, необходимые клиенту для подключения к серверу HealthCast Web API Server. HealthCastServer=<https-адрес> SecurityMode=<default, full, warning, low> ClientCertificate=<имя-файла-сертификата-в-формате-pfx>

Например: HealthCastServer=https://server1.example.com SecurityMode=full ClientCertificate=client-cert.pfx.

Функционал HealthCast SSO в ThinOS

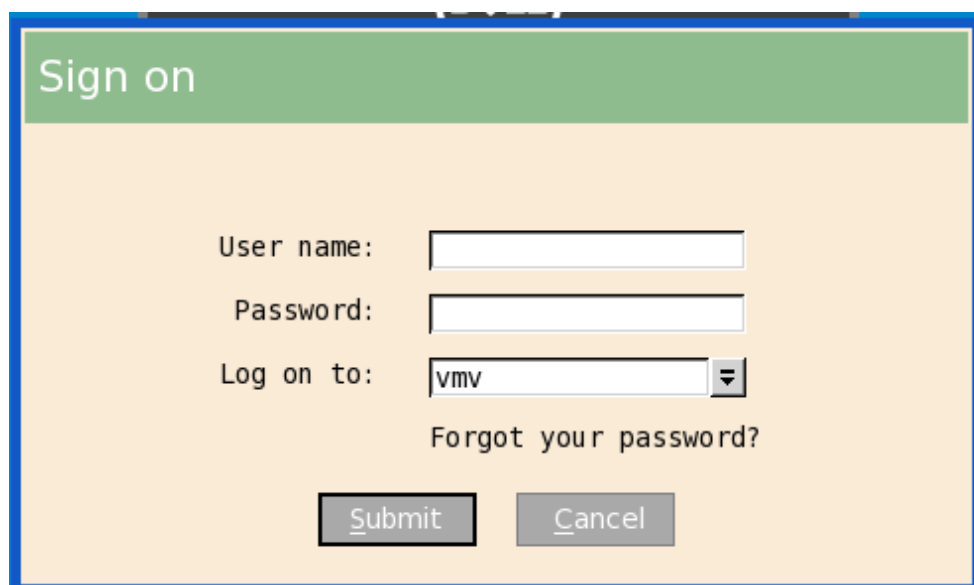
Функционал HealthCast SSO в ThinOS следующий:

- **регистрация бесконтактных карт:** HealthCast поддерживает саморегистрацию карт силами пользователей. Теперь не нужно приносить карту на специальную регистрационную станцию или обращаться к ИТ-персоналу. Просто прикоснитесь незарегистрированной бесконтактной картой к терминалу и зарегистрируйте ее. Это нужно проделать один раз, после чего карта может быть использована везде, где установлен HealthCast.



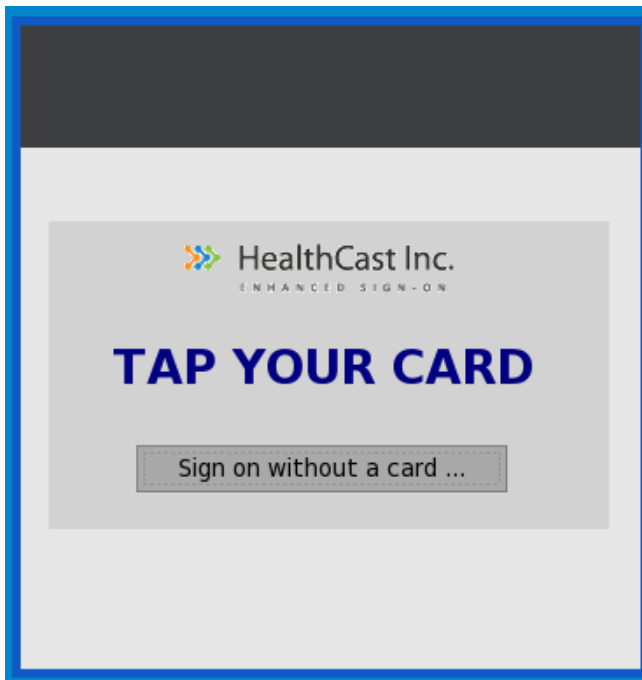
The image shows a 'Register' dialog box with a green header. The main text reads: 'Your card is not yet registered. Registration is quick and easy.' Below this is the question 'Do you want to register your card now?' and two buttons: 'Yes' and 'No'.

- **вход в систему по имени пользователя и паролю и блокировка/разблокировка терминалов:** при отсутствии карты возможен вход в систему по имени пользователя и паролю. Администратор при желании может отключить вход в систему по имени пользователя и паролю, чтобы пользователи работали только с картами. Если пользователь вошел в систему на терминале с помощью имени пользователя и пароля, он может заблокировать или разблокировать его, используя имя пользователя и пароль.



The image shows a 'Sign on' dialog box with a green header. It contains three input fields: 'User name:', 'Password:', and 'Log on to:'. The 'Log on to:' field has a dropdown menu with 'vmv' selected. Below the fields is a link 'Forgot your password?' and two buttons: 'Submit' and 'Cancel'.

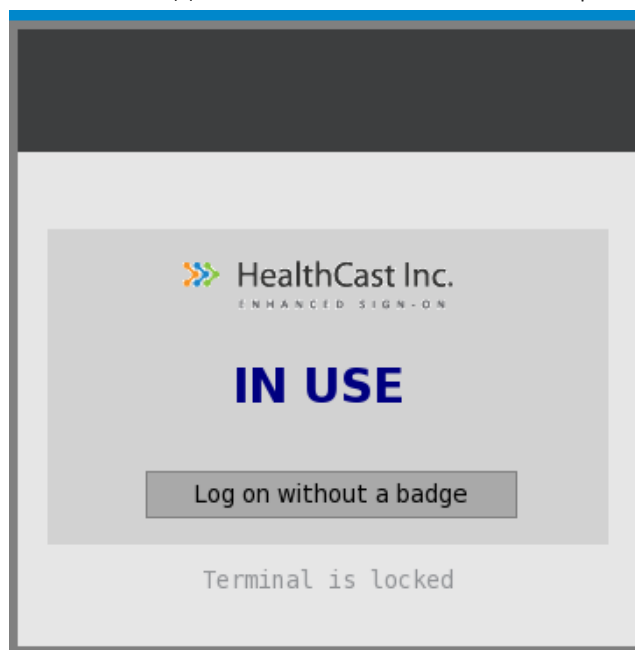
- **вход в систему и блокировка/разблокировка терминалов по бесконтактной карте:** после регистрации бесконтактной карты приложите ее к терминалу, чтобы войти в систему.



Пользователь может заблокировать сеанс, но при этом не разрывать подключение, чтобы быстро вернуться к работе по возвращении. Для этого необходимо прикоснуться бесконтактной картой к считывателю, и сеанс будет заблокирован.

Для возобновления работы прикоснитесь картой к считывателю еще раз.

- **Walk away** (Автоблокировка, если пользователь отлучился): терминалы можно настроить на блокировку или завершение сеанса, если пользователь ушел и оставил терминал открытым. Период времени, после которого происходит автоблокировка или автоотключение, задает администратор в веб-приложении;
- **Tap-over** (Перекрытие сеанса): если сеанс заблокирован или оставлен открытым, другой пользователь может прикоснуться своей бесконтактной картой и тем самым завершить первый сеанс, открыв новый уникальный сеанс для себя;
- **Forgotten card** (Пользователь забыл карту): можно получить временную бесконтактную карту и зарегистрировать ее сроком на один день;
- **Lost or stolen card** (Карта потеряна): если карта была утеряна, администратор может немедленно отключить ее в веб-приложении. После этого никто уже не



сможет ею воспользоваться;

- **Self-Service Password Reset (SSPR)** (Самостоятельный сброс пароля пользователем): если администратор разрешил SSPR, то появляется возможность зарегистрироваться в этой программе и сбрасывать пароль, не обращаясь в поддержку;



- **Easy to use web-based administration tool** (Веб-интерфейс администратора): администраторы могут легко и быстро настраивать параметры, управлять бесконтактными картами и пользователями через веб-интерфейс.

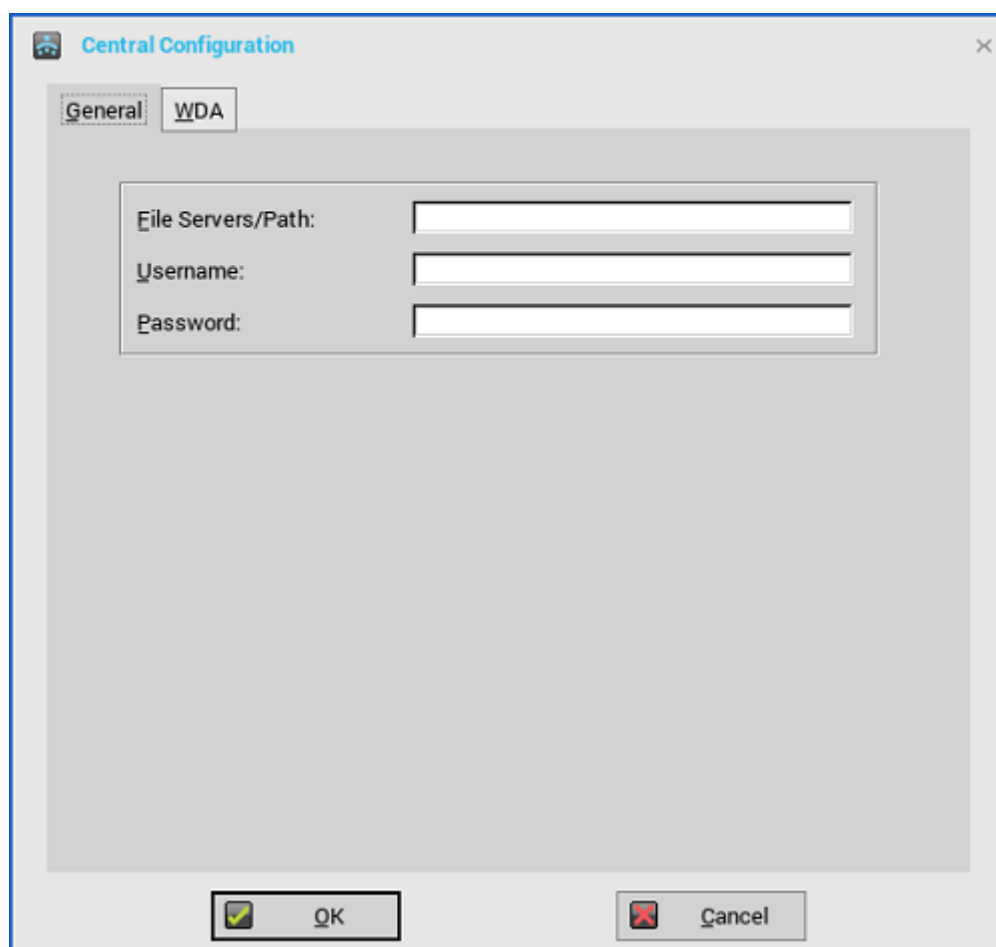
НАСТРОЙКА ЦЕНТРАЛЬНЫХ КОНФИГУРАЦИЙ

С помощью диалогового окна **Central Configuration** (Центральная конфигурация) настройте параметры файлового сервера, сервера WDM и сервера WMS.

НАСТРОЙКА ОБЩИХ ЦЕНТРАЛЬНЫХ КОНФИГУРАЦИЙ

Для настройки общих центральных конфигураций выполните следующие действия:

1. Из меню рабочего стола выберите **System Setup** (Настройка системы), а затем **Central Configuration** (Центральная конфигурация). Откроется диалоговое окно **Central Configuration** (Центральная конфигурация).
2. Откройте вкладку **General** (Общее):



File Servers/Path (Файловые серверы/путь), **Username** (Имя пользователя) и **Password** (Пароль): введите IP-адрес или имя хоста для файлового сервера, с которого должны поступать образы системного ПО и обновлений. Если используется DHCP, этот адрес может сообщаться посредством DHCP.

- 2.1. **File Servers/Path** (Файловые серверы/путь): не более 127 знаков для файлового сервера и не более 127 знаков для корневого пути. Эти данные указывают часть пути, которая должна использоваться при обращении к серверу.

Для файловых серверов поддерживается список резервных файловых серверов. Он состоит из одной или нескольких пар файловых серверов, перечисленных в порядке предпочтения. Можно перечислить несколько файловых серверов, разделенных двоеточиями или точками с запятой. Длина списка не должна превышать 127 знаков. При

подключении к файловому серверу клиент пытается подключиться к каждой паре в порядке следования, пока не найдет работающую пару файловых серверов.

2.2. **Username** (Имя пользователя): укажите имя пользователя для входа на файловый сервер. Длина не более 31 знака.

2.3. **Password** (Пароль): укажите пароль для входа на файловый сервер. Длина не более 31 знака.

3. Нажмите на кнопку **OK**, чтобы сохранить настройки.

НАСТРОЙКА ПАРАМЕТРОВ WDA

На этой вкладке происходит настройка параметров WMS и WDM. ThinOS поддерживает все параметры групповых политик WMS.

В WDA добавлена поддержка следующих трех типов сред безопасности для заказчиков:

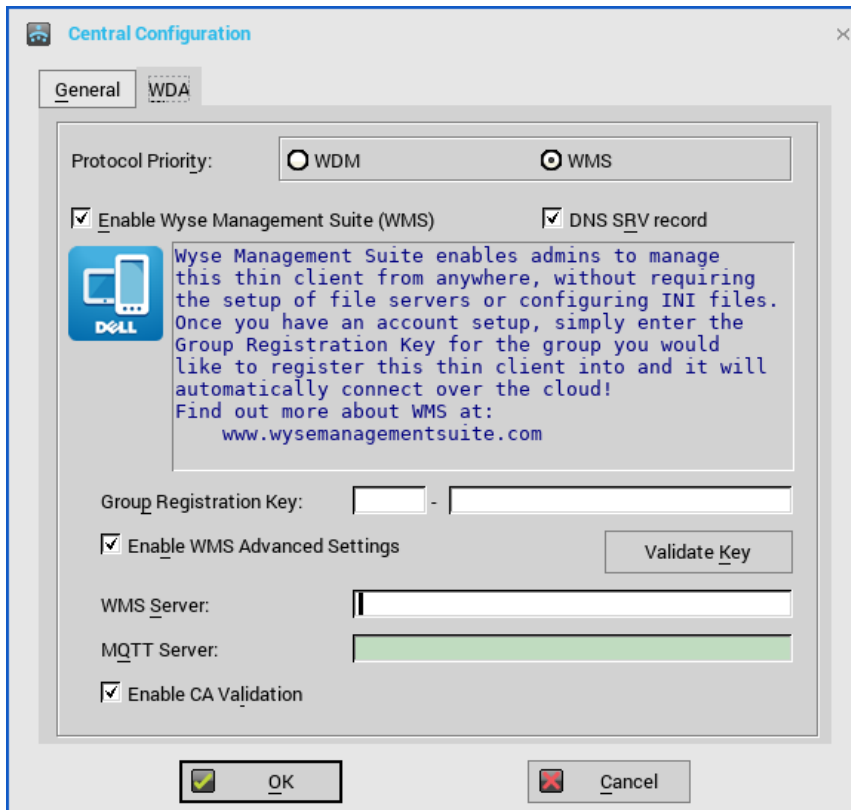
- **Среда с высоким уровнем безопасности:** администраторы должны входить в систему на каждом устройстве и использовать USB-носители или файловые серверы для импорта сертификата сервера. Сертификат сервера сохраняется на устройстве до тех пор, пока не будет выполнен сброс в заводские настройки. Устройство безопасно и неуязвимо для обнаружения новых устройств посторонними серверами DHCP или DNS. Администраторы могут использовать как самоподписанные сертификаты, так и сертификаты, подписанные CA.
- **Безопасная среда:** администраторы могут настраивать отпечаток пальца сертификата сервера в виде записи DNS_Text или опции DHCP_Score. Если WDA обнаруживает запись DNS_Text или опцию DHCP_Score, отпечаток пальца сертификата сервера рассылается по сети и добавляется на устройство локально. При перезаписи образа устройства отпечаток сертификата удаляется с него. Администраторы могут использовать как самоподписанные сертификаты, так и сертификаты, подписанные CA.
- **Обычная среда:** Вы можете использовать для обнаружения устройств как самоподписанные сертификаты, так и сертификаты, подписанные CA. Устройство должно установить подключение к CA для проверки сертификата. Это применяется в случае, если запись DNS_Text и опция DHCP_Score отсутствуют, но сертификат устройства подписан CA.

Если сертификат самоподписан, необходимо подтвердить сообщение о безопасности сертификата.

Для настройки параметров WMS выполните следующие действия:

1. Из меню рабочего стола выберите System Setup (Настройка системы), а затем Central Configuration (Центральная конфигурация). Откроется диалоговое окно Central Configuration (Центральная конфигурация).

2. Выберите **WDA > WMS** и затем выполните следующие действия:



По умолчанию выбран вариант **WMS**. Служба WMS автоматически запускается после загрузки клиента.

Если, например, первая попытка обнаружения службы WMS закончилась неудачей, выполняется поиск следующего варианта по уровню приоритета, например службы WDM. Процесс продолжается до тех пор, пока что-либо не будет успешно обнаружено. Если не удалось обнаружить ничего, поиск автоматически начинается снова через фиксированное время – 24 часа.

- 2.1. **Enable WMS (WMS)** (Разрешить WMS): установите этот флажок, чтобы разрешить WMS обнаруживать тонкий клиент.
- 2.2. **DNS SRV record** (Запись DNS SRV): установите этот флажок, если необходимо, чтобы тонкий клиент получал значения WMS от сервера DNS, а затем пытался зарегистрироваться на сервере WMS. По умолчанию этот флажок установлен. Если он снят, тонкий клиент не сможет получать значения WMS от сервера DNS.

Для создания записей DNS на сервере DNS используйте следующую информацию:

WMS server URL

Тип записи DNS: DNS SRV

Имя записи: `_WMS_MGMT._TCP.<домен>`

Возвращаемое значение: URL сервера WDMNG

Пример: `_WMS_MGMT._TCP.WDADEV.com`

MQTT Server URL

Тип записи DNS: DNS SRV

Имя записи: `_WMS_MQTT._TCP.<домен>`

Возвращаемое значение: URL сервера WMS

Пример: `_WMS_MQTT._TCP.WDADEV.com # Group Token`

Тип записи DNS: DNS Text

Имя записи: `_WMS_GROUPTOKEN.<домен>`

Возвращаемое значение: групповой токен (в строковом формате)

Пример: `_WMS_GROUPTOKEN.WDADEV.com # CA Validation`

Тип записи DNS: DNS Text

Имя записи: `_WMS_CAVALIDATION.<Домен>`

Возвращаемое значение: TRUE или FALSE (в строковом формате)

Пример: `_WMS_CAVALIDATION.WDADEV.com`

- 2.3. **Group Registration Key** (Групповой регистрационный ключ): введите групповой регистрационный ключ в таком формате, в каком он настроен администратором WMS для нужной группы. Для проверки ключа нажмите на Validate Key (Проверить ключ).

Для закрытого сервера WMS групповой регистрационный ключ не нужен. Вы можете указать данные сервера WMS, чтобы устройство могло подключиться к WMS. ThinOS регистрируется как карантинный съемщик (quarantine tenant) в WMS.

- 2.4. **Enable WMS Advanced Settings** (Разрешить дополнительные параметры WMS): установите этот флажок, чтобы ввести данные сервера WMS, данные сервера MQTT и разрешить проверку CA. По умолчанию вариант сервера MQTT отключен. Значение для сервера MQTT заполняется после того, как устройство ThinOS подключится к WMS.

ПРИМЕЧАНИЕ: если разрешен WMS, убедитесь в том, что введен групповой регистрационный ключ и настроены дополнительные параметры WMS.

Проверка CA (CA validation) необходима при импорте сертификатов на сервер WMS. По умолчанию флажок CA Validation установлен, чтобы обеспечивать безопасность при работе с облаком WMS. Изменение этого параметра влияет на подключения к следующим серверам:

- *.dellmobilitymanager.com
- *.cloudclientmanager.com
- *.wysemanagementsuite.com

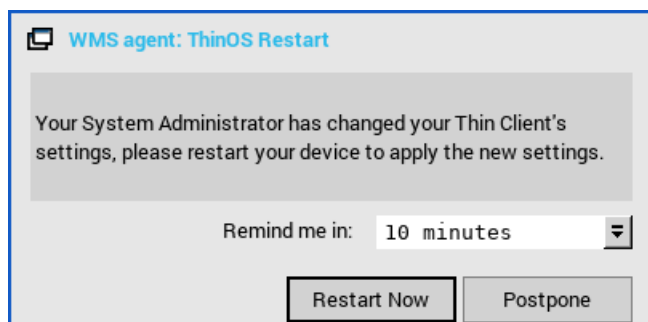
Таблица 8. Проверка CA

Развертывание WMS	Проверка CA
В закрытом облаке	При развертывании WMS в закрытом облаке флажок Enable CA Validation (Разрешить проверку CA) можно настроить после указания данных сервера в поле WMS Server (Сервер WMS) . По умолчанию этот флажок установлен.
В открытом облаке	При развертывании WMS в открытом облаке флажок Enable CA Validation (Разрешить проверку CA) установлен по умолчанию. Снять флажок Enable CA Validation (Разрешить проверку CA) нельзя.

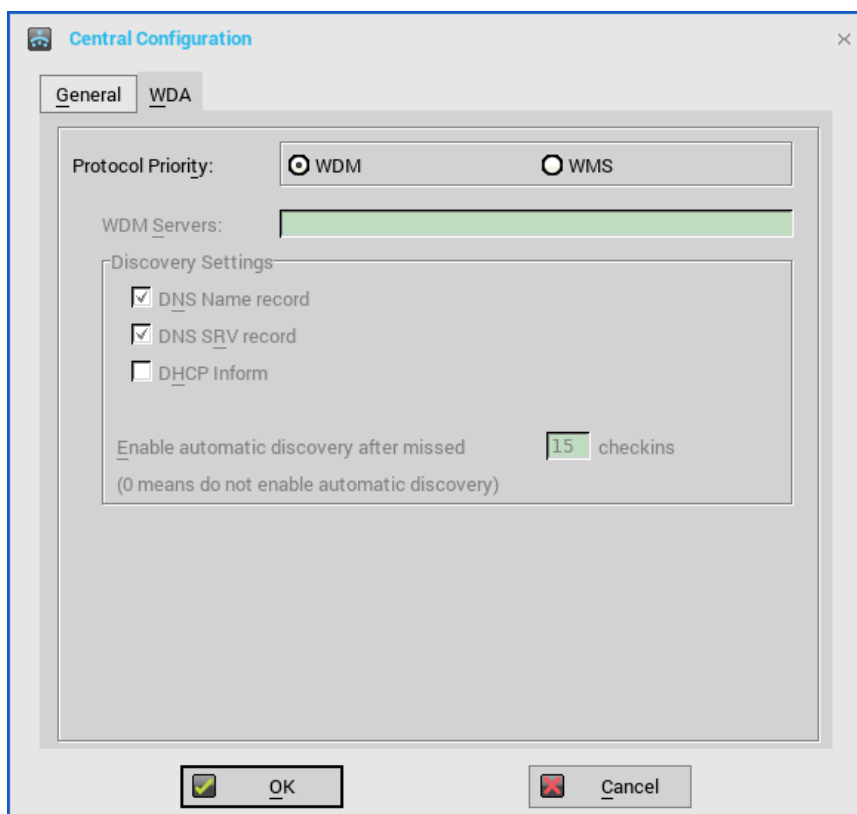
Для получения дополнительных сведений об управлении устройствами ThinOS с помощью WMS см. документ «WMS Руководство Администратора WMS».

3. Нажмите на кнопку **OK**, чтобы сохранить настройки.

При изменении политики ThinOS policy для зарегистрированного тонкого клиента с помощью WMS, появляется диалоговое окно с приглашением перезагрузить тонкий клиент сейчас или позже. Чтобы немедленно применить новые настройки, нажмите на кнопку **Restart Now** (Перезапустить сейчас). При необходимости перезапустить тонкий клиент позже, нажмите на кнопку **Postpone** (Отложить).



Для настройки параметров WDM выполните следующие действия:



1. Установите переключатель на **WDM** и следуйте инструкциям ниже:
 - 1.1. **WDM Servers** (Серверы WDM): если используется WDM, укажите здесь IP-адреса или имена хостов серверов. Если используются INI-профили пользователей, расположения можно указать в этих профилях.
 - 1.2. **DNS Name Record** (Запись имени DNS): (Динамическое обнаружение) – позволяет устройствам обнаруживать сервер WDM методом поиска по имени хоста DNS.
 - 1.3. **DHCP Inform**: (Динамическое обнаружение) – позволяет устройствам обнаруживать сервер WDM с помощью DHCP Inform.
 - 1.4. **Enable Automatic Discovery After Missed Check-ins** (Разрешить автообнаружение после неудачных подключений): выберите, сколько должно быть неудачных подключений, чтобы включилось автообнаружение.
2. Нажмите на кнопку **OK**, чтобы сохранить настройки.

Опцию WDM можно отключить с помощью следующих параметров INI:

```
WMSService=no
```

```
Service=wdm disable=yes
```

```
RapportDisable=yes
```

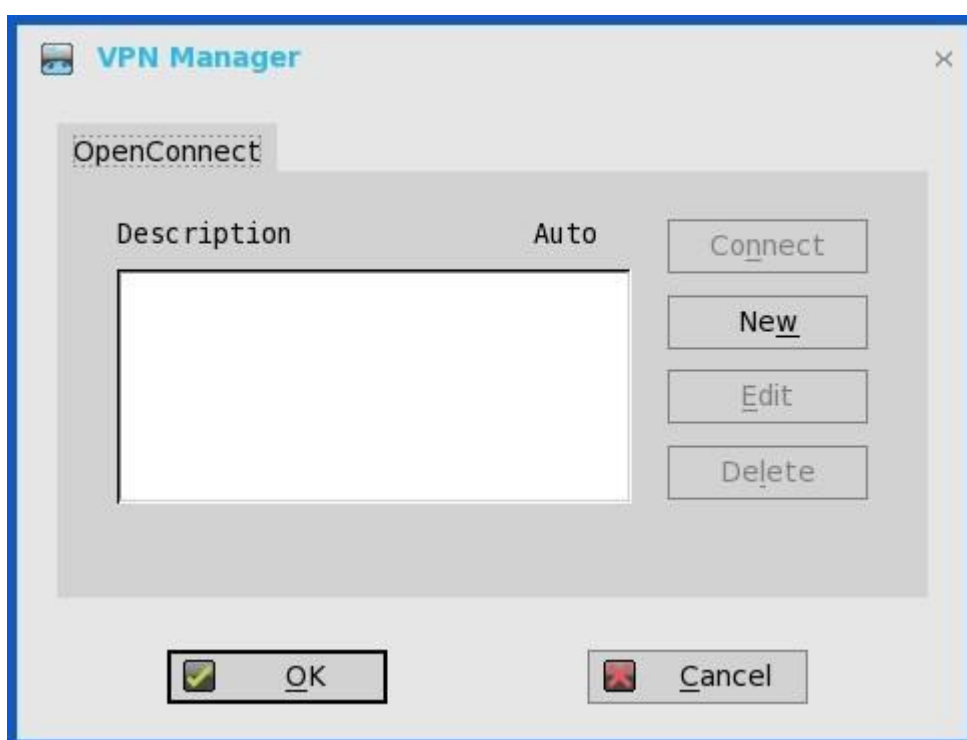
НАСТРОЙКА VPN MANAGER

Приложение VPN Manager служит для управления подключениями VPN (виртуальных частных сетей). В ThinOS для подключения к VPN используется клиент OpenConnect, основанный на протоколе SSL. Виртуальная частная сеть (VPN) расширяет частную сеть, используя общедоступные сети, например Интернет. Технология VPN позволяет устройствам обмениваться данными по общим или публичным сетям, при этом пользуясь функциональностью и безопасностью частных сетей.

Для настройки VPN Manager выполните следующие действия:

1. В классическом режиме выберите из меню рабочего стола **System Setup** (Настройка системы), а затем **VPN Manager** (Диспетчер VPN). В режиме Zero откройте вкладку **VPN Manager** (Диспетчер VPN) на панели **System Settings** (Параметры системы).
2. Щелкните **VPN Manager** (Диспетчер VPN).

Появится диалоговое окно **VPN Manager** (Диспетчер VPN).



3. Щелкните **New** (Создать), чтобы создать новый сеанс.
 - 3.1. **Session Name** (Имя сеанса) (не больше 21 знака): введите имя сеанса. Это необязательный параметр. Если оставить это поле пустым, то в качестве имени сеанса будет использоваться имя сервера VPN.
 - 3.2. **VPN Server** (Сервер VPN) (не больше 63 знаков): введите IP-адрес сервера VPN или имя хоста. Этот параметр обязателен.
 - 3.3. **Login Username** (Имя пользователя для входа в систему) (не больше 31 знака): введите имя пользователя для входа в систему. Этот параметр обязателен.
 - 3.4. **Login Password** (Пароль для входа в систему) (не больше 31 знака): введите пароль пользователя. Это необязательный параметр.

- 3.5. Если требуется, установите флажок **Auto-connect on system startup** (Автоподключение при включении системы).



- 3.6. Также при желании установите флажок **Show progress in detail** (Показывать прогресс).
- 3.7. Нажмите на кнопку **OK**.

При создании подключений в столбце **Description** (Описания) указывается имя сеанса, а в столбце **Auto** (Автоподключения) – устанавливается ли подключение автоматически при перезапуске системы. Автоподключение можно установить только для одного сеанса.

ГЛАВА 4. НАСТРОЙКА СОЕДИНЕНИЙ БРОКЕРОВ

В среде инфраструктуры виртуальных рабочих столов (VDI) брокер соединений — это программный объект, позволяющий подключаться к доступному рабочему столу. Брокер подключений позволяет безопасно и эффективно управлять инфраструктурой виртуальных рабочих столов.

НАСТРОЙКА CITRIX

Citrix предлагает комплексное решение для виртуализации, где все приложения и ресурсы развертываются на централизованном сервере и публикуются на удаленных устройствах. Клиентское программное обеспечение Citrix Receiver, установленное на тонком клиенте, позволяет взаимодействовать с графическим интерфейсом приложения, в то время как все процессы приложения выполняются на сервере.

В этом разделе содержится информация о том, как настроить соединение с брокером Citrix на устройстве ThinOS, а также о других функциях Citrix.

НАСТРОЙКА СОЕДИНЕНИЯ С БРОКЕРОМ CITRIX

Чтобы установить брокер Citrix:

1. В меню рабочего стола выберите **System Setup** (Настройка системы), а затем нажмите **Remote Connections** (Удаленные подключения). Откроется диалоговое окно **Remote Connections** (Удаленные подключения).
2. На вкладке **Broker Setup** (Настройка брокера) в раскрывающемся списке выберите **Citrix Xen** и выполните следующие действия:
 - 2.1. Установите флажок, чтобы включить стиль **StoreFront**.
 - 2.2. **Broker Server** (Сервер брокера): введите IP-адрес / имя хоста / полное доменное имя сервера брокера.
 - 2.3. **Auto Connect List** (Список автоматического подключения): введите имена рабочих столов, которые Вы хотите запускать автоматически после входа в соответствующий брокер. Можно ввести более одного рабочего стола через точку с запятой. Написание имени рабочего стола должно быть сделано с учетом регистра.
 - 2.4. Установите флажок, чтобы включить автоматическое переподключение при входе в систему.

ПРИМЕЧАНИЕ: если Вы включите автоматическое переподключение, Вы сможете выбрать один из вариантов переподключения. Можно подключиться либо только к отключенным сеансам, либо как к активным, так и к отключенным сеансам.
 - 2.5. Установите флажок, чтобы включить автоматическое переподключение в меню кнопок.

ПРИМЕЧАНИЕ: если Вы включите автоматическое переподключение, Вы сможете выбрать один из вариантов переподключения. Можно подключиться либо только к отключенным сеансам, либо как к активным, так и к отключенным сеансам.
 - 2.6. **Account Self-Service Server** (Сервер самообслуживания учетной записи): введите IP-адрес сервера самообслуживания учетной записи.
 - 2.7. **XenApp**: используйте эту опцию, если необходимо установить по умолчанию **XenApp**.
 - 2.8. **XenDesktop**: используйте эту опцию, если необходимо установить по умолчанию **XenDesktop**.

3. Нажмите **OK**, чтобы сохранить настройки.

ИСПОЛЬЗОВАНИЕ CITRIX ADC

ThinOS поддерживает контроллер доставки приложений Citrix (ADC), ранее известный как Citrix NetScaler. В ThinOS поддерживаются следующие методы аутентификации:

- Lightweight Directory Access Protocol (LDAP);
- RSA;
- DUO;
- SMS PASSCODE;
- OKTA.

Настройка Citrix NetScaler Gateway с использованием LDAP и RSA

Чтобы настроить Citrix NetScaler Gateway с использованием аутентификации LDAP и RSA, выполните следующие действия:

1. Перейдите в **NetScaler> NetScaler Gateway> Virtual Servers** и нажмите **Edit** (Изменить).
2. Установите первичную и вторичную аутентификации на основе следующих сценариев:
 - если Вы используете вход в систему LDAP и RSA, убедитесь, что основной аутентификацией является протокол LDAP, а вторичной аутентификацией – протокол RADIUS;
 - если Вы используете вход в систему RSA и LDAP, убедитесь, что основной аутентификацией является протокол RSA, а вторичной аутентификацией – протокол LDAP;
 - если Вы используете только вход в систему LDAP, убедитесь, что основной аутентификацией является протокол LDAP, а вторичной аутентификации нет.
3. Добавьте следующий параметр INI в файл wnos.ini и настройте свой файловый сервер:

```
pnliteserver=<fqdn of NS Server> CAGAuthMethod={LDAP,LDAP+RSA,RSA+LDAP} Storefront={yes,no}
```

Конфигурирование Citrix NetScaler Gateway с использованием DUO

Чтобы настроить Citrix NetScaler Gateway с использованием аутентификации DUO, выполните следующие действия:

1. Перейдите в **NetScaler> NetScaler Gateway> Virtual Servers** и нажмите **Edit** (Изменить).
2. Убедитесь, что основной аутентификацией является протокол RADIUS, который настроен с использованием аутентификации DUO RADIUS.
3. Убедитесь, что вторичная аутентификация отсутствует.
4. Добавьте следующий параметр INI в файл wnos.ini и настройте свой файловый сервер:

```
pnliteserver=<fqdn of NS Server> Storefront={yes,no}
```

Использование Citrix NetScaler с аутентификацией SensorNet MFA

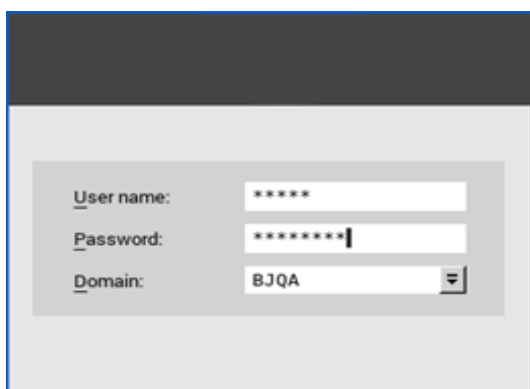
После ребрендинга SMS PASSCODE получил новое наименование: SensorNet MFA. Вы можете настроить шлюз NetScaler на использование одноразового пароля (One Time Passcode/Password)(OTP) в виде PIN-кода или кода доступа. Чтобы получить этот разовый пароль, Вам необходимо установить приложение SensorNet на мобильный телефон. После ввода кода доступа или PIN-кода сервер аутентификации объявляет этот разовый пароль недействительным. Нельзя ввести тот же самый пароль или PIN еще раз. Для получения дополнительных сведений о настройке разовых паролей см. документацию по Citrix.

Необходимые условия

- на клиенте должен быть установлен NetScaler v12.0 или более поздней версии;
- в вашей сети должен быть установлен и настроен SMS PASSCODE v9.0 SP1. Вы можете загрузить файл SMS PASSCODE v9.0 по адресу download.smpasscode.com/public/6260/SmsPasscode-900sp1;
- политика аутентификации RADIUS (Remote Authentication Dial-In User Service) настроена и привязана к серверу шлюза NetScaler;
- на мобильном телефоне установлено и настроено приложение SensorNet. Для использования одноразового пароля в ThinOS выполните следующие действия:

1. Войдите в систему ThinOS и подключитесь к URL шлюза NetScaler.
2. Введите свой ID пользователя и пароль, затем нажмите **Enter**.

Появится диалоговое окно PASSCODE. В этот момент на Ваш телефон придет push-уведомление с кодом от приложения SensorNet.



A screenshot of a login form. It has three input fields: 'User name:' with a masked password '*****', 'Password:' with a masked password '*****|', and 'Domain:' with a dropdown menu showing 'BJQA'.



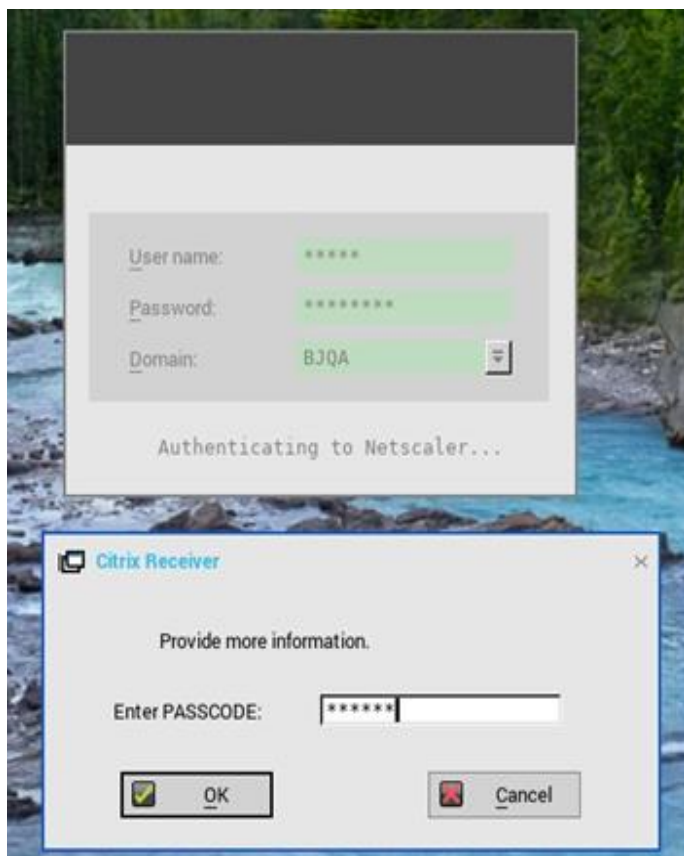
Message

NON-TRUSTED LOCATION
 PASSCODE: ihyhyw
 Country: unknown
 Org: ???

Message downloaded 2019/10/11 16:32:53

3. Нажмите на кнопку **OK**.

Если аутентификация прошла успешно, Вы подключились к сеансу Citrix.



Настройка Citrix NetScaler с помощью Okta

Okta реализует функцию Single Sign-On (SSO) с помощью службы RADIUS для Citrix Virtual Apps and Desktops. ThinOS поддерживает Okta посредством Citrix NetScaler Gateway 11.0 или более поздней версии. Для аутентификации пользователя используется агент Okta RADIUS Agent. Серверный агент Okta RADIUS назначает аутентификацию пользователя в Okta с помощью однофакторной (SFA) или многофакторной аутентификации (MFA).

Для получения дополнительной информации о настройке шлюза Citrix NetScaler на работу с Okta RADIUS Agent см. документацию *Citrix NetScaler Gateway Radius Configuration Guide* по адресу help.okta.com.

ПРИМЕЧАНИЕ: на тонком клиенте ThinOS необходимо указать полное доменное имя в окне входа в систему. Если Вы не используете имя пользователя и FQDN во время входа в систему, Вы должны установить следующий параметр INI:

```
pnliteserver=https://<fqdn of NS Server> CAGUserAsUPN=yes
```

После установки этого параметра INI домен должен использовать формат domain.com в окне входа в систему.

Ограничения

ThinOS версии 8.6 поддерживает только Okta в режиме NetScaler Radius.

ОБЛАЧНЫЕ СЕРВИСЫ CITRIX

ThinOS поддерживает облачные сервисы Citrix. Она выступает в качестве единой консоли управления для развертывания приложений и рабочих столов в любой виртуальной или облачной среде для создания безопасного цифрового рабочего пространства. Для получения дополнительных сведений об облачных сервисах Citrix см. статью о Citrix Cloud на сайте docs.citrix.com.

ОБНОВЛЕНИЕ CITRIX ПО КНОПКЕ REFRESH

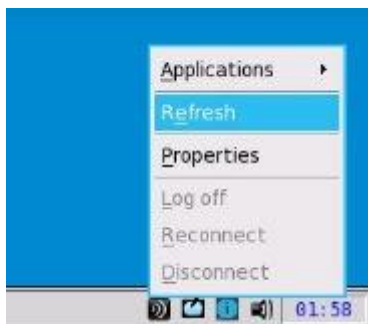
Приложения Citrix можно обновлять, щелкая **Refresh** (Обновить) в меню PNMenu. Обновить приложение Citrix можно двумя способами:

- вручную;
- автообновление с помощью параметра INI.

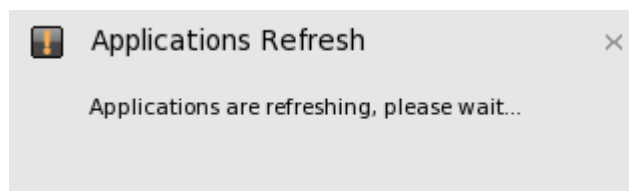
Обновление приложений Citrix вручную

Чтобы обновить приложение Citrix вручную, выполните следующие действия:

1. Для одного сервера StoreFront или PNAgent измените приложение в брокере и нажмите на **Refresh** (Обновить) в PNMenu.



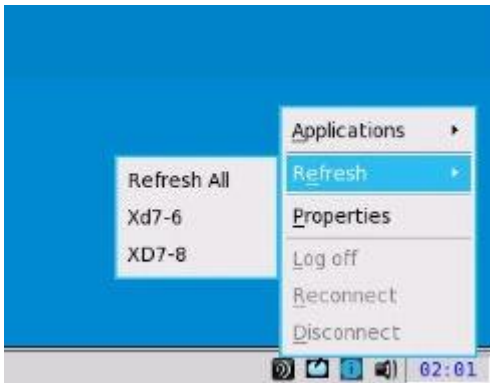
Во время обновления приложения в нижней правой части экрана появится следующее сообщение.



2. Приложения обновляются в списке панелей сеансов, в списке диспетчера подключений Connect Manager и в списке меню приложений. В окне журнала событий отображается следующее:

ICA: refresh store "xxx" ... или "ICA: refresh PNAgent"xxx" ...

3. Для серверов MultiFarm (StoreFront или PNAgent) или Multilogon (StoreFront или PNAgent) выберите один сервер для обновления или же щелкните **Refresh All** (Обновить все), чтобы обновить все серверы.



ПРИМЕЧАНИЕ: при попытке открыть, изменить или удалить приложения во время обновления отображается предупреждающее сообщение.



4. Обновление охватывает такие аспекты, как удаление, добавление, дублирование, отключение, включение приложения, смена значка/названия, помещение на рабочий стол/удаление с рабочего стола.

Запущенные активные сеансы не затрагиваются обновлением приложений.

5. Отключенный сеанс можно переподключить после обновления приложения, если для удаленного подключения установлен флажок **Automatic reconnection at logon** (Автоматическое переподключение при входе в систему).

Автоматическое обновление приложений Citrix с помощью параметра INI

Чтобы обновлять приложение Citrix автоматически, задайте следующий параметр INI:

SessionConfig=ICA RefreshTimeOut=дд:чч:мм

Например, 01:01:22 означает, что приложение будет начинать обновляться автоматически с интервалом в 1 день, 1 час и 22 минуты.

Ограничения обновления Citrix с помощью значков

- обновление Citrix с помощью значков поддерживается только в классическом режиме и режиме StoreFront;
- режим VDI не поддерживается.

РАБОТА С НЕСКОЛЬКИМИ АУДИОУСТРОЙСТВАМИ В СЕАНСЕ CITRIX

ThinOS поддерживает работу с несколькими аудиоустройствами в XenDesktop или XenApp версии 7.6 и более поздних. Вы можете подключать и отключать аудиоустройства в любой момент

сеанса, но их поведение аналогично поведению на локальном рабочем столе. При поддержке нескольких устройств Вы можете подключить несколько аудиоустройств и затем выбрать конкретное устройство для конкретного приложения.

На рабочем столе Citrix RDS должна быть активирована политика **Audio Plug N Play** (Plug N Play для аудиоустройств). Настройки этой политики разрешают или запрещают использование нескольких аудиоустройств для записи и проигрывания звука. По умолчанию оно разрешено.

ПРИМЕЧАНИЕ: на рабочем столе Citrix VDI предварительная настройка не требуется.

Поддерживаемые устройства: поддерживаются USB-гарнитуры, веб-камеры (без перенаправления USB) и аналоговые гарнитуры. Ниже приведены допустимые рабочие условия для нескольких аудиоустройств:

При использовании стандартного аудио Citrix HDX:

1. Выберите аудиоустройство как **PC Mic and Speaker** (Микрофон и динамик PC).
2. Настройте наушники или динамик.
3. Для второго звонящего выберите аудиоустройства, отличные от уже выбранных.

При использовании Citrix RealTime Multimedia Engine (RTME):

1. Выберите аудиоустройство как **HID headset with PC Mic and Speaker** (Гарнитура HID с микрофоном и динамиком PC).
2. Задайте **PC Mic and Speaker** (Микрофон и динамик PC) для настройки динамика или микрофона.
3. Для второго звонящего выберите аудиоустройства, отличные от уже выбранных. При работе с несколькими аудионастройками необходимо учитывать следующие сценарии:
 - в качестве аудиоустройства по умолчанию в ThinOS выбрано аудиоустройство, подсоединенное к тонкому клиенту последним;
 - в качестве аудиоустройства по умолчанию для сеанса выбрано аудиоустройство ThinOS по умолчанию. Однако этот параметр можно изменить;
 - перезапуск клиента Skype for Business/Lync после подсоединения и отсоединения устройства;
 - поддержка аудио ICA RTP с несколькими аудиоподключениями;
 - во время звонка можно менять настройки аудиоустройства без физического подключения/отключения устройства;
 - можно совместно использовать несколько аудио для разных каналов.

НАСТРОЙКА ПОДКЛЮЧЕНИЙ ICA

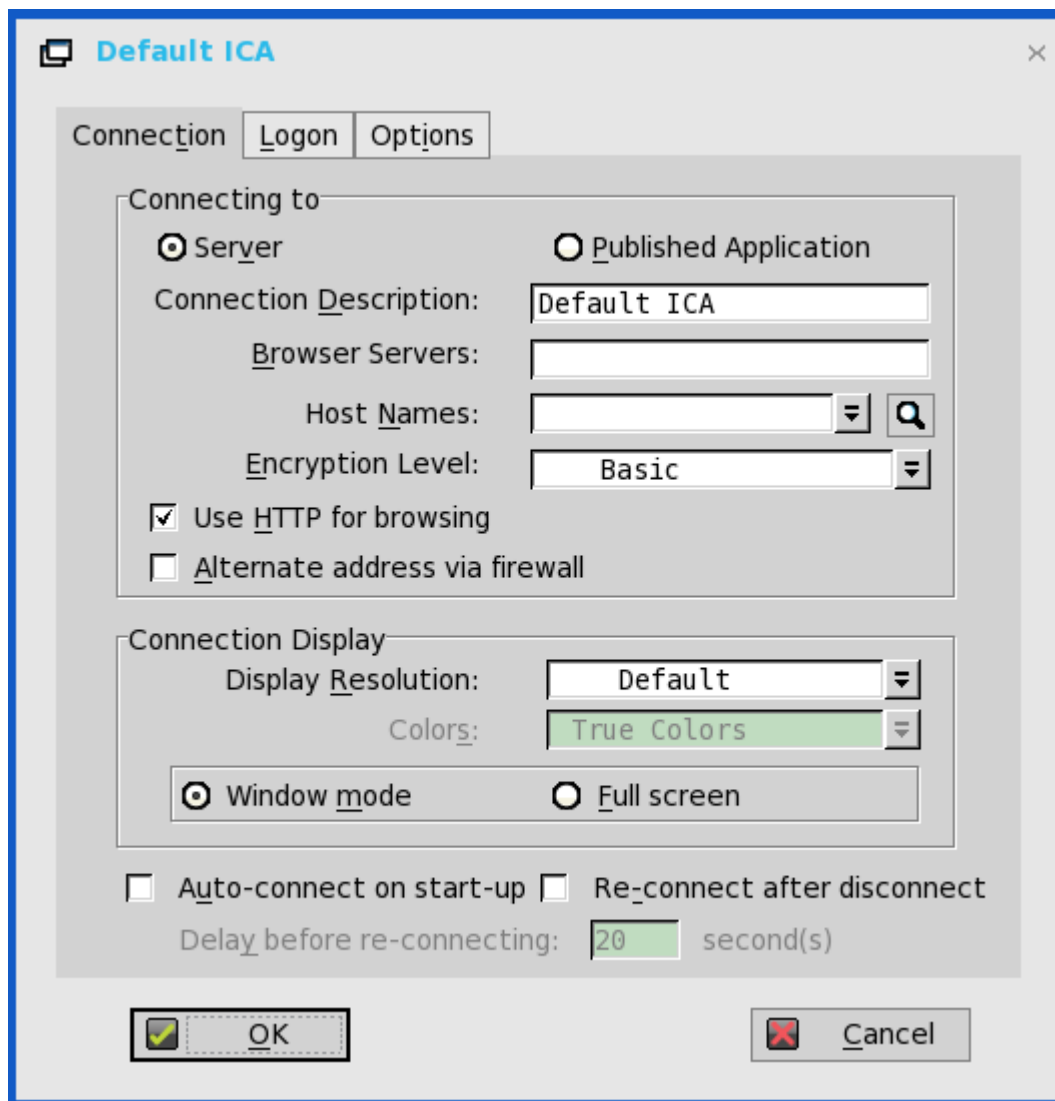
Для настройки подключений ICA выполните следующие действия:

1. Из меню рабочего стола выберите **System Setup** (Настройка системы), а затем **Remote Connections** (Удаленные подключения). Откроется диалоговое окно **Remote Connections** (Удаленные подключения).
2. На вкладке **Broker Setup** (Настройка брокера) выберите из раскрывающегося списка **Broker type** (Тип брокера) значение **None** (Нет).
3. Нажмите на протокол подключения **ICA** и затем щелкните **Configure** (Настроить). Появится диалоговое окно **Default ICA** (ICA по умолчанию).

ПРИМЕЧАНИЕ: ICA по умолчанию всегда используется для прямого подключения к опубликованному приложению, но не для StoreFront или PNAgent.

4. Откройте вкладку **Connection** (Подключение).

Для настройки подключений ICA используйте следующие параметры:



- **Server** (Сервер) или **Published Application** (Опубликованное приложение): выберите тип подключения, к которому будут применяться настройки.
- **Connection Description** (Описание подключения): введите описательное имя, которое будет отображаться в списке подключений (не больше 38 знаков).
- **Browser Servers** (Серверы браузеров): введите список IP-адресов или зарегистрированных в DNS имен серверов ICA, содержащих главный список браузеров или направляющих запрос на другой сервер, на котором есть такой список. В качестве разделителей в списке адресов используйте запятые или точки с запятой. Главный список браузеров генерируется автоматически на одном из серверов ICA. Он служит для предоставления информации, отображающейся в поле **Server Name or IP** (Имя сервера или IP). Если список находится на сервере ICA в том же сегменте сети, что и тонкий клиент, ничего указывать не нужно. Также ничего не нужно указывать, если подключение осуществляется к серверу или имя сервера или его IP-адрес содержит IP-адрес сервера.
- **Host Name / Application Name** (Имя хоста / имя приложения) (зависит от того, выбран ли вариант **Server** или **Published Application**): можно указать список имен хостов или IP-адресов серверов ICA либо опубликованных приложений, полученных от главного браузера ICA, разделенных запятыми или точками с запятой.

Если Вы указали список серверов с разделителями, то после неудачной попытки подключения тонкий клиент будет пытаться подключиться к следующему серверу в списке. Если Вы использовали список, то после неудачной попытки подключения к выбранному серверу тонкий клиент будет пытаться подключиться к следующему в списке.

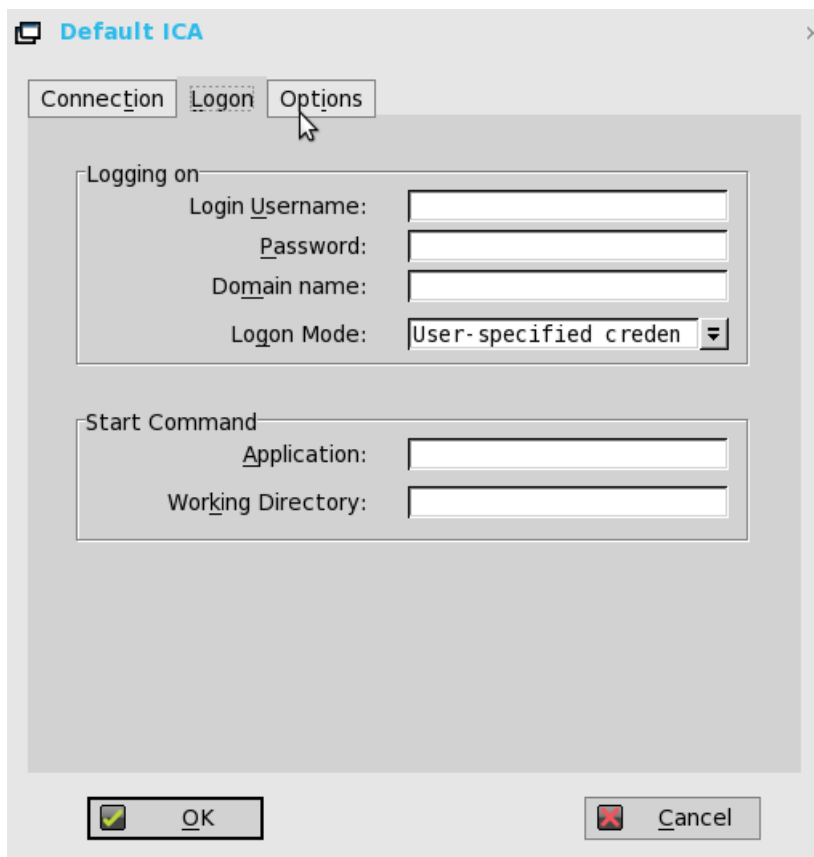
ПРИМЕЧАНИЕ: преобразование имени хоста может осуществляться с помощью одного из трех механизмов: главный браузер ICA, DNS или WINS. При этом только главный браузер может преобразовывать имена опубликованных приложений, если только для них не сделаны вручную записи в DNS. DNS при попытке сконструировать полное доменное имя использует доменное имя по умолчанию с панели управления сетью. Однако он пытается преобразовать имя без применения значения по умолчанию.

- **Encryption Level** (Уровень шифрования): позволяет выбрать уровень безопасности для обмена данными между тонким клиентом и сервером ICA.
- **Basic** (Базовый) (значение по умолчанию): самый низкий уровень безопасности. Базовый уровень обеспечивает самую высокую скорость коммуникации между устройством и сервером ICA за счет меньших затрат времени на обработку.

ПРИМЕЧАНИЕ: выбранный уровень шифрования регулирует уровень безопасности только при обмене данными между тонким клиентом и сервером ICA. Он не зависит от параметров безопасности отдельных приложений на сервере ICA. Например, для большинства финансовых транзакций в WWW от тонкого клиента требуется 128-разрядное шифрование. Однако при этом данные транзакций могут оказаться недостаточно защищенными, если на тонком клиенте тоже не используется 128-разрядное шифрование.

- **Use HTTP for browsing** (Использовать HTTP для обзора): если установлен этот флажок, то тонкий клиент по умолчанию использует HTTP для обзора.
- **Alternate address via firewall** (Альтернативный адрес через брандмауэр): если установлен этот флажок, тонкий клиент использует альтернативный IP-адрес, возвращенный от главного браузера ICA, так, чтобы обмен данными шел через брандмауэр. Этот пункт служит для входа в систему Windows при активации подключения.
- **Display Resolution** (Разрешение экрана): настройте разрешение экрана для этого подключения.
- Если выбран переключатель **Published Application** (Опубликованное приложение), то в разделе **Connection Display** (Экран подключения) можно выбрать вариант **Seamless Display Resolution** (Бесшовный экран).
- **Colors** (Цвета): выберите глубину цвета для сеанса ICA. Если выбран вариант High Colors (16-bit) или True Colors, а сервер ICA не поддерживает эту глубину цвета, то тонкий клиент устанавливает более низкое значение, например 256 цветов (8-бит).
- **Window mode** (В окне) и **Full screen mode** (Полный экран): выберите первоначальный режим отображения для приложения и рабочего стола: развернуть на полный экран или выводить в окне.
- **Auto-connect on start-up** (Автоподключение при запуске): если установлен этот флажок, тонкий клиент автоматически подключает этот сеанс при запуске.
- **Reconnect after disconnect** (Восстановление подключения при разрыве): если установлен этот флажок, тонкий клиент автоматически восстанавливает подключение после разрыва, произошедшего не по инициативе оператора. Интервал ожидания задается в поле **Delay before reconnecting** (Задержка перед повторным

подключением). Допустимый диапазон значений от 1 до 3600 секунд. По умолчанию установлено 20 секунд, если для данного подключения не задан параметр INI или Вы являетесь автономным пользователем.



5. Откройте вкладку **Logon** (Вход в систему):

- **Блок Logging on** (Параметры входа): введите имя пользователя, пароль, доменное имя и режим входа. Если поля для ввода имени пользователя, пароля и доменного имени недоступны, введите эти данные вручную на экране входа на сервер ICA.
 - **Login Username** (Имя пользователя для входа): не более 31 знака;
 - **Password** (Пароль): не более 19 знаков;
 - **Domain Name** (Доменное имя): не более 31 знака;
 - **Logon Mode** (Режим входа): выберите **User-specified credentials** (Ввод учетных данных пользователем), **Smart Card** (Смарт-карта) или **Local User** (Локальный пользователь).
- **Блок Start Command** (Стартовая команда): только при выборе варианта **Server Connection**. Этот блок недоступен для варианта **Published Application**.

- **Application** (Приложение) (не более 127 знаков) и **Working Directory** (Рабочий каталог) (не более 63 знаков): введите строку инициализации и аргументы (включая связанный рабочий каталог), которые должны автоматически запускаться на сервере при подключении.

6. Откройте вкладку **Options** (Параметры):

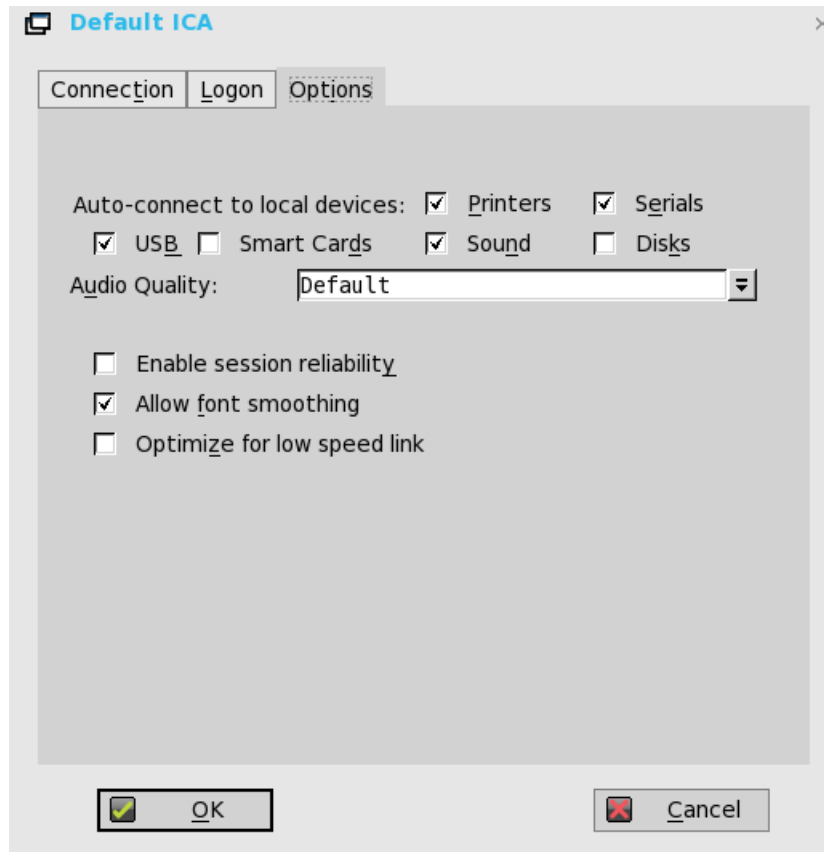
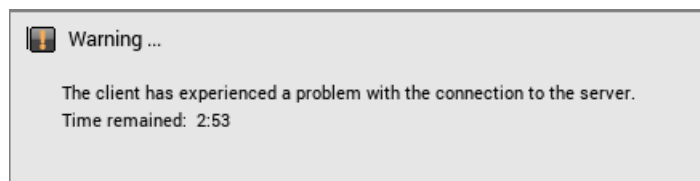


Рис. 14. Окно Default ICA – Options.

- **Autoconnect to local devices** (Автоподключение к локальным устройствам): установите флажки для любых устройств (принтеров, последовательных портов, USB, смарт-карт или дисков), к которым тонкий клиент должен подключаться автоматически.
- **Allow font smoothing** (Разрешить сглаживание экранных шрифтов): если этот флажок установлен, будет применяться сглаживание экранных шрифтов.
- **Optimize for low speed link** (Оптимизировать для медленных соединений): если установлен этот флажок, выполняется оптимизация для низкоскоростных соединений, например, снижение качества аудио или сокращение размера кэша протокола. Этот флажок предназначен для модемных подключений и распределенных каналов WAN.
- **Enable session reliability** (Разрешить обеспечение надежности сеанса): если установлен этот флажок, средства обеспечения надежности сеанса позволяют Вам обходиться без повторной аутентификации при кратковременной потере связи. Подключение остается активным на сервере и после восстановления связи снова доступно клиенту. Надежность сеансов более всего важна для беспроводных устройств.

7. Нажмите на кнопку **ОК**, чтобы сохранить настройки.

Если надежность сеанса включена для активного подключения, а ваша сеть не настроена соответствующим образом, появится предупреждение с указанием оставшегося времени.



ПОДДЕРЖКА НЕСКОЛЬКИХ МОНИТОРОВ В СЕАНСЕ CITRIX

Этот раздел относится к тонким клиентам СИЛА PC4-1221. ThinOS поддерживает несколько мониторов для рабочего стола ICA в версиях XenDesktop/XenApp 7.6 и более поздних.

Необходимые условия:

1. Увеличьте значение REG_DWORD **MaxVideoMemoryBytes** так, чтобы можно было поддерживать один или несколько мониторов с разрешением 4K. Для получения дополнительных сведений см. документацию Citrix на сайте support.citrix.com.
2. Увеличьте лимит видеопамати для поддержки большой глубины цвета и большого разрешения. Для получения дополнительных сведений см. документацию Citrix на сайте citrix.com.

Пользовательский сценарий:

1. Подключите несколько мониторов к устройству ThinOS.
2. В диалоговом окне **Display Setup** (Настройка экрана) отключите **Mirror Mode** (Зеркальный режим) и настройте расположение мониторов.
3. Запустите рабочий стол ICA в полноэкранном режиме.

Таблица 14. Параметры экрана.

Платформы	Максимальное разрешение экрана	Максимальное число системных мониторов	
		Стандартный рабочий стол или RDS — Windows 10 /2012 R2/ 2016	Рабочий стол HDX 3D Pro — Windows 10 с GRID K1/K2 GPU
Тонкий клиент СИЛА PC4-1221 Extended	1920 x 1080	6	4
	2560 x 1440	6	4
	3840 x 2160	6	Не поддерживается вследствие ограничений профиля GRID K1/K2 vGPU.
Тонкий клиент СИЛА PC4-1221 — процессор	1920 x 1080	3	3
	2560 x 1440	3	3

Платформы	Максимальное разрешение экрана	Максимальное число системных мониторов	
		Стандартный рабочий стол или RDS — Windows 10 /2012 R2/ 2016	Рабочий стол HDX 3D Pro — Windows 10 с GRID K1/K2 GPU
Pentium	3840 x 2160	3	Не поддерживается вследствие ограничений профиля GRID K1/K2 vGPU.
Тонкий клиент СИЛА PC4-1221 — процессор Celeron	1920 x 1080	2	2
	2560 x 1440	2	2
	3840 x 2160	2	Не поддерживается вследствие ограничений профиля GRID K1/K2 vGPU.

Ограничения

1. Для стандартного рабочего стола или RDS (Windows10/ 2012 R2 /2016) на тонком клиенте СИЛА PC4-1221 Extended рекомендуется подключать до четырех мониторов 4K, а оставшиеся мониторы использовать с разрешением 1920 x 1080.
2. Для рабочего стола HDX 3D Pro с vGPU или GPU поддерживаемое разрешение и количество мониторов зависит от матрицы поддержки NVIDIA GRID.

ПРИМЕЧАНИЕ: для получения дополнительных сведений об официальной поддержке нескольких мониторов для Citrix см. документацию Citrix на сайте support.citrix.com.

САМОСТОЯТЕЛЬНЫЙ СБРОС ПАРОЛЯ ДЛЯ ICA

Вы можете самостоятельно сбросить пароль или разблокировать учетную запись, если Вы зарегистрировали свои секретные вопросы.

Поддерживаемая среда:

1. Citrix Virtual Apps and Desktops 7.11 и более поздних версий.
2. Support Storefront Server 3.7 и более поздних версий
3. Self-Service Password Reset Server 1.0 и более поздних версий

Поддерживаемые платформы: поддерживаются все платформы.

Ограничения:

1. Поддерживается только сервер Storefront.
2. Сервис Legacy Account Self-Service(Самообслуживание устаревших учетных записей), не зависит от версии Storefront. Этот сервис требует настройки сервера самообслуживания учетных записей в разделе Remote Connections (Удаленные подключения) ThinOs. Storefront при

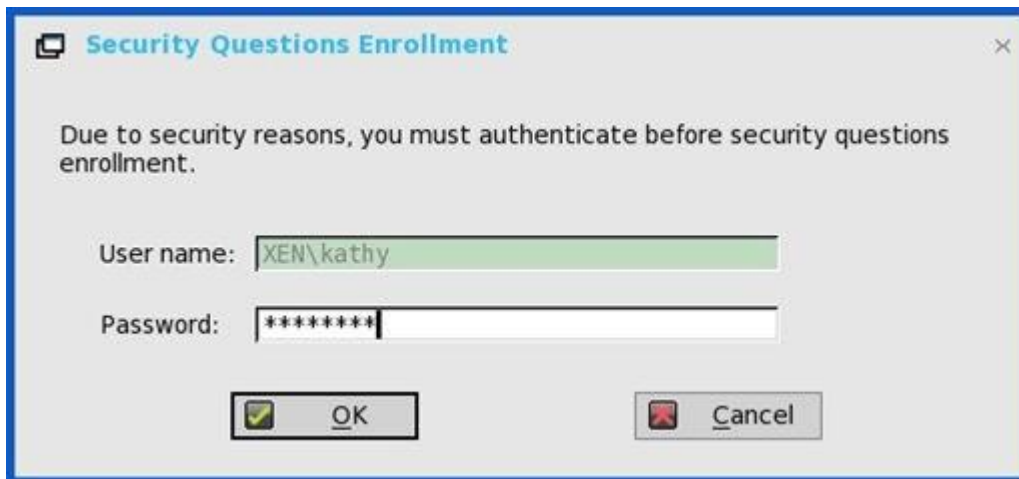
этом включает сервис Legacy Account Self-Service(Самообслуживание устаревших учетных записей).

3. Система секретных вопросов не поддерживает режим VDI.

Действия до сброса пароля или разблокировки учетной записи

До сброса пароля или разблокировки учетной записи Вы должны зарегистрировать свои секретные вопросы. Для этого выполните следующие действия:

1. В PNMenu щелкните **Manage Security Questions** (Управление секретными вопросами) (только классический рабочий стол и StoreFront). Появится окно **Security Questions Enrollment** (Регистрация секретных вопросов).



Security Questions Enrollment

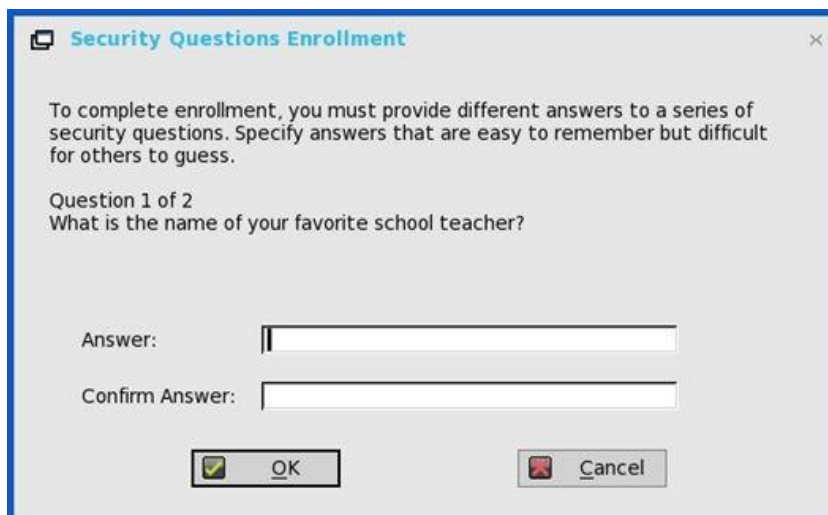
Due to security reasons, you must authenticate before security questions enrollment.

User name: XEN\kathy

Password: *****

OK

2. Введите свои ответы на вопросы.



Security Questions Enrollment

To complete enrollment, you must provide different answers to a series of security questions. Specify answers that are easy to remember but difficult for others to guess.

Question 1 of 2
What is the name of your favorite school teacher?

Answer:

Confirm Answer:

OK

- Для регистрации секретных вопросов нажмите на кнопку **OK**.

Работа с функцией самообслуживания учетной записи

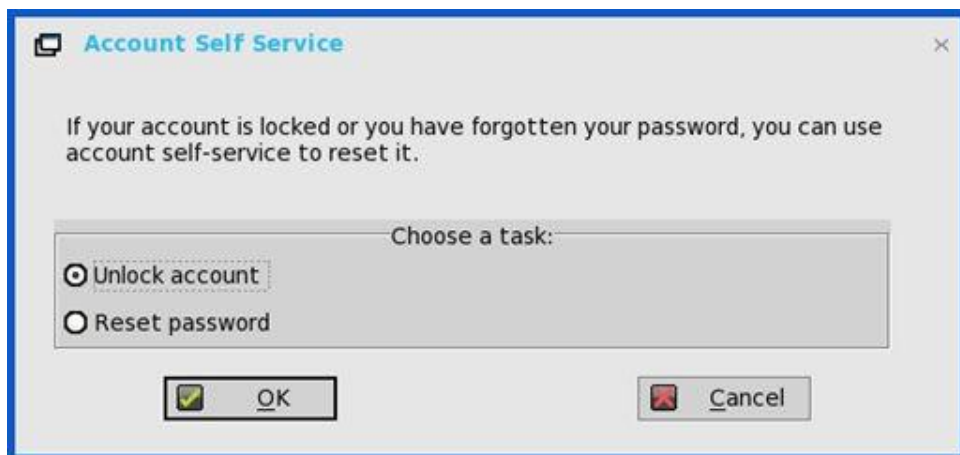
После того как ответы на секретные вопросы будут зарегистрированы, при подключении ThinOS к серверу StoreFront с разрешенной функцией самостоятельного сброса пароля в окне входа в систему будет отображаться значок **Account Self-Service** (Самообслуживание учетной записи).

ПРИМЕЧАНИЕ: если Вы введете неправильный пароль в окне входа в систему больше четырех раз, клиент автоматически запускает процесс разблокировки учетной записи.

- Щелкните значок **Account Self-Service** (Самообслуживание учетной записи), чтобы разблокировать учетную запись или сбросить пароль.

ПРИМЕЧАНИЕ: для использования функции разблокировки учетной записи или сброса пароля вам следует предварительно зарегистрировать секретные вопросы для пользователей.

- Установите переключатель **Unlock account** (Разблокировать учетную запись) или **Reset password** (Сбросить пароль) в зависимости от того, что Вам требуется, и затем нажмите на кнопку **OK**.

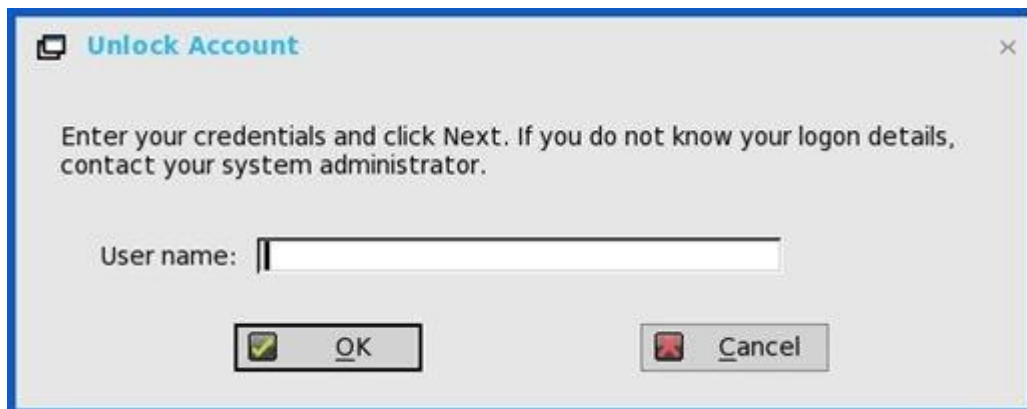


Разблокировка учетной записи

Если Вы зарегистрировали секретные вопросы, для разблокировки учетной записи выполните следующие действия:

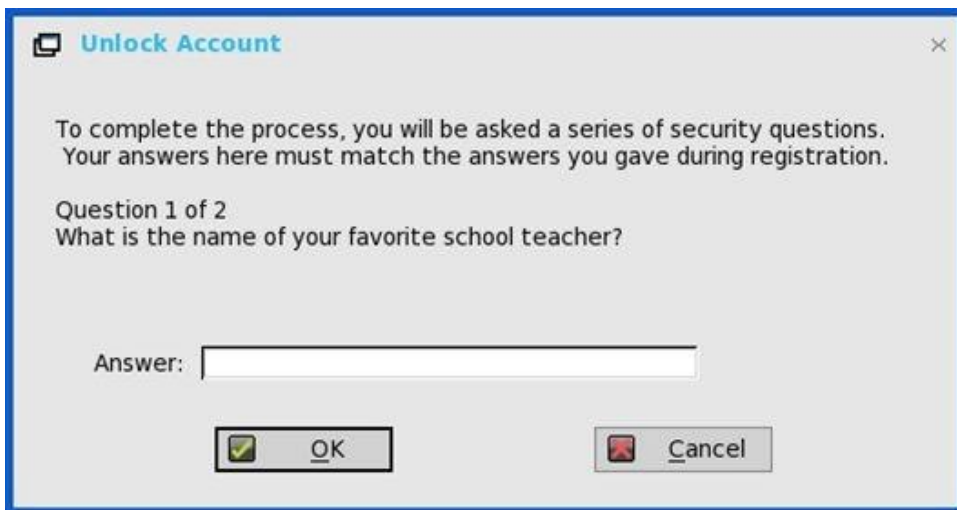
1. Выберите переключатель **Unlock account** (Разблокировать учетную запись) в окне **Account Self-Service** (Самообслуживание учетной записи).
2. Введите имя пользователя.

Появится диалоговое окно **Unlock Account** (Разблокировка учетной записи).

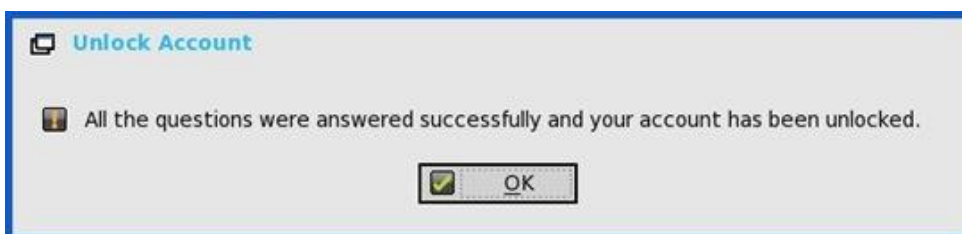


3. Введите зарегистрированные ответы на секретные вопросы.

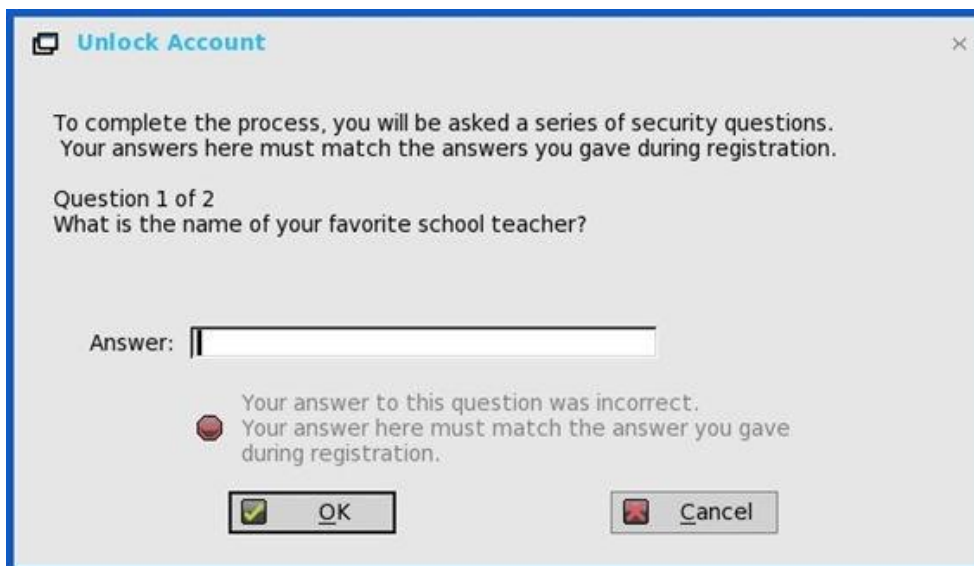
Если ваши ответы совпадают с зарегистрированными, появится диалоговое окно **Unlock Account** (Разблокировка учетной записи).



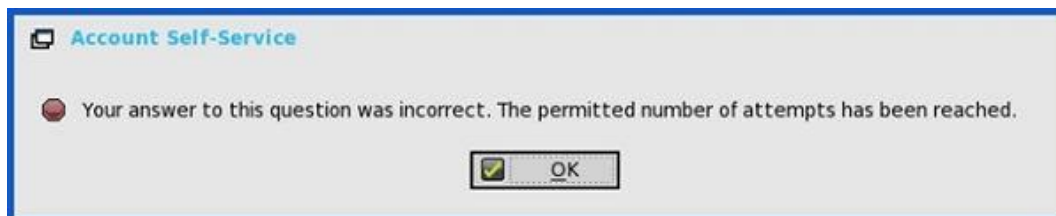
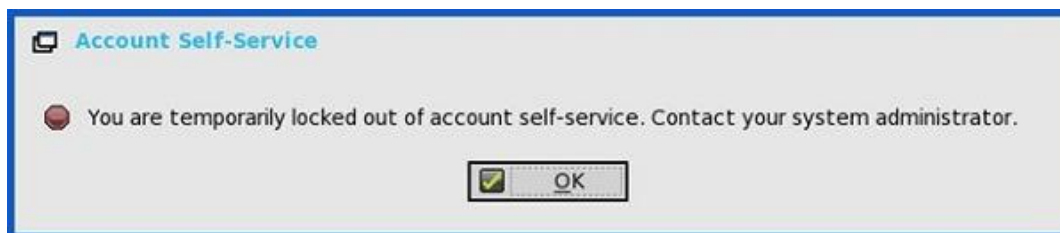
4. Нажмите на кнопку **OK**. Ваша учетная запись разблокирована.



Если приведенные ответы неправильны, появляется следующее сообщение об ошибке:



Если Вы дали неправильные ответы больше трех раз, Вы больше не можете разблокировать свою учетную запись или сбросить пароль. При этом появляются следующие сообщения об ошибках:

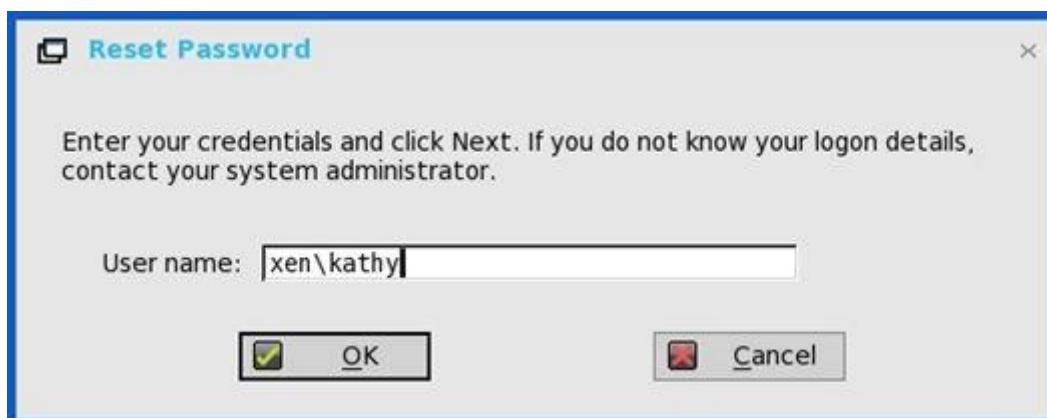


Сброс пароля

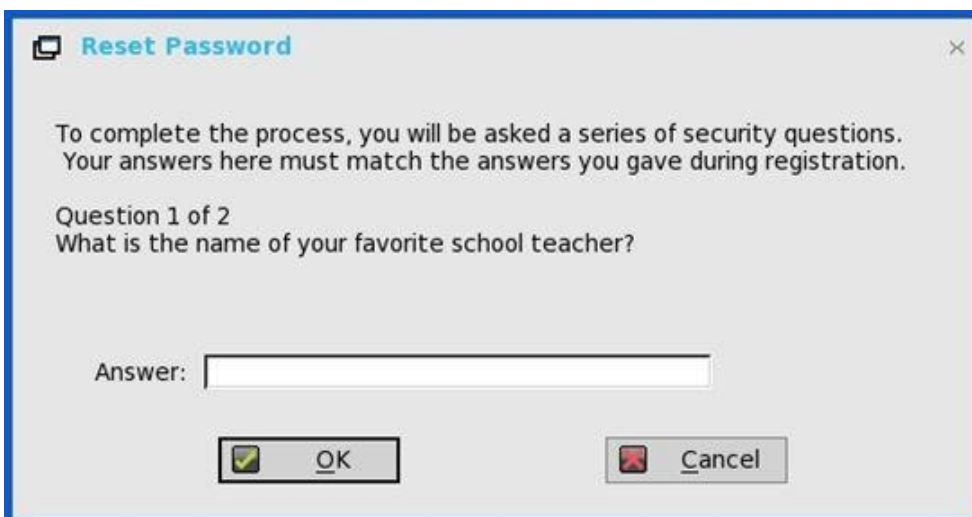
Если Вы зарегистрировали секретные вопросы, для сброса пароля выполните следующие действия:

1. Выберите переключатель **Reset password** (Сбросить пароль) в окне **Account Self-Service** (Самообслуживание учетной записи).
2. Введите имя пользователя.

Появится диалоговое окно **Reset Password** (Сброс пароля).



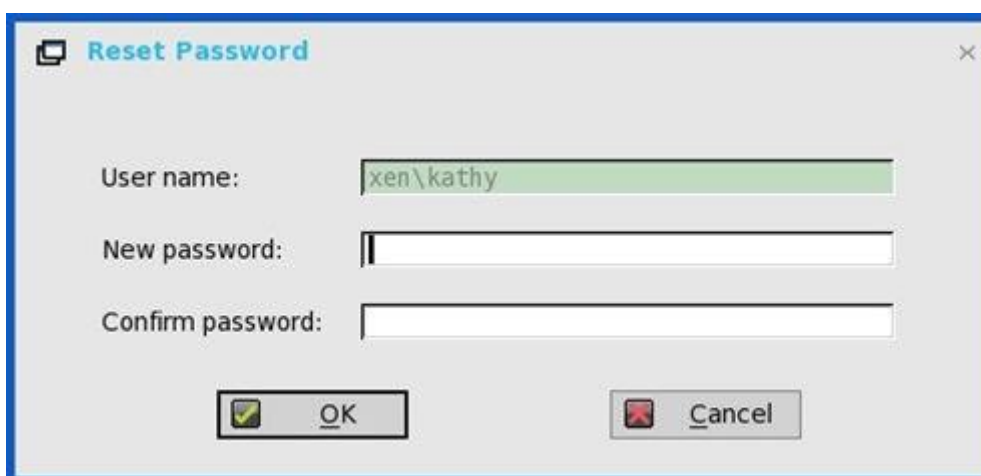
3. Введите зарегистрированные ответы на секретные вопросы.



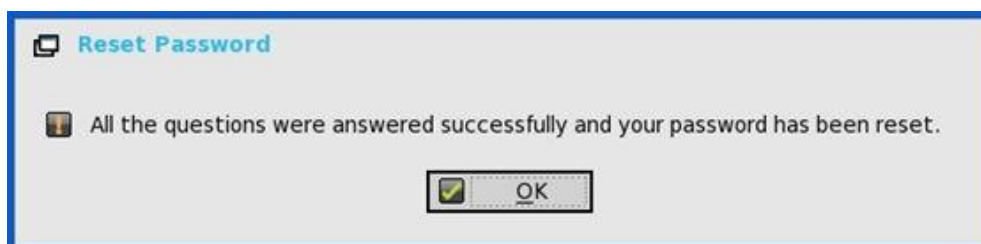


Если Ваши ответы совпадают с зарегистрированными, появится следующее диалоговое окно **Reset Password** (Сброс пароля).

4. Введите и подтвердите новый пароль.



5. Нажмите на кнопку **OK**. Пароль успешно сброшен.



Если Вы дали неправильные ответы, Вы больше не можете сбросить пароль. При этом появляется сообщение об ошибке.

ПЕРЕНАПРАВЛЕНИЕ URL ДЛЯ QUMU ИЛИ ICA MULTIMEDIA

QUMU использует функцию ICA Multimedia URL Redirection. Для пользования этой функцией Вам необходимо установить соответствующий плагин для браузера.

В более ранних версиях ThinOS поддержка ICA Multimedia URL Redirection была реализована частично. Начиная с выпуска ThinOS 8.4, в реализацию этой функции внесен ряд улучшений для повышения производительности.

Поддерживаемые протоколы:

- RTPS HLS;
- HTTP.

Проверка работы функции QUMU Multimedia URL Redirection: во время воспроизведения видео попытайтесь подвигать окно браузера по экрану или прокрутить его. Если Вы заметите существенный рывок картинки или задержку воспроизведения, это означает, что осуществляется перенаправление видео.

ПЕРЕНАПРАВЛЕНИЕ ВИДЕО HTML5

Функция HTML5 Video Redirection контролирует и оптимизирует способ, которым серверы XenApp и XenDesktop осуществляют доставку мультимедийного веб-контента HTML5 пользователям. В XenApp и XenDesktop 7.12 эта функция доступна только для внутренних веб-страниц. Для ее реализации требуется добавить JavaScript на веб-страницы, на которых имеется мультимедиа-контент HTML5, например видео на внутреннем обучающем сайте.

Следует разрешить следующие серверные политики:

- Windows Media Redirection – разрешена по умолчанию;
- HTML5 Media Redirection – запрещена по умолчанию.

Проверка работы HTML5 Video Redirection

Во время воспроизведения видео попытайтесь подвигать окно браузера по экрану или прокрутить его. Если Вы заметите существенный рывок картинки или задержку воспроизведения, это означает, что осуществляется перенаправление видео.

Также отображается журнал событий ThinOS для RAVE MMR.

Иногда первоначальное проигрывание не работает. Через несколько секунд видео автоматически обновляется, и Вам требуется снова щелкнуть, чтобы начать воспроизведение сначала. За этот промежуток времени и осуществляется перенаправление видео.

ICA SUPERCODEC

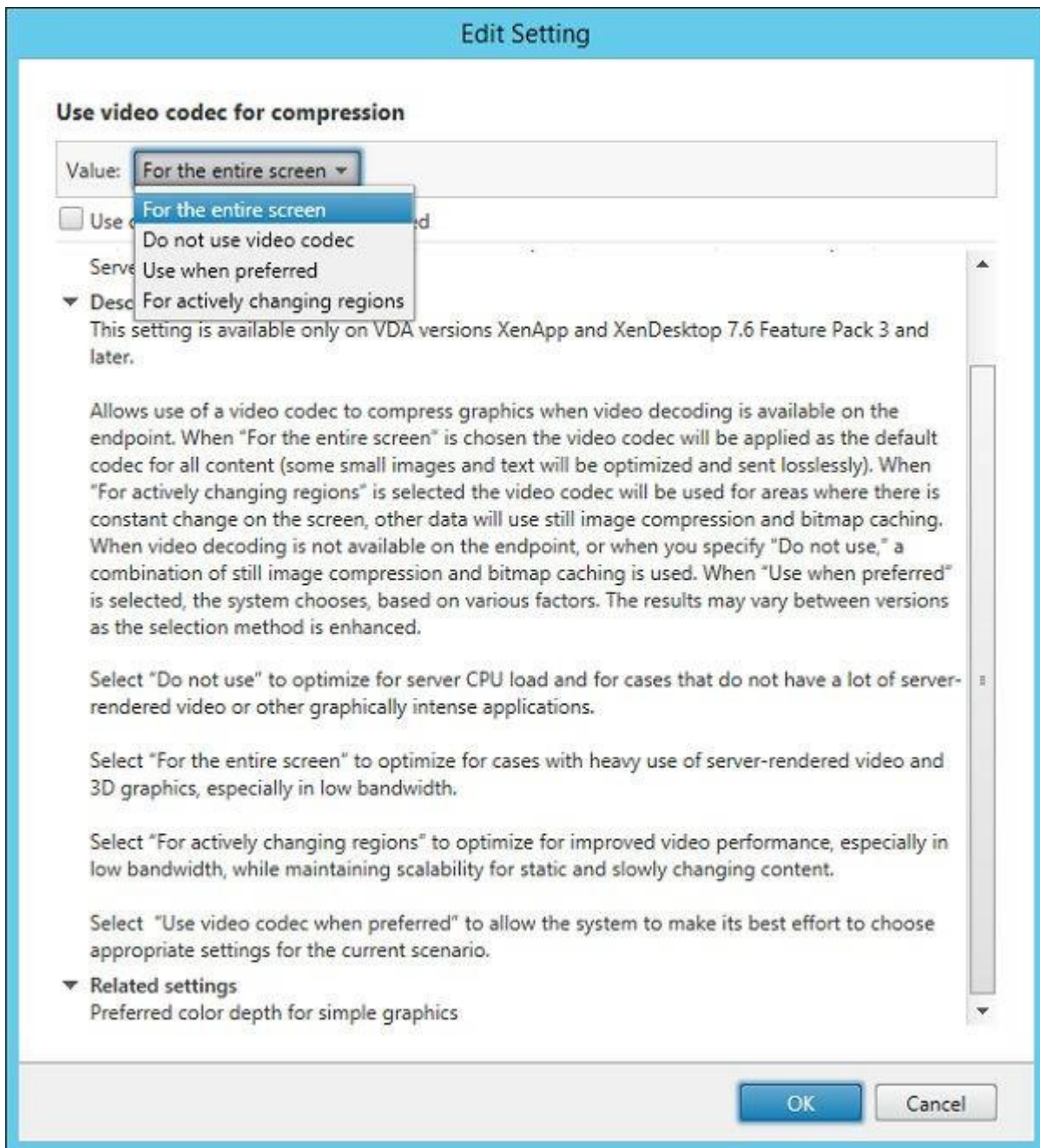
ICA SuperCodec – это декодер H.264, встроенный в ICA-клиент ThinOS. Сервер кодирует образ сеанса в поток H.264 и в таком виде отправляет клиенту. Клиент декодирует поток H.264 с помощью SuperCodec и отображает на экране. Эта функция улучшает комфорт пользователя, особенно на рабочих столах HDX 3D Pro.

Поддерживаемая среда

Citrix Virtual Apps and Desktops (ранее XenDesktop) и Citrix Virtual Apps (ранее XenApp) версии 7.5 и более старших.

Необходимые условия

В Citrix Virtual Apps and Desktops (ранее XenDesktop) и Citrix Virtual Apps (ранее XenApp) версии 7.9 и старше для политики **Use video codec for compression** (Использовать видеокодек для сжатия) по умолчанию установлено значение **Use when preferred** (Использовать при предпочтении). Для лучшего быстродействия устройств ThinOS рекомендуется настроить для политики **Use video codec for compression** (Использовать видеокодек для сжатия) значение **For the entire screen** (Для всего экрана). В качестве альтернативы Вы можете выбрать значение **Do not use video codec** (Не использовать видеокодек). В этом случае ThinOS сможет использовать **ThinWire Plus**, что сэкономит полосу пропускания и снизит нагрузку на процессор.



- **ThinWire Plus:** эквивалент значения **Do not use video codec** (Не использовать видеокодек);
- **Fullscreen H.264:** эквивалент значения **For the entire screen** (Для всего экрана);
- **Selective H.264:** эквивалент значения **For actively changing regions** (Для активно изменяемых участков).

Проверка состояния для подключений ICA

- **для тонких клиентов СИЛА РС4-1210:** по умолчанию ICA SuperCodec используется, если разрешение экрана ThinOS не превосходит 1920 x 1200. Если разрешение выше 1920 x 1200, в журнале событий ThinOS появляется следующее:

System resolution exceeds hardware limitation (1920 x 1200), disable SuperCodec

- **для тонких клиентов СИЛА PC4-1242, PC4-1221:** ICA SuperCodec используется всегда и без ограничений. В журнале событий ThinOS появляется следующее:

```
ICA: SuperCodec enabled
```

ПРИМЕЧАНИЕ: для подключений ICA параметра INI отсутствует.

Если в политике **Use video codec for compression** (Использовать видеокодек для сжатия) установлено значение **Do not use video codec** (Не использовать видеокодек), то ICA SuperCodec отключается и ThinOS ничего не пишет о нем в журнале.

АНОНИМНЫЙ ВХОД В СИСТЕМУ

Функция анонимного входа в систему позволяет пользователям входить на сервер StoreFront, настроенный на хранение без аутентификации, не предъявляя своих учетных данных Active Directory (AD). Таким образом, пользователи могут обращаться к приложениям без аутентификации.

ПРИМЕЧАНИЕ: анонимный вход в систему не поддерживается в legacy-режиме сервера StoreFront.

FLASH REDIRECTION

Решение Flash Redirection предназначено для выгрузки flash-контента на тонкий клиент с последующим локальным рендерингом и декодированием. Выгрузку осуществляет функция Citrix HDX Flash Redirection. Локальный процесс рендеринга и декодирования осуществляется кастомизированным flash-проигрывателем и другими процессами мультимедиа, выполняемыми локально в ThinOS.

Поддерживаемая среда: поддерживаются только подключения Citrix с XenApp 6.5 и более поздних версий или XenDesktop 7.0 и новее.

Поддерживаемые платформы:

- СИЛА PC4-1263 под управлением ThinOS;
- СИЛА PC4-1263 с PCoIP;
- СИЛА PC4-1210 под управлением ThinOS;
- СИЛА PC4-1210 с PCoIP;
- СИЛА PC4-1240 под управлением ThinOS (D10D);
- СИЛА PC4-1240 с PCoIP (D10DP);
- СИЛА МК2-1240 AIO(5212);
- СИЛА МК2-1240 AIO с PCoIP(5213);
- СИЛА PC4-1242 под управлением ThinOS;
- СИЛА PC4-1242 с PCoIP;
- СИЛА PC4-1243 под управлением ThinOS (Z10D).

Необходимые пакеты

Для работы этой функции пользователь должен установить пакет FR.i386.pkg.

Установка пакетов

Для установки необходимых пакетов выполните следующие действия:

1. Загрузите пакеты в каталог `\wnos\pkg\`.
2. Убедитесь, что параметр автозагрузки в INI не установлен в 0. Задайте значения `AutoLoad=1` `AddPkg=FR` в файле `wnos.ini`.
3. Перезапустите клиент, чтобы он считал данные с файлового сервера, и ждите завершения автоматической установки пакетов. Просмотреть установленные пакеты Вы можете на вкладке **Packages** (Пакеты) диалогового окна **System Tools** (Системные инструменты).

4. Конфигурация сервера для функции Flash Redirection:

Чтобы игнорировать различия версий flash-проигрывателей, пользователю следует добавить на рабочий стол ключи реестра `FlashPlayerVersionComparisonMask` и `ClientFlashPlayerVersionMinimum`.

В Citrix Virtual Apps 6.5 для игнорирования различий в версиях браузера IE необходим ключ реестра `IEBrowserMaximumMajorVersion`.

Начиная с Citrix Virtual Apps and Desktops 7.9, требуется добавлять новые ключи в реестр для работы HDX FR. Для получения сведений об этих дополнительных ключах см. техническую документацию Citrix.

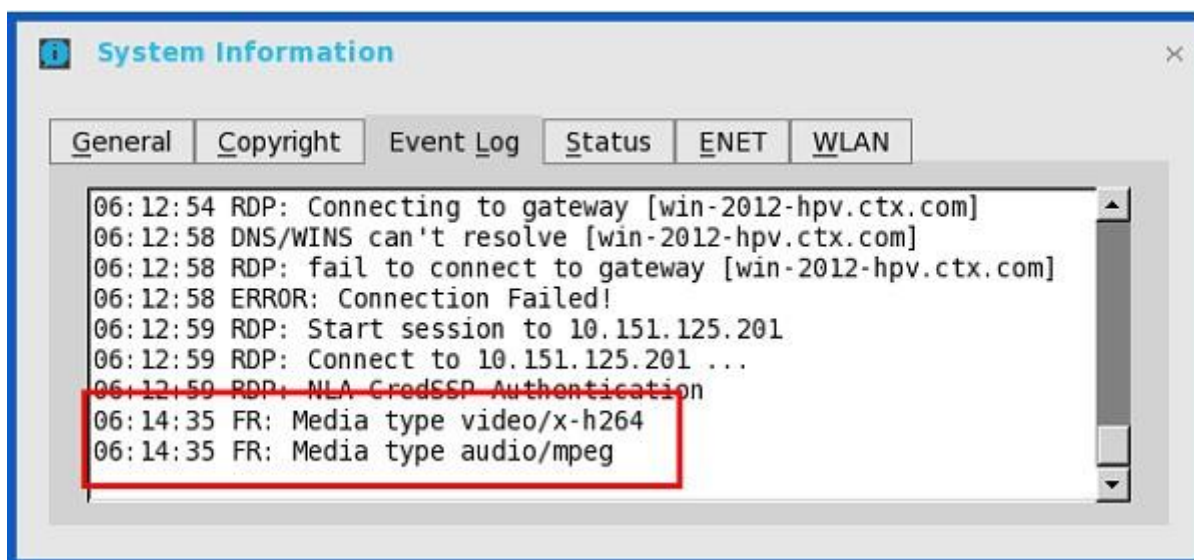
5. Конфигурация клиента для функции Flash Redirection:

По умолчанию на клиенте не требуется никакой настройки. Для поддержки клиентских конфигураций HDX FR добавлены новые параметры INI (например, для загрузки контента с сервера). Это следующие параметры:

```
SessionConfig=ICA\
HDXFlashUseFlashRemoting=Never | Always (default) \
HDXFlashEnableServerSideContentFetching=Disabled (default) | Enabled \
```

Как проверить, работает функция или нет

- Щелкните правой кнопкой по flash-видео, чтобы узнать версию проигрывателя. Отображается информация о версии специализированного проигрывателя для клиентской стороны ThinOS. Это версия 11.1.102.59. Если указана другая версия flash-проигрывателя, значит, настройка не удалась и проводится рендеринг на сервере.
- Во время воспроизведения flash-видео в диалоговом окне **System Information** (Системная информация) должны выдаваться записи журнала событий для HDX FR:
 - FR: Media type video/x-264;
 - FR: Media type audio/mpeg.



Для получения сведений о базовых операциях и настройке политик для функции Citrix HDX Flash Redirection см. документацию Citrix.

Известные проблемы

1. Проигрывание flash-видео в браузере Internet Explorer осуществляется с обычными параметрами безопасности.
2. Проигрывание осуществляется для видео $\leq 720p$; видео 1080p может выдавать ошибки графики.
3. Проигрывание полноэкранный видео с разрешением $\leq 1920 \times 1200$ может выдавать ошибки графики.
4. После загрузки flash-видео сохраняется первоначальный размер видеоконтента. Например, изменение размеров браузера не влияет на размер видеоконтента.
5. Поддерживаются только английские шрифты. В частности, субтитры на других языках могут отображаться некорректно.
6. Возможны проблемы при воспроизведении видео с YouTube.com. Например, для воспроизведения видео необходимо скопировать его URL и вставить его в браузер.

Ограничения: не поддерживаются URL, содержащие нелатинские символы.

НАСТРОЙКА VMWARE

Виртуализация VMware позволяет запускать несколько виртуальных машин на одной физической машине. VMware Horizon Client — это локально установленное приложение, которое обеспечивает связь между View Connection Server и ОС тонкого клиента. Он обеспечивает доступ к централизованно размещенным виртуальным рабочим столам с ваших тонких клиентов.

В каждом выпуске ThinOS версия Horizon Client может быть обновлена до более новой версии.

ПРИМЕЧАНИЕ: если Вы обновляете тонкий клиент до последней версии ThinOS, необходимо убедиться, что сервер Horizon или версия агента обновляется для поддержки последней версии клиента Horizon.

В этом разделе содержится информация о том, как настроить подключение к брокеру VMware на Вашем устройстве.

НАСТРОЙКА СВЯЗИ С БРОКЕРОМ VMWARE

Для настройки брокера VMware выполните следующие действия:

1. Из меню рабочего стола выберите **System Setup**(Настройка системы), а затем нажмите **Remote Connections** (Удаленное подключение). Отобразится окно **Remote Connections** (Удаленные подключения).
2. Во вкладке **Настройка брокера** (Broker Setup) из выпадающего списка выберите **Vmware View** и сделайте следующее:
 - **Сервер брокера** (Broker Server): введите IP-адрес/Имя хоста/FQDN сервера брокера;
 - **Список автоматического подключения** (Auto Connect List): введите названия рабочих столов, которые Вы хотите запустить автоматически после подключения к соответствующему брокеру. Можно ввести несколько настольных компьютеров. Каждое имя рабочего стола разделено запятой и чувствительно к этому случаю;
 - **Режим безопасности** (Security mode): выберите предпочтительный режим безопасности из следующих вариантов:
 - **Предупреждение** (Warning): предупреждать, о неверном FQDN или самоподписанном сертификате или без сертификата, но соответствующее предупреждение после отображения предлагает пользователю установить подключение;
 - **Полный** (Full): требуется действительный сертификат с корректным FQDN;
 - **Низкий** (Low): разрешает любые FQDN, IP адреса, сертификаты или отсутствие сертификата;

- **По умолчанию:** следует настройкам глобального режима безопасности.
- **Протокол подключения** (Connection Protocol): из выпадающего списка выберите протокол соединения. По умолчанию опция установлена на **Server Default**.

ПРИМЕЧАНИЕ: протокол подключения только PCoIP применим только к клиентам PCoIP. Если Вы не установите пакет Horizon, то опция протокола Blast недоступна для выбора. Протокол PCoIP необходим для сеанса PCoIP. Пакет Horizon необходим для сеанса Blast.

Доступные варианты:

- **Server default** (Умолчания сервера): выберите это соединение протокола, чтобы отобразить рабочий стол с протоколом по умолчанию, настроенным в консоли администратора VMware View, для каждого пула в брокере. Если пул рабочих столов настроен с протоколом по умолчанию как RDP в консоли администратора **View**, то только соединение RDP рабочего стола отображается в ThinOS после входа пользователей в устройство;
- **All Supported** (Все поддерживаемые): выберите это соединение протокола, чтобы отобразить рабочий стол во всех доступных соединениях, если пул рабочих столов настроен так, чтобы пользователи могли выбрать протокол;
- **RDP only** (Только RDP): выберите это подключение по протоколу, чтобы рабочий стол отображался только в режиме подключения по протоколу RDP.
- **PCoIP only** (Только PCoIP): параметр доступен только для клиентов с поддержкой PCoIP. Выберите подключение по данному протоколу, чтобы отображать только рабочий стол при подключении по протоколу PCoIP для каждого пула в посреднике. Если для пула рабочего стола протоколом по умолчанию является RDP в консоли View Admin и пользователю запрещено выбирать протокол, то этот рабочий стол не отображается в ThinOS после входа пользователя в устройство.
- **Blast only** (Только Blast): протокол VMware Blast может использоваться для удаленных приложений и удаленных рабочих столов, использующих виртуальные машины или рабочие столы с общим сеансом на узле RDS. Выберите это соединение протокола, чтобы отобразить рабочий стол с протоколом Blast;
- **Blast and RDP** (Blast и RDP): параметр доступен как на клиентах с поддержкой PCoIP, так и на клиентах без PCoIP. Выберите этот протокол связи для отображения рабочего стола через Blast или RDP;
- **Blast and PCoIP** (Blast и PCoIP): параметр доступен только для клиентов с поддержкой PCoIP. Выберите этот протокол для отображения рабочего стола через Blast или PCoIP;
- **PCoIP and RDP** (PCoIP и RDP): параметр доступен только для клиентов с поддержкой PCoIP. Выберите этот протокол для отображения рабочего стола через RDP или PCoIP.
- **Анонимный вход с использованием неавторизованного доступа** (Log in anonymously using Unauthenticated Access): установите этот флажок, чтобы выполнить анонимный вход в сеанс VMware с удаленным подключением приложений.

3. Нажмите **ОК**, чтобы сохранить настройки.

Ограничения

1. ThinOS поддерживает четыре дисплея с разрешением 4K в сеансе Horizon blast. Если производительность тонкого клиента низкая, не рекомендуется использовать четыре дисплея с разрешением 4K.
2. Вертикальная синхронизация не работает в сеансе Blast с четырьмя дисплеями с разрешением 4K.

3. Низкая производительность видео при воспроизведении видео в сеансе Blast с разрешением 4K.
4. ThinOS поддерживает перенаправление USB аудиоустройства. Однако не рекомендуется использовать аудиоустройство USB direction из-за низкого качества звука.
5. Функция копирования и вставки текста между локальным сеансом и сеансом Blast работает только после выполнения переключения сеанса.

ИСПОЛЬЗОВАНИЕ БРОКЕРА И РАБОЧЕГО СТОЛА VMWARE HORIZON VIEW

VMware Horizon View Broker timeout (Тайм-аут брокера VMware Horizon View): тайм-аут брокера VMware Horizon View больше не заставляет пользователя выходить из брокера, когда включен безопасный туннель.

В более ранней версии ThinOS, когда время ожидания брокера истекает, сеанс пользователя отключается, и пользователь выходит из брокера. Начиная с выпуска ThinOS 8.2, ThinOS отключает сеанс пользователя от брокера, но не заставляет пользователя выходить из системы. Это связано с тем, что у пользователя есть локальные соединения, отличные от рабочего стола брокера, и эти соединения остаются активны при достижении тайм-аута брокера.

PCoIP session NUM/CAP keyboard status synchronizes with session instead of thin client (Статус клавиатуры NUM/CAP синхронизируется с сессией PCoIP вместо сессии на тонком клиенте): это применимо только для запуска сеанса. Состояние клавиатуры сеанса PCoIP num/CAP синхронизируется от удаленного сеанса к клиенту, в то время как RDP/ICA синхронизирует состояние от локального к удаленному сеансу.

Пример:

1. Установите `NUM LOCK = off` в текущем сеансе PCoIP.
2. Отсоедините сеанс.
3. Установите на клиентской клавиатуре `NUM LOCK = on`
4. Повторно подключитесь к сеансу PCoIP.
5. Состояние NUM LOCK клавиатуры в сеансе и клиенте обновляется до `NUM LOCK = off`.

RDS desktop through PCoIP/Blast (RDS через PCoIP/Blast): Вы можете просматривать и подключаться к рабочему столу службы удаленных рабочих столов (RDS) через протокол PCoIP / Blast в брокере, используя PCoIP / Blast для клиентов ThinOS. В VMware Horizon View 6.0 и более поздних версиях рабочий стол RDS имеет подключения RDP, PCoIP или Blast на основе конфигурации сервера.

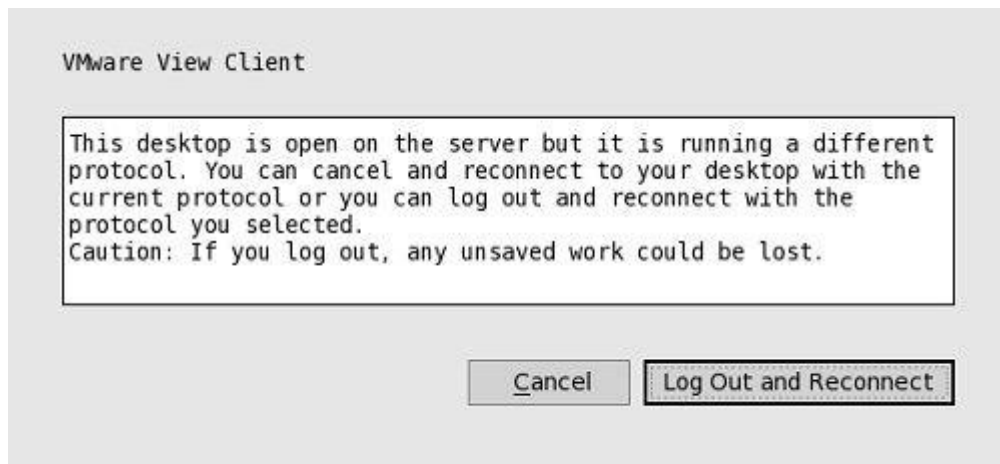
ПРИМЕЧАНИЕ: приложение Horizon поддерживается на PCoIP и Blast, RDP не поддерживается.

В этом выпуске выводится сообщение о переключения протокола рабочего стола RDS. Типичный пользовательский сценарий:

1. Подключайтесь к рабочему столу RDS через протокол. Например, RDP.
2. Отключение от рабочего стола.
3. Подключитесь к тому же рабочему столу RDS через другой протокол. Например, PCoIP.
4. Отобразится диалоговое окно.

Доступные варианты:

- **Cancel** (Отмена): Вы можете закончить подключение PCoIP и подключиться к рабочему столу в RDP снова;
- **Log Out and Reconnect** (Войти в систему и восстановить соединение): Вы можете подключиться к рабочему столу через PCoIP, и ранее открытый сеанс RDP будет завершен.



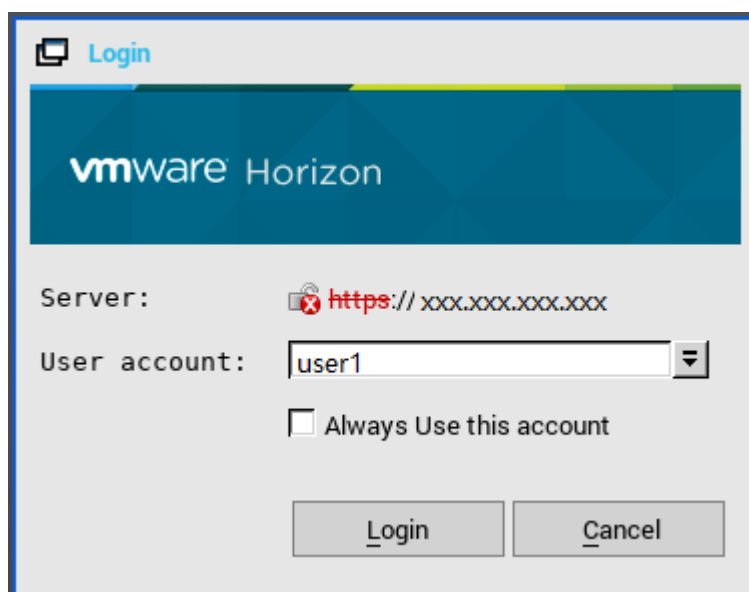
USB redirection RDS desktop through PCoIP/Blast (Перенаправление USB).

USB audio redirection (Перенаправление USB аудио): перенаправление звука USB позволяет использовать аудиоустройства USB в удаленном сеансе. Однако не рекомендуется включать перенаправление звука USB из-за качества звука.

Using unauthenticated access (Использование несанкционированного доступа): Вы можете анонимно войти в сеанс VMware. Для использования анонимного доступа, выполните следующие действия:

1. На сервере AD создайте двух анонимных пользователей, например, anonymous1 и anonymous2.
2. Войдите на веб-портал View Admin.
3. Перейдите на вкладку **Users and Groups > Unauthenticated Access** и добавьте двух новых анонимных пользователей в View Connection Manager.
4. Перейдите на вкладку **View Configurations > Select Servers > Connection Servers** и выберите сервер соединений.
5. Нажмите **Edit > Authentication** и установите флажок **Enabled for unauthenticated access**. Не выбирайте пользователей для пользователя, не прошедшего проверку подлинности по умолчанию.
6. Перейдите в **Application Pools**, добавьте несколько приложений, установленных на виртуальной машине, и предоставьте права на приложения пользователю anonymous1 и anonymous2.
7. В диалоговом окне настроек брокера ThinOS для VMware View установите флажок **Log in anonymously** (Вход в систему анонимно) с использованием доступа без аутентификации.
8. Перезапустите тонкий клиент.

Откроется следующее диалоговое окно:



9. Установите флажок **Always use this account** (Всегда использовать эту учетную запись), чтобы использовать указанную учетную запись входа. Вы не можете изменить эту учетную запись для других пользователей.

Hide Server URL (Скрыть адрес сервера): URL-адрес сервера может быть скрыт в пользовательском интерфейсе брокера Horizon View. Этот параметр можно настроить любым из следующих способов:

9.1. Через веб-портал View Connection Server:

9.1.1. Войдите на веб-портал View Connection Server.

9.1.2. Перейдите к **View Configuration > Global Settings > Edit**, установите флажок **Hide server information in client user interface**, и снимите флажок **Hide domain list in client user interface**.

9.1.3. Нажмите **OK**.

9.1.4. Войдите в брокер VMware Horizon.

URL-адрес сервера скрыт и отображается список доменов.

9.2. Через параметры INI:

Используйте параметр INI `ConnectionBroker=vmware DisableShowServer=yes`.

Hide Domain List (Скрыть список доменов): список доменов можно скрыть в пользовательском интерфейсе входа в систему Horizon View Broker. Чтобы настроить этот параметр, выполните следующие действия:

1. Войдите на веб-портал View Connection Server.
2. Перейдите к **View Configuration > Global Settings > Edit**, установите флажок **Hide domain list in client user interface** и снимите флажок **Hide server information in client user interface**.
3. Нажмите **OK**.
4. Войдите в брокер VMware Horizon.
5. Список доменов скрыт и URL-адрес сервера отображается.

ПОДСТАНОВКА ИМЕНИ ПОЛЬЗОВАТЕЛЯ ДЛЯ ВХОДА С ИСПОЛЬЗОВАНИЕМ СМАРТ-КАРТЫ

Можно позволить пользователям указать учетную запись, которая будет использоваться в поле **Username hint** для подстановки имени пользователя, когда пользователь входит в сеанс Horizon View с помощью смарт-карты. Включение этой опции позволяет использовать один сертификат смарт-карты для проверки подлинности нескольким учетным записям пользователей.

Для включения подстановки имени пользователя сделайте следующее:

1. Войдите в консоль администратора **View Administrator** и выберите **View Configuration > Servers** (Просмотр конфигурации > Серверы).
2. На вкладке **Connection Servers** (Серверы подключения) выберите экземпляр сервера подключения View и нажмите кнопку **Edit** (Редактировать). Отобразится страница настроек.
3. Нажмите на вкладку **Authentication** (Проверка подлинности).
4. В разделе **View Authentication** (Проверка подлинности) установите флажок **Allow smart card user hints** (Разрешить подстановку пользователя смарт-карт).
Вы не можете настроить функцию подстановки имени пользователя смарт-карты при установке проверки подлинности смарт-карты на недопустимую (Not Allowed).
5. Нажмите **OK**.

В клиенте ThinOS войдите в сеанс Horizon View с помощью смарт-карты. В окне входа брокера VMware Horizon View введите имя пользователя и PIN-код карты для проверки подлинности пользователя.

ПРИМЕЧАНИЕ: если имя пользователя не совпадает с именем пользователя сертификата смарт-карты, появится сообщение об ошибке «No user could be found for your Certificate».

ПОДДЕРЖКА ПЕРЕДАЧИ АУДИО-ВИДЕО В РЕАЛЬНОМ ВРЕМЕНИ В VMWARE

Используйте функцию аудио-видео в режиме реального времени для запуска Skype и других приложений онлайн-конференций на удаленном рабочем столе. С помощью этой функции аудио и видео-устройства, подключенные к тонкому клиенту, можно использовать для VoIP на удаленном рабочем столе.

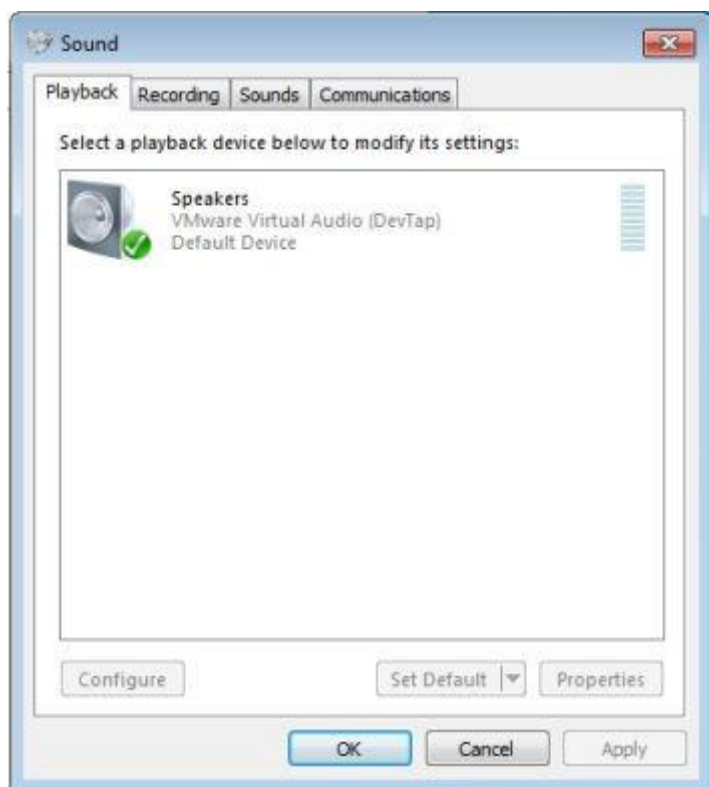
ПРИМЕЧАНИЕ: никаких дополнительных настроек ThinOS не требуется. Для видео RTAV требуется пакет RTME установленный на Вашем устройстве.

Для проверки аудио-видео VMware в режиме реального времени сделайте следующее:

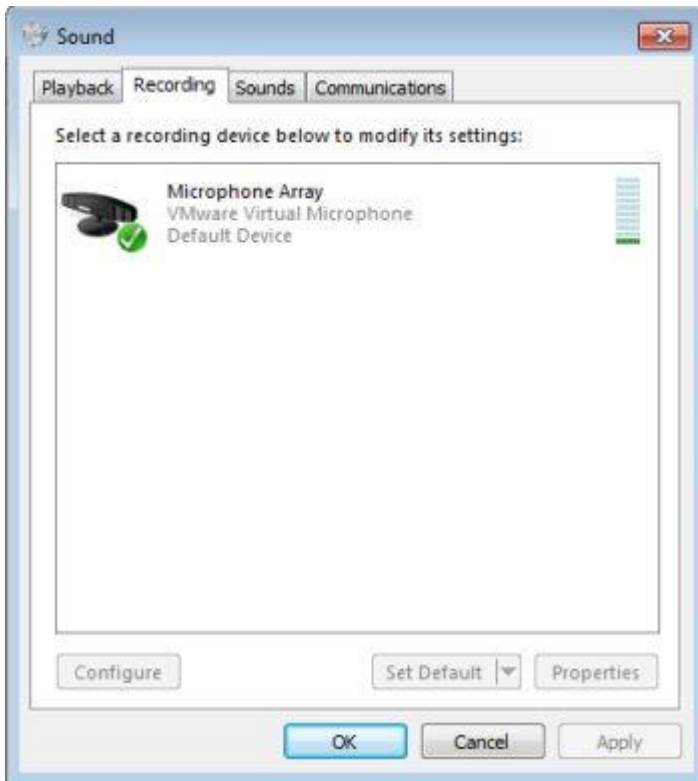
1. Подключитесь к рабочему столу VMware PCoIP или Blast с аудио и/или видео устройствами.

ПРИМЕЧАНИЕ: перенаправление USB должно быть отключено для аудио-видеоустройств.

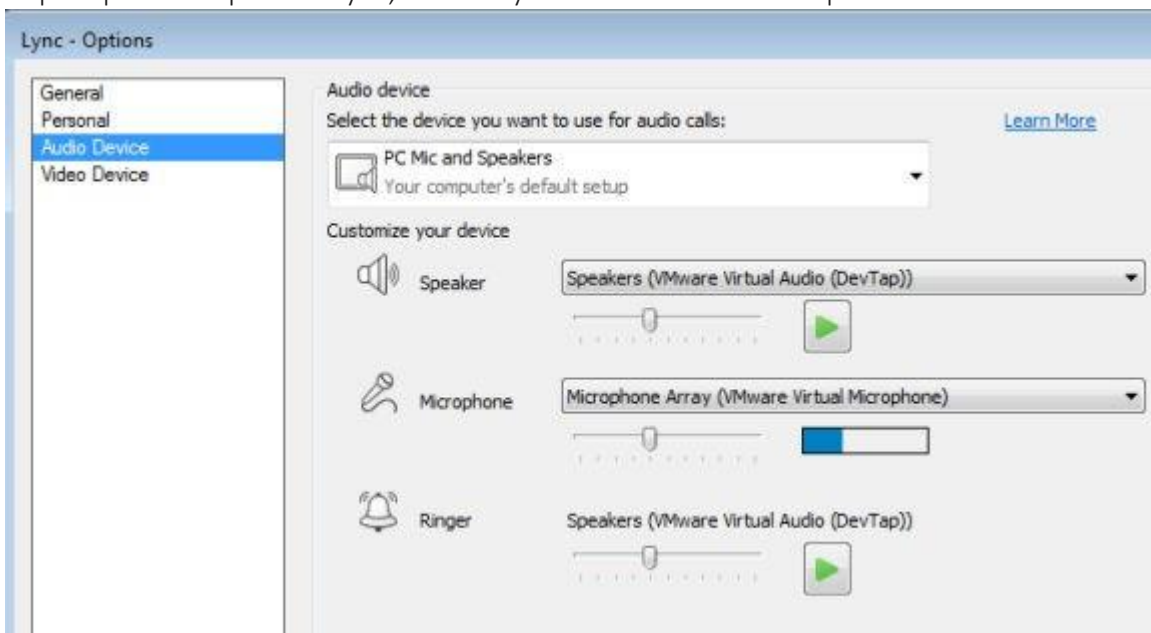
Убедитесь, что звук воспроизводится через устройство VMware virtual audio.



- Убедитесь, что звук записывается через устройство VMware virtual audio.

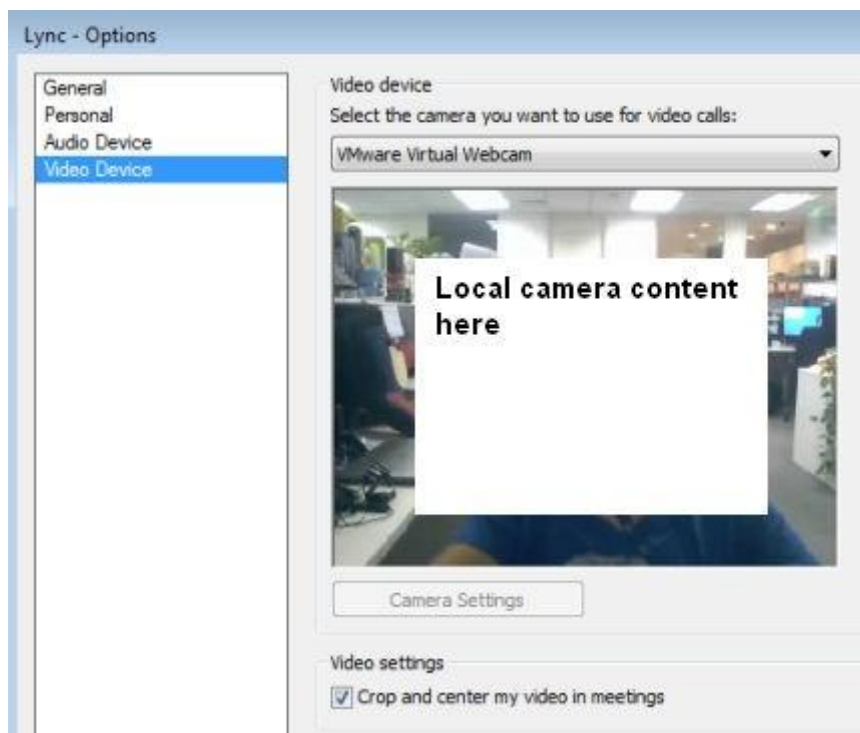


- Проверьте настройки звука, используя VMware virtual microphone.



- Проверьте настройки звука в приложении VoIP.

5. Убедитесь, что в Вашем приложении используется видеоустройство VMware virtual webcam.



6. Выполните ауди-видео звонок.

Зависимости и известные проблемы

- зависимость: RTME.i386.pkg должен быть установлен;
- кнопка ответа на вызов на локальном устройстве не поддерживается в RTAV;
- RTAV не поддерживает RDS, например, 2008 R2/ 2012 R2;
- поддерживается только протоколами PCoIP и Blast. RDP не поддерживается;
- настройки web-камеры не поддерживаются;
- передача HD видео с web-камеры не поддерживается.

VMWARE HORIZON VIRTUALIZATION PACK ДЛЯ SKYPE ДЛЯ БИЗНЕСА

Пакет виртуализации VMware Horizon для Skype для бизнеса позволяет использовать Skype для бизнеса на рабочем столе VMware Horizon. Microsoft Skype for Business: это единая коммуникационная платформа, обеспечивающая функции онлайн-сообщений, аудио, видеозвонков и другие.

ThinOS поддерживает VMware Horizon Virtualization Pack для Skype для бизнеса только в сеансе Blast. Протоколы PCoIP и RDP не поддерживают эту функцию.

Установка пакета Horizon на ThinOS

Вы должны установить пакет horizon.i386 на ThinOS, чтобы использовать протокол VMware Blast.

Для установки пакета горизонта:

1. Извлеките пакет horizon.
2. Загрузите horizon.i386.pkg на сервер в каталог \wnos\pkg\.
3. Убедитесь, что значение INI-параметра **Autoload** отличен от «0».
4. Перезапустите тонкий клиент и дождитесь завершения автоматической установки пакетов.

Настройка сеанса Skype для бизнеса в VMware Blast

В этом разделе описывается установка и использование Microsoft Skype для бизнеса (SFB) на рабочем столе VMware Blast.

1. Войдите как администратор Horizon и запустите установку VMware Horizon Agent в виртуальном рабочем столе.
2. Во время инсталляции VMware Horizon Agent выберите опцию **VMware Horizon Virtualization Pack for Skype for Business** для установки VMware Horizon Virtualization Pack for SFB.

VMware Horizon Virtualization Pack for Skype for включает следующие компоненты:

- Horizon Media Proxy — устанавливается на виртуальном рабочем столе;
- Horizon Media Provider — устанавливается на клиенте.

3. Установите приложение Skype for Business на рабочем столе VMware Blast.
4. Обновите прошивки ThinOS и установите Horizon.i386.pkg на клиенте ThinOS.
5. На ThinOS подключитесь к рабочему столу VMware Blas и войдите в Skype for Business.

Для проверки установки VMware Horizon Virtualization Pack for Skype for на виртуальной машине проверьте наличие в реестре ключей:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Lync\VdiMediaProvider – GUID (REG_SZ)

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Lync\ VdiMediaProvider – GUID (REG_SZ)

ПРИМЕЧАНИЕ: чтобы проверить статистику вызовов Skype для бизнеса, щелкните правой кнопкой мыши значок пакета виртуализации в правом нижнем углу виртуального рабочего стола и выберите команду статистика вызовов.

Ограничения

- Horizon Client версии 4.8 и старше и Horizon Agent версии 7.5 и старше несовместимы с более ранними выпусками Client и Agent. Из-за этого ограничения при использовании Horizon Client 4.8 и Horizon Agent 7.5 со старыми выпусками клиента и агента вызовы Skype для бизнеса выполняются в резервном режиме и не оптимизируются.
- ThinOS использует бинарные файлы, предоставленные VMware. Дополнительные сведения об ограничениях Skype для бизнеса см. в документе Configuring Skype for Business на docs.vmware.com.

Известные проблемы

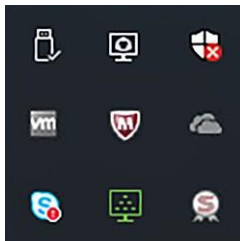
Таблица 18. Известные проблемы

Описание	Решение
Если разрешение сеанса Blast превышает 1920x1080 во время вызовов SFB с полным экраном, мышь перестает реагировать	Не используйте полный экран во время вызовов SFB в сеансе blast с разрешением больше или равным 2560 x 1440
После установки пакета JVDI при переключении устройства воспроизведения с HD audio на DP audio во время вызова Horizon SFB возникает ошибка Trap 14	Не загружайте пакет JVDI если Вы хотите использовать только пакет Horizon
Вы не можете использовать кнопки на гарнитуре для приема или завершения вызова	Эта функция не предусмотрена

Optimized mode (Оптимизированный режим) и Fallback mode (Резервный режим)

В оптимизированном режиме Skype для бизнеса обеспечивает оптимальную производительность. В резервном режиме вызовы Skype для бизнеса не оптимизируются. В правом нижнем углу виртуального рабочего стола всплывающая подсказка значка пакета виртуализации указывает на режим работы пакета виртуализации VMware Horizon для Skype для бизнеса.

На снимке экрана показан пакет виртуализации для Skype для бизнеса в оптимизированном режиме:



Если значок оптимизированного режима не отображается, пакет виртуализации работает в резервном режиме. Это происходит из-за несоответствия версий между клиентом Horizon на тонком клиенте и агентом Horizon на виртуальном рабочем столе.

Смена оптимизированного режима на резервный

Чтобы изменить оптимизированный режим на резервный или отключить пакет виртуализации для Skype для бизнеса на рабочем столе Horizon, выполните следующие действия:

1. На рабочем столе VMware Horizon откройте редактор реестра Windows.
2. Переименуйте ключи реестра на основе следующих сценариев развертывания:

Таблица 19. Ключи от реестра

Сценарий развертывания	Ключ реестра
View Desktops (64-bit) и Skype for Business (64-bit)	Переименуйте HKLM/Software/Microsoft/Office/Lync/VdiMediaProvider в HKLM/Software/Microsoft/Office/Lync/VdiMediaProviderDisabled.
View Desktops (64-bit) и Skype for Business (32-bit)	Переименуйте HKLM/Software/Wow6432Node/Microsoft/Office/Lync/VdiMediaProvider в HKLM/Software/Wow6432Node/Microsoft/Office/Lync/VdiMediaProviderDisabled.
View Desktops (32-bit) и Skype for Business (32-bit)	Переименуйте HKLM/Software/Microsoft/Office/Lync/VdiMediaProvider в HKLM/Software/Microsoft/Office/Lync/VdiMediaProviderDisabled.

3. Закройте редактор реестра Windows.
4. Перезапустите Skype для бизнеса.

Skype for Business настроен в режиме Fallback, аудио-видео в режиме реального времени (RTAV) используется для вызовов SFB.

ИСПОЛЬЗОВАНИЕ НЕСКОЛЬКИХ МОНИТОРОВ В СЕАНСЕ VMWARE BLAST

Этот раздел применим к тонкому клиенту CP4-1221. ThinOS поддерживает отображение нескольких мониторов для запуска виртуальных машин на каждом мониторе.

Необходимо обновить пакет VMware Blast до последней версии.

Сценарий использования:

1. Подключите несколько мониторов к устройству ThinOS.
2. В диалоговом окне **Display Setup** (Настройки дисплея) отключите **Mirror Mode** (Зеркальный режим) и настройте расположение мониторов.
3. Запустите полноэкранный режим сеанса VMware Horizon.
 - **Display numbers** (Количество дисплеев): виртуальная машина нуждается в достаточной производительности видеопамати для поддержки нескольких мониторов. Вы можете использовать до четырех мониторов при наличии достаточного количества оперативной памяти.

Таблица 21. Матрица расположения дисплеев.

Разрешение	1920 x 1080					2560 x 1440				
	2	3	4	5	6	2	3	4	5	6
Количество дисплеев	2	3	4	5	6	2	3	4	5	6
Горизонтальное	Да	Да	Да	Нет	Нет	Да	Да	Да	Нет	Нет
Вертикальное	Да	Да	Да	Нет	Нет	Да	Да	Да	Нет	Нет
Сетки	Да	Да	Да	Нет	Нет	Да	Да	Да	Нет	Нет

- **4K display:** ThinOS поддерживает четыре дисплея с разрешением 4K в сессии Blast Horizon. Если производительность тонкого клиента низкая, рекомендуется не использовать четыре дисплея с разрешением 4K.

Таблица 22. Поддержка дисплеев с разрешением 4K.

Аппаратная версия	Версия для Windows	Количество поддерживаемых дисплеев 4K
10 (ESXi 5.5.x совместимый)	7, 8, 8.x и 10	1
11 (ESXi 6.0 совместимый)	7 — функция рендеринга 3D и Windows Aero отключены	3
11	7 — включена функция рендеринга 3D	1
11	8, 8.x и 10	1

- **3D визуализация:** для подключенных рабочих столов может быть настроена 3D-визуализация. Для использования функции 3D-рендеринга используйте до двух мони-

торов с разрешением до 1920 x 1200. Для разрешения 4K (3840 x 2160) поддерживается только один монитор.

- **Blast H.264:** таблица 23 описывает производительность декодера H.264 в сессиях VMware Horizon, которые используют протокол отображения VMware Blast.

Таблица 23. Декодирование Blast H.264.

Разрешение экрана в рамках Blast сессии VMware Horizon	Blast H.264 декодирование в рамках Blast сессии VMware Horizon	Описание
Ширина дисплея сеанса меньше или равна 1920 пикселям	Декодирование H.264 всегда включено	Клиент Horizon использует декодирование Blast H.264, даже если декодер H.264 отключен с помощью опций GUI или INI
Ширина дисплея сеанса превышает 1920 пикселей	Декодирование H.264 в Blast отключено по умолчанию. Вы можете включить декодирование H.264 в GUI ThinOS или путем изменения параметра INI.	По умолчанию клиент Horizon не использует декодирование H.264. Если настройка декодера Blast H.264 включена на ThinOS, то клиент Horizon использует H.264. Включение H.264 может понизить производительность сеанса.

Не рекомендуется использовать четыре дисплея с разрешением 4K из-за низкой производительности тонкого клиента.

ВИРТУАЛЬНАЯ ПЕЧАТЬ VMWARE BLAST

Виртуальная печать с VMware Blast позволяет использовать локальные или сетевые принтеры без необходимости установки дополнительных драйверов печати на удаленном рабочем столе. Для каждого принтера, настроенного локально на ThinOS, необходимо сопоставить принтер с VMware Blast рабочего стола. Отображение принтера ThinOS Blast эквивалентно виртуальной печати VMware Blast.

Чтобы сопоставить принтер, выполните следующие действия:

ПРИМЕЧАНИЕ: принтер LPT рассматривается в качестве примера для объяснения сценария сопоставления принтера. Сопоставление принтеров в ThinOS работает по аналогии с LPT для принтеров LPD и SMB.

1. Установите протокол связи на **All Supported** (Все поддерживаемые). Перейдите к глобальным настройкам **Global Connection Settings > Session** и проверьте, что установлен флажок **Exclude printer devices** (Исключить устройства принтера). Эта опция выбрана по умолчанию.
2. Подключите USB-принтер к клиентскому терминалу ThinOS.
3. Перейти к настройке системы.
4. Отображается диалоговое окно **Printer Setup** (Установки принтера).
5. В диалоговом окне **Printer Setup** (Настройки принтера) сделайте следующее:
 - 5.1. Из выпадающего списка **Select Port** выберите **LPT 1**. Введите действительное имя принтера и ID принтера.
 - 5.2. Введите действительное имя принтера и идентификатор принтера.

5.3. Выберите флажок **Enable the printer device**.

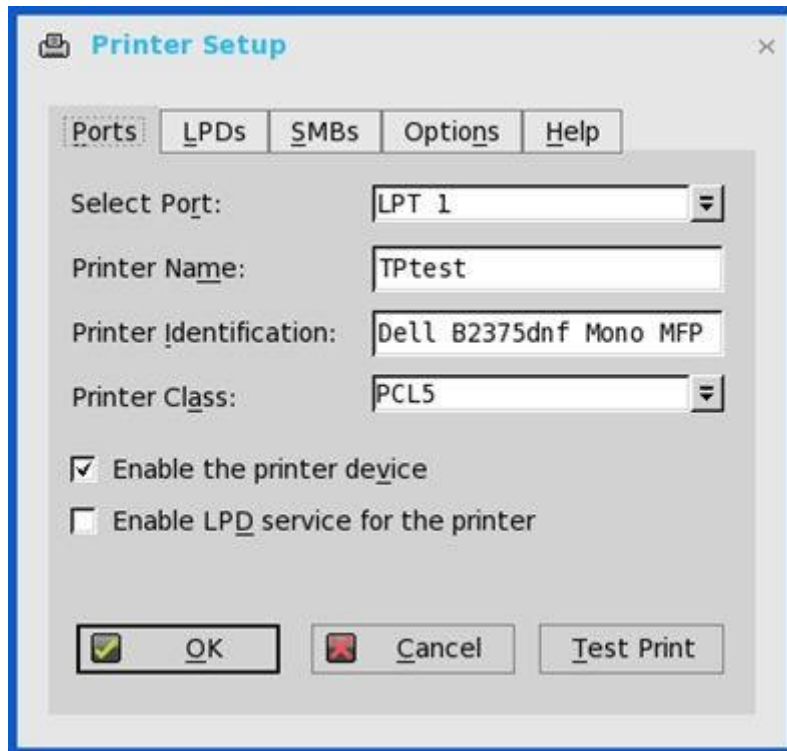


Рисунок 18. Настройка принтера.

5.4. Нажмите **OK** для сохранения конфигурации.

6. Нажмите на вкладку **Options** (Параметры) и выполните следующие действия:

6.1. Установите **LPT1: <Имя принтера>** в качестве принтера по умолчанию.

ПРИМЕЧАНИЕ: не устанавливайте флажок **Enable .print Client**.

6.2. Нажмите **OK** для сохранения конфигурации.

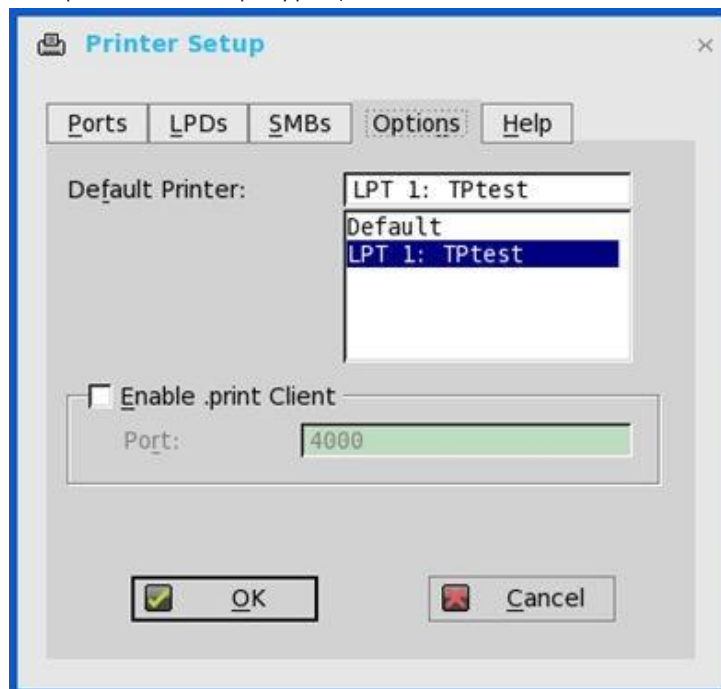


Рисунок 19. Вкладка **Параметры**.

6.3. Подключитесь к сеансу VMware Blast. Перейдите к **Control Panel > Devices and Printers**. Принтер, настроенный локально в ThinOS, подключен к сеансу.

Драйвером отображаемого принтера является TP PS Driver, портом - порт TPVM.

Виртуальный принтер позволяет отображать локальный принтер ThinOS в сессии VMware Blast без установки драйвера принтера в сеансе.

ВКЛЮЧИТЬ АППАРАТНЫЙ КУРСОР В СЕАНСЕ BLAST

Аппаратный курсор позволяет графическому процессору управлять отображением курсора мыши. Аппаратные курсоры имеют меньшую задержку.

ThinOS поддерживает аппаратный курсор в сессии VMware Horizon с помощью протокола отображения Blast. Поддерживаются только два цвета курсора – черный и белый.

По умолчанию программный курсор используется в сеансе Blast. Если аппаратный курсор не включен, курсор использует заданный цвет. Если аппаратный курсор включен, курсор использует черно-белые цвета.

Для включения аппаратного курсора в сеансе Blast используйте следующий параметр INI:

```
SessionConfig=Blast EnableHardwareCursor=yes
```

ВКЛЮЧИТЬ ФУНКЦИЮ ОТНОСИТЕЛЬНОГО ПОЗИЦИОНИРОВАНИЯ МЫШИ

Функция относительного позиционирования мыши применима как для PCoIP, так и для других тонких клиентов. При включении функции относительного позиционирования мыши Horizon Client использует относительные координаты для передачи данных о движении указателя мыши, что улучшает ее производительность. Относительное позиционирование мыши поддерживается на следующих платформах PC4-1263, PC4-1210, PC4-1240, PC4-1242 и PC4-1221.

Для тонких клиентов с поддержкой PCoIP

Для включения функции относительного позиционирования мыши в режиме **Classic** выполните следующие действия:

1. Подключитесь к удаленному рабочему столу с помощью протокола отображения PCoIP.
2. Щелкните по значку удаленного рабочего стола на панели задач ThinOS.
3. Кликните **Enable Relative Mouse** (Включить относительное позиционирование мыши).

ПРИМЕЧАНИЕ: чтобы отключить функцию относительного позиционирования мыши, щелкните правой кнопкой по значку удаленного рабочего стола в панели задач ThinOS и нажмите **Disable Relative Mouse**.

Для включения относительной функции относительного позиционирования мыши в режиме **Zero** выполните следующие действия:

1. Подключитесь к удаленному рабочему столу с помощью протокола отображения PCoIP.
2. В меню соединения ThinOS щелкните по значку **A**, отображаемому после имени сеанса PCoIP.

ПРИМЕЧАНИЕ: чтобы отключить функцию относительной мыши, щелкните по значку **R**, который отображается после имени сеанса PCoIP.

Для тонких клиентов с поддержкой Blast

1. Добавьте `SessionConfig=Blast EnableRelativeMouse=yes` в файл INI.
2. Перезагрузите тонкий клиент

Если включено относительное позиционирование мыши, то соответствующая запись появляется в журнале событий.

НАСТРОЙКА УДАЛЕННОГО РАБОЧЕГО СТОЛА MICROSOFT

Приложение Microsoft Remote Desktop позволяет получать доступ к данным и ресурсам удаленных устройств с помощью интернет-соединения.

В этом разделе содержится информация о том, как настроить соединение удаленного брокера рабочих столов на устройстве ThinOS и другие функции удаленного рабочего стола, которые можно настроить на ThinOS.

НАСТРОЙКА ПОДКЛЮЧЕНИЯ К БРОКЕРУ MICROSOFT REMOTE DESKTOP

Для настройки подключения к брокеру Microsoft Remote Desktop:

1. В меню рабочего стола щелкните **System Setup** (Настройка системы), а затем нажмите **Remote Connections** (Удаленное подключение). Отобразится окно настройки удаленных подключений.
2. Во вкладке **Broker Setup** (Настройка брокера) из выпадающего списка выберите **Microsoft** и выполните следующие действия:
 - 2.1. **Broker Server** (Сервер брокера): введите IP-адрес/имя хоста/FQDN сервера брокера.
 - 2.2. **Auto Connect List** (Список автоматического подключения): введите имена рабочих столов, которые Вы хотите запустить автоматически после подключения к соответствующему брокеру. Можно ввести несколько имен, разделенных точкой с запятой. Имена чувствительны к регистру.
 - 2.3. Нажмите **OK** для сохранения настроек.

НАСТРОЙКА RDP-СОЕДИНЕНИЙ

Для настройки соединения RDP выполните следующие действия:

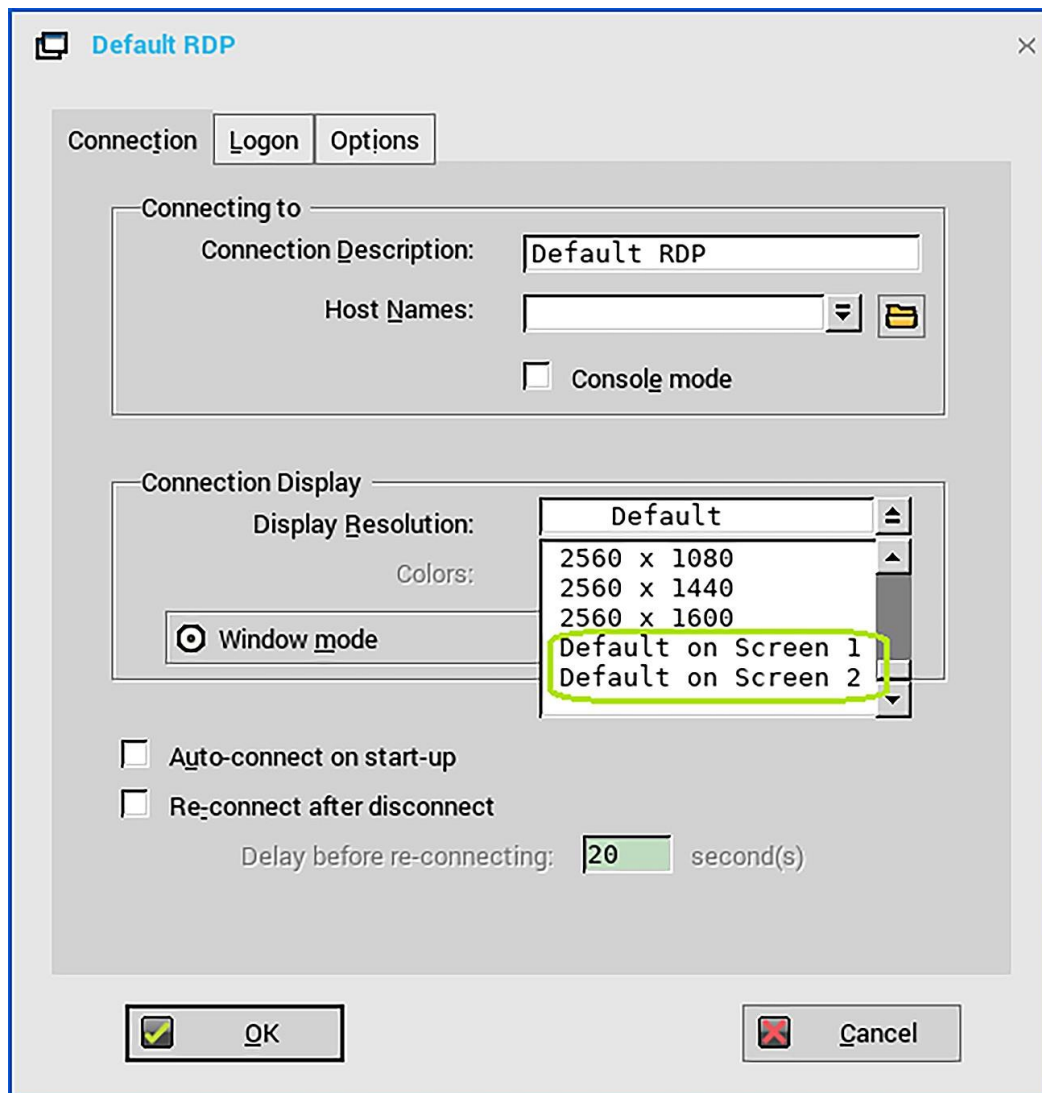
1. Из меню рабочего стола нажмите **System Setup** (Настройка системы), а затем нажмите **Remote Connections** (Удаленные подключения).
2. Во вкладке **Broker Setup** (Настройка брокера) из выпадающего списка **Broker type** (Тип брокера) выберите **None**.
3. Нажмите **RDP** и нажмите **Configure** (Настройка). Отобразится окно RDP по умолчанию.
4. Нажмите на вкладку **Connection** и используйте следующие рекомендации:
 - 4.1. **Connection Description** (Описание соединения): введите описательное имя, которое должно появиться в списке подключений (38 символов максимум);
 - 4.2. **Host Names** (Имена хостов): используйте этот список, чтобы выбрать действительное имя DNS-сервера или IP-адрес сервера, к которому будет подключен тонкий клиент. Можно использовать кнопку **Browse** (Обзор) рядом с полем, чтобы выбрать сервер.

ПРИМЕЧАНИЕ: имя сервера может быть разрешено с помощью одного из двух механизмов: DNS и WINS. DNS использует доменное имя по умолчанию в панели управления сети, чтобы попытаться построить FQDN, но также будет пытаться разрешить имя без использования значения по умолчанию.

 - 4.3. **Console mode** (Режим консоли): выберите для установки RDP-соединения в режиме консоли Windows.
 - 4.4. **Display Resolution** (Разрешение дисплея): выберите разрешение дисплея для соединения RDP.

В версии ThinOS 8.6 Вы можете выбрать предпочтительный монитор, на котором Вы хотите начать сеанс RDP в полноэкранном режиме на основе следующих сценариев:

- **Mirror mode is enabled on multi-display or single display:** опция **Default on screen x** (По умолчанию на экране X) не отображается. Разрешение дисплея соединения RDP устанавливается в значение по умолчанию, независимо от настроек в INI-парамetre onscreen=x.



- **Span mode is enabled on multi-display:** Отображается опция **Default on screen x** (По умолчанию на экране X). Вы можете выбрать предпочтительный дисплей, на котором Вы хотите начать сеанс RDP. Вы также можете установить предпочтительный дисплей с помощью параметра INI на экране. После развертывания параметра INI опция **Default on screen x** (По умолчанию на экране X) устанавливается автоматически в соответствии с настройками INI.

ПРИМЕЧАНИЕ: если значение, определенное в параметре экрана для Вашего соединения RDP выше, чем количество дисплеев, подключенных к тонкому клиенту, разрешение дисплея устанавливается в значение по умолчанию. При переключении режима отображения между Span и Mirror необходимо перезагрузить тонкий клиент для применения настроек INI.

- **Colors (Цвета):** выберите глубину цвета сеанса RDP. Если выбираются **High Colors** (16 бит) или **True Colors** (32 бита) и сервер RDP не поддерживает эту глубину цвета, тонкий клиент устанавливает значение глубины цвета ниже, например, 256 цветов (8 бит). Установка самого высокого значения (32-бит) возможна, если аппаратное обеспечение поддерживает такое значение глубины цвета.

- **Window mode on 1 monitor or Full screen span all monitors** (Режим окна на 1 мониторе или полный экран охватывает все мониторы): выберите исходное представление сеанса в оконном режиме или полноэкранном режиме.
- **Auto-connect on start-up** (Автоматическое подключение при запуске): при выборе автоматически подключается сеанс при запуске.
- **Re-connect after disconnect** (Повторное подключение после отключения): при выборе этой опции тонкий клиент автоматически подключается к сеансу после отключения, не инициированного оператором. Если этот параметр выбран, то интервал ожидания устанавливается в поле **Delay before re-connecting** (Задержка перед повторным подключением), введите количество секунд от 1 до 3600. По умолчанию установлено значение 20 секунд, если иное не указано в INI-файле.

Можно сбросить параметры во вкладке **Connection** диалогового окна **Connection Settings (RDP)** (Настройки соединения RDP). Чтобы сбросить, нажмите кнопку команды **Reset VM** (Сбросить VM). Эта кнопка расположена в верхнем правом углу диалогового окна. Она появляется только с подключением брокера VDM.

The screenshot shows the 'Connection Settings (RDP)' dialog box with the 'Logon' tab selected. The 'Logging on' section has three input fields: 'Login Username', 'Password', and 'Domain name'. The 'Start Command' section has two input fields: 'Application' and 'Working Directory'. The 'TS Gateway' section has two checkboxes, 'Use TS Gateway' and 'Use Same Info', both of which are unchecked. Below the checkboxes are four input fields: 'Server name', 'User name', 'Password', and 'Domain name'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Нажмите на вкладку **Logon** (Вход) и используйте следующие рекомендации:

- **Logging on area** (Поле входа в систему): введите имя пользователя, пароль и имя домена для входа. Если данные поля не заполнены, Вы можете ввести информацию вручную в окне входа в систему сервера RDP при установленном соединении. Используйте следующие рекомендации:
 - **Login Username** (Имя пользователя для входа): разрешено не более 31 символа.
 - **Password** (Пароль): допускается не более 19 символов.
 - **Domain Name** (Название домена): допускается не более 31 символа.
- **Application** (Приложение) (максимум 127 символов) и **Working Directory** (Рабочий каталог) (максимум 63 символа): введите строку инициализации и аргументы, включая со-

поставленный рабочий каталог, который Вы хотите автоматически запускать на сервере при подключении.

- **Use TS Gateway** (Использовать TS Gateway): включает серверы шлюза служб терминалов (TS Gateway) при подключении. Если необходимо, введите IP-адрес или URL сервера TS Gateway в поле **Server name** (Имя сервера). Вы также можете включить параметр **Use Same Info** (Использовать аналогичные данные), если учетные данные сервера совпадают с учетными данными Вашего удаленного рабочего стола (учетные данные основного удаленного компьютера) в полях: **Login Username** (Имя пользователя для входа в систему), **Password** (Пароль) и **Domain name** (Имя домена) или отключить **Use Same Info** (Использовать аналогичные данные) и ввести **Server name** (Имя сервера), **User name** (Имя пользователя), **Password** (Пароль) и **Domain name** (Имя домена) сервера TS Gateway, если необходимо.

ПРИМЕЧАНИЕ: сервер TS Gateway — это тип шлюза, который позволяет авторизованным пользователям в корпоративной сети подключаться к удаленным компьютерам с любого компьютера, подключенного к интернету. Сервер TS Gateway делает возможными подключения удаленного рабочего стола к корпоративной сети через интернет без необходимости устанавливать подключения виртуальной частной сети (VPN). Узнайте у вашего администратора сети, нужно ли Вам указывать сервер TS Gateway.

- **User Name** (Имя пользователя): введите имя пользователя для подключения.
- **Password** (Пароль): введите пароль.
- **Domain** (Домен): введите имя домена.

ПРИМЕЧАНИЕ: поля имени пользователя, пароля и имени домена являются необязательными. Если Вы оставите любое из этих полей пустым, потребуется интерактивное имя входа, и пользователи должны будут вводить информацию во время входа в систему.

TS GATEWAY В MICROSOFT BROKER (ПОСРЕДНИКЕ MICROSOFT)

Пользовательский сценарий:

1. Войдите в Microsoft Broker (Посредник Microsoft) с настроенным TS Gateway.
2. Запустите опубликованную коллекцию.

Будет установлено соединение TS Gateway.

В таблице 27 перечислены версии TS Gateway, поддерживаемые Windows Server.

Таблица 27. Поддерживаемые версии TS Gateway.

Серверная операционная система	TS Gateway II	TS Gateway III	Протокол WebSocket
Windows 2008 R2	Поддерживает	Не поддерживает	Не поддерживает
Windows 2012 R2	Поддерживает	Поддерживает	Не поддерживает
Windows 2016	Поддерживает	Поддерживает	Поддерживает

TS Gateway — WebSocket является новой функцией, представленной в ThinOS версии 8.5.

При подключении к TS Gateway II или III используется 2 полудуплексных соединения между тонким клиентом и сервером шлюзом терминальных серверов (Terminal Server Gateway).

При подключении к WebSocket при настройке подключения сеанса используется дуплексная связь между TS Gateway и тонким клиентом.

TS Gateway II и TS Gateway III обратно совместимы с Windows Server 2016. Это означает, что в случае сбоя подключения WebSocket или если сервер TS Gateway или версия тонкого клиента не поддерживают WebSocket, тогда используется TS Gateway II или TS Gateway III.

На рисунке 23 представлен журнал настройки подключения к TS Gateway II.

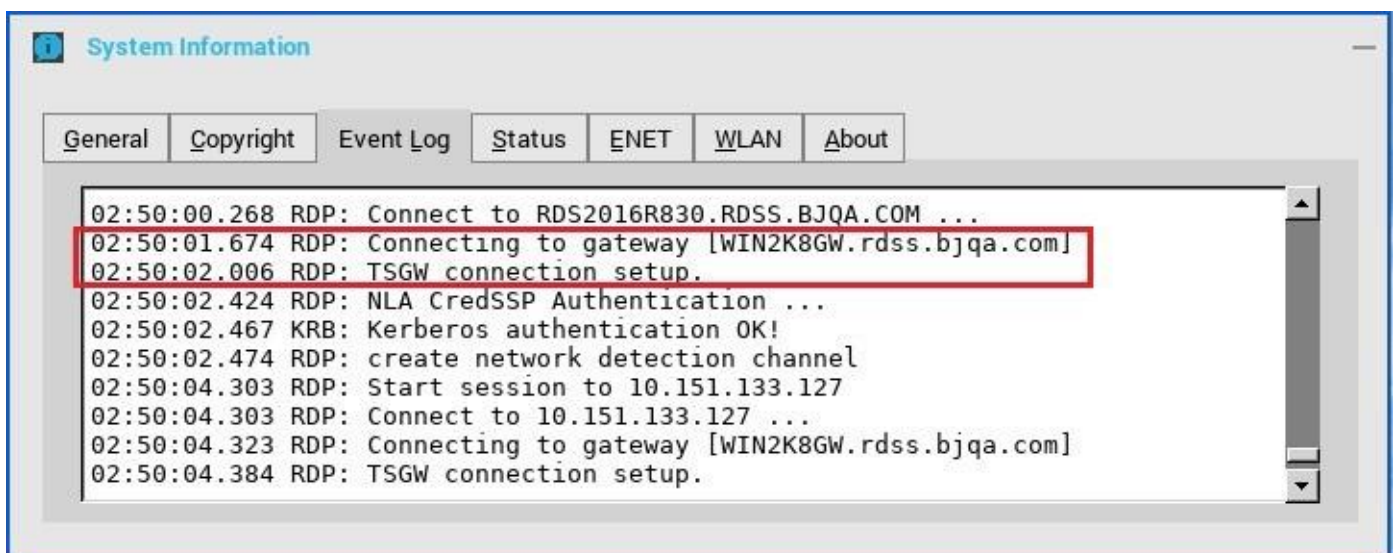


Рисунок 23. Вкладка Event log.

На рисунке 24 представлен журнал настройки подключения к TS Gateway III.

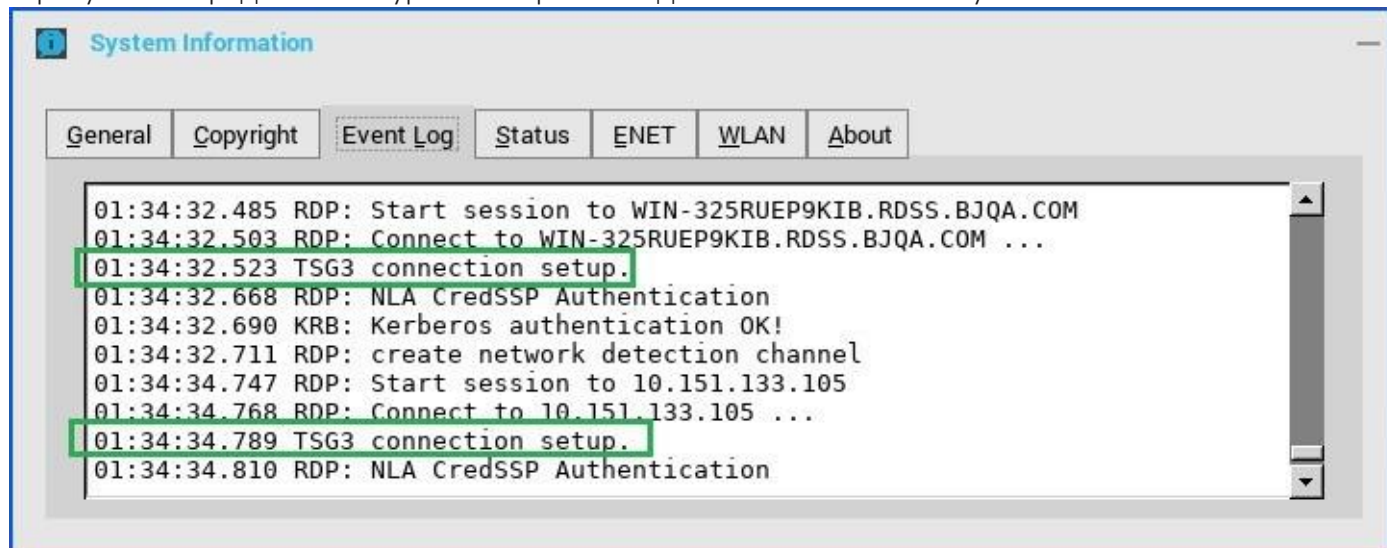


Рисунок 24. Вкладка Event log.

ПРИМЕЧАНИЕ

Журнал подключений WebSocket скрыт и не отображает вкладку **Event log** (Журнал системных событий). Если Вы хотите посмотреть журнал подключений WebSocket, перейдите в раздел **Troubleshooting > Capture** (Устранение неполадок > Захват) и включите **Persistent** (Сохраняемый) для экспорта журнала системных событий.

Начиная с выпуска ThinOS версии 8.6, функция WebSocket по умолчанию отключена. Чтобы включить WebSocket, примените следующий параметр INI: `Sessionconfig=RDP TSGWWebSock=yes`.

ПОДКЛЮЧИТЕСЬ К СЕАНСУ RDP, ИСПОЛЬЗУЯ ПРОТОКОЛ UDP С TS GATEWAY

Чтобы подключиться к Сеансу удаленного рабочего стола, используя User Datagram Protocol (UDP) (Протокол передачи датаграмм) с TS Gateway, выполните следующие действия:

1. Примените следующий параметр INI к тонкому клиенту:
`SessionConfig=RDP TSGWUDP=yes`
2. Включите **Terminal Services Gateway** (Шлюз служб терминалов) (TSGW) для приложений и рабочих столов из сервера посредника Microsoft RDS.
3. В клиенте ThinOS начните сеанс удаленного рабочего стола, используя посредник соединения RDS.
4. Подключитесь к опубликованному рабочему столу.

На рисунке 25 представлен журнал системных событий рабочего стола ThinOS в окне **System Information** (Информация системы).

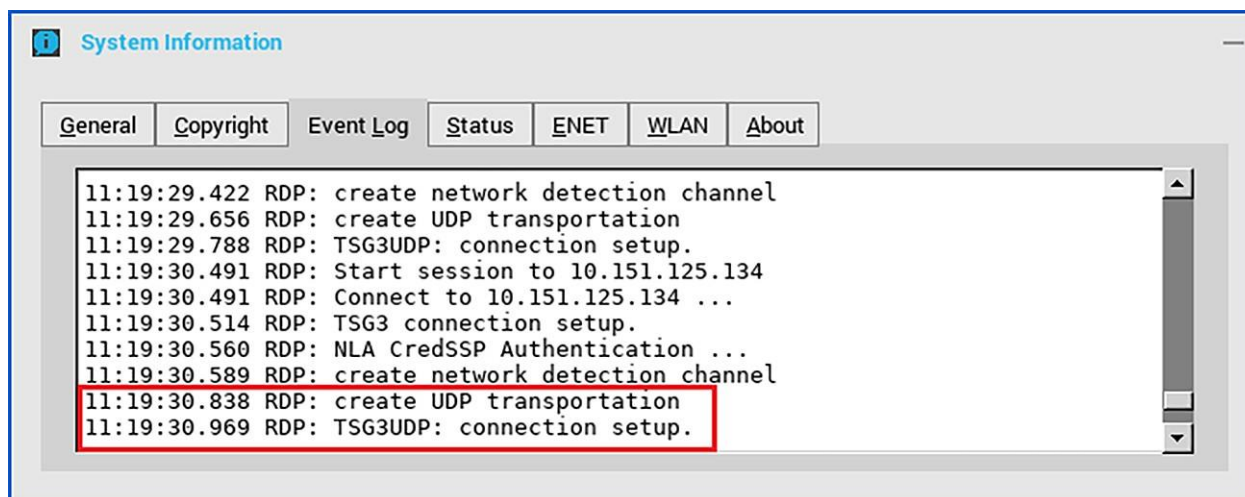


Рисунок 25. Журнал системных событий.

НАСТРОЙКА DELL VWORKSPACE

Виртуализация рабочего пространства предоставляет единый список приложений и рабочих столов в виде единого виртуального рабочего пространства. Полное вычислительное пространство изолируется и централизуется, vWorkspace обеспечивает гибкий, независимый от местоположения и платформы доступ посредством предоставления виртуального рабочего пространства с нескольких платформ виртуализации.

Данный раздел предоставляет информацию о том, как настроить соединение с посредником Dell vWorkspace на вашем устройстве ThinOS.

НАСТРОЙКА СОЕДИНЕНИЯ С ПОСРЕДНИКОМ DELL VWORKSPACE

Для того чтобы управлять конфигурацией настройки посредника vWorkspace выполните следующие действия:

1. В меню рабочего стола нажмите **System Setup** (Настройка системы), затем нажмите **Remote Connections** (Удаленные подключения). Откроется диалоговое окно **Remote Connections** (Удаленные подключения).
2. Во вкладке **Broker Setup** (Настройка посредника) в раскрывающемся списке выберите **Dell vWorkspace** и выполните следующие действия:
 - 2.1. **Broker Server** (Сервер посредника): введите IP-адрес/Название главного узла/ FQDN (полное доменное имя) сервера посредника.
 - 2.2. **Auto Connect List** (Список автоматического подключения): введите имена рабочих столов, которые необходимо автоматически запустить после входа в соответствующий посредник. Можно указать больше одного рабочего стола. Каждое имя рабочего стола отделяется точкой с запятой и чувствительно к регистру.
 - 2.3. Для включения vWorkspace Gateway установите соответствующий флажок.
 - 2.4. **vWorkspace Gateway** (Шлюз vWorkspace): введите IP-адрес Шлюза vWorkspace.
3. Нажмите **OK** (Да), чтобы сохранить настройки.

ГЛАВА 5. НАСТРОЙКА ЛОКАЛЬНЫХ ПАРАМЕТРОВ

В данном разделе описываются доступные параметры тонкого клиента. В зависимости от уровня привилегий пользователя некоторые диалоговые окна и параметры могут быть недоступны для использования.

ПРИМЕЧАНИЕ: хотя не рекомендуется использовать диалоговые окна для настроек конфигурации тонкого клиента, допускается их использование в том случае, если Вы хотите временно переопределить централизованные конфигурации со значениями параметров по умолчанию или если у Вас нет возможности настроить централизованную конфигурацию (небольшие среды). Рекомендуется использовать централизованную конфигурацию, которая позволит Вам автоматически отправлять всем тонким клиентам, поддерживаемым в вашей среде, обновления и любую желаемую конфигурацию со значениями параметров по умолчанию.

МЕНЮ ЛОКАЛЬНЫХ НАСТРОЕК

Чтобы получить доступ к меню локальных настроек выполните следующие действия:

1. **Zero desktop** (Исходный рабочий стол): нажмите значок **System Settings** (Настройки системы) на исходной панели инструментов. Администраторы также могут нажать кнопку **Admin Mode** (Режим администратора) в диалоговом окне **Login** (Вход в систему).
2. **Classic desktop** (Классический рабочий стол): нажмите **User Name** (Имя пользователя) и выберите **System Setup** (Настройка системы).

ПРИМЕЧАНИЕ: **User Name** (Имя пользователя) находится в левой нижней области панели задач.

НАСТРОЙКА ПАРАМЕТРОВ СИСТЕМЫ

Используйте диалоговое окно **System Preference** (Параметр системы) для выбора персональных установок, таких как: экранная заставка, время, дата и настройки устанавливаемой пользователем информации.

НАСТРОЙКА ПАРАМЕТРОВ ПЕРИФЕРИЙНЫХ УСТРОЙСТВ

Диалоговое окно **Peripherals** (Периферийные устройства) позволяет настроить параметры клавиатуры, мыши, звука, последовательного интерфейса, камеры, сенсорного экрана и функции Bluetooth.

НАСТРОЙКА ПАРАМЕТРОВ КЛАВИАТУРЫ

Для настройки параметров клавиатуры выполните следующие действия:

1. В меню рабочего стола выберите **System Setup** (Настройка системы), а затем нажмите **Peripherals** (Периферийные устройства). Откроется диалоговое окно **Peripherals** (Периферийные устройства).
2. Нажмите вкладку **Keyboard** (Клавиатура) и установите параметры **Character Set** (Набор символов), **Keyboard Layout** (Раскладка клавиатуры), **Delay Before Repeat** (Задержка перед повтором) и **Repeat Rate** (Частота повторения). В таблице 35 приведены настройки параметров клавиатуры.

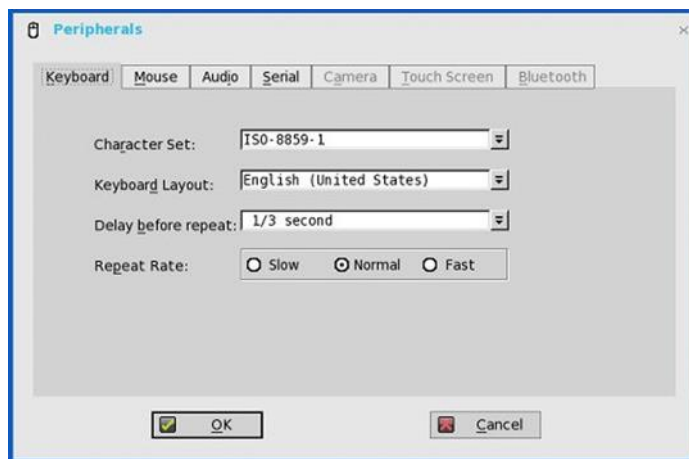


Таблица 35. Настройки параметров клавиатуры.

Параметр	Описание
Character Set (Набор символов)	Определяет кодировку символов. Каждый символ представлен числовым кодом. Например, набор символов ASCII использует числа от 0 до 127 для представления всех английских символов и специальных управляющих символов. Наборы европейских символов ISO похожи на ASCII, но они содержат дополнительные символы для европейских языков.
Keyboard Layout (Раскладка клавиатуры)	В настоящее время поддерживаются языки клавиатуры, перечисленные в раскрывающемся списке Keyboard layout (Раскладка клавиатуры). Значение по умолчанию — English (United States) — Английский (США).
Delay Before Repeat (Задержка перед повтором)	Задаёт параметры повтора для удерживаемой клавиши. Выберите значение Delay before repeat (Задержка перед повтором): 1/5 секунды, 1/4 секунды, 1/3 секунды, 1/2 секунды, 3/4 секунды, 1 секунда, 2 секунды, или No Repeat (Без повтора). По умолчанию — 1/3 секунды.
Repeat Rate (Частота повторения)	Выберите Slow (Медленно), Normal (Нормально), или Fast (Быстро). Значение по умолчанию — Среднее.

3. Нажмите **ОК** (Да), чтобы сохранить настройки.

НАСТРОЙКА ПАРАМЕТРОВ МЫШИ

Для настройки параметры мыши выполните следующие действия:

1. В меню рабочего стола выберите **System Setup** (Настройка системы), а затем нажмите **Peripherals** (Периферийные устройства). Откроется диалоговое окно **Peripherals**(Периферийные устройства).
2. Нажмите вкладку **Mouse** (Мышь) для выбора скорости и направления мыши.
3. Выберите окно флажка **Swap left and right mouse buttons** (Поменять местами левую и правую кнопки мыши), чтобы поменять местами кнопки мыши для режима работы левой рукой.
4. Выберите окно флажка **Reverse mouse wheel scroll direction** (Обратное направление прокрутки колеса мыши), чтобы поменять направление прокрутки колеса мыши.

5. Выберите окно флажка **Enable big mouse pointer** (Включить большой курсор мыши), чтобы увеличить размер локального курсора мыши в два раза.

ПРИМЕЧАНИЕ: данная опция влияет на локальный курсор мыши ThinOS

6. Нажмите **ОК** (Да), чтобы сохранить настройки.

НАСТРОЙКА ПАРАМЕТРОВ ЗВУКА

Для настройки параметров звука выполните следующие действия:

1. В меню рабочего стола выберите **System Setup** (Настройка системы), а затем нажмите **Peripherals** (Периферийные устройства). Откроется диалоговое окно **Peripherals** (Периферийные устройства).
2. Нажмите вкладку **Audio** (Звук) для выбора настроек громкости подключенных устройств.

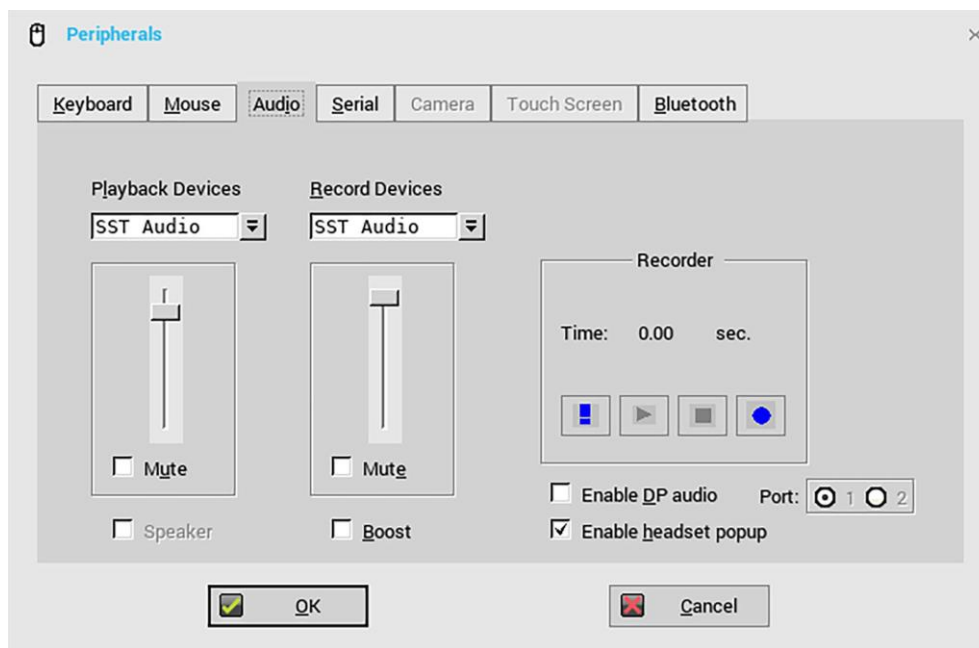


Рисунок 33. Вкладка Audio.

- 2.1. Нажмите вкладку **Playback Devices** (Устройства воспроизведения), чтобы выбрать тип звука из раскрывающегося меню.
 - 2.1.1. Если в устройствах воспроизведения доступны функции HD audio и DP audio, тонкий клиент определяет приоритет между HD audio и DP audio, когда подключен кабель DP. В данном сценарии выберите тип устройства воспроизведения, соответствующий Вашим параметрам, и нажмите **ОК** (Да). Устройство воспроизведения, которое Вы выбрали, является приоритетным.
 - 2.1.2. Используйте ползунок для управления настройками громкости для устройств воспроизведения.
 - 2.1.3. Установите флажок **Mute** для отключения звука.
- 2.2. Нажмите вкладку **Recorded Devices** (Устройства записи), чтобы выбрать тип записи из раскрывающегося списка.
 - 2.2.1. Используйте ползунок для управления настройками громкости устройств записи.
 - 2.2.2. Установите флажок **Mute** для отключения звука.
- 2.3. Нажмите **Play** (Воспроизведение) для воспроизведения звука.
- 2.4. Нажмите на вкладку **Recorder** (Устройство записи) и выполните следующие действия:
 - 2.4.1. Соберите информацию об используемых динамике и микрофоне.
 - 2.4.2. Проверьте характеристики используемых динамика и микрофона. Например, подключенные USB-гарнитуры отображаются в раскрывающемся списке. Выберите опцию **HD audio** (Звук высокого разрешения) для применения аналоговых наушников,

флажок динамика для включения внутреннего динамика и флажок **Boost** (Повышение) для улучшения звука.

- 2.5. Выберите флажок **Speaker** (Динамик) для подключения динамика.
- 2.6. Выберите флажок **Boost** (Усиление) для усиления звука подключенных устройств.
- 2.7. Выберите флажок **Enable DP audio** (Включение звука DP) для включения функции звука дисплейного порта на тонком клиенте. Вы должны нажать либо **Port 1** (Порт 1), либо **Port 2** (Порт 2) для выбора необходимого дисплейного порта.
- 2.8. Выберите флажок **Enable headset popup** (Включить всплывающее окно гарнитуры), если требуется, чтобы всплывающее диалоговое окно гарнитуры отображалось, когда Вы подключаете аналоговую гарнитуру к переднему разъему для гарнитуры. Во всплывающем диалоговом окне гарнитуры выберите любое из следующих аудиоустройств:
 - гарнитура;
 - наушники;
 - динамик.

ПРИМЕЧАНИЕ: для отключения всплывающего диалогового окна гарнитуры установите флажок **Not show again** (Больше не показывать) и нажмите **OK** (Да). Вы также можете использовать параметр INI для включения или отключения всплывающего диалогового окна гарнитуры.

3. Нажмите **OK** (Да) для сохранения изменений.

Использование звука дисплейного порта

Используйте интерфейс DisplayPort (DP) (Дисплейный порт) для подключения тонких клиентов к устройствам отображения. Интерфейс может включать аудиосигналы в том же кабеле, что и видеосигналы. Для включения звука дисплейного порта убедитесь, что Вы установили следующие компоненты:

1. Тонкий клиент, который поддерживает звук дисплейного порта или двойной режим со звуком.
2. Устройство отображения, например, монитор, которое поддерживает воспроизведение звука в сеансах ICA, RDP, Blast или PCoIP.
3. Аналоговое аудиоустройство или встроенный в динамик монитор. Для включения звука дисплейного порта на ThinOS выполните следующие действия:
 - 3.1. Настройте монитор с поддержкой звука DP.
 - 3.2. Подключите клиент ThinOS к монитору с использованием кабеля DP.
 - 3.3. Подключите аналоговую гарнитуру к интерфейсу звука DP монитора.
 - 3.4. На рабочем столе ThinOS нажмите **System Setup > Peripherals > Audio > Playback devices** (Настройка > Системы > Периферийные условия > Звук Устройства воспроизведения) и выберите флажок **Enable DP audio** (Включить звук DP).
 - 3.5. На вкладке **Audio** (Звук) выберите **Port 1** (Порт 1) или **Port 2** (Порт 2).
 - 3.6. Запустите сеанс RDP, ICA, PCoIP или Blast.
 - 3.7. Воспроизведите видео и проверьте вывод звука с помощью аналоговой гарнитуры.

ПРИМЕЧАНИЕ:

1. ThinOS поддерживает только воспроизведение звука дисплейного порта. Запись звука с использованием дисплейного порта не поддерживается.
2. Звук дисплейного порта поддерживается только для тонких клиентов СИЛА PC4-1263, СИЛА PC4-1242 и СИЛА PC4-1221.
3. По умолчанию звук DP отображается на тонком клиенте СИЛА PC4-1210. Если Вы обновите ThinOS до более новой версии, установка по умолчанию для звука DP не установится автоматически. Необходимо сбросить настройки тонкого клиента до заводских настроек для загрузки

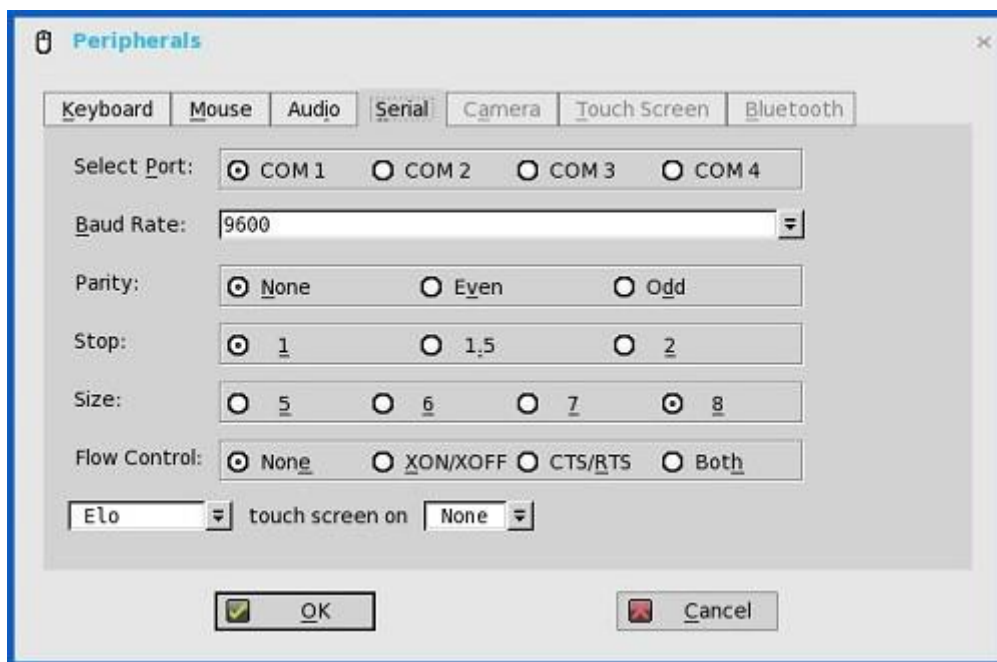
настроек по умолчанию для звука DP. Тонкие клиенты, поставляемые с последней версией ThinOS, уже настроены с настройками по умолчанию.

Если Вы включите звук DP и выберете звук DP в качестве устройства воспроизведения, будут наблюдаться следующие проблемы: во время перезагрузки системы в течение нескольких секунд отображается черный экран; звук DP перестает отвечать, и при воспроизведении аудиофайла отображается черный экран.

НАСТРОЙКА ПАРАМЕТРОВ ПОСЛЕДОВАТЕЛЬНОГО ПОРТА

Для настройки параметров последовательных портов выполните следующие действия:

1. В меню рабочего стола выберите **System Setup** (Настройка системы), а затем нажмите **Peripherals** (Периферийные устройства). Откроется диалоговое окно **Peripherals** (Периферийные устройства).
2. Нажмите на вкладку **Serial**(Последовательный порт) и выполните следующие действия:



- **Select Port**(Выбрать порт): нажмите на кнопку для выбора порта. Значение по умолчанию: **COM 1**.
- **Baud Rate**(Скорость в бодах): выберите скорость в бодах из раскрывающегося списка. Значение по умолчанию: **9600**.
- **Parity** (Контроль четности): нажмите кнопку для выбора контроля четности.
- **Stop** (Стоп-бит): нажмите кнопку для выбора стоповых разрядов **1, 1.5, 2**. Значение по умолчанию: **1**.
- **Size**(Размер): нажмите кнопку для выбора количества бит в символе — **5, 6, 7** или **8** бит. Значение по умолчанию: **8**.
- **Flow Control**(Управление потоками): нажмите на кнопку для выбора управления потоками. Могут быть выбраны **None** (Отсутствует), **XON/XOFF**, **CTS/RTS** или **Both** (Оба). Значение по умолчанию: **None** (Отсутствует).
- **Serial Touch Screen selections**(Выбор типа сенсорного экрана): выбор необходимого сенсорного экрана из раскрывающегося списка. Доступными вариантами являются ELO, MicroTouch и FastPoint.
- **Touch Screen on** (Выбор COM-порта для сенсорного экрана): выберите из раскрывающегося списка необходимый последовательный порт (COM-порт) или **None** (Отсутствует).

3. Нажмите **OK** (Да), чтобы сохранить настройки.

ThinOS позволяет отключить встроенный последовательный порт на следующих платформах:

- тонкий клиент СИЛА PC4-1221 с процессором Celeron;
- тонкий клиент СИЛА PC4-1221 с процессором Pentium;
- расширенный тонкий клиент СИЛА PC4-1221 с процессором Pentium.

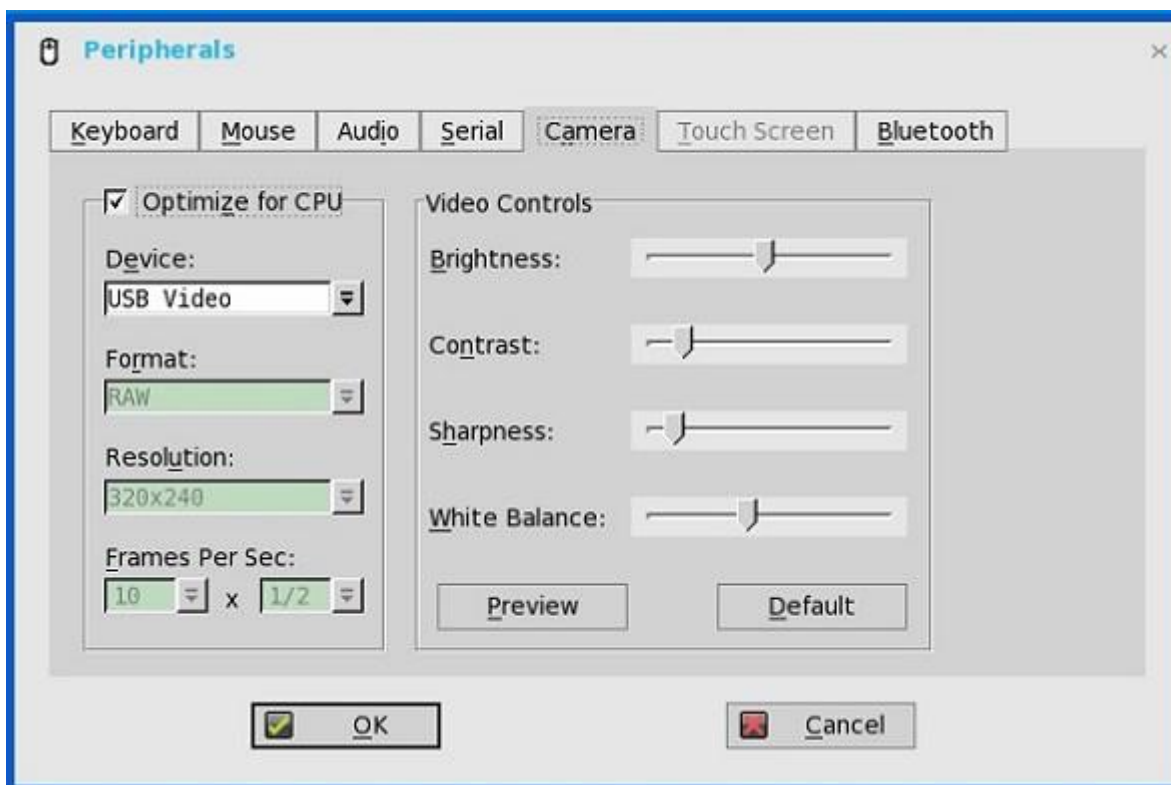
Для отключения или включения встроенного последовательного порта используйте INI-параметр `Device=SerialDisable={yes, no}`. Значение по умолчанию — «Нет». Данная опция не влияет на последовательные USB-устройства. Указанное значение сохраняется в NVRAM, для вступления изменений в силу требуется перезагрузка системы.

После отключения встроенного порта все имена порта — COM1, COM2, COM3 и COM4 — становятся доступными для подключения последовательного USB-COM-устройства. Вы можете просмотреть журнал событий ThinOS, чтобы узнать имя локального последовательного порта, которое используется при подключении последовательного USB-устройства тонкому клиенту.

НАСТРОЙКА ПАРАМЕТРОВ КАМЕРЫ

Используйте вкладку **Camera** (Камера) для взаимодействия с камерами, которые локально подключены к тонкому клиенту (USB) и поддерживаются драйвером UVC. При использовании функции веб-камеры HDX RealTime в Citrix Virtual Apps и настольных компьютерах Вы можете настроить максимальное разрешение и количество кадров в секунду (рекомендуется 10 кадров в секунду).

По умолчанию формат камеры USB установлен на **RAW**.



ПРИМЕЧАНИЕ: Вы можете оптимизировать производительность и изменять частоту кадров в секунду непосредственно на тонком клиенте (если веб-камера поддерживает универсальный видеодрайвер), когда не установлен флажок **Optimize for CPU** (Оптимизировать для процессора).

Поддерживаемые значения включают 1/1, 1/2, 1/3, 1/4, 1/5 и 1/6.

Кроме того, данная функция интенсивно использует процессор и рекомендуется для высокопроизводительных продуктов.

НАСТРОЙКА ПАРАМЕТРОВ СЕНСОРНОГО ЭКРАНА

Используйте вкладку **Touch Screen** (Сенсорный экран) для настройки сенсорных экранов, которые подключены к тонкому клиенту. Вкладка доступна (не отображается серым цветом), если тонкий клиент обнаруживает подключение сенсорного экрана через USB-порт или последовательный портс невыполненной настройкой или калибровкой. Окно **Touch Setup** (Сенсорный экран) предложит коснуться двух кругов на экране для выполнения необходимой калибровки. Отрегулированные калиброванные значения сохраняются в локальном терминале NVRAM до тех пор, пока система не будет сброшена до заводских настроек по умолчанию или не будет подключен сенсорный монитор другого типа.

НАСТРОЙКА ПАРАМЕТРОВ BLUETOOTH

Функция Bluetooth помогает подключить тонкий клиент к устройствам с поддержкой Bluetooth, таким как гарнитуры и мыши. ThinOS поддерживает беспроводные чипсеты Intel 7260 и 7265.

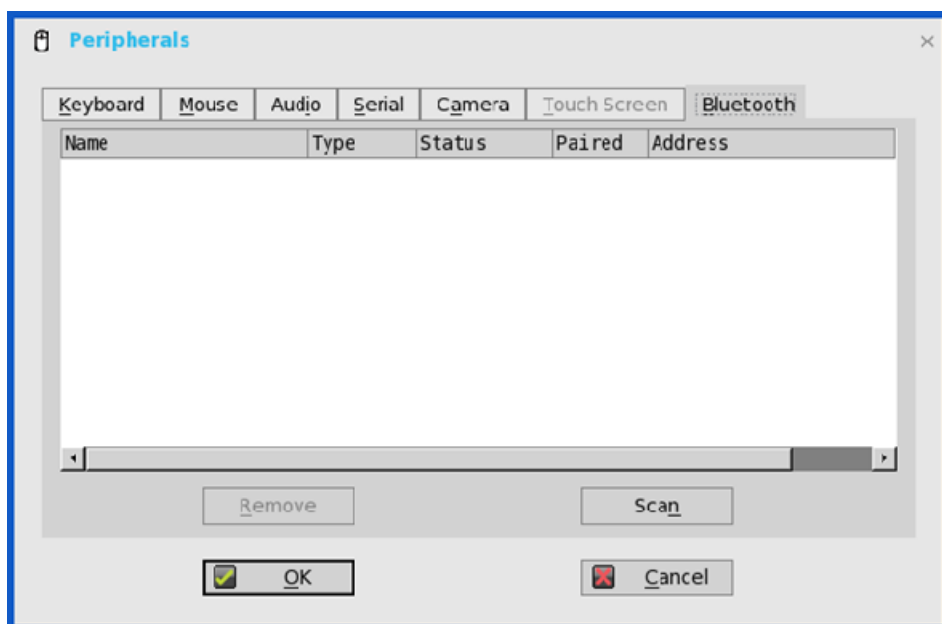
ThinOS поддерживает чипсет Intel Dual Band Wireless AC 9560 на тонком клиенте СИЛА PC4-1221. Для мыши, клавиатуры и гарнитуры ThinOS поддерживает Bluetooth 3.0 и 4.0.

Bluetooth 4.0 поддерживает Classic и Bluetooth Low Energy (BLE). Альтернативный MAC / PHY Bluetooth (AMP) не поддерживается.

ПРИМЕЧАНИЕ: начиная с ThinOS v8.4.1, функция Bluetooth поддерживается тонким клиентом СИЛА PC4-1210 с тонким клиентом ThinOS и СИЛА PC4-1210 с PCoIP.

Для настройки параметров Bluetooth выполните следующие действия:

1. В меню рабочего стола выберите **System Setup** (Настройка системы), а затем нажмите **Peripherals** (Периферийные устройства). Откроется диалоговое окно **Peripherals** (Периферийные устройства)



2. Нажмите на вкладку **Bluetooth** и используйте следующие рекомендации:

Устройства с поддержкой Bluetooth, такие как гарнитуры и мыши, доступные в среде тонкого клиента, перечислены на странице **Bluetooth**. В списке отображаются следующие атрибуты:

- **Name** (Имя): указывает имя устройства с поддержкой Bluetooth;
- **Type** (Тип): определяет тип устройств, совместимых с Bluetooth, таких как: гарнитуры, мыши и клавиатуры. Поддерживаются как устройства взаимодействия с человеком (HID), так и гарнитура Bluetooth;
- тип HID:
 - HID включает мышь и клавиатуру;

- максимально можно подключить семь устройств HID.
- тип гарнитуры:
 - в данном выпуске поддерживается гарнитура Bluetooth;
 - максимально можно подключить одно устройство Bluetooth.

ПРИМЕЧАНИЕ: другие типы устройств Bluetooth не сканируются и не поддерживаются. В гарнитуре поддерживается качество звука на уровне вызова. Тем не менее, мультимедиа все еще не поддерживается.

- **Status** (Состояние): страница **Bluetooth** имеет две колонки, а именно, **Status** (Состояние) и **Paired** (Сопряженные);

Таблица 36. Состояние Bluetooth.

Атрибут	Значение	Описание
Состояние	Подключено	Устройство Bluetooth подключено к устройству ThinOS. Готово к использованию
	Подключение	Устройство Bluetooth, подключающееся к устройству ThinOS
	Отключено	Устройство Bluetooth не подключено к устройству ThinOS
Сопряжено	Да	Устройство Bluetooth сопряжено с устройством ThinOS
	Нет	Устройство Bluetooth не сопряжено с устройством ThinOS

- **Address** (Адрес): отображает адрес устройства Bluetooth, подключенного к тонкому клиенту.

В таблице 37 приведены пользовательские сценарии и соответствующие статусы Bluetooth, отображаемые на странице Bluetooth:

Таблица 37. Пользовательские сценарии.

Пользовательский сценарий	Состояние
Устройство отключено	Отключено Сопряжено
Устройство включено	Подключено Сопряжено
Устройство отключено от ThinOS	Отключено Не сопряжено

- **Scan** (Сканирование): все устройства Bluetooth входят в режим **Page Scan** (Доступно для сканирования). Различные устройства Bluetooth входят в режим сканирования страницы в разных случаях, например, если конкретная кнопка нажата три раза или определенная кнопка нажата и удерживается до тех пор, пока светодиод не загорится синим цветом;
- **Connect** (Подключение): выберите конкретное Bluetooth-совместимое устройство и нажмите **Connect** (Подключение) для подключения выбранного устройства к тонкому клиенту. Если устройство Bluetooth успешно подключено, статус отображается как **Connected** (Подключено) в окне **Bluetooth**;
- **Remove** (Удаление): выберите определенное устройство Bluetooth и нажмите **Remove** (Удаление) для его отключения, удалите устройство из списка;
- **Auto Connect function** (Функция автоматического подключения): функция автоматического подключения предназначена для HID:

- ThinOS не имеет подключенных HID, таких как HID USB или Bluetooth;
- HID Bluetooth настроены как режим сканирования.

Если Вы запускаете клиент ThinOS, Bluetooth HID могут автоматически подключаться к ThinOS без операций сканирования или сопряжения. HID Bluetooth автоматически повторно подключаются после перезапуска клиента ThinOS.

- **Reconnect function** (Функция повторного подключения): функция повторного подключения предназначена для устройств HID и гарнитур.

При перезапуске системы с устройством Bluetooth (HID/гарнитура), которое уже сопряжено и подключено, устройство Bluetooth автоматически повторно подключается в течение нескольких секунд.

Например, Вам потребуется подвигать мышью, а затем кликнуть несколько раз, чтобы мышь переподключилась. Гарнитура Bluetooth переподключается автоматически, но в некоторых случаях может потребоваться остановить и снова запустить устройство вручную.

ПОДДЕРЖКА USB

USB port (Порт USB): тонкий клиент СИЛА PC4-1243 с ThinOS (Z10D) поддерживает два порта USB 3.0. USB 3.0 совместим с USB 2.0. Если устройство USB 2.0 подключено к портам 3.0, характеристики устройства остаются неизменными. Для подключения устройства USB 3.0 к портам 3.0 тип устройства должен быть 5 Гбит/с. Все типы устройств USB работают при подключении к порту USB 3.0.

USB hard disk (Жесткий диск USB): не подключайте жесткий диск USB с 10 или более приводами, не подключайте более 10 ключей USB к клиенту ThinOS. ThinOS не обнаруживает USB-диск с 10 или более приводами.

Поддержка USB типа C

Тонкий клиент СИЛА PC4-1221 поддерживает порт USB типа C. Коннектор USB 3.1 типа C может применяться для выполнения следующих действий:

- передача данных с помощью запоминающего устройства USB;
- подключение мониторов;

ПРИМЕЧАНИЕ: если используется USB-C, то порт DP2 на задней панели отключается.

- зарядка смартфонов;
- подключения USB 2.0, 3.0 и совместимые с 3.1 устройств.

USB 3.1 типа C нельзя использовать для следующих подключений:

- режимы Thunderbolt, HDMI и MHL alt;
- док-станции;
- питания тонкого клиента;

Ограничение: в тонком клиенте СИЛА PC4-1221 XHCI используется для всех типов устройств USB. Расхождение скорости передачи данных между USB 3.0 и USB-C является незначительным.

ВОССТАНОВЛЕНИЕ ЗАВОДСКИХ НАСТРОЕК

ВОССТАНОВЛЕНИЕ ЗАВОДСКИХ НАСТРОЕК ПО УМОЛЧАНИЮ С ПОМОЩЬЮ СБРОСА G-КЛАВИШИ

Высокопривилегированные или самостоятельные пользователи могут сбросить тонкий клиент до заводских настроек по умолчанию с помощью функции сброса по клавише **G**.

Для сброса тонкого клиента до заводских настроек по умолчанию, перезапустите тонкий клиент и постоянно нажимайте клавишу **G** во время процесса перезапуска. Сброс по клавише **G** влияет на все элементы конфигурации, включая как сетевую конфигурацию, так и подключения, определенные в локальной NV-RAM.

ПРИМЕЧАНИЕ: сброс по G-клавише отключен для низкопривилегированных и непривилегированных пользователей в режиме блокировки.

ВОССТАНОВЛЕНИЕ ЗАВОДСКИХ НАСТРОЕК ПО УМОЛЧАНИЮ С ПОМОЩЬЮ СБРОСА ПРИ ОТКЛЮЧЕНИИ

Высокопривилегированный или самостоятельный пользователь может сбросить тонкий клиент до заводских настроек по умолчанию из диалогового окна **Shutdown** (Отключение). Для сброса тонкого клиента до заводских настроек по умолчанию выполните следующие действия:

1. В меню на рабочем столе нажмите **Shutdown** (Отключение). Откроется диалоговое окно **Shutdown** (Отключение).
2. Нажмите **Restart the system** (Перезагрузить систему) для перезапуска тонкого клиента.
3. Установите флажок **Reset the system setting to factory default** (Сброс настроек системы до заводских настроек по умолчанию) для сброса системных настроек по умолчанию.
4. Нажмите **OK** (Да), чтобы сохранить настройки.

Сброс при отключении влияет на все элементы конфигурации, включая без ограничения конфигурацию сети и подключения, определенные в локальной памяти NV-RAM. Имя терминала не будет изменено.

ПРИМЕЧАНИЕ: сброс при отключении выключен для низкопривилегированных и непривилегированных пользователей независимо от статуса блокировки.

СБРОС НАСТРОЕК ДИСПЛЕЯ С ПОМОЩЬЮ СБРОСА ПО КЛАВИШЕ V

Если настройки дисплея не соответствуют конкретному подключенному монитору, возможно, дисплей не будет работать должным образом при перезагрузке тонкого клиента. Для исправления включите тонкий клиент, постоянно нажимая клавишу **V**. Это перезапустит тонкий клиент, разрешение экрана будет установлено по умолчанию.

ГЛАВА 6. МОДУЛЬ TCX

Модуль TCX представляет собой единое программное решение, которое обеспечивает преимущества облачных клиентских вычислений. Для модуля TCX поддерживаются следующие системные среды: службы удаленных рабочих столов Microsoft, виртуальные приложения Citrix и настольные компьютеры, виртуальные приложения Citrix, Teradici и VMware Horizon View. Совместная архитектура системной обработки (CPA), применяемая в TCX, распределяет рабочую нагрузку между сервером и устройствами USB Plug-n-Play. Модуль TCX использует установленные программные протоколы для обеспечения передовых мультимедийных и звуковых технологий для облачных клиентских вычислительных системных сред.

Модуль TCX обеспечивает воспроизведение флеш с широкими функциональными возможностями, поддержку нескольких мониторов, воспроизведение мультимедиа с широкими функциональными возможностями, высококачественные двунаправленные аудиофункции и удобный доступ к устройствам USB для облачных клиентов.

Модуль TCX обеспечивает следующие функции:

- **TCX Flash Acceleration** (Ускорение TCX) и **TCX Flash Redirection** (Перенаправление флеш TCX): повышает производительность видеоконтента флеш в удаленной вычислительной среде;
- **TCX Multidisplay** (Мультидисплей TCX): обеспечивает производительность, расширяя преимущества для облачных клиентов с несколькими мониторами с помощью виртуальных рабочих столов;
- **TCX Multimedia** (Мультимедиа TCX): поддерживает улучшенное воспроизведение MPEG, WAV, WMV, H.264 и других форматов мультимедийных файлов. Программное обеспечение включает в себя сервер и клиентские компоненты, которые перенаправляют задачи обработки мультимедиа между клиентом и сервером для обеспечения восприятия пользователем с широкими функциональными возможностями;
- **TCX Rich Sound**: обеспечивает возможности двунаправленного аудио для виртуальных рабочих столов и приложений, а также поддерживает приложения для записи и воспроизведения звука. Поддерживает бескомпромиссное развертывание;
- **TCX USB Virtualizer**: делает USB-устройства, подключенные к тонким клиентам или конечным точкам, видимыми для виртуальных рабочих столов и приложений. Устраняет любые зависимости от ограниченных драйверов локальных устройств для широкого спектра подключенных посредством USB принтеров, сканеров, устройств хранения данных, КПК Palmtop, BlackBerry, Pocket PC, HID устройств, веб-камер, гарнитур, iPhone, терминалов для оплаты покупок кредитными картами и смарт-карт;
- **TCX Monitor**: помогает эффективно определять состояние системы для правильного функционирования модулей USB и Flash Redirection.

TCX FLASH REDIRECTION

TCX Flash Redirection использует клиентский центральный процессор для дешифрирования и отображения Flash-контента. TCX Flash Redirection использует плагин Adobe Flash Player, который поддерживает интерфейс NPAPI на клиенте. TCX Flash Redirection поддерживает протоколы RDP и PCoIP. TCX Flash Redirection использует меньше циклов серверного центрального процессора.

Обязательные условия

- **TCX.i386.pkg** должен быть установлен на клиенте, чтобы эта функция работала;
- **TFRSServerBHO Class** должен быть включен в надстройках браузера;

- отключена опция **Enable Protected Mode** (Включить защищенный режим) в **Security options** (Параметры безопасности) браузера Internet Explorer;
- включена опция **Enable third-party browser extensions** (Включить сторонние расширения браузера) в **Advanced options** (Дополнительные параметры) браузера Internet Explorer.

Проверка рабочего состояния TCX Flash Redirection

Проверка состояния TCX Flash Redirection аналогична HDX FR. Используйте следующий параметр INI для отображения метки HW:

```
MMRConfig=VIDEO flashingHW=1
```

ПРИМЕЧАНИЕ: TCX FR на ThinOS не работает на некоторых страницах с флеш-видео. При FR по RDP и при FR по PCoIP результаты одинаковы. Перед развертыванием TCX FR на всех системах рекомендуется проверить и заблокировать URL-адрес, который не работает.

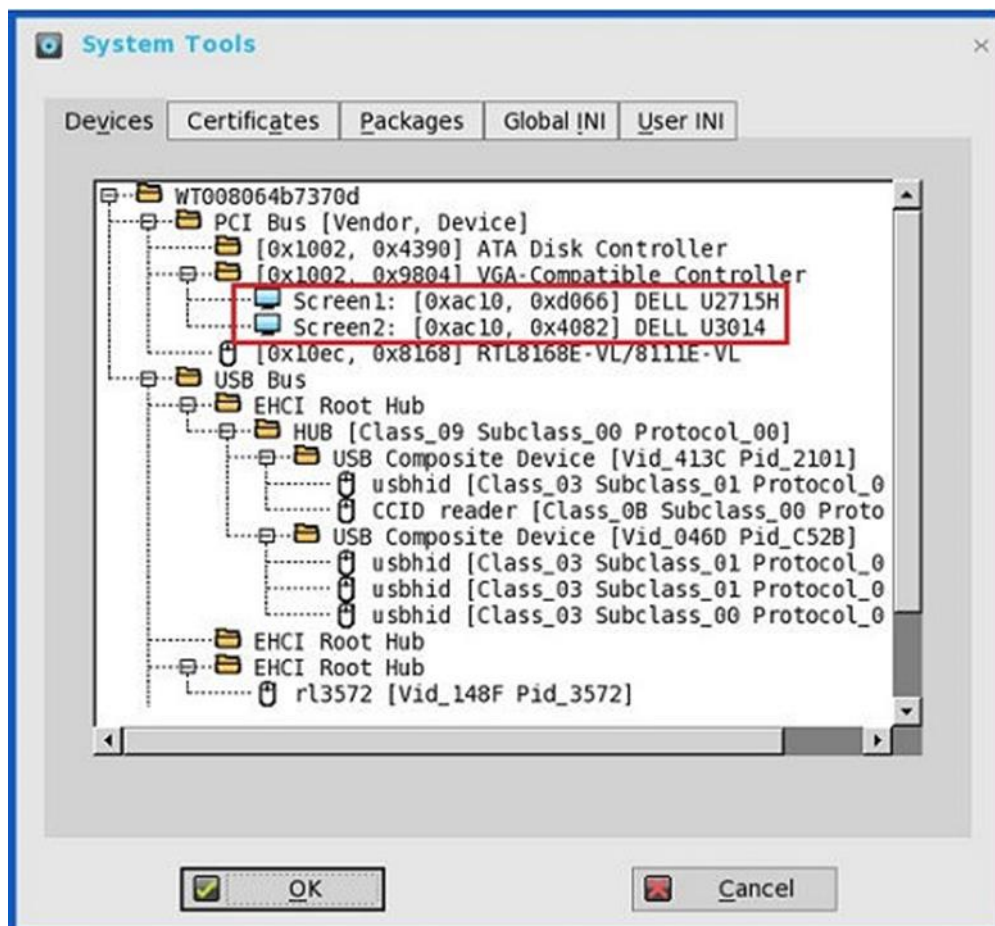
ГЛАВА 7. ВЫПОЛНЕНИЕ ДИАГНОСТИКИ

Эта глава поможет Вам определить и устранить неполадки тонкого клиента с помощью параметров устранения неполадок.

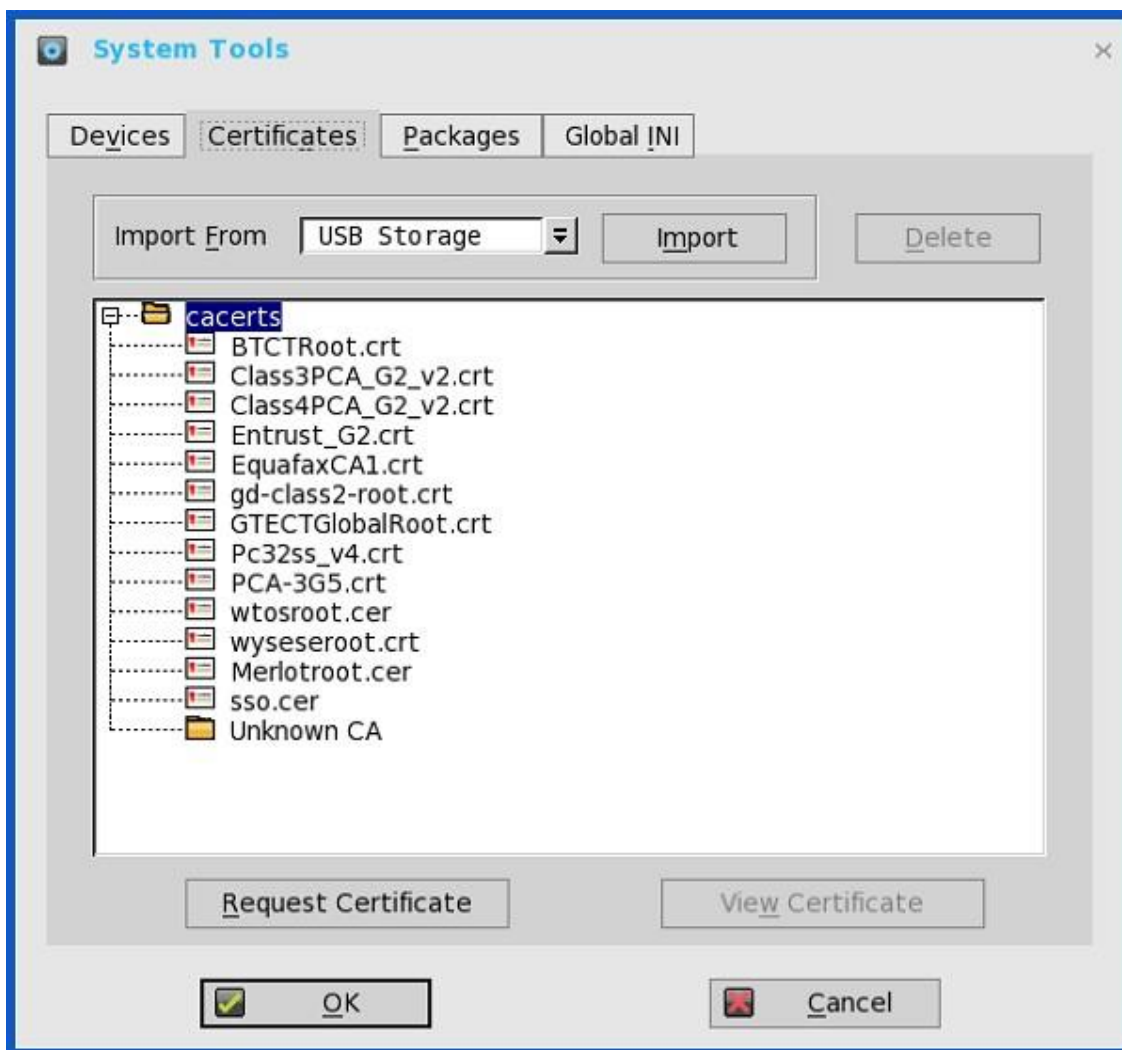
СИСТЕМНЫЕ ИНСТРУМЕНТЫ

Используйте диалоговое окно **System tools** (Системные инструменты) для просмотра сведений об устройстве, программном пакете и информации Global INI/User INI. Также Вы можете импортировать сертификаты, используя вкладку **Certificates** (Сертификаты).

1. В меню на рабочем столе выберите **System Tools** (Системные инструменты). Откроется диалоговое окно **System Tools** (Системные инструменты).
2. Перейдите на вкладку **Devices** (Устройства), там отображаются все локально подключенные устройства, включая USB, последовательный порт и параллельный порт на соответствующих платформах. Также отображаются сведения о мониторах, подключенных к тонкому клиенту.



3. Перейдите на вкладку **Certificates** (Сертификаты) и используйте следующие рекомендации:



- 3.1. Импортируйте сертификаты, выбрав в раскрывающемся списке USB Storage (USB-накопитель) или **File Server** (Файловый сервер), а затем нажмите **Import** (Импорт), чтобы импортировать требуемый сертификат.
- 3.2. Нажмите **Delete** (Удалить), чтобы удалить импортированный сертификат.
- 3.3. Нажмите **View Certificate** (Сертификат), чтобы просмотреть информацию об импортированном сертификате, такую как: версия, срок действия и серийный номер. Также Вы можете просмотреть путь к сертификату и статус сертификата.
- 3.4. Нажмите **Request Certificate** (Запрос сертификата), чтобы вручную запросить сертификат для вашего клиента.
4. Перейдите на вкладку **Packages** (Пакеты) и используйте следующие рекомендации:

Пакеты ThinOS, установленные на тонком клиенте, перечислены на вкладке **Packages** (Пакеты).

- 4.1. Нажмите кнопку **Delete** (Удалить), чтобы удалить выбранный пакет.
- 4.2. Нажмите кнопку **Delete all** (Удалить все), чтобы удалить все пакеты. На вкладке **Package** (Пакет) отображаются следующие пакеты:
- base.i386.pkg;
 - FR.i386.pkg: этот пакет необходим для поддержки Flash Redirection;
 - RTME.i386.pkg: этот пакет необходим для поддержки Citrix RTME.;

- Horizon.i386.pkg: этот пакет необходим для поддержки протокола VMware Blast. Номер версии пакета обновляется в соответствии с последним клиентом Horizon.

Для установки этого пакета необходимо изменить файл INI по установке пакета на AddPkg="horizon".

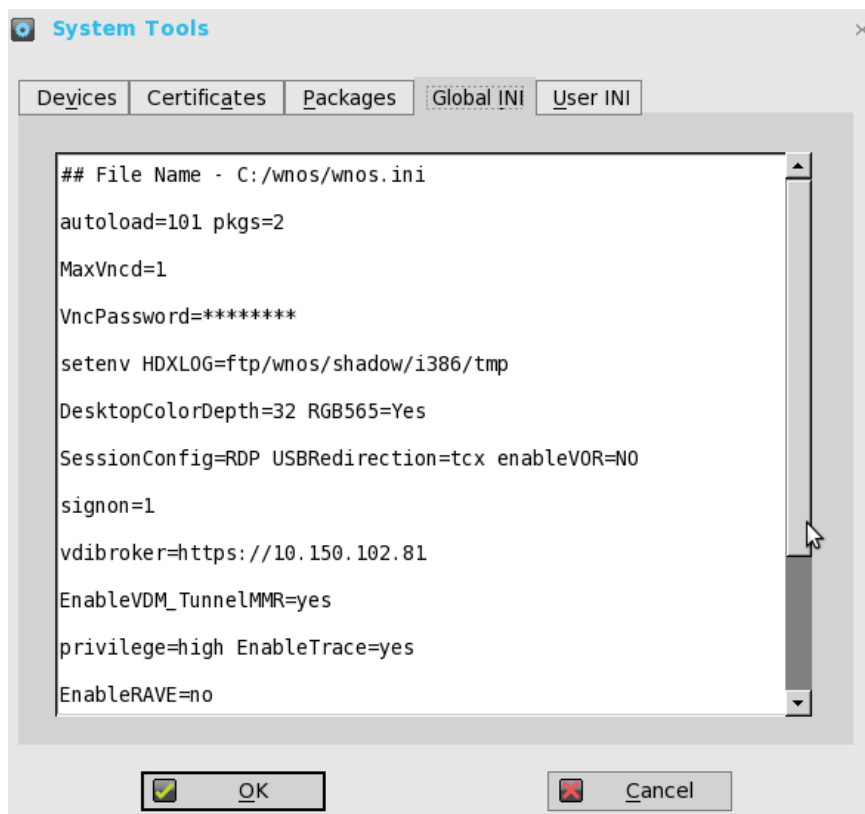
- JVDI.i386.pkg: этот пакет необходим для поддержки Cisco Jabber;
- rcoip.i386.pkg: этот пакет доступен для тонких клиентов СИЛА PC4-1263 с PCoIP, PC4-1210 с PCoIP, PC4-1240 с PCoIP (D10DP), MK2-1240 AIO с PCoIP (5213) и PC4-1242 с PCoIP;
- TCX.i386.pkg: этот пакет необходим для поддержки ТСХ.

Вы не можете удалить базовый пакет отдельно. Если Вы нажмете **Delete All** (Удалить все), будут удалены все пакеты, включая базовый пакет. При нажатии **Delete All** (Удалить все) отображается сообщение, предлагающее перезагрузить устройство.

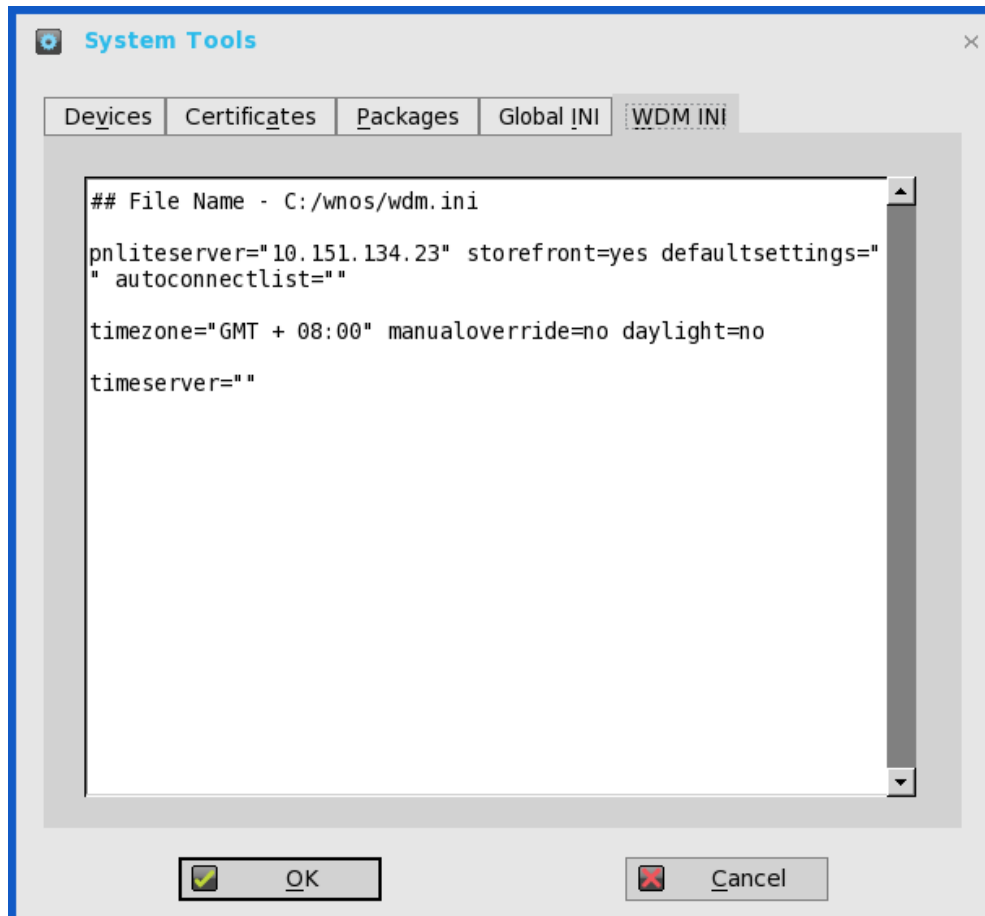
Base.i386.pkg является обязательным для всех клиентов ThinOS. В настоящее время пакет PCoIP является обязательным для тонких клиентов с поддержкой PCoIP. Другие пакеты не являются обязательными. Базовый пакет и пакет PCoIP интегрированы в образ прошивки ThinOS. При установке последнего образа прошивки ThinOS автоматически установится последняя версия этих пакетов на клиент ThinOS. Вы не можете вручную установить или обновить эти встроенные пакеты. Однако сведения о версии соответствующих пакетов отображаются на вкладке **Packages** (Пакеты) только в рамках предоставления технической информации.

ПРИМЕЧАНИЕ: при установке пакетов или перезагрузке устройства ThinOS клиент ThinOS проверяет версию установленного пакета. Если Вы не установили последнюю версию пакета, сведения о текущей версии пакета и рекомендуемой версии пакета отображаются на вкладке Event Log (Журнал событий). В каждом выпуске ThinOS пакеты могут быть обновлены до последней версии.

5. Перейдите на вкладку **Global INI**, чтобы просмотреть информацию wnos.ini.



6. Перейдите на вкладку **User INI**, чтобы просмотреть информацию wnos.ini.
7. Нажмите **WDM INI**, чтобы просмотреть полученные конфигурации WCM.



Функция WCM поддерживается от WDM для комплексной конфигурации клиента. При отсутствии конфигурации с сервера клиент загружает кэшированные настройки (wdm.ini), если они доступны.

Ограничение

Для повышения или понижения версии прошивки/образа через WCM необходимо включить функцию файлового сервера WDM, установив флажок **WTOS INI path upon checkin (FTP/HTTPS/HTTP/CIFS)** (Путь к WTOS INI при регистрации (FTP/HTTPS/HTTP/CIFS)) в настройках WTOS в диспетчере конфигурации WDM.

8. Нажмите **ОК (Да)**, чтобы сохранить настройки.

SIMPLIFIED CERTIFICATE ENROLLMENT PROTOCOL (ПРОТОКОЛ ИНФРАСТРУКТУРЫ PKI)

Протокол SCEP используется в закрытой сети, где все конечные точки являются надежными. Целью SCEP является поддержка безопасной выдачи сертификатов сетевым устройствам в настраиваемой форме. Внутри корпоративного домена он позволяет сетевым устройствам, которые не работают с учетными данными домена, регистрироваться для получения сертификатов от Центра сертификации.

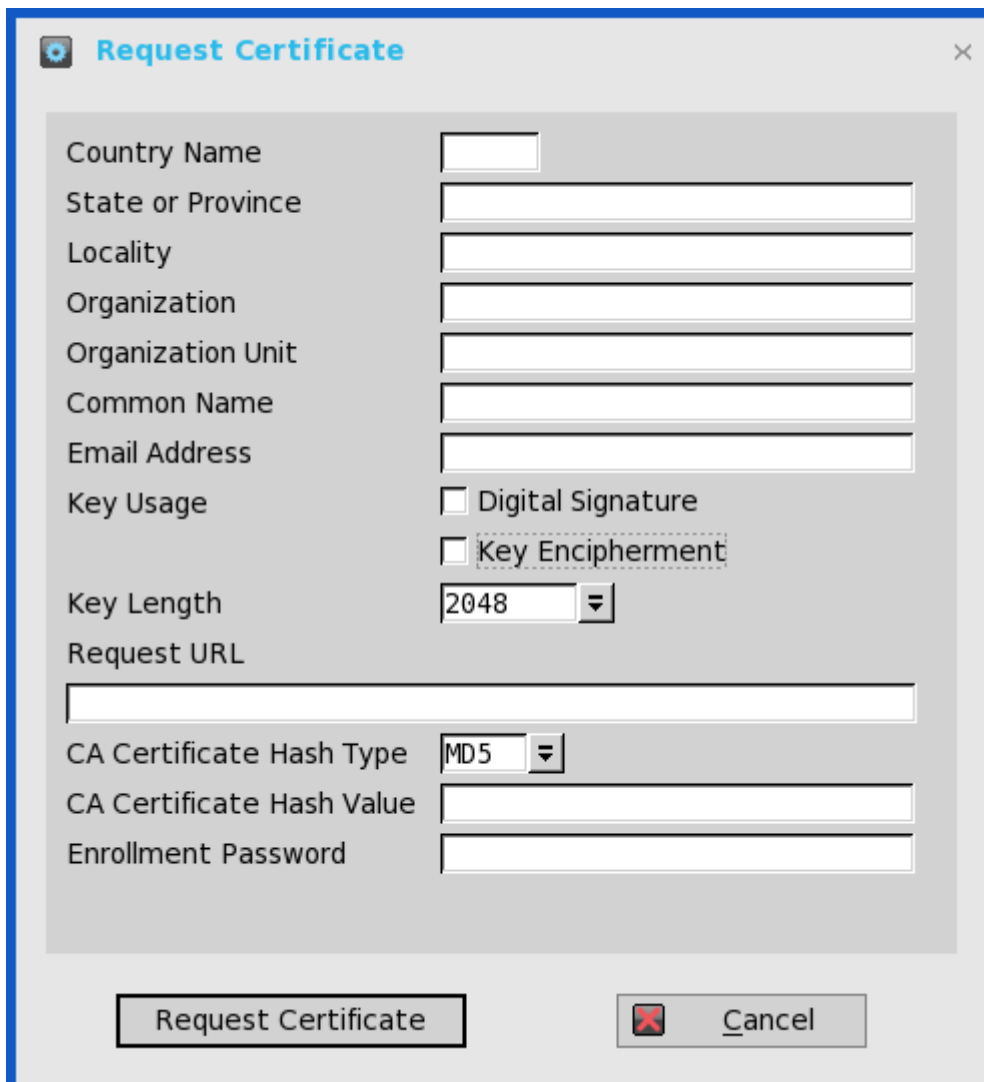
В конце транзакций, определенных в этом протоколе, сетевое устройство имеет закрытый ключ и связанный с ним сертификат, выданный Центром сертификации. Приложения на устройстве могут использовать ключ и связанный с ним сертификат для взаимодействия с другими объектами в сети. Наиболее распространенным использованием этого сертификата на сетевом устройстве является аутентификация устройства в сеансе IPsec.

ThinOS рассматривается как сетевое устройство. Функциональность ThinOS SCEP включает ручной запрос сертификата, автоматический запрос сертификата и автоматическое продление срока действия сертификата.

ЗАПРОС СЕРТИФИКАТА ВРУЧНУЮ

Для запроса сертификата вручную, выполните следующие действия:

1. Перейдите в **System Tools > Certificates > Request Certificate** (Системные инструменты > Сертификаты > Запрос сертификата). Откроется диалоговое окно **Request Certificate** (Запрос сертификата).



The screenshot shows the 'Request Certificate' dialog box with the following fields and options:

- Country Name: [Text input field]
- State or Province: [Text input field]
- Locality: [Text input field]
- Organization: [Text input field]
- Organization Unit: [Text input field]
- Common Name: [Text input field]
- Email Address: [Text input field]
- Key Usage: Digital Signature, Key Encipherment
- Key Length: [Dropdown menu] 2048
- Request URL: [Text input field]
- CA Certificate Hash Type: [Dropdown menu] MD5
- CA Certificate Hash Value: [Text input field]
- Enrollment Password: [Text input field]

Buttons: Request Certificate, Cancel

2. Введите соответствующие значения в этом диалоговом окне и нажмите кнопку **Request Certificate** (Запрос сертификата).

Запрос сертификата отправляется на сервер, клиент получает ответ от сервера и устанавливает сертификат Центра сертификации и сертификат клиента.

3. Нажмите **OK** (Да), чтобы сохранить изменения.

ПРИМЕЧАНИЕ: тип хэша сертификата Центра сертификации в настоящее время поддерживает MD5, SHA1 и SHA256.

URL-адрес сервера может быть ссылкой HTTP или HTTPS. Вы можете добавить префикс протокола перед URL.

АВТОМАТИЧЕСКИЙ ЗАПРОС СЕРТИФИКАТА

Используйте параметры INI для автоматизации запроса и возобновления процесса получения сертификата. Связанные параметры INI имеют глобальную область видимости и должны использоваться с параметром INI ScepAutoEnroll.

О СЕРТИФИКАТАХ ПО УМОЛЧАНИЮ

Сертификаты по умолчанию, встроенные в ThinOS, отображаются в диалоговом окне Certificate (Сертификат). Чтобы просмотреть сертификат по умолчанию, установите для ThinOS заводские настройки по умолчанию и на рабочем столе выберите **System Settings** > **System Tools** > **Certificates** (Системные настройки > Системные инструменты > Сертификаты). Следующие сертификаты по умолчанию отображаются в папке cacerts в формате раскрываемой древовидной структуры:

- BTCTRoot.crt;
- Class3PA_G2_v2.crt;
- Class4PA_G2_v2.crt;
- Entrust_G2.crt;
- EquafaxCA1.crt;
- gd-class2-root.crt;
- GTECTGlobalRoot.crt;
- Pc32ss_v4.crt;
- PCA-3G5.crt.

Чтобы просмотреть каждый сертификат, выберите нужный сертификат и нажмите **View Certificate** (Сертификат). В диалоговом окне **Certificate** (Сертификат) перейдите на любую из следующих вкладок, чтобы просмотреть соответствующие атрибуты сертификата:

1. **General** (Общие): отображаются следующие параметры:
 - назначение сертификата;
 - сертификат выдан (кому);
 - сертификат выдан (кем);
 - срок действия сертификата.
2. **Details** (Сведения): сведения о сертификате перечислены вместе с соответствующими значениями по умолчанию. Информацию об отдельных сертификатах смотрите в разделе **Certificate Details** (Сведения о сертификате).
3. **Certification Path** (Путь к сертификату): отображается путь к папке, в которой хранится сертификат. Статус сертификата можно посмотреть в нижней части окна.

СВЕДЕНИЯ О СЕРТИФИКАТЕ

В этом разделе перечислены сертификаты с действительными атрибутами и соответствующими значениями по умолчанию.

Название сертификата — BTCTRoot.crt.

Таблица 38. Сведения о сертификате BTCTRoot.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V3
Серийный номер	02 00 00 b9
Алгоритм подписи	sha1RSA
Поставщик	Baltimore CyberTrust Root CN=Baltimore CyberTrust Root OU=CyberTrust O=Baltimore C=IE
Действителен с	2000-05-12 18:46:00
Действителен по	2025-05-12 23:59:00
Субъект	Baltimore CyberTrust Root CN=Baltimore CyberTrust Root OU=CyberTrust O=Baltimore C=IE
Открытый ключ	RSA (2048 бит) Бит ключа отображается в нижней части окна
Использование ключа	Получение сертификата, создание списка отозванных сертификатов (CRL)
Идентификатор ключа субъекта	e5 9d 59 30 82 47 58 cc ac fa 08 54 36 86 7b 3a b5 04 4d f0
Основные ограничения	Subject Type=CA, Path Length Constraints=None
Алгоритм отпечатка	sha1
Отпечаток	d4 de 20 d0 5e 66 fc 53 fe la 50 88 2c 78 db 28 52 ca e4 74

Таблица 39. Сведения о сертификате Class3PCA_G2_v2.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V1
Серийный номер	7d d9 fe 07 cf a8 le b7 10 79 67 fb a7 89 34 c6
Алгоритм подписи	sha1RSA
Поставщик	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. — только для санкционированного использования OU=Class 3 Public Primary Certification Authority — G2 O=VeriSign, Inc C=US
Действителен с	1998–05–18 00:00:00
Действителен по	2028–08–12 23:59:59
Субъект	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. — только для санкционированного использования OU=Class 3 Public Primary Certification Authority — G2 O=VeriSign, Inc. C=US
Открытый ключ	RSA (1024 бита) Бит ключа отображается в нижней части окна
Алгоритм отпечатка	sha1
Отпечаток	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

Название сертификата — Class4PCA_G2_v2.crt.

Таблица 40. Сведения о сертификате Class4PCA_G2_v2.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V1
Серийный номер	32 88 8e 9a d2 f5 eb 13 47 f8 7f c4 20 37 25 f8
Алгоритм подписи	sha1RSA
Поставщик	VeriSign Trust Network
	OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. — только для санкционированного использования OU=Class 4 Public Primary Certification Authority — G2 O=VeriSign, Inc. C=US
Действителен с	1998–05–18 00:00:00
Действителен по	2028–05–01 23:59:59
Субъект	VeriSign Trust Network OU=VeriSign Trust Network OU=(c) 1998 VeriSign, Inc. — только для санкционированного использования OU=Class 4 Public Primary Certification Authority — G2 O=VeriSign, Inc. C=US
Открытый ключ	RSA (1024 бита) Бит ключа отображается в нижней части окна
Алгоритм отпечатка	sha1
Отпечаток	0b 77 be bb cb 7a a2 47 05 de cc 0f bd 6a 02 fc 7a bd 9b 52

Таблица 41. Сведения о сертификате Entrust_G2.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V3
Серийный номер	4a 53 8c 28
Алгоритм подписи	sha256RSA
Поставщик	Entrust Root Certification Authority CN=Entrust Root Certification Authority—G2 OU=(c) 2009 Entrust, Inc. — только для санкционированного использования OU=Смотрите entrustdatacard.com/resource-center/licensing-and-agreements O=Entrust, Inc. C=US
Действителен с	2009–07–07 17:25:54
Действителен по	2030–12–07 17:55:54
Субъект	Entrust Root Certification Authority CN=Entrust Root Certification Authority—G2 OU=(c) 2009 Entrust, Inc. — только для санкционированного использования OU=Смотрите entrustdatacard.com/resource-center/licensing-and-agreements O=Entrust, Inc. C=US
Открытый ключ	RSA (2048 бит) Бит ключа отображается в нижней части окна
Поле сертификата	Значение/формат по умолчанию
Использование ключа	Получение сертификата, создание списка отозванных сертификатов (CRL)
Идентификатор ключа субъекта	6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Основные ограничения	Subject Type=CA, Path Length Constraints=None
Алгоритм отпечатка	sha1
Отпечаток	8c f4 27 fd 79 0c 3a d1 66 06 8d e8 1e 57 ef bb 93 22 72 d4

Название сертификата — EquifaxCA1.crt.

Таблица 42. Сведения о сертификате EquifaxCA1.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V3
Серийный номер	04
Алгоритм подписи	md5RSA
Поставщик	Equifax Secure eBusiness CN=Equifax Secure eBusiness CA-1 O=Equifax Secure Inc. C=US
Действителен с	1999-06-21 04:00:00
Действителен по	2020-06-21 04:00:00
Субъект	Equifax Secure eBusiness CN=Equifax Secure eBusiness CA-1 O=Equifax Secure Inc. C=US
Открытый ключ	RSA (1024 бита) Бит ключа отображается в нижней части окна
Использование ключа	Цифровая подпись, шифрование ключей, шифрование данных, согласование ключей, получение сертификата, создание списка отозванных сертификатов (CRL), толь- ко шифрование, только расшифровка
Идентификатор ключа субъекта	4a 78 32 52 11 db 59 16 36 5e df c1 14 36 40 6a 47 7c 4c a1
Идентификатор ключа Центра сертификации	80 14 4a 78 32 52 11 db 59 16 36 5e df c1 14 36 40 6a 47 7c 4c a1
Основные ограничения	Subject Type=CA, Path Length Constraints=None
Алгоритм отпечатка	sha1
Отпечаток	da 40 18 8b 91 89 a3 ed ee ae da 97 fe 2f 9d f5 b7 d1 8a 41

Таблица 43. Сведения о сертификате gd-class2–root.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V3
Серийный номер	00
Алгоритм подписи	sha1RSA
Поставщик	Go Daddy Class 2 Certification Authority OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
Действителен с	2004–06–29 17:06:20
Действителен по	2034–06–29 17:06:20
Субъект	Go Daddy Class 2 Certification Authority OU=Go Daddy Class 2 Certification Authority O=The Go Daddy Group, Inc. C=US
Открытый ключ	RSA (2048 бит) Бит ключа отображается в нижней части окна
Использование ключа	Цифровая подпись, шифрование ключей, шифрование данных, согласование ключей, получение сертификата, создание списка отозванных сертификатов (CRL), только шифрование, только расшифровка
Идентификатор ключа субъекта	d2 c4 b0 d2 91 d4 4c 11 71 b3 61 cb 3d a1 fe dd a8 6a d4 e3
Идентификатор ключа Центра сертификации	Бит ключа отображается в нижней части окна
Основные ограничения	Subject Type=CA, Path Length Constraints=None
Алгоритм отпечатка	sha1
Отпечаток	27 96 ba e6 3f 18 01 e2 77 26 1b a0 d7 77 70 02 8f 20 ee e4

Название сертификата — GTECTGlobalRoot.crt.

Таблица 44. Сведения о сертификате GTECTGlobalRoot.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V1
Серийный номер	01 a5
Алгоритм подписи	md5RSA
Поставщик	GTE CyberTrust Global Root CN=GTE CyberTrust Global Root OU=GTE CyberTrust Solutions, Inc.O=GTE Corporation C=US
Действителен с	1998-08-13 00:29:00
Действителен по	2018-08-13 23:59:00
Субъект	GTE CyberTrust Global Root CN=GTE CyberTrust Global Root OU=GTE CyberTrust Solutions, Inc. O=GTE Corporation C=US
Алгоритм отпечатка	sha1
Отпечаток	97 81 79 50 d8 1c 96 70 cc 34 d8 09 cf 79 44 31 36 7e f4 74

ThinOS 8.6

Название сертификата — Pc32ss_v4.crt.

Таблица 45. Сведения о сертификате Pc32ss_v4.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V1
Серийный номер	70 ba e4 1d 10 d9 29 34 b6 38 ca 7b 03 cc ba bf
Алгоритм подписи	md2RSA
Поставщик	Class 3 Public Primary Certification Authority OU=Class 3 Public Primary Certification Authority O=VeriSign, Inc. C=US
Действителен с	1996-01-29 00:00:00
Действителен по	2028-08-01 23:59:59
Субъект	Class 3 Public Primary Certification Authority OU=Class 3 Public Primary Certification Authority O=VeriSign, Inc. C=US
Открытый ключ	RSA (1024 бита) Бит ключа отображается в нижней части окна
Алгоритм отпечатка	sha1
Отпечаток	74 2c 31 92 e6 07 e4 24 eb 45 49 54 2b e1 bb c5 3e 61 74 e2

Название сертификата — PCA-3G5.crt.

Таблица 46. Сведения о сертификате PCA-3G5.crt.

Поле сертификата	Значение/формат по умолчанию
Версия	V3
Серийный номер	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Алгоритм подписи	sha1RSA
Поставщик	VeriSign Class 3 Public Primary Certification Authority — G5 CN=VeriSign Class 3 Public Primary Certification Authority — G5 OU=(c) 2006 VeriSign, Inc. — только для санкцио- нированного использования OU=VeriSign Trust Network O=VeriSign, Inc. C=US
Действителен с	2006–11–08 00:00:00
Действителен по	2036–07–16 23:59:00
Субъект	VeriSign Class 3 Public Primary Certification Authority — G5 CN=VeriSign Class 3 Public Primary Certification Authority — G5 OU=(c) 2006 VeriSign, Inc. — только для санкцио- нированного использования OU=VeriSign Trust Network O=VeriSign, Inc. C=US
Открытый ключ	RSA (2048 бит) Бит ключа отображается в нижней части окна
Использование ключа	Получение сертификата, создание списка отозванных сертификатов (CRL)
Идентификатор ключа субъекта	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Основные ограничения	Subject Type=CA, Path Length Constraints=None
Алгоритм отпечатка	sha1
Отпечаток	4e b6 d5 78 49 9b 1c cf 5f 58 le ad 56 be 3d 9b 67 44 a5 e5

УСТРАНЕНИЕ НЕПОЛАДОК

Используйте диалоговое окно **Troubleshooting** (Устранение неполадок) для настройки параметров трассировки и журнала событий, графиков монитора производительности, которые отображают информацию о центральном процессоре, памяти и сети клиента, а также управления CMOS для извлечения и восстановления параметров CMOS. Оно также позволяет просматривать кэшированную информацию wpos.ini в целях устранения неполадок.

Для устранения неполадок:

1. В меню на рабочем столе нажмите **Troubleshooting** (Устранение неполадок). Откроется диалоговое окно **Troubleshooting** (Устранение неполадок).
2. Перейдите на вкладку **General** (Общие) и выполните следующие действия:

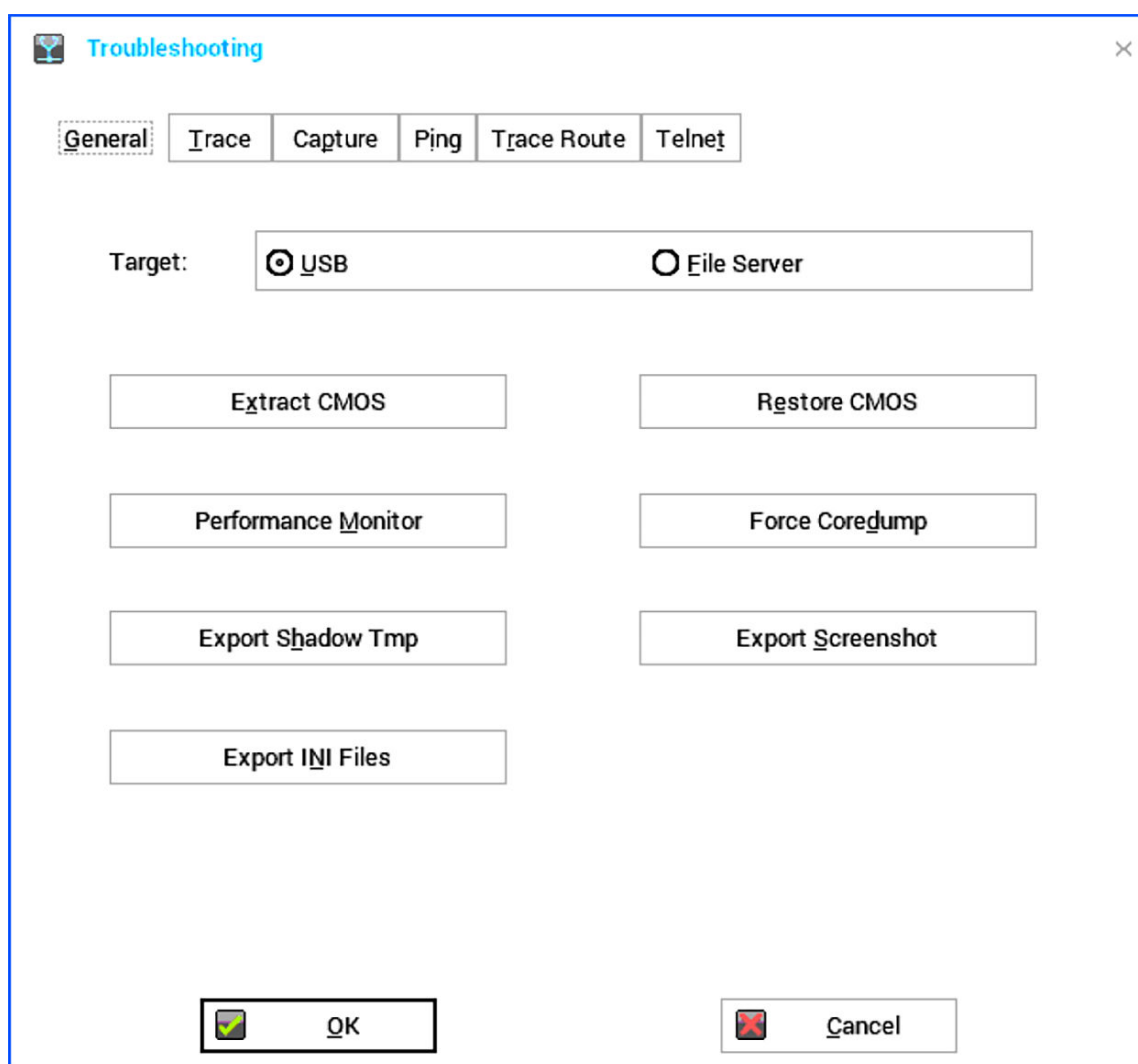


Рисунок 36. Вкладка General.

- 2.1. Нажмите либо **USB** либо **File Server** (Файловый сервер), чтобы выбрать целевое устройство, которое необходимо использовать для управления CMOS.
- 2.2. **Extract CMOS** (Извлечение CMOS): выберите этот параметр, чтобы извлечь параметры CMOS и некоторые параметры BIOS на USB-накопитель или файловый сервер в зависимости от выбранного целевого устройства. ThinOS считывает параметры CMOS с помощью интерфейса SMBIOS для Standard BIOS и интерфейса CMOS для устаревшего/традиционного BIOS.

ПРИМЕЧАНИЕ: Вы можете извлечь только те параметры BIOS, которые поддерживаются параметрами INI Device=CMOS и Device=DellCMOS.

- 2.3. **Restore CMOS** (Восстановление CMOS): выберите этот параметр, чтобы записать параметры CMOS и BIOS с USB-накопителя на целевой тонкий клиент.

ПРИМЕЧАНИЕ: Вы можете восстановить параметры BIOS, которые поддерживаются параметрами INI Device=CMOS и Device=DellCMOS.

- 2.4. **Performance Monitor** (Монитор производительности): выберите этот параметр, чтобы отобразить историю использования центрального процессора с информацией о кадровой частоте (FPS), памяти и сети. Графики отображаются в верхней части всех окон.
- 2.5. **Force Coredump** (Принудительное создание дампа памяти): используйте этот параметр, чтобы принудительно генерировать информацию об отладке для технического обследования, когда система не отвечает. Файл coredump и информация о прерываниях сохраняются на локальном диске. После перезагрузки тонкого клиента файл coredump и снимок экрана с прерываниями загружаются в директорию /wnos/Troubleshoot/ файлового сервера или USB-накопителя.
- 2.6. **Export Shadow Tmp** (Экспорт теневых копий временных журналов): используйте этот параметр для экспорта временных журналов с целью отладки. Все файлы журнала можно экспортировать на USB-накопитель или файловый сервер в зависимости от целевой конфигурации.
- 2.7. **Export Screenshot** (Экспорт снимков экрана): используйте этот параметр для экспорта снимков экрана на файловый сервер или USB-накопитель. К имени экспортированного файла добавляется информация о сборке для более эффективного устранения неполадок. Если в буфере обмена присутствует снимок экрана, он экспортируется в целевое местоположение. Если снимок экрана недоступен, полный экран автоматически копируется и экспортируется в целевое местоположение.
- 2.8. **Export INI files** (Экспорт файлов INI): используйте этот параметр для экспорта глобального файла INI (wnos.ini или хен.ini), wdm.ini, ccm.ini, mac.ini или другого файла INI на файловый сервер или USB-накопитель. Только файл username.ini не может быть экспортирован.

3. Перейдите на вкладку **Trace** (Трассировка), чтобы настроить действия трассировки и задержку при трассировке. Доступные параметры для действия трассировки: **None** (Нет), **Capture** (Захват) и **Playback** (Воспроизведение).

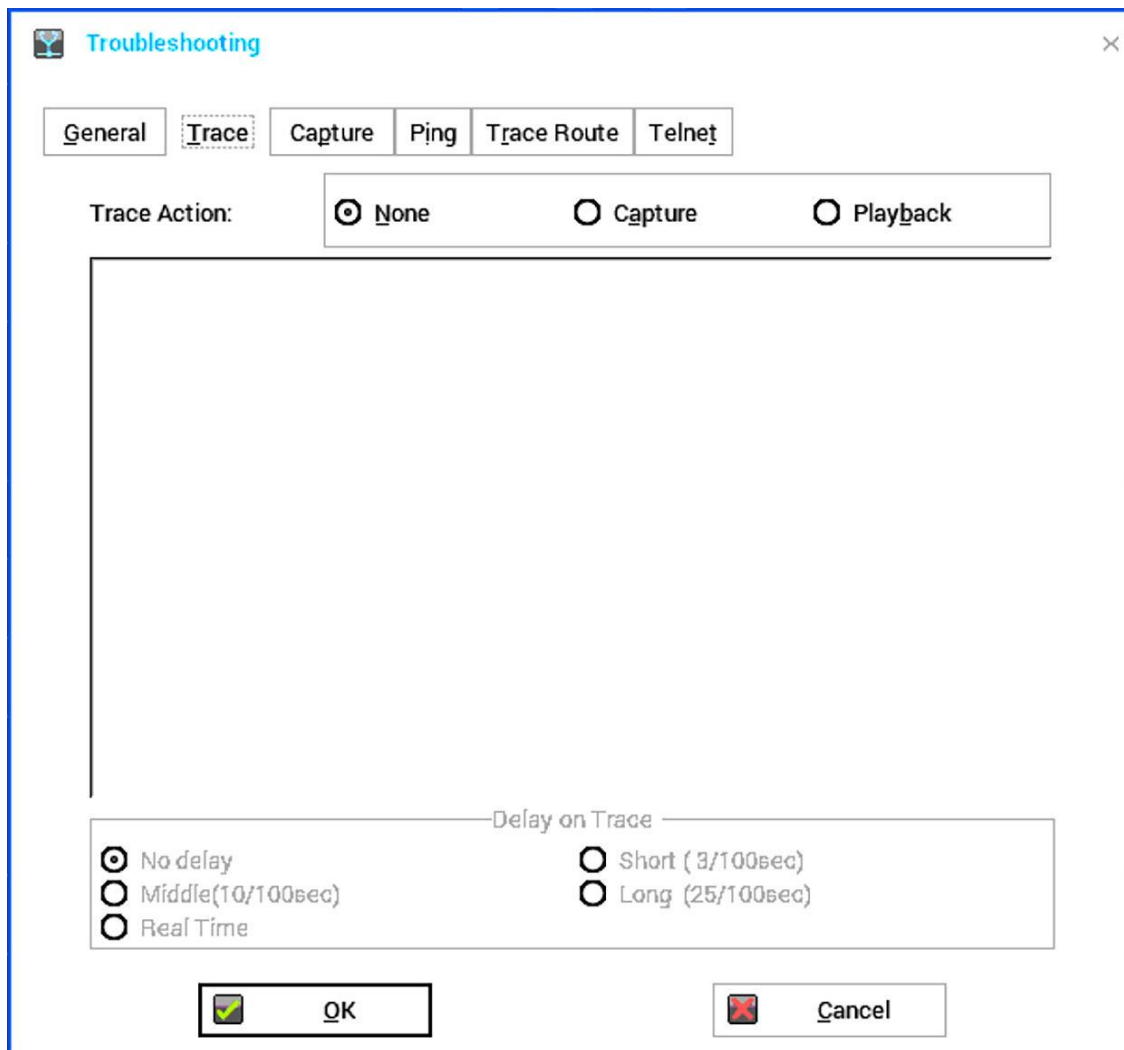
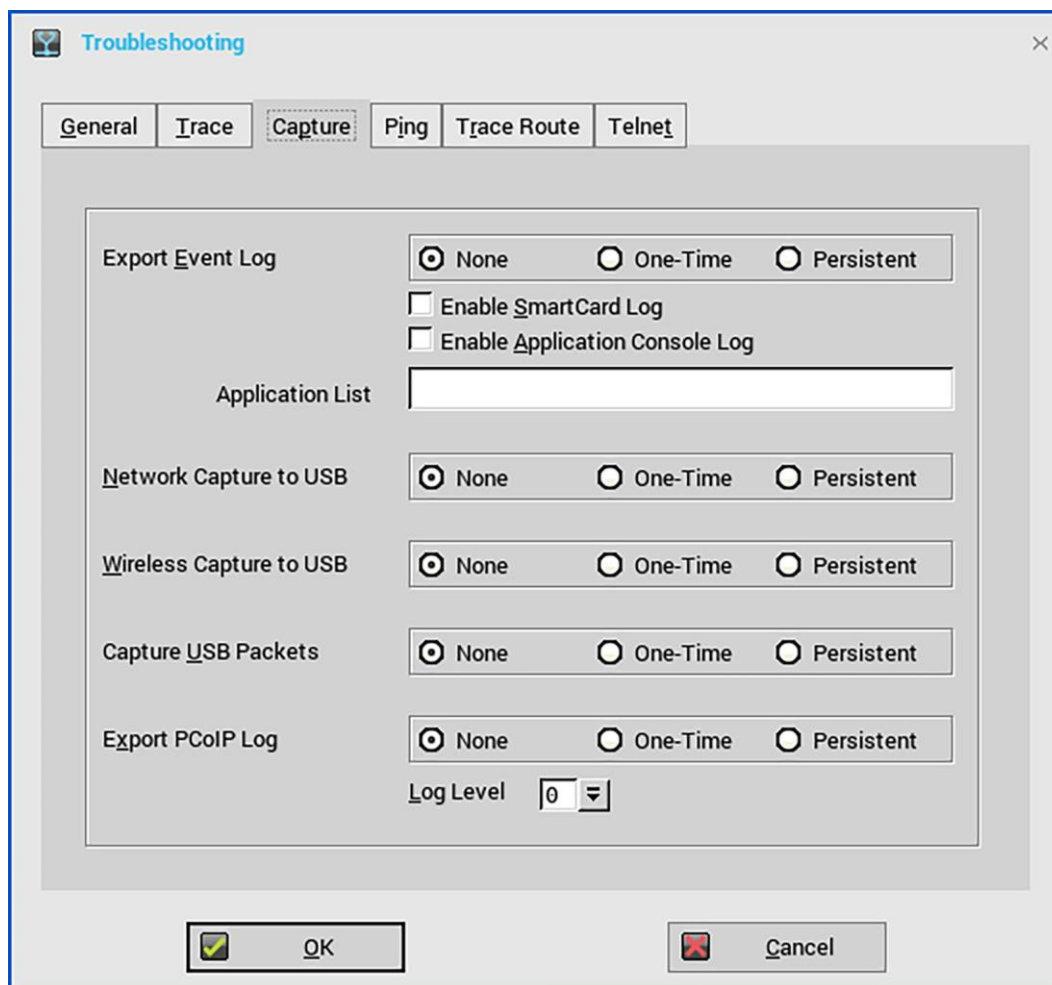


Рисунок 37. Вкладка Trace (Трассировка).

4. Перейдите на вкладку **Capture** (Захват) и настройте экспорт журнала событий, запись параметров сети, запись параметров беспроводной сети и запись данных, переданных с USB-устройств, в соответствии с вашими требованиями.

Рисунок 38. Вкладка **Capture** (Захват).

- 4.1. **Export Event log** (Экспорт журнала событий): выберите параметр **One-time** (Однократный) или **Persistent** (Постоянный), чтобы включить ведение журнала любых неожиданных сообщений об ошибках. Вы можете отключить ведение журнала и проверить файл журнала в папке ftp://wnos/problem_shoot. Убедитесь, что активирована опция **Enable Trace** (Включить трассировку) параметра Privilege (Привилегия) в файле wnos.ini.
- 4.2. **Enable SmartCard log** (Включить журнал смарт-карты): чтобы разрешить клиенту регистрировать сообщения об ошибках смарт-карты, установите флажок Enable SmartCard log (Включить журнал смарт-карты).
- 4.3. **Enable Application Console Log** (Включить журнал консоли приложения): чтобы разрешить клиенту регистрировать сообщения об ошибках консоли приложения, установите флажок Enable Application Console Log (Включить журнал консоли приложения). Все журналы сохраняются в папке trouble_shoot в файле с именем TerminalName_proc_name_date_time.log.

В поле **Application List** (Список приложений) введите имя приложения, для которого требуется создать журналы. Имя в списке может быть частью имени приложения. Например, именем приложения PCoIP является /rcoip/rcoip, а имя приложения Blast — /usr/lib/vmware/view/usb/horizon. Если Вы хотите создать журналы для приложений PCoIP и Blast, введите rcoip;vmware в поле **Application List** (Список приложений). По умолчанию фильтры **Application List** (Списка приложений) не применяются, и все журналы сохраняются в целевой папке.

- 4.4. **Network capture to USB** (Захват параметров сети на USB): выберите параметр **One-time** (Однократный) или **Persistent** (Постоянный), чтобы включить запись информации о сети. При включении этого параметра трассировка сети всего трафика, входящего и исходящего от тонкого клиента, записывается на USB-накопитель, вставленный в тонкий клиент.

После входа и использования сервера или сети Citrix Apps and Desktops Вы можете просмотреть файл `/wnos/Troubleshoot/[Имя терминала]_[ENET или WS].[Date_Time].pcap` на USB-накопителе. Вы можете проводить анализ с помощью программного обеспечения, такого как анализатор пакетов, который используется для устранения неполадок в сети и анализа сетевой активности.

Например, для Ethernet имя файла — `yx008064b2bfd7_ENET.20150415_064455.pcap`. Для беспроводной сети имя файла — `yx008064b2bfd7_WS.20150415_064455.pcap`.

ПРИМЕЧАНИЕ: убедитесь, что Вы вставили USB-накопитель в тонкий клиент, прежде чем выбрать опцию записи параметров сети. Если USB-накопитель не вставлен и Вы выходите из диалогового окна, запись параметров сети автоматически сбрасывается.

- 4.5. **Wireless capture to USB** (Захват параметров беспроводной сети на USB): выберите параметр **One-time** (Однократный) или **Persistent** (Постоянный), чтобы включить захват информации о беспроводной сети. При включении этого параметра трассировка беспроводной сети всего трафика, входящего и исходящего от тонкого клиента, записывается на USB-накопитель, вставленный в тонкий клиент.
- 4.6. **Capture USB Packets** (Захват USB-пакетов): выберите параметр **One-time** (Однократный) или **Persistent** (Постоянный), чтобы включить захват USB-пакетов.
- 4.7. **Export PCoIP log** (Экспорт журналов PCoIP): выберите параметр **One-time** (Однократный) или **Persistent** (Постоянный), чтобы экспортировать журналы PCoIP на клиентах с поддержкой PCoIP.
5. Перейдите на вкладку **Ping** (Проверка соединений) и используйте следующие рекомендации, чтобы запустить утилиту диагностики ping и отобразить ответные сообщения:



Рисунок 39. Вкладка Ping (Проверка соединений)

- 5.1. **Enter Hostname or IP** (Введите имя хоста или IP-адрес): введите IP-адрес, имя DNS-хоста или имя WINS-хоста целевого объекта для проверки соединения
- 5.2. **Data area** (Область данных): отображает ответные сообщения при проверке соединения. Команда ping отправляет один эхо-запрос в секунду, рассчитывает время прохождения сигнала в обоих направлениях и статистику потери пакетов и отображает краткую сводку по завершении расчета.
- 5.3. **Start** (Старт): выполняет команду ping. Если хост работает и находится в сети, он отвечает на эхо-запрос. По умолчанию эхо-запросы отправляются до тех пор, пока это не будет прервано нажатием кнопки **Stop** (Стоп).
- 5.4. **Stop** (Стоп): завершает отправку запросов, оставив диалоговое окно **Ping** (Проверка соединений) открытым, чтобы Вы могли прочитать сводку, расположенную в области данных.

ПРИМЕЧАНИЕ: Ping отправляет эхо-запрос на хост сети. Параметр хоста является допустимым именем хоста или IP-адресом. Если хост работает и находится в сети, он отвечает на эхо-запрос. Ping отправляет один эхо-запрос в секунду и рассчитывает время прохождения сигнала в обоих направлениях и статистику потери пакетов. В результате расчета отображается краткая сводка.

Утилита ping может быть использована для следующих задач:

- определения состояния сети и различных внешних хостов;
- отслеживания и выявления проблем аппаратного и программного обеспечения;
- тестирования, измерения и управления сетями;
- определения IP-адреса хоста, если известно только имя хоста.

ПРИМЕЧАНИЕ: не все сетевое оборудование реагирует на пинг-пакеты, так как данный механизм может использоваться для атак, с целью спровоцировать отказ в обслуживании. Отсутствие ответа не обязательно указывает на то, что цель пинга недоступна для последующего подключения.

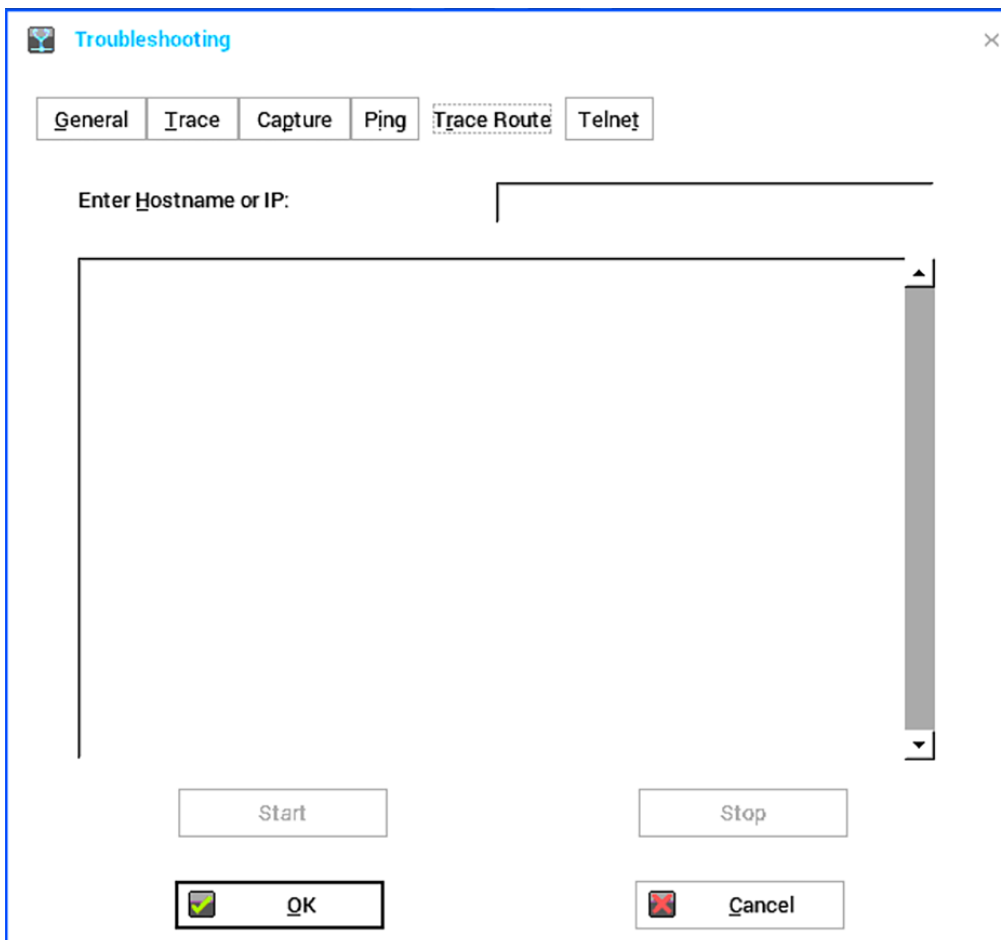


Рисунок 40. Вкладка Trace route (Трассировка маршрута).

6. Перейдите на вкладку **Trace Route** (Трассировка маршрута) и используйте следующие рекомендации, чтобы запустить утилиту диагностики `tracert` и отобразить ответные сообщения:
 - 6.1. **Enter Hostname or IP** (Введите имя хоста или IP-адрес): введите IP-адрес, имя DNS-хоста или имя WINS-хоста целевого объекта для трассировки.
 - 6.2. **Data area** (Область данных): отображает время отклика при прохождении сигнала в обоих направлениях и идентифицирующую информацию для каждого устройства в пути.
 - 6.3. **Start** (Старт): выполняет команду `tracert`.
 - 6.4. **Stop** (Стоп): завершает команду `tracert`, оставив диалоговое окно **Trace Route** (Трассировка маршрута) открытым, чтобы Вы могли прочитать информацию, расположенную в области данных.

Утилита `tracert` отслеживает путь от тонкого клиента до сетевого хоста. Параметр хоста является допустимым именем хоста или IP-адресом. Утилита `tracert` отправляет пакет информации каждому устройству (маршрутизаторам и компьютерам) в пути три раза и отображает время отклика при прохождении сигнала в обоих направлениях и идентифицирующую информацию в окне сообщения.

7. Перейдите на вкладку **Telnet** и выполните следующие действия:

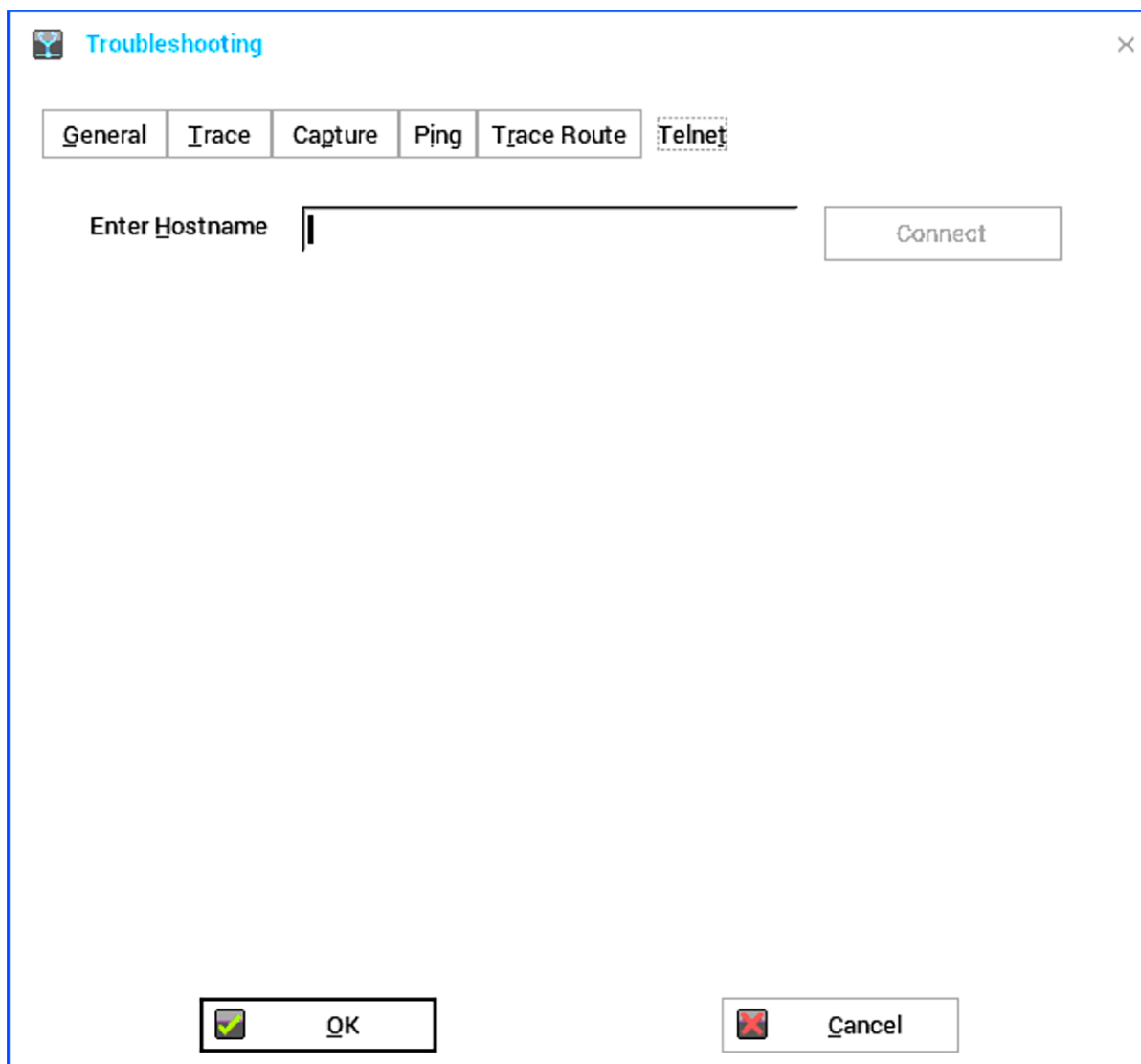


Рисунок 41. Вкладка Telnet

- 7.1. Введите имя хоста.
- 7.2. Нажмите **Connect** (Подключиться), чтобы подключиться к удаленному хосту или устройству.

Отображается окно Telnet, окно устранения неполадок закрывается автоматически.

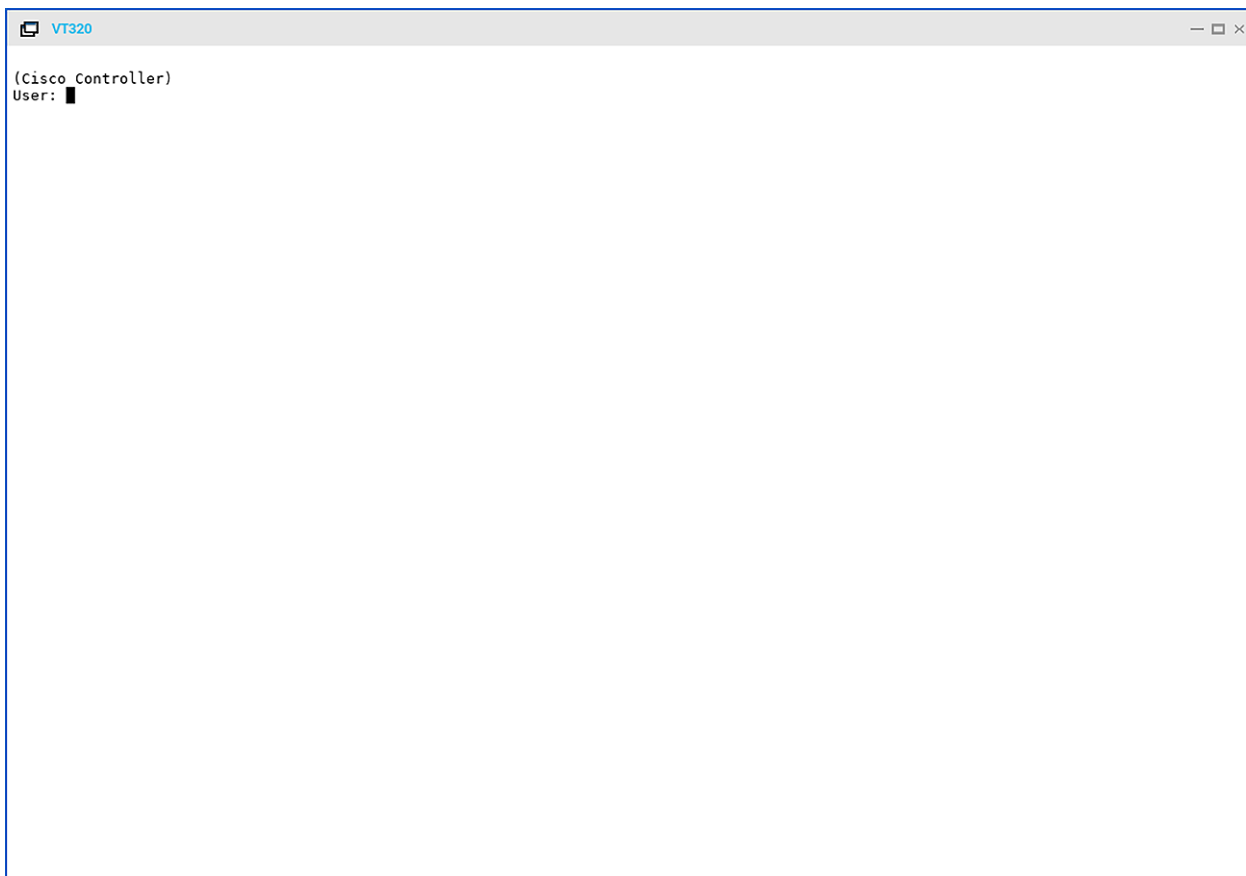


Рисунок 42. Окно Telnet

8. Нажмите **OK** (Да), чтобы сохранить настройки.

ГЛАВА 8. УПРАВЛЕНИЕ BIOS НА THINOS

В этом приложении описывается управление BIOS на устройствах ThinOS с BIOS (CMOS) или Standard BIOS.

Чтобы обеспечить управление BIOS, согласованное между BIOS и Standard BIOS, для BIOS введен параметр INI Device=Cmos, а для Standard BIOS — параметр Device=DellCmos.

Если для конфигурации BIOS настроен пароль, то Вы должны вводить соответствующий пароль для обновления любых настроек. Например, параметр INI для обновления настроек должен сопровождаться “CurrentPassword={}”. Это обязательно для Dell BIOS.

После обновления BIOS на тонком клиенте СИЛА PC4-1240, МК2-1240, PC4-1243, PC4-1242 и PC4-1263 с помощью файлового сервера управление BIOS может оказаться невозможным до тех пор, пока Вы самостоятельно не войдете и не выйдете из меню конфигурации BIOS. Это связано с несоответствием CMOS. Чтобы устранить эту проблему выполните следующие действия:

1. Запустите устройство и нажмите клавишу **Delete** во время загрузки, чтобы войти в меню BIOS.
2. Введите пароль BIOS.
3. Нажмите **F10**, чтобы сохранить настройки BIOS и устранить несоответствие CMOS.

МАТРИЦА ФУНКЦИОНАЛЬНОСТИ BIOS

Таблица 47. Матрица функциональности BIOS.

Основное требование	Параметр INI для управления BIOS	PC4-1240, МК2-1240, PC4-1243	PC4-1242	PC4-1263	PC4-1210
Включение питания без звуковых сигналов	Н/Д	Да	Да	Да	Да
Обновление BIOS с файлового сервера	Н/Д	Да	Да	Да	Да
Изменение пароля BIOS с помощью INI	Device=DellCmos CurrentPassword={} NewPassword={} Device=Cmos CurrentPassword={}	Да	Да	Да	Да

Основное требование	Параметр INI для управления BIOS	PC4-1240, MK2-1240, PC4-1243	PC4-1242	PC4-1263	PC4-1210
	NewPassword={}				
Изменение порядка загрузки с помощью INI	Device=cmos BootOrder={PXE, HardDisk, USB}	Да	Да	Да	Не применимо
Включение/выключение отображения посредством PXE с помощью INI	Device=DellCmos PXEBootSupport={yes, no}	Не применимо	Не применимо	Не применимо	Да
Включение/выключение отображения посредством USB с помощью INI	Device=cmos BootFromUSB={yes, no} Device=DellCmos USBBootSupport={yes, no}	Да	Да	Да	Да
Управление восстановлением при отключении питания с помощью INI	Device=cmos AutoPower={yes, no} Device=DellCmos ACRecovery={PowerOff, PowerOn, LastState}	Да	Да	Да	Да
Управление автоматическим режимом с установлением точного времени с помощью INI	Device=DellCmos AutoPower={Disable, Daily, Workday} AutoPowerTime=hh:mm De-	Да	Да	Да	Да

Основное требование	Параметр INI для управления BIOS	PC4-1240, MK2-1240, PC4-1243	PC4-1242	PC4-1263	PC4-1210
	<pre> vice=Cmos AutoPowerDate=yes AutoPowerTime=2:30:30 </pre>				
	<pre> AutoPowerDays=Sunday; Fri day </pre>				
Извлечение и восстановление CMOS	<pre> Device=cmos Action={extract, restore} CurrentPassword={} Device=DellCmos Action={extract, restore} CurrentPassword={} </pre>	Да	Да	Да	Да
Управление аудио с помощью INI	<pre> Device=cmos OnboardAudio={yes, no} Device=DellCmos Audio={yes, no} </pre>	Да	Да	Да	Да
Управление USB-портом с помощью INI	<pre> Device=cmos USBController={yes, no} Device=DellCmos USBRearPort={yes, no} USBFrontPort={yes, no} (Rear/Front for Dell BIOS only) </pre>	Да	Да	Да	Да

Основное требование	Параметр INI для управления BIOS	PC4-1240, MK2-1240, PC4-1243	PC4-1242	PC4-1263	PC4-1210
Управление блокировкой администратора с помощью INI	Device=DellCmos AdminLock={yes, no}	Не применимо	Не применимо	Не применимо	Да
Wake on USB support (выход из режима ожидания при помощи USB-устройств)	Device=DellCmos WakeOnUSB={yes, no}	Не применимо	Не применимо	Не применимо	Да
Wake On LAN (технология дистанционного включения по сети)	Device=cmos WakeOnLan={yes, no} Device=DellCmos WakeOnLan={Disable, LAN, PXE}	Да	Да	Да	Да

ДОСТУП К НАСТРОЙКАМ BIOS

Сразу после запуска тонкого нажмите и удерживайте клавишу Delete или клавишу F2 в зависимости от модели тонкого клиента.

- клавиша **Delete**: нажмите и удерживайте клавишу **Delete**, чтобы войти в настройки BIOS на клиентах ThinOS с CMOS BIOS;
- клавиша **F2**: нажмите и удерживайте клавишу **F2**, чтобы войти в настройки BIOS на клиентах ThinOS с Standard BIOS.

При появлении запроса введите пароль **Fireport** для просмотра экрана настроек BIOS. Например, Вы можете использовать клавишу **F7**, чтобы применить оптимизированные значения по умолчанию — загрузить оптимальные значения по умолчанию для всех элементов в утилите BIOS Setup.

ПРИМЕЧАНИЕ: эти настройки BIOS не применимы к тонкому клиенту СИЛА PC4-1261 и тонкому клиенту СИЛА PC4-1262, поскольку на платформе ARM нет BIOS. Чтобы получить доступ к WLOADER на платформе ARM, нажмите и удерживайте кнопку питания в течение четырех секунд, пока индикатор питания не загорится зеленым, а затем нажмите клавишу **Delete**.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ CMOS И ИЗВЛЕЧЕНИЕ НАСТРОЕК CMOS НА ФАЙЛОВЫЙ СЕРВЕР ДЛЯ РАСПРОСТРАНЕНИЯ НА ЦЕЛЕВЫЕ УСТРОЙСТВА

Централизованное управление CMOS позволяет администраторам ThinOS легко управлять настройками CMOS для масштабных развертываний тонких клиентов, используя методологии централизованной конфигурации. В качестве примера здесь рассматривается тонкий клиент СИЛА PC4-1240 с ThinOS (D10D). Следующие инструкции предназначены для тонкого клиента СИЛА PC4-1240 с ThinOS (D10D) BIOS версии 3.0D. Однако инструкции также применимы для других поддерживаемых аппаратных платформ и версий BIOS.

1. Чтобы подготовить эталонный диск с BIOS версии 3.0D или более поздней:
 - 1.1. Эталонное устройство представляет собой золотой образ, который используется для распространения на другие тонкие клиенты. Чтобы использовать эталонный диск, войдите в утилиту BIOS Setup. Нажмите клавишу **Delete**, введите пароль **Fireport** (с учетом регистра) и нажмите **Enter**. Настройте параметры CMOS, включая Auto Power (Автоматическое включение), Boot Order (Порядок загрузки), P-key setting (Настройка P-key) и BIOS Password (Пароль BIOS).
 - 1.2. Сохраните настройки CMOS.
 - 1.3. Перезагрузите тонкий клиент.
2. Для создания INI-файла в CMOS-памяти файлового сервера необходимо:
 - 2.1. Создать файл `cmos.ini` и поместить его в папку `wpos` в каталоге `ini` на сервере. Убедитесь, что загрузка файлов в папку `wpos` разрешена.
 - 2.2. В файле `cmos.ini` ввести следующие данные: `Device=cmos Action=extract`.
3. Для перезапуска эталонного устройства для файлового сервера, содержащего INI-файл в CMOS-памяти, необходимо:
 - 3.1. Запустить устройство тонкого клиента для эталонного использования.
 - 3.2. В диалоговом окне **Login** (Вход) ввести учетные данные, необходимые для доступа к файлу `cmos.ini`.
 - 3.3. После входа в систему для просмотра вкладки **Event Log** (Журнал событий) необходимо выполнить следующие действия:
Кликните на значок System Information icon > System Information dialog box > Event Log.

Для просмотра CMOS-памяти можно также открыть журнал событий: `extract to D10D_cmos.3.0D event`. Теперь файл централизованного управления CMOS-памятью (содержащий параметры CMOS с эталонного устройства) будет скопирован в папку `wpos` на файловом сервере. Поскольку это D10D BIOS, версия 3.0D, имя файла централизованного управления CMOS-памятью будет прописано как `D10D_cmos.3.0D`. Эти настройки CMOS-памяти теперь готовы для загрузки на устройства других тонких клиентов.
4. Для подготовки файлового сервера с INI-файлом в CMOS-памяти к распространению необходимо:
 - 4.1. Вписать строку `Device = cmos Action = restore` в файл `cmos.ini` на файловом сервере.
 - 4.2. Сохранить файл.
5. Для входа на все целевые устройства на файловом сервере с INI-файлом в CMOS-памяти необходимо выполнить следующие действия:

- 5.1. Запустить устройства тонких клиентов, на которые необходимо распространить настройки CMOS-памяти эталонного устройства.
- 5.2. Чтобы войти в smos.ini файл, введите ваши учетные данные в диалоговое окно **Login** (Вход).
- 5.3. Для того чтобы открыть **Event Log** (Журнал событий), нужно нажать на значок **System Information** (Информация о системе) и в диалоговом окне выбрать вкладку **Event Log** (Журнал событий).

Вы можете увидеть событие "CMOS: restore from D10D_cmos.3.0D". Это означает, что файл централизованного управления, содержащий настройки CMOS-памяти эталонного устройства, скопирован на целевые устройства тонких клиентов.

ПРИМЕЧАНИЕ: после завершения настройки нужных параметров CMOS на устройствах тонких клиентов, не входите на сервер с файлом smos.ini и не запускайте операцию восстановления (если Вы не хотите запустить процесс восстановления повторно). Администраторы могут удалить файл smos.ini, чтобы предотвратить нежелательное затирание данных на CMOS.

ПРИМЕЧАНИЕ: рекомендуется сначала выполнить описанные выше действия на тестовом файловом сервере для проверки настроек / процесса центрального управления CMOS-памятью. Хотя централизованный метод конфигурирования данных можно использовать для принудительного применения настроек CMOS в рабочей среде, следует помнить, что любой тонкий клиент, подключенные к серверу с файлом smos.ini и его команды на извлечение и восстановление, будут выполнять предписанные программным кодом команды (включая команду на затирание данных CMOS).

ЛОКАЛЬНОЕ УПРАВЛЕНИЕ CMOS-ПАМЯТЬЮ И ИЗВЛЕЧЕНИЕ НАСТРОЕК CMOS НА USB-НАКОПИТЕЛЬ ДЛЯ РАСПРОСТРАНЕНИЯ НА ТОНКИЕ КЛИЕНТЫ

Локальное управление CMOS-памятью позволяет администраторам ThinOS легко управлять настройками CMOS на небольшом количестве тонких клиентов, используя методы распределения USB-накопителей. Тонкий клиент СИЛА PC4-1240 на ThinOS (D10D) рассматривается в данном руководстве в качестве примера. Приведенные ниже инструкции относятся к тонкому клиенту СИЛА PC4-1240 с ThinOS (D10D) BIOS, версии 3.0D.

1. Для подготовки эталонного диска с BIOS версией 3.0D или выше необходимо:
 - 1.1. Эталонное устройство является стандартом, используемым для распространения на другие устройства. Для использования эталонного диска необходимо войти в утилиту настройки BIOS, нажать клавишу **Delete** (Удалить), ввести пароль — **Fireport** (с учетом регистра) и нажать **Enter** (Ввод). Настроить параметры CMOS, включая автоматическое включение, порядок загрузки, настройку P-ключа и пароль BIOS.
 - 1.2. Сохранить настройки CMOS.
 - 1.3. Перезагрузить устройство.
2. Для извлечения настроек CMOS на USB-накопитель необходимо выполнить следующие действия:

- 2.1. Подключить отформатированный USB-накопитель к выбранному тонкому клиенту (эталонному). Например, для форматирования в Windows 7 нужно подключить USB-накопитель, щелкнуть правой кнопкой мыши по значку USB-накопитель, выбрать **Format** (Форматировать), нажать **Restore device defaults** (Восстановить настройки устройства по умолчанию), выбрать **Quick Format** (Быстрое форматирование), а затем нажать **Start** (Начать).
- 2.2. Использовать функцию извлечения CMOS настроек на USB-накопитель в системе ThinOS. Для этого необходимо щелкнуть правой кнопкой мыши на рабочем столе стандартного типа и выбрать **Extract CMOS to USB** (Извлечь CMOS на USB). При работе с рабочим столом **Zero**, на вкладке **General** (Общее) диалогового окна **System Tools** (Системные инструменты) (**System Settings icon >System Tools >General tab**) нужно нажать **Extract CMOS to USB** (Извлечь CMOS на USB).
- 2.3. После успешного извлечения появится всплывающее сообщение: «CMOS: extract to D10D_cmos.3.0D», далее нужно правильно отсоединить USB-накопитель. Настройки CMOS-памяти на USB-накопителе теперь готовы для распространения на другие тонкие клиенты.
3. Для восстановления настроек CMOS-памяти на целевых устройствах необходимо выполнить следующие действия:
 - 3.1. Запустить все тонкие клиенты, на которые необходимо установить настройки CMOS-памяти эталонного устройства.
 - 3.2. Использовать функцию ThinOS восстановления CMOS настроек с USB-накопителя. При работе с классическим рабочим столом необходимо щелкнуть правой кнопкой мыши и выбрать **Restore CMOS from USB**. При работе с нулевым рабочим столом на вкладке **General** диалогового окна **System Tools** (System Settings значок> System Tools> General) нужно нажать **Restore CMOS from USB**.
 - 3.3. После успешного восстановления появится следующее сообщение: «CMOS: restore from D10D_cmos.3.0D». Далее правильно отсоедините USB-накопитель. Настройки CMOS на USB-накопителе теперь будут записаны на целевое устройство.

РАБОТА СО STANDARD BIOS

В данном разделе дана информация по настройке и работе с клиентами ThinOS с помощью Standard BIOS.

Поддерживаемые устройства:

- тонкий клиент СИЛА PC4-1210 на ThinOS;
- тонкий клиент СИЛА PC4-1210 на PCoIP;
- тонкий клиент СИЛА PC4-1221 на ThinOS;
- тонкий клиент СИЛА PC4-1221 Extended.

Приведенные в таблице 48 конфигурации Standard BIOS поддерживаются с помощью файлового сервера (параметры INI).

Таблица 48. Параметры конфигурации Standard BIOS.

Параметры	Настройки
Конфигурации системы	Аудио
Безопасность	<p>Блокировка входа в программу настройки системы администратором.</p> <p>Пароль администратора:</p> <ul style="list-style-type: none"> ▪ Включить / отключить пароль администратора; ▪ Обновить пароль администратора
Конфигурация USB	<p>Включить порты USB на передней панели</p> <p>Включить задний левый двойной порт USB 2.0</p>
Управление питанием	<p>Wake-On-LAN (технология, позволяющая удаленно включить компьютер через локальную сеть с помощью отправки пакета данных):</p> <ul style="list-style-type: none"> ▪ Использование запрещено; ▪ LAN Only (только устройства, соединенные в одну сеть); ▪ Локальная сеть с загрузкой PXE <p>AC Recovery (повторный запуск устройства после восстановления питания)</p> <ul style="list-style-type: none"> ▪ Выключение; ▪ Включение; ▪ Последнее состояние. <p>Время автоматического включения:</p> <ul style="list-style-type: none"> ▪ Использование запрещено; ▪ Ежедневно; ▪ Будни; ▪ Выберите дни <p>Wake-On-USB (возможность вывода устройства из режима ожидания при помощи USB)</p>
Загрузка устройства	<p>USB загрузка</p> <p>PXE загрузка (загрузка с помощью сетевой карты, без локальных носителей)</p>

Примеры параметров INI:

```
Device=DellCmos newpassword=1234567 or newpasswordenc=encrypted strings
```

Данный INI-параметр используется для создания пароля администратора в случае, если пароль не установлен.

```
Device=DellCmos currentpassword=1234567 newpassword="" or currentpasswordenc=encrypted strings
```

Данный INI-параметр используется для изменения существующего пароля.

Device=DellCmos newpassword=1234567 или newpasswordenc=encrypted strings — Используйте этот параметр INI, чтобы создать пароль администратора, если пароль не задан.

Device=DellCmos currentpassword=1234567 newpassword="" или currentpasswordenc=encrypted strings

Используйте этот параметр INI, чтобы удалить существующий пароль.

ГЛАВА 9. БЕЗОПАСНОСТЬ СИСТЕМЫ

Для операционной системы ThinOS создана новая глобальная политика безопасности, которая применяется ко всем типам защищенных соединений (соединения https / SSL) с некоторыми исключениями.

Цель данной политики: повысить уровень безопасности по умолчанию и улучшить общие настройки системы. Данная политика безопасности объединяет настройки безопасности для каждого приложения.

Таблица 49. INI-параметр.

INI-параметр	Описание
SecurityPolicy={full warning (default) low} SecuredNetworkProtocol={yes no (default)} TLSMinVersion={1 (default), 2, 3} TLSMaxVersion={1, 2, 3 (default)}	<p>Full (Высокий) – SSL-соединение с обязательной проверкой сертификата сервера. При подключении к подозрительным ресурсам необходимо отменить соединение.</p> <p>Warning (Предупреждение) (по умолчанию) – SSL-соединение с обязательной проверкой сертификата сервера. При подключении к подозрительным ресурсам пользователь может продолжить или отменить соединение.</p> <p>Low (Низкий) – сертификат сервера не подтвержден. Значение установлено для нескольких приложений.</p> <p>После обновления прошивки значение по умолчанию устанавливается сразу для всех установленных приложений.</p> <p>Существует исключение для файлового сервера и WDM.</p> <p>Предыдущий протокол iniSecurityLevel SecureProtocol удален из привилегированного сегмента.</p>

Все приложения, работающие по умолчанию в режиме безопасности SSL, следуют глобальному режиму. В глобальном режиме значением по умолчанию является **Warning** (Предупреждение). Уязвимыми приложениями являются VMware View, Amazon WorkSpaces (AWS), файловый сервер, WDM Service, Caradigm Server и OneSign Server.

Исключениями являются:

- WDM и файловый сервер в состоянии сброса к заводским настройкам. Перед загрузкой любого INI-параметра уровень Безопасности SSL является низким (Low), а после загрузки значение изменяется в соответствии со значением глобального режима. Например, значением по умолчанию является Предупреждение, если загрузка INI-параметра его не изменяет. Система с более ранней версией настроек (значение по умолчанию установлено как низкое) следует глобальному режиму после обновления

устройства. Например, значением по умолчанию является Предупреждение, если загрузка INI-параметра его не изменяет;

- брокеры VMware View и AWS имеют собственные настройки безопасности (GUI и INI). В версии ThinOS 8.3 добавлена дополнительная опция, которая обновляется вслед за глобальным режимом по умолчанию. Контекст режима GUI-безопасности обновлен для лучшего понимания;
- при работе с WMS, Microsoft RDS broker, Citrix broker и SecureMatrix уровень будет указан как высокий.

Протокол FTP файлового сервера по умолчанию сохраняется без каких-либо настроек из WDM / DHCP / INI и всегда отображает полный адрес с префиксом протокола. Например, ftp://.

Новая прошивка / информация о развертывании клиента

1. Рекомендуется определить политику безопасности перед обновлением до версии 8.3 и выше. Если ее нет, Вы можете получить предупреждающие сообщения, требующие ручного вмешательства для продолжения.
2. Перед обновлением до версии 8.3 и выше рекомендуется определить требуемый уровень безопасности SSL и добавить необходимые параметры политики безопасности в глобальный INI- файл.
3. Для SecurityPolicy=Fullorwarning нужно добавить сертификаты соответствующих серверов File, View, AWS, WDM, WMS, OneSign и / или Caradigm в клиент ThinOS перед обновлением прошивки.
4. Протоколом файлового сервера по умолчанию все еще является FTP, префикс ftp добавляется автоматически, если протокол не указан.
5. В более ранних версиях при сбое подключения к файловому серверу, работающему на https-протоколе, в режиме полной безопасности, отображалось диалоговое окно с предложением нажать кнопку ОК. Начиная с версии ThinOS 8.5 HF2, в правом нижнем углу экрана появляется всплывающая подсказка.
6. Предупреждения и ошибки описаны в новых, удобных для пользователя системных сообщениях.

ПРИМЕЧАНИЕ: если сервер WDM установлен как https, адрес сервера не преобразуется в http.

БЕЗОПАСНОСТЬ НА ТРАНСПОРТНОМ УРОВНЕ (ПРОТОКОЛ TLS)

Безопасность на транспортном уровне (протокол TLS): это протокол, обеспечивающий безопасность связи между клиентскими и серверными приложениями.

Обновление Протокола TLS. В системной версии ThinOS 8.2 протокол TLS обновлен с версии 1.0 до версии 1.2. По умолчанию клиент ThinOS использует TLS 1.2 для защиты любых протоколов связи, соединений или приложений SSL / TLS в целом и при согласовании с сервером возвращается к предыдущей версии SSL / TLS.

МИКРОПРОЦЕССОРНЫЕ КАРТЫ И УСТРОЙСТВА ДЛЯ ИХ ЧТЕНИЯ

Микропроцессорная карта — это токен безопасности со встроенными интегральными схемами, что позволяет хранить и обрабатывать данные. Устройство чтения микропроцессорных карт — это устройство ввода, которое считывает данные с карты.

Микропроцессорная карта Gemalto IDPrime MD840: поддерживает микропроцессорные карты Gemalto IDPrime MD830 и MD840. Версии IDGo 800 1.2.1 — 01 для работы с ПО Windows промежуточного слоя требуется поддержка микропроцессорные карты Gemalto IDPrime MD840.

Функция безопасного обмена сообщениями поддерживается для использования новейших карт MD830 Rev B.

ПРИМЕЧАНИЕ

Проблема с картой Prime MD 840: если используется первый контейнер, то вход в систему брокера Xen завершится неудачно.

Считыватели микропроцессорных карт OMNIKEY: поддерживают следующие считыватели микропроцессорных карт OMNIKEY:

- считыватель Omnikey 5427 СК (0x5427, 0x076b) поддерживает карты iclass15693, 14443a, 125k;
- Omnikey 5422;
- Omnikey 5326 DFR (0x5326, 0x076b) поддерживает карту iclass15693;
- Omnikey 5025 CL (0x502a, 0x076b) поддерживает карту 125k;
- Ominkey 5325 CL, 5125 (0x5125, 0x076b) поддерживает карту 125k;
- Omnikey 5321 V2 CLi (0x532a, 0x076b) поддерживает 13,56 МГц карту;
- Omnikey 5321 V2 (076b, 5321) поддерживает 13,56 МГц карту;
- Omnikey 5021 CL (0x5340, 0x076b) поддерживает 13,56 МГц карту;
- Omnikey 5321 V2 Cl Sam (0x5341, 0x076b) поддерживает 13,56 МГц карту;
- Omnikey 5421 (0x5421, 0x076b) поддерживает карту 13,56 МГц;
- Omnikey 5321 CR (0x5320, 0x076b);
- Omnikey 5022 CL.

Встроенный считыватель микропроцессорных карт работает и с обычными микропроцессорными картами. Его функциональность аналогична другим внешним USB устройствам для чтения смарт карт.

СЧИТЫВАТЕЛЬ МИКРОПРОЦЕССОРНЫХ КАРТ RUTOKEN

Rutoken — это USB-токен для двухфакторной аутентификации. Позволяет создавать и хранить ключи шифрования для электронных подписей, использовать его для шифрования ключей и выполнять электронную подпись. Также устройства можно использовать для шифрования хранилища цифровых сертификатов и других данных.

ThinOS 8.6 MR3 поддерживает Rutoken 2151 и Rutoken ECP 2.0 (2100).

ГЛАВА 10. УСТРАНЕНИЕ НЕПОЛАДОК В РАБОТЕ

Ниже описаны некоторые основные способы устранения неполадок в случае возникновения любой проблемы.

1. Устройства ThinOS разрешают безопасные SSL-подключения — `SecurityMode=Full` — только после проверки сертификатов. В таком случае устройства предупреждают об угрозе после определения сервера через действительный IP-адрес.

Ниже приведены обходные пути, позволяющие избежать проблемы с SSL-подключением:

- 1.1. Убедитесь, что устройство имеет действительный сертификат и на устройстве выбрано правильное время.
- 1.2. Определите сервер по имени, а не по IP-адресу.
- 1.3. Установите высокий уровень глобальной политики безопасности.
- 1.4. Используйте следующий INI-параметр для обеспечения режима высокой безопасности:

```
SecurityPolicy=high TLSCheckCN=Yes
```

2. Blast-соединение — при наличии проблем с запуском проверьте состояние удаленного рабочего стола и состояние сети, перезагрузите устройство несколько раз, и рабочий стол успешно подключится.

ПРИЛОЖЕНИЕ А. ОБЩИЕ НАСТРОЙКИ ПЕЧАТИ

В данном разделе описаны примеры использования диалогового окна **Printer Setup** (Настройка принтера) и параметров INI ThinOS для распространенных настроек печати.

ПРИМЕЧАНИЕ: хост-принтеры не поддерживаются.

ПЕЧАТЬ НА ЛОКАЛЬНЫХ ПРИНТЕРАХ ЧЕРЕЗ USB ИЛИ ПАРАЛЛЕЛЬНЫЕ ПОРТЫ

ПРИМЕЧАНИЕ: программное обеспечение Microsoft Remote Desktop Session Host (RDSH), терминальный сервер Microsoft и Citrix XenApp имеют свои собственные настройки печати, которые должны соответствовать стандартам для печати на стороне клиента. Подробнее о настройке печати в этих средах см. в инструкциях поставщика.

ИСПОЛЬЗОВАНИЕ ДИАЛОГОВОГО ОКНА PRINTER SETUP (НАСТРОЙКА ПРИНТЕРА) ДЛЯ ЛОКАЛЬНЫХ ПРИНТЕРОВ

Примером послужит принтер HP LaserJet 4000, подключенный к USB-порту тонкого клиента.

При подключении USB-принтеров у некоторых принтеров заполняются поля **Printer Name** (Название принтера) и **Printer Identification** (Идентификация принтера).

Чтобы настроить для печати локальный принтер, подключенный через USB или параллельный порт, необходимо:

1. В меню рабочего стола выбрать **System Setup > Printer** (Настройка системы > Принтер). Откроется диалоговое окно **Printer Setup** (Настройка принтера).
2. Нажать **Printer Setup** (Настройка принтера) и использовать следующие рекомендации для вкладки Порты при печати на локальном USB-принтере:
 - 2.1. **Select Port** (Выбрать порт): порт LPT1 или LPT2.
 - 2.2. **Printer Name** (Название принтера): ввести имя, которое отобразится в списке принтеров, большинство принтеров с прямым подключением по USB указывают свои имена автоматически.
 - 2.3. **Printer Identification** (Идентификация принтера): ввести тип или модель принтера в соответствии с именем драйвера принтера в системе Windows, включая заглавные буквы и пробелы. Большинство принтеров с прямым подключением USB указывают свои идентификаторы автоматически. В данном случае необходимо ввести HP LaserJet 4000 Series PCL.
 - 2.4. **Printer Class** (Класс принтера): это значение можно установить по умолчанию.
 - 2.5. **Enable the printer device** (Включить удаленное устройство принтера): необходимо настроить принтер на включение удаленного устройства и его отображение на хосте.
3. Нажать **ОК**, чтобы сохранить настройки.

ИСПОЛЬЗОВАНИЕ INI-ПАРАМЕТРОВ ДЛЯ ЛОКАЛЬНЫХ ПРИНТЕРОВ

Настройка локальной печати с использованием параметров ThinOS INI — это простой способ настройки принтера для всех клиентов в одной сети при условии, что различий по маркам и моделям у принтеров нет.

В таком случае INI-параметры будут выглядеть примерно так:

```
Printer=LPT1 \
Name="HP LaserJet 4000" \
PrinterID="HP LaserJet 4000 Series PCL" \ Enabled=yes
```

ПРИМЕЧАНИЕ: PrinterID — это точное название драйвера принтера Windows. Если драйвер носит название HP LaserJet 4000 Series PCL в Windows, данное название должно полностью дублироваться в поле PrinterID в INI-параметрах, включая заглавные буквы и пробелы.

ПЕЧАТЬ НА СЕТЕВЫХ ПРИНТЕРАХ ВНЕ СИСТЕМЫ WINDOWS

В системе ThinOS есть возможность печатать через настроенные на удаленные запросы LPR-печати сетевые принтеры вне системы Windows. Среди настроек большинства крупных сетей есть возможность удаленной печати, однако стоит уточнить у поставщика услуги о целесообразности настройки данного типа печати.

После подготовки к удаленной печати тонкий клиент перенаправит запрос через RDP или ICA соединение на внутреннюю инфраструктуру системы. Таким образом, клиент будет подключаться к внутренней инфраструктуре, сетевой принтер будет отображаться как локальный принтер клиента.

ИСПОЛЬЗОВАНИЕ ДИАЛОГОВОГО ОКНА PRINTER SETUP (НАСТРОЙКА ПРИНТЕРА) ДЛЯ СЕТЕВЫХ ПРИНТЕРОВ ВНЕ СИСТЕМЫ WINDOWS

Для использования диалогового окна **Printer Setup** (Настройка принтера) для сетевых принтеров вне системы Windows (LPD) необходимо выполнить следующие действия:

1. В меню рабочего стола нажать **System Setup** (Настройка системы), а затем нажать **Printer** (Принтер). Откроется диалоговое окно **Printer Setup** (Настройка принтера).

В качестве примера рассмотрим принтер HP LaserJet 4200n, подключенный к тонкому клиенту через LPR.

2. При переходе на вкладку **LPD** (LPDs tab) необходимо использовать следующие рекомендации при печати на сетевом принтере вне системы Windows:
 - 2.1. **Select LPD** (Выбрать LPD): порт LPD1 или LPD2.
 - 2.2. **Printer Name** (Название принтера): ввести имя, которое отобразится в списке принтеров.
 - 2.3. **Printer Identification** (Идентификация принтера): ввести точный тип или модель принтера в соответствии с именем драйвера принтера в системе Windows, включая заглавные буквы и пробелы.

В этом примере необходимо ввести HP LaserJet 4200n PCL6.

- 2.4. **LPD Hosts** (LPD сервер): имя DNS-сервера или WINS-сервера для сетевого принтера. Также можно ввести IP-адрес принтера в сети, следуя примеру, использованному выше.

ПРИМЕЧАНИЕ: если принтер подключен к другому тонкому клиенту в сети, запись в поле Сервер размещения LPD — это имя или адрес конкретно этого тонкого клиента.

- 2.5. **LPD Queue Name** (Название очереди LPD): сервер размещения LPD создает именную очередь для каждого подключенного принтера. Необходимо ввести название очереди в соответствии с используемым принтером. Это название может отличаться у каждого поставщика. Данное поле необходимо правильно заполнять для корректного приема сетевым принтером входящих заданий на печать. В данном примере название auto может использоваться для HP LaserJet 4200n PCL6 в соответствии с документацией, размещенной на веб-сайте HP.

ПРИМЕЧАНИЕ: если принтер подключен к другому тонкому клиенту в сети, название LPD-очереди должно соответствовать содержимому поля Printer Name (Название принтера) на устройстве тонкого клиента с подключенным принтером.

- 2.6. **Printer Class** (Класс принтера): данное значение можно оставить по умолчанию.
 2.7. **Enable the printer device** (Включить устройство принтера): необходимо, чтобы при запросе на удаленную печать принтер активировал подключенное к нему устройство для отображения на удаленном хосте.

ИСПОЛЬЗОВАНИЕ INI-ПАРАМЕТРОВ ДЛЯ СЕТЕВЫХ ПРИНТЕРОВ ВНЕ СИСТЕМЫ WINDOWS

Настройка сетевой печати с использованием параметров ThinOS INI — это легкий способ настройки принтера для всех клиентов в рамках одной сети при условии подключения одной модели принтеров.

В таком случае INI-параметры будут выглядеть примерно так:

```
Printer=LPD1 \
LocalName="HP LaserJet 4200n" \ Host=10.10.10.1 \
Queue=auto \
PrinterID="HP LaserJet 4200 PCL6" \ Enabled=yes
```

ПРИМЕЧАНИЕ: PrinterID — это точное название драйвера принтера Windows. В случае, если драйвер носит название HP LaserJet 4200n PCL6 в Windows, данное название должно полностью дублироваться в поле PrinterID в INI-параметрах, включая заглавные буквы и пробелы.

ПЕЧАТЬ НА СЕТЕВЫХ ПРИНТЕРАХ WINDOWS

В системе ThinOS есть возможность печатать на принтерах, подключенных к серверам печати Microsoft. При выборе настроек SMB-печати в ThinOS необходимо учитывать некоторые требования к конфигурации, которые могут потребовать изменения настроек тонкого клиента.

Поскольку для подключения к серверу печати Microsoft Windows требуются учетные данные домена, необходимо предоставить учетные данные ThinOS либо по требованию во

время использования принтера, либо при настройке администратора, предоставив учетные данные, сохраненные в кэше с экрана входа в систему, см. пример 3: «Определение SMB-принтера для использования учетных данных пользователя, кэшированных ThinOS (Advanced)», в разделе **Использование INI-параметров на сетевых принтерах Windows (SMB)**. В данном разделе описаны все методы подключения.

ИСПОЛЬЗОВАНИЕ ДИАЛОГОВОГО ОКНА НАСТРОЙКИ ПРИНТЕРА ДЛЯ СЕТЕВЫХ ПРИНТЕРОВ WINDOWS

Настройка параметров в SMB-принтерах требует от пользователя введения своих учетных данных перед началом каждой печати. Таким образом, пользователи будут временно отключены от удаленного сеанса для ввода своих учетных данных (следуя инструкциям в разделе **Использование INI-параметров для сетевых принтеров Windows** можно избежать подобного отключения).

Для настройки сетевого принтера Windows выполните следующие действия:

1. В меню рабочего стола выберите **System Setup >Printer** (Настройки системы> Принтер). Откроется диалоговое окно настройки принтера.
2. Откройте вкладку **SMBS** (SMBS tab) и используйте следующие рекомендации при печати на сетевом принтере Windows:

ПРИМЕЧАНИЕ: имя принтера в системе Windows не должно содержать пробелов, иначе ThinOS не сможет его использовать.

- 2.1. **Select SMB** (Выбрать SMB): выберите нужный SMB-принтер из списка.
- 2.2. **\\ Host \ Printer** – щелкните на значок папки для просмотра доступных сетей Microsoft и выберите сетевой принтер с доступным DNS-именем или IP-адресом сервера печати Windows.

После ввода необходимых учетных данных домена появится диалоговое окно **Printer Setup** (Настройка принтера).

- 2.3. **Printer Name** (Название принтера): введите имя, которое отобразится в списке принтеров.
- 2.4. **Printer Identification** (Идентификация принтера): введите точный тип или модель принтера в соответствии с именем драйвера принтера в системе Windows, включая заглавные буквы и пробелы.

В этом примере необходимо ввести HP LaserJet 4100 Series PCL.

- 2.5. **Printer Class** (Класс принтера): данное значение можно оставить по умолчанию.
- 2.6. **Enable the printer device** (Включить устройство принтера): необходимо, чтобы при запросе на удаленную печать принтер активировал подключенное к нему устройство для отображения на удаленном хосте.
- 2.7. Нажмите кнопку **Test Print** (Проверить печать) и введите свои учетные данные в систему Windows, эти учетные данные будут использоваться для доступа к общему ресурсу принтера. Это же диалоговое окно будет отображаться пользователю при попытке запустить печать на этом принтере.

ИСПОЛЬЗОВАНИЕ INI-ПАРАМЕТРОВ ДЛЯ СЕТЕВЫХ ПРИНТЕРОВ WINDOWS

Настройки параметров SMB-печати с использованием параметров ThinOS INI — это простой и легкий способ настройки принтеров, совместно используемых сервером Windows, для всех клиентов одной сети. Основное преимущество настройки SMB-печати с использованием параметров ThinOS INI заключается в том, что предварительно можно определить учетную запись домена для использования при аутентификации принтера. Примеры настройки данной функции:

1. Определение SMB-принтера с общими учетными данными пользователя в виде простого текста:

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \ Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \ Enabled=yes \
Username=Username1 \ Password=Password \ Domain=contoso
```

2. Определение SMB-принтера с общими зашифрованными учетными данными пользователя:

```
Printer=SMB1 \
LocalName="Demo SMB Printer" \ Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \ Enabled=yes \
Username-enc=PACGOGDBPKDOPGDGKC \ Password-
enc=PFDBOHDBODCJPODP \ Domain=contoso
```

ПРИМЕЧАНИЕ: также можно использовать инструмент Генератор конфигурации (ConfGen) для создания INI-параметров в ThinOS. ConfGen можно загрузить с сайта techhelp.de.

ПРИМЕЧАНИЕ: этот инструмент не поддерживается системой и приведен исключительно в рамках конкретного примера.

3. Определение SMB-принтера для использования учетных данных пользователя, кэшированных в ThinOS (продвинутый уровень):

ПРИМЕЧАНИЕ: в этом случае необходимо, чтобы пользователь выполнил вход в ThinOS для кэширования учетных данных для последующего использования. В приведенном ниже примере описаны необходимые минимальные требования к INI-разделу.

```
SIGNON = NTLM
Connect=RDP \
Host=1.2.3.4 \
Username=$UN \
Password=$PW \
Domain=$DN \
AutoConnect=1
Printer=SMB1 \
LocalName="Demo SMB Printer" \
Host=\\dp-dc-ftp \
Name="TechSupportPrinter" \
PrinterID="HP LaserJet 4100 Series PCL" \
Enabled=yes \
Username=$UN \ Password=$PW \ Domain=$DN
```

ИСПОЛЬЗОВАНИЕ ТОНКОГО КЛИЕНТА В КАЧЕСТВЕ СЕРВЕРА ПЕЧАТИ

Тонкий клиент ThinOS можно настроить как базовый сетевой сервер печати для совместного использования локальными принтерами с другими тонкими клиентами.

ИСПОЛЬЗОВАНИЕ ДИАЛОГОВОГО ОКНА НАСТРОЙКА ПРИНТЕРА ДЛЯ НАСТРОЙКИ LPD-СЛУЖБ

Только при работе с классическим компьютером можно настроить тонкого клиента на работу с протоколом LPD (сетевой протокол прикладного уровня для передачи документов на печать) и создать сетевой сервер печати на базе этого клиента.

Для того, чтобы тонкий клиент предоставлял услуги печати LPD необходимо выполнить следующие действия:

1. В меню рабочего стола нажмите **System Setup > Network Setup** (Настройка системы > Настройка сети), чтобы открыть диалоговое окно **Настройка сети** (Network Setup).
2. Введите статический IP-адрес тонкого клиента.
3. В меню рабочего стола нажмите **System Setup > Printer** (Настройка системы > Принтер), чтобы открыть диалоговое окно **Printer Setup** (Настройка принтера) и выберите любой из перечисленных портов.
4. Выберите LPT.
5. Введите название принтера в поле **Printer Name** (Название принтера).
6. Введите точный тип или модель принтера (**Printer Identification**) в соответствии с именем драйвера принтера в системе Windows, включая заглавные буквы и пробелы. В этом примере необходимо ввести HP LaserJet 4000 Series PCL.
7. Значение **Printer Class** (Класс принтера) можно оставить по умолчанию.
8. Выберите команду **Enable the Printer Device** (Включить устройство принтера).
9. Выберите команду **Enable LPD service for the printer** (Включить LPD-протокол для принтера).

ИСПОЛЬЗОВАНИЕ INI-ПАРАМЕТРОВ ДЛЯ НАСТРОЙКИ LPD-СЛУЖБ

Настройка LPD-печати с использованием параметров ThinOS INI — это простой и легкий способ настроить тонкий клиент в ThinOS в качестве основного сетевого сервера печати для совместного использования другими тонкими клиентами.

В таком случае INI-параметры будут выглядеть примерно так:

```
Printer=LPT1 \  
Name="HP LaserJet 4000" \  
PrinterID="HP LaserJet 4000 Series PCL" \  
Enabled=yes  
EnableLPD=yes
```

ПРИМЕЧАНИЕ: PrinterID — это точное название драйвера принтера Windows. Если драйвер носит название HP LaserJet 4000 Series PCL в Windows, данное название должно полностью дублироваться в поле PrinterID в INI-параметрах, включая заглавные бук-

вы и пробелы.

НАСТРОЙКА ТЕХНОЛОГИИ THINPRINT

Технология ThinPrint не используется для работы с тонкими клиентами. Для использования ThinPrint пользователь должен сначала настроить принтер в соответствии с пользовательской документацией, а затем настроить ThinPrint на тонком клиенте с помощью диалогового окна **Printer Setup** (Настройка принтера).

Для настройки ThinPrint воспользуйтесь следующими рекомендациями:

1. Используйте поле Printer Identification (Идентификация принтера) для ввода класса принтера (при необходимости можно изменить имя принтера).
2. Идентификаторы принтера назначаются (в зависимости от физического порта) следующим образом:
 - COM1 = 1;
 - COM2 = 2;
 - LPT1 = 3 — USB-принтеры автоматически определяются на LPT1;
 - LPT2 = 4;
 - LPD0 = 5 — название очереди LPD передается как имя принтера; Идентификация класса принтера;
 - LPD1 = 6 — название очереди LPD передается как имя принтера; Идентификация класса принтера;
 - LPD2 = 7 — название очереди LPD передается как имя принтера; Идентификация класса принтера;
 - LPD3 = 8 — название очереди LPD передается как имя принтера; Идентификация класса принтера;
 - SMB1 = 9 — в форме `\\ host \ printershare`;
 - SMB2 = 10;
 - SMB3 = 11;
 - SMB4 = 12;
3. Чтобы установить соответствующую версию ThinPrint на сервер, необходимо придерживаться следующих рекомендаций:
 - 3.1. Объекты принтера создаются администратором вручную.
 - 3.2. После установки .print Engine нужно создать на сервере объект принтера, чтобы использовать собственный драйвер и ThinPort в качестве порта принтера. Можно использовать любой протокол (TCP, RDP или ICA), поскольку клиенты ThinOShas.print поддерживаются всеми протоколами. Объект принтера должен соблюдать соглашения о присвоении имен ThinPrint, например, HPLJ5 #_: 2, и в этом случае задания на печать отправляются на локальный принтер с идентификатором .2, ссылаясь на идентификатор порта клиента .print. Если идентификационный номер отсутствует, клиент .print отправляет задание на печать в качестве текущего задания.
 - 3.3. **Объекты принтера, созданные автоматически с помощью ThinPrintAutoConnect.** При использовании ThinPrintAutoConnect тонкий клиент идентифицируется с идентификатором 84 тонкого клиента и, таким образом, распознается как тонкий клиент без локального диспетчера в очереди на печать. Здесь можно настроить шаблон на сервере, который использует пример собственного драйвера (HPLJ5) и ThinPort, а затем дать имя этому шаблону в формате `_#Любое имя`.
 - 3.4. Затем необходимо убедиться, что установка ThinPrintAutoconnect [1] и настройки, требуемые для использования этого шаблона, работают корректно на локальных принтерах. Заданный принтер с использованием драйвера HPLJ5 и ThinPort пользо-

ватель увидит в процессе работы. Имя присваивается автоматически в соответствии с соглашением о присвоении имен ThinPrint, включая имя принтера со стороны клиента. Кроме того, есть возможность определить имя шаблона в соответствии с именем принтера клиента (например, `replace.AnyName.` с именем принтера 4. и 5. выше, `_# HP Laserjet 5` идентифицирует его как объект локального принтера (в данном случае название `HP Laserjet 5.` используется как пример, без соотношения с `ThinPrintAutoconnect`)).

ПРИЛОЖЕНИЕ Б. ВАЖНЫЕ ПРИМЕЧАНИЯ

Обновление версии VNC RFB: начиная с ThinOS 8.0_214, версия VNC RFB была обновлена до 3.8. Данное обновление обеспечивает поддержку приложений, например DameWare. Администратор может удаленно подключаться к устройству ThinOS, используя DameWare или VNC Viewer. В ранних версиях можно было использовать только VNC Viewer.

Режим удаленной загрузки — ThinOS поддерживает удаленный режим работы, что позволяет загружать операционную систему без использования монитора.

Сообщения о локально подключенных устройствах в WDM. Начиная с версии ThinOS 8.6, локально подключенные устройства (монитор и USB-устройство) передаются на сервер WDM. Эта информация отображается в разделе сведений об устройстве на консоли WDM.

ПРИМЕЧАНИЕ: возможно одновременное подключение более 20 USB-устройств к системе ThinOS через USB-разветвитель. Но WDM сервер отобразит только 10 устройств.

ПРИЛОЖЕНИЕ В. КАК ВКЛЮЧИТЬ ПЕРЕНАПРАВЛЕНИЕ USB ПРИ РАБОТЕ RDP WINDOWS 10

Для включения перенаправления USB в сеансе RDP Windows 10 разрешите перенаправление поддерживаемых устройств Plug and Play в разделе Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Service > Remote Desktop Session Host > Device and Resource Redirection > Do not allow supported Plug and Play device redirection.

КОНТАКТНАЯ ИНФОРМАЦИЯ

ООО «СИЛА»

ОГРН 1177746928864

ИНН 7713445809

КПП 771301001

127434, г. Москва, шоссе Дмитровское, дом 9Б

+7 (495) 933-37-01

info@rossila.ru

www.rossila.ru

Техническая поддержка

+7(495)662-10-52 для звонков из Москвы

+7(800)600-96-22 для звонков из регионов

service@rossila.ru

Если Вам требуется квалифицированная помощь, позвоните на телефон «горячей линии поддержки», напишите письмо или воспользуйтесь другими способами обращения в техническую поддержку:

- система учета заявок Service Desk: <https://rossila.intraservice.ru/>
- форма регистрации заявки на сайте: <http://rossila.ru/support>
- мобильное приложение IntraService: [iOS](#) и [Android](#)