Lenovo

Lenovo XClarity Management Hub Руководство по установке и руководство пользователя

Версия 2.1

Примечание

Перед тем как воспользоваться этой информацией и самим продуктом, обязательно прочтите замечания по общим и юридическим вопросам в документации по XClarity Orchestrator в Интернете.

Второе издание (Июль 2024 г.)

Содержание

Глава 1. Планирование для Lenovo XClarity Management Hub

Ознакомьтесь со следующими замечаниями и обязательными требованиями, которые помогут спланировать установку Lenovo XClarity Management Hub.

Поддерживаемое оборудование и программное обеспечение

Убедитесь, что ваша среда соответствует требованиям к оборудованию и программному обеспечению для Lenovo XClarity Management Hub.

Хост-системы

Требования к гипервизору

Следующие гипервизоры поддерживаются для установки Lenovo XClarity Management Hub.
- VMware ESXi 7.0, U1, U2 и U3
- VMware ESXi 6.7, U1, U2[1] и U3

Для VMware ESXi виртуальное устройство является шаблоном OVF.

Важно:

- Для VMware ESXi 6.7 U2 необходимо использовать образ ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso или более поздней версии.

Требования к оборудованию

В следующей таблице перечислены *минимальные рекомендуемые* конфигурации для XClarity Management Hub на основании количества управляемых пограничных клиентских устройств. В зависимости от среды могут потребоваться дополнительные ресурсы для обеспечения оптимальной производительности.

Количество управляемых пограничных клиентских устройств	Процессоры	Память	Хранилище
От 0 до 100 устройств	6	32 ГБ	340 ГБ
От 100 до 200 устройств	8	34 ГБ	340 ГБ
От 200 до 400 устройств	10	36 ГБ	340 ГБ
От 400 до 600 устройств	12	40 ГБ	340 ГБ
От 600 до 800 устройств	14	44 ГБ	340 ГБ
От 800 до 1000 устройств	16	48 ГБ	340 ГБ

1. Это минимальный объем хранилища для использования виртуальным устройством XClarity Management Hub в качестве хранилища данных SSD.

Требования к программному обеспечению

Для XClarity Management Hub требуется следующее программное обеспечение.

- **Сервер NTP**. Сервер протокола сетевого времени (Network Time Protocol, NTP) необходим для обеспечения того, чтобы отметки времени для всех событий и оповещений, полученных от диспетчеров ресурсов и управляемых устройств, были синхронизированы с XClarity Management Hub. Убедитесь, что сервер NTP доступен через сеть управления (обычно это интерфейс Eth0).

Управляемые устройства

Максимальное число устройств ThinkEdge Client (без контроллеров управления материнской платой), которые XClarity Management Hub может контролировать и подготавливать, а также управлять ими — 10,000.

Полный список поддерживаемых устройств ThinkEdge Client и дополнительных компонентов (таких как средства ввода-вывода, модули DIMM и адаптеры устройств хранения), минимально необходимые уровни микропрограмм и замечания по ограничениям можно найти на Серверы TXClarity Management Hub.

Общие сведения о конфигурациях оборудования и аппаратных компонентах для определенного устройства см. в разделе Веб-страница Lenovo Server Proven.

Веб-браузеры

Веб-интерфейс XClarity Management Hub работает в следующих веб-браузерах.
- Chrome 80.0 или выше
- Firefox ESR 68.6.0 или выше
- Microsoft Edge 40.0 или выше
- Safari 13.0.4 или выше (выполняется на macOS 10.13 или выше)

Брандмауэры и прокси-серверы

Для некоторых функций служб и поддержки, включая Call Home и состояние гарантии, требуется доступ к Интернету. При наличии брандмауэров в сети настройте их таким образом, чтобы разрешить XClarity Orchestrator и диспетчерам ресурсов выполнять эти операции. Если у Lenovo XClarity Orchestrator и диспетчеров ресурсов нет прямого доступа к Интернету, настройте их для использования прокси-сервера.

Брандмауэры

Если применимо, убедитесь, что в брандмауэре открыты следующие имена DNS и порты для XClarity Orchestrator и применимых диспетчеров ресурсов (Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub и Lenovo XClarity Administrator). Каждая DNS представляет собой географически распределенную систему с динамическим IP-адресом.

Примечание: IP-адреса могут быть изменены. По возможности используйте имена DNS.

Имя DNS	**Порты**	**Протоколы**
Загрузка обновлений (обновлений сервера управления и микропрограмм, пакетов UpdateXpress System Packs (драйверов устройств ОС) и пакетов репозитория)		
download.lenovo.com	443	HTTPS
support.lenovo.com	443 и 80	HTTPS и HTTP
Отправка данных по обслуживанию в службу поддержки Lenovo (Call Home) — только XClarity Orchestrator		
soaus.lenovo.com	443	HTTPS

Имя DNS	Порты	Протоколы
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 и более поздних версий) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx (XClarity Orchestrator v1.5 и более ранних версий)	443	HTTPS
Отправка периодических данных в Lenovo — только XClarity Orchestrator		
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 и более поздних версий) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx (XClarity Orchestrator v1.5 и более ранних версий)	443	HTTPS
Получение информации о гарантии		
supportapi.lenovo.com	443	HTTPS и HTTP

Прокси-сервер

Если XClarity Orchestrator или диспетчеры ресурсов не имеют прямого доступа к Интернету, убедитесь, что они настроены для использования прокси-сервера HTTP (см. раздел Настройка сетив документации по XClarity Orchestrator в Интернете).

- Убедитесь, что на прокси-сервере настроено использование базовой аутентификации.
- Убедитесь, что прокси-сервер настроен в качестве непрерывающего прокси.
- Убедитесь, что прокси-сервер настроен в качестве прокси переадресации.
- Убедитесь, что балансировщики нагрузки настроены таким образом, чтобы поддерживать сеансы с одним прокси-сервером и не переключаться между ними.

Внимание: XClarity Management Hub должен иметь прямой доступ к Интернету. Прокси-сервер HTTP в настоящее время не поддерживается.

Доступность портов

Lenovo XClarity Orchestrator и диспетчеры ресурсов требуют, чтобы определенные порты были открыты для обеспечения связи. Если требуемые порты заблокированы или используются другим процессом, некоторые функции могут работать неверно.

XClarity Orchestrator, Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub и Lenovo XClarity Administrator — это соответствующие требованиям REST приложения, которые безопасно взаимодействует по протоколу TCP в порту 443.

XClarity Orchestrator

XClarity Orchestrator прослушивает и отвечает через порты, которые перечислены в следующей таблице. Если XClarity Orchestrator и все управляемые ресурсы находятся за брандмауэром и вы намерены получить доступ к этим ресурсам из браузера, который находится *за пределами* брандмауэра, вы должны убедиться, что открыты необходимые порты.

Примечание: XClarity Orchestrator можно также настроить для создания исходящих подключений к нескольким внешним службам, например LDAP, SMTP и syslog. Для этих подключений могут потребоваться дополнительные порты, которые обычно определяются пользователями и не

включены в данный список. Для них также может потребоваться доступ к серверу службы доменных имен (DNS) через TCP- или UDP-порт 53 для разрешения имен внешних серверов.

Обслуживание	**Исходящие (порты, открытые во внешних системах)**	**Входящие (порты, открытые на устройстве XClarity Orchestrator)**
Программно-аппаратный комплекс XClarity Orchestrator	• DNS — TCP/UDP на порте **53**	• HTTPS — TCP на порте **443**
Внешние серверы аутентификации	• LDAP — TCP на порте **389**[1]	Неприменимо
Службы перенаправления событий	• Сервер электронной почты (SMTP) — UDP на порте **25**[1] • Веб-служба REST (HTTP) — UPD на порте **80**[1] • Splunk — UDP на порте **8088**[11], **8089**[1] • Syslog — UDP на порте **514**[1]	Неприменимо
Службы Lenovo (включая Call Home)	• HTTPS (Call Home) — TCP на порте **443**	Неприменимо

1. Это порт по умолчанию. Его можно настроить в пользовательском интерфейсе XClarity Orchestrator.

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 требует, чтобы определенные порты были открыты для обеспечения связи. Если необходимые порты заблокированы или используются другим процессом, некоторые функции концентратора управления могут работать неверно.

Если устройства находятся за брандмауэром и ими предполагается управлять с концентратора управления, расположенного за пределами этого брандмауэра, необходимо обеспечить, чтобы все порты, через которые осуществляется связь между концентратором управления и контроллером управления материнской платой в каждом устройстве, были открыты.

Служба или компонент	**Исходящие (порты, открытые для внешних систем)**	**Входящие (порты, открытые на целевых устройствах)**
XClarity Management Hub 2.0	• DNS — UDP на порте **53** • NTP — UDP на порте **123** • HTTPS — TCP на порте **443** • SSDP — UDP на порте **1900** • DHCP — UDP на порте **67**	• HTTPS — TCP на порте **443** • SSDP — UDP на портах **32768**–**65535**
Серверы ThinkSystem и ThinkAgile	• HTTPS — TCP на порте **443** • Обнаружение SSDP — UDP на порте **1900**	• HTTPS — TCP на порте **443**

XClarity Management Hub

XClarity Management Hub прослушивает и отвечает через порты, которые перечислены в следующей таблице.

Служба или компонент	Исходящие (порты, открытые во внешних системах)	Входящие (порты, открытые на программно-аппаратном комплексе XClarity Management Hub)
Программно-аппаратный комплекс XClarity Management Hub[1]	• DNS — TCP/UDP на порте **53**[2]	• HTTPS — TCP на порте **443** • MQTT — TCP на порте **8883**
Устройства ThinkEdge Client[3]	Неприменимо	• MQTT — TCP на порте **8883**

1. При использовании XClarity Management Hub для управления устройствами с помощью XClarity Orchestrator определенные порты должны быть открыты для обеспечения связи. Если требуемые порты заблокированы или используются другим процессом, некоторые функции XClarity Orchestrator могут работать неверно.
2. XClarity Management Hub можно также настроить для создания исходящих подключений к внешним службам. Для них также может потребоваться доступ к серверу службы доменных имен (DNS) через TCP- или UDP-порт 53 для разрешения имен внешних серверов.
3. Если управляемые устройства находятся за брандмауэром и ими предполагается управлять с XClarity Management Hub, расположенного за пределами брандмауэра, необходимо обеспечить, чтобы все порты, через которые осуществляется связь между XClarity Management Hub и пограничными устройствами, были открыты.

XClarity Administrator

При использовании Lenovo XClarity Administrator для управления устройствами с помощью Lenovo XClarity Orchestrator определенные порты должны быть открыты для обеспечения связи. Если требуемые порты заблокированы или используются другим процессом, некоторые функции XClarity Orchestrator могут работать неверно.

Сведения о портах, которые должны быть открыты для XClarity Administrator, см. в разделе Доступность портов в документации по XClarity Administrator в Интернете.

Замечания по сети

Lenovo XClarity Management Hub можно настроить так, чтобы использовать для связи один сетевой интерфейс (eth0) или два отдельных сетевых интерфейса (eth0 и eth1).

Lenovo XClarity Management Hub выполняет функции связи по следующим сетям.

- *Сеть управления* используется для связи между Lenovo XClarity Management Hub и управляемыми устройствами.
- *Сеть передачи данных* обычно применяется для связи между операционными системами, установленными на серверах, и внутренней сетью компании, Интернетом либо обеими этими сетями.

Один интерфейс (eth0)

При использовании одного сетевого интерфейса (eth0) функции управления, передачи данных и развертывания операционной системы выполняются по одной сети.

При настройке Lenovo XClarity Management Hub определите сетевой интерфейс eth0 с учетом следующих замечаний.

- Сетевой интерфейс необходимо настроить для поддержки обнаружения устройств и управления ими (включая обновления микропрограмм). Lenovo XClarity Management Hub должен иметь возможность взаимодействовать со всеми устройствами, которыми он будет управлять из сети

управления.Lenovo XClarity Management Hub должен иметь возможность взаимодействовать со всеми устройствами, которыми он будет управлять из сети.

- Для развертывания образов ОС интерфейс eth0 должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к операционной системе хоста.
- **Важно!** Реализация общей сети передачи данных и управления может привести к сбоям трафика, например потере пакетов или неполадкам подключения сети управления в зависимости от конфигурации вашей сети (например, если трафик от серверов имеет высокий приоритет, а трафик от контроллеров управления — низкий). Сеть управления использует UDP-трафик в дополнение к TCP. UDP-трафик может иметь более низкий приоритет при высоком сетевом трафике.

Два отдельных интерфейса (eth0 и eth1)

При использовании двух сетевых интерфейсов (eth0 и eth1) можно настроить физически раздельные или виртуально раздельные сети.

При определении сетевых интерфейсов eth0 и eth1 примите во внимание следующие замечания.

- Сетевой интерфейс eth0 необходимо подключить к сети управления и настроить для поддержки обнаружения устройств и управления ими. Lenovo XClarity Management Hub должен иметь возможность взаимодействовать со всеми устройствами, которыми он будет управлять из сети управления.
- Сетевой интерфейс eth1 можно настроить для взаимодействия с внутренней сетью передачи данных, сетью передачи данных общего пользования или с обеими сетями.
- Для развертывания образов операционной системы сетевой интерфейс eth1 должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к операционной системе хоста.
- Функции могут выполняться в любой сети.
- При использовании виртуально раздельных сетей пакеты из сети управления и пакеты из сети передачи данных отправляются через одно физическое подключение. Для разделения трафика двух сетей во все пакеты данных сети управления добавляются метки виртуальной локальной сети (VLAN).

Замечания по IP-адресам

Прежде чем настраивать сеть, ознакомьтесь со следующими замечаниями по IP-адресам.

- Изменение IP-адреса виртуального устройства после настройки и запуска XClarity Management Hub приведет к неполадкам подключения к XClarity Orchestrator и всем управляемым устройствам. Если необходимо изменить IP-адрес, отключите XClarity Management Hub от XClarity Orchestrator и прекратите управление всеми управляемыми устройствами, прежде чем изменить IP-адрес, а затем снова включите управление устройствами и подключите XClarity Management Hub к XClarity Orchestrator после изменения IP-адреса.
- Настройте устройства и компоненты таким образом, чтобы свести к минимуму изменения IP-адресов. Рассмотрите возможность использования статических IP-адресов вместо протокола динамической настройки хостов (DHCP). Если используется DHCP, обеспечьте, чтобы изменения IP-адресов были сведены к минимуму, например, настройте сервер DHCP так, чтобы он предоставлял адреса на основе MAC-адресов или с бесконечным сроком аренды.В случае изменения IP-адреса управляемого устройства (кроме устройства ThinkEdge Client) необходимо прекратить управление устройством, а затем снова начать управлять им.
- Трансляция сетевых адресов (NAT), которая перераспределяет одно пространство IP-адресов в другое, не поддерживается.
- Сетевые интерфейсы необходимо настроить с адресами IPv4 для управления следующими устройствами. Адреса IPv6 не поддерживаются.

  - Серверы ThinkServer
  - Устройства Lenovo Storage
- Управление устройствами RackSwitch с использованием локального адреса канала IPv6 через порт передачи данных или порт управления не поддерживается.

Замечания по высокому уровню доступности

Чтобы настроить высокую доступность для Lenovo XClarity Orchestrator, используйте функции высокой доступности, которые являются частью операционной системы хоста.

Microsoft Hyper-V

Используйте функцию высокой доступности, предоставленную для среды Hyper-V.

VMware ESXi

В среде высокой доступности VMware несколько хостов настроены как кластер. Общее хранилище используется для создания образа диска виртуальной машины (ВМ) для хостов в кластере. ВМ работает одновременно только на одном хосте. При возникновении проблемы с виртуальной машиной на резервном хосте запускается другой экземпляр этой виртуальной машины.

VMware High Availability требует следующие компоненты.

- Как минимум два хоста, на которых установлен ESXi. Эти хосты становятся частью кластера VMware.
- Третий хост, на котором установлен VMware vCenter.

  Рекомендация. Убедитесь, что вы устанавливаете версию VMware vCenter, которая совместима с версиями ESXi, установленными на хостах, которые будут использоваться в кластере.

  VMware vCenter может быть установлен на одном из хостов, которые используются в кластере. Однако, если этот хост отключен или недоступен, вы также теряете доступ к интерфейсу VMware vCenter.
- Общее хранилище (хранилища данных), доступ к которому могут получить все хосты в кластере. Можно использовать любой тип общего хранилища, поддерживаемый VMware. Хранилище данных используется VMware для определения того, должна ли виртуальная машина переключаться на другой хост (частота обмена).

Глава 2. Настройка XClarity Management Hub для пограничных клиентских устройств

При первом доступе к Lenovo XClarity Management Hub необходимо выполнить несколько действий для начальной настройки XClarity Management Hub.

Процедура

Для начальной настройки XClarity Management Hub выполните следующие действия.

Шаг 1. Войдите в веб-интерфейс XClarity Management Hub.

Шаг 2. Прочитайте и примите лицензионное соглашение.

Шаг 3. Создайте дополнительные учетные записи пользователей.

Шаг 4. Настройте сетевой доступ, включая IP-адреса для сетей данных и управления.

Шаг 5. Настройте дату и время.

Шаг 6. Зарегистрируйте XClarity Management Hub с помощью сервера Orchestrator.

Вход в XClarity Management Hub для пограничных клиентских устройств

Вы можете запустить веб-интерфейс XClarity Management Hub с любого компьютера, который имеет сетевое подключение к виртуальной машине XClarity Management Hub.

Перед началом работы

Убедитесь, что используется один из следующих поддерживаемых веб-браузеров.
- Chrome 80.0 или выше
- Firefox ESR 68.6.0 или выше
- Microsoft Edge 40.0 или выше
- Safari 13.0.4 или выше (выполняется на macOS 10.13 или выше)

Доступ к веб-интерфейсу осуществляется через защищенное соединение. Убедитесь, что используется протокол **https**.

При удаленной настройке XClarity Management Hub должна быть возможность подключения к той же сети второго уровня. До завершения начальной настройки доступ должен осуществляться из адреса без маршрутизации. Поэтому рекомендуется получить доступ к XClarity Management Hub из другой виртуальной машины, у которой есть подключение к XClarity Management Hub. Например, доступ к XClarity Management Hub можно получить из другой виртуальной машины хоста, где установлен XClarity Management Hub.

Через 60 минут XClarity Management Hub выполняет автоматический выход из сеансов пользователей независимо от активности пользователей.

Процедура

Чтобы войти в веб-интерфейс XClarity Management Hub, выполните следующие действия.

Шаг 1. Введите в адресной строке браузера IP-адрес XClarity Management Hub.
`https://<IPv4_address>`

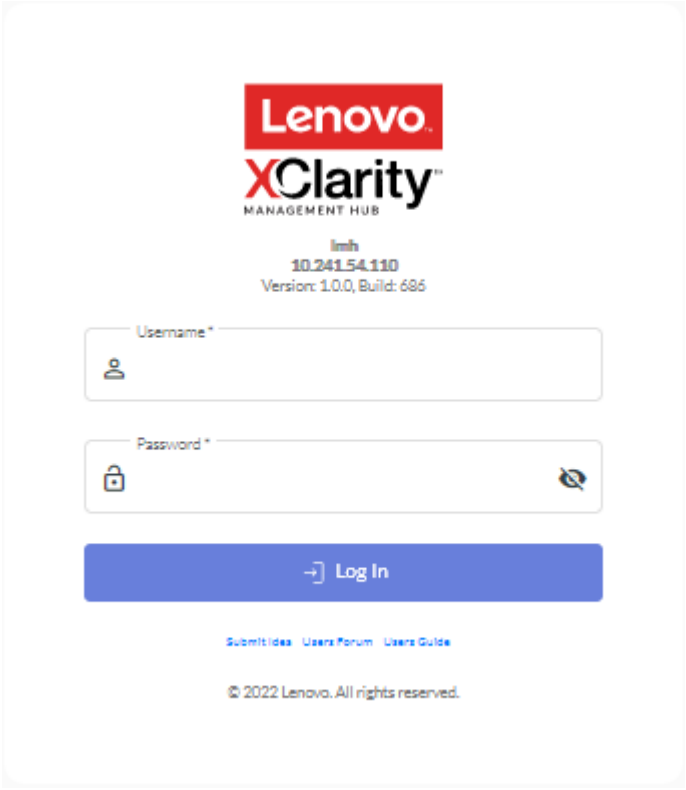
Например:

```
https://192.0.2.10
```

Используемый IP-адрес зависит от настроек вашей среды.

- Если в eth0_config указан адрес IPv4, используйте для доступа к XClarity Management Hub этот адрес.
- Если DHCP-сервер настроен в том же домене широковещательного трафика, что и XClarity Management Hub, используйте для доступа к XClarity Management Hub адрес IPv4, который отображается на консоли виртуальной машины XClarity Management Hub.
- Если интерфейсы eth0 и eth1 относятся к разным подсетям и в обеих подсетях используется протокол DHCP, для получения доступа к веб-интерфейсу при первоначальной настройке укажите IP-адрес интерфейса *eth1*. При первом запуске XClarity Management Hub интерфейсы eth0 и eth1 получают IP-адреса по протоколу DHCP, а в качестве шлюза XClarity Management Hub по умолчанию задается шлюз, назначенный с помощью DHCP интерфейсу *eth1*.

Появится страница первоначального входа XClarity Management Hub:



Шаг 2. Выберите в раскрывающемся списке **Язык** желаемый язык.

Примечание: Параметры конфигурации и значения, которые предоставляются управляемыми устройствами, могут быть доступны только на английском языке.

Шаг 3. Введите учетные данные пользователя и нажмите **Войти**.

При первом входе в XClarity Management Hub введите учетные данные по умолчанию **USERID** и **PASSW0RD** (где 0 равно нулю).

Шаг 4. Прочитайте и примите лицензионное соглашение.

Шаг 5. Если вы впервые вошли в систему с использованием учетных данных по умолчанию, вам будет предложено изменить пароль. По умолчанию пароли должны содержать от **8** до **256** символов и соответствовать следующим критериям.

Важно: Рекомендуется использовать надежные пароли длиной 16 и более символов.
- (1) Должен содержать по меньшей мере одну заглавную букву
- (2) Должен содержать по меньшей мере одну строчную букву
- (3) Должен содержать по меньшей мере одну цифру
- (4) Должен содержать по меньшей мере один специальный символ
- (5) Не должен совпадать с именем пользователя

Шаг 6. Если вы впервые вошли в систему, вам будет предложено выбрать, нужно ли использовать текущий самозаверяющий сертификат или сертификат, подписанный сторонним центром сертификации. Если вы решили использовать сертификат, подписанный сторонним центром сертификации, отобразится страница «Сертификат сервера».

Внимание: Самозаверяющий сертификат не является безопасным. Рекомендуется создать и установить собственный сертификат, подписанный сторонним центром сертификации.

Сведения об использовании сертификата, подписанного сторонним центром сертификации, см. в разделе Установка доверенного сертификата сервера, подписанного сторонним центром сертификации, для XClarity Management Hub для пограничных клиентских устройств.

После завершения

В меню **Учетная запись пользователя** (), расположенном в правом верхнем углу веб-интерфейса XClarity Management Hub, можно выполнить следующие действия.

- Выйти из текущего сеанса, нажав **Выйти**. Откроется страница входа в XClarity Management Hub.
- Вы можете задавать вопросы и получать ответы на Веб-сайт форума сообщества Lenovo XClarity.
- Поделитесь своими идеями о XClarity Management Hub, для чего нажмите **Отправить идеи** в меню **Учетная запись пользователя** () в правом верхнем углу веб-интерфейса или перейдите непосредственно на Веб-сайт Lenovo XClarity Ideation.
- Просмотрите документацию в Интернете, нажав **Руководство пользователя**.
- Просмотреть сведения о выпуске XClarity Management Hub, нажав **О системе**.
- Изменить язык пользовательского интерфейса, нажав **Изменить язык**. Поддерживаются следующие языки.
  - Английский (en)
  - Упрощенный китайский (zh-CN)
  - Традиционный китайский (zh-TW)
  - Французский (fr)
  - Немецкий (de)
  - Итальянский (it)
  - Японский (ja)
  - Корейский (ko)
  - Португальский (Бразилия) (pt-BR)
  - Русский (ru)
  - Испанский (es)
  - Тайский (th)

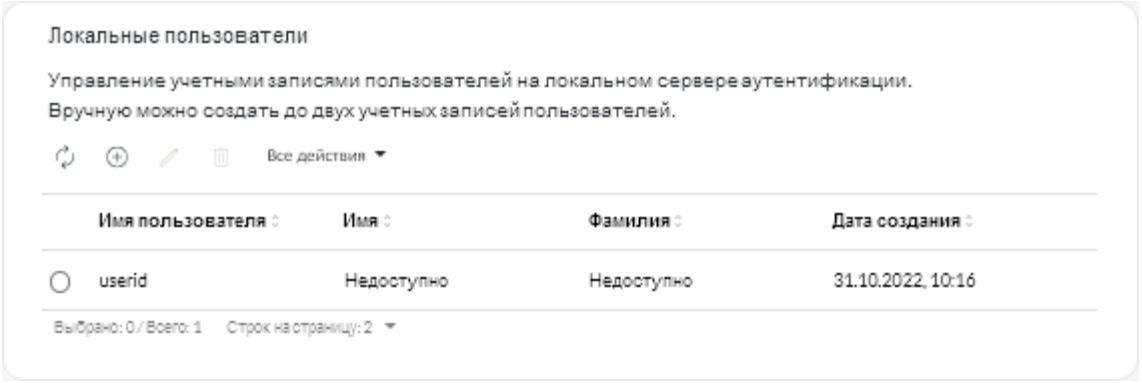
Создание учетных записей пользователей Lenovo XClarity Management Hub для пограничных клиентских устройств

Можно создать до 10 учетных записей пользователей Lenovo XClarity Management Hub.

Процедура

Для создания учетной записи пользователя выполните следующие действия.

Шаг 1. В строке меню Lenovo XClarity Management Hub нажмите **Безопасность (⚙) → Локальные пользователи**, чтобы открыть карту Локальные пользователи.



Шаг 2. Нажмите значок **Создать** (⊕), чтобы создать пользователя. Откроется диалоговое окно Создать нового пользователя.

Шаг 3. Заполните следующую информацию в диалоговом окне.

- Введите уникальное имя пользователя. Можно указать до 32 символов, включая буквы, цифры, символы точки (.), тире (-) и подчеркивания (_).

  Примечание: Имена пользователей вводятся без учета регистра.

- Введите новый пароль и подтверждение пароля. По умолчанию пароли должны содержать от **8** до **256** символов и соответствовать следующим критериям.

  Важно: Рекомендуется использовать надежные пароли длиной 16 и более символов.
  - (1) Должен содержать по меньшей мере одну заглавную букву
  - (2) Должен содержать по меньшей мере одну строчную букву
  - (3) Должен содержать по меньшей мере одну цифру
  - (4) Должен содержать по меньшей мере один специальный символ
  - (5) Не должен совпадать с именем пользователя

Шаг 4. Нажмите **Создать**.

Учетная запись пользователя добавляется в таблицу.

После завершения

На карте «Локальные пользователи» можно выполнить следующие действия.

- Чтобы изменить пароль и свойства учетной записи пользователя, нажмите значок **Изменить** (✎). Обратите внимание, что срок действия паролей не истекает.
- Удалить выбранного пользователя, нажав значок **Удалить** (🗑).

Настройка параметров сети XClarity Management Hub для пограничных клиентских устройств

Можно настроить один сетевой интерфейс IPv4 и параметры интернет-маршрутизации.

Перед началом работы

Прежде чем настраивать сеть, ознакомьтесь с замечаниями по ней (см. раздел Замечания по сети).

Процедура

Чтобы настроить параметры сети, нажмите **Администрирование (⚙) → Сетевое подключение** в строке меню XClarity Management Hub, а затем выполните одно или несколько следующих действий.

- **Настройка параметров IP-адресов**Для интерфейса eth0 перейдите на вкладку **Интерфейс Eth0**, настройте применимые параметры адреса IPv4 и нажмите **Применить**.

  Внимание:

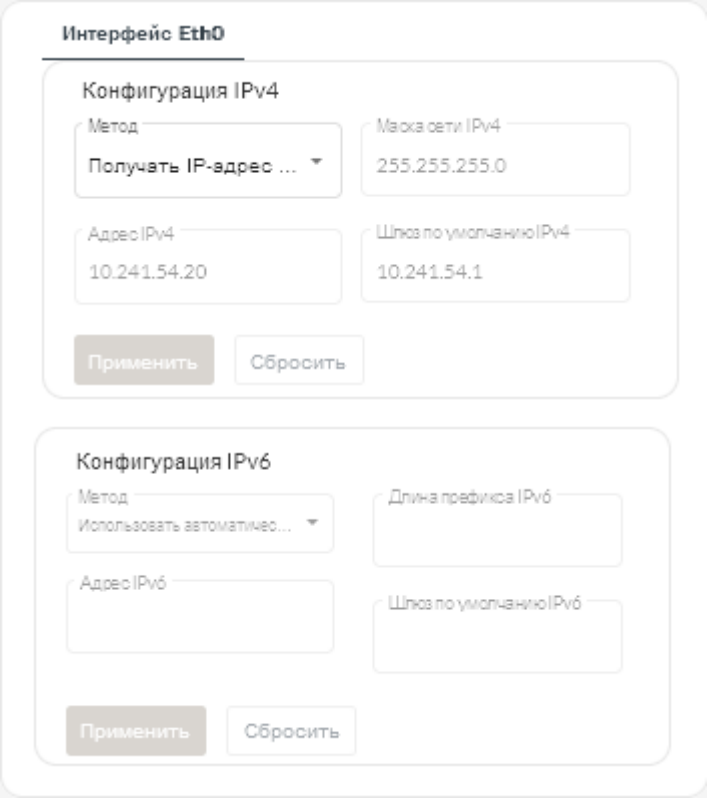
  – Изменение IP-адреса виртуального устройства после настройки и запуска XClarity Management Hub приведет к неполадкам подключения к XClarity Orchestrator и всем управляемым устройствам. Если необходимо изменить IP-адрес, отключите XClarity Management Hub от XClarity Orchestrator и прекратите управление всеми управляемыми устройствами, прежде чем изменить IP-адрес, а затем снова включите управление устройствами и подключите XClarity Management Hub к XClarity Orchestrator после изменения IP-адреса.

  В настоящее время поддерживаются только адреса IPv4.

  – **Параметры IPv4**. Можно настроить способ назначения IP-адресов, адрес IPv4, маску сети и шлюз по умолчанию.В качестве способа назначения IP-адресов можно выбрать использование статически назначенного IP-адреса или получение IP-адреса от сервера DHCP. При использовании статического IP-адреса необходимо указать IP-адрес, маску сети и шлюз по умолчанию.

    Шлюз по умолчанию должен иметь действительный IP-адрес, и для него должна использоваться та же маска сети (та же подсеть), что и для включенного интерфейса (eth0).

    Если какой-либо из интерфейсов использует DHCP для получения IP-адресов, шлюз по умолчанию также использует DHCP.

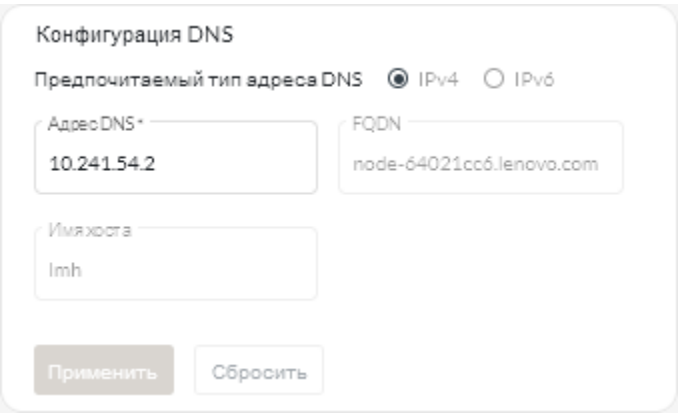


- **Настройка параметров интернет-маршрутизации**При необходимости настройте параметры системы доменных имен (DNS) с помощью карты Конфигурация DNS. Затем нажмите **Применить**.

  В настоящее время поддерживаются только адреса IPv4.

  Можно изменить IP-адрес сервера DNS.

  Полное доменное имя (FQDN) и имя хоста для сервера DNS такое же, как у сервера XClarity Management Hub, и их невозможно изменить.



Настройка даты и времени XClarity Management Hub для пограничных клиентских устройств

Необходимо настроить по крайней мере один (до четырех) сервер протокола сетевого времени (NTP) для синхронизации меток времени между XClarity Management Hub и всеми управляемыми устройствами.

Перед началом работы

Каждый сервер NTP должен быть доступен по сети. Желательно настроить сервер NTP на одной локальной системе с XClarity Management Hub.

После изменения времени на сервере NTP синхронизация XClarity Management Hub с новым временем может занять некоторое время.

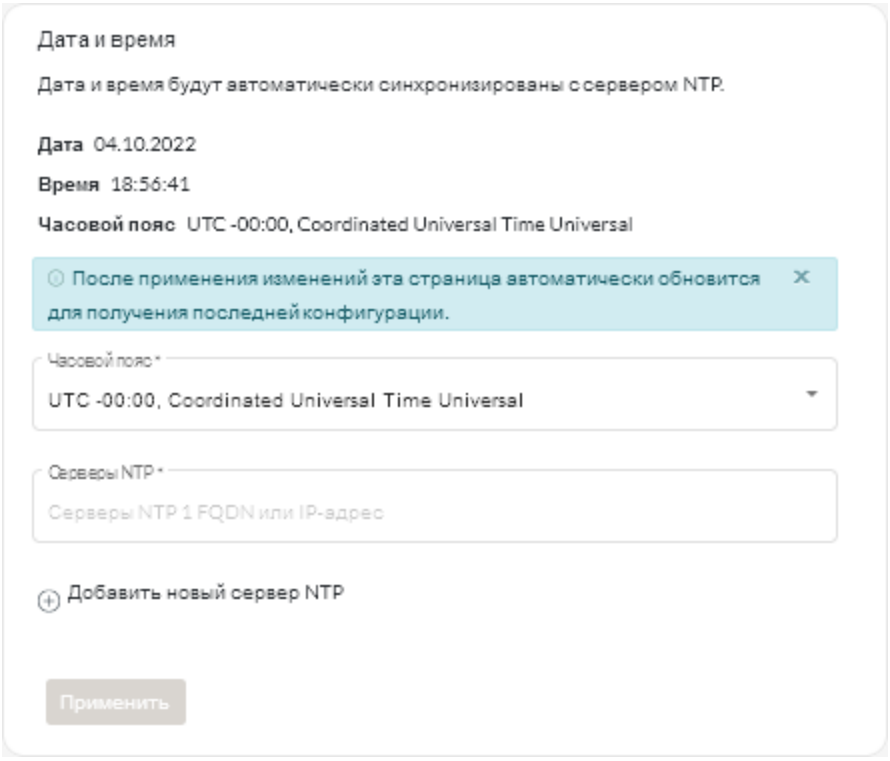
Внимание: Виртуальное устройство XClarity Management Hub и его хост необходимо настроить для синхронизации с одним и тем же источником времени, чтобы предотвратить случайную неправильную синхронизацию времени между программным обеспечением XClarity Management Hub и его хостом. Обычно хост настраивается так, чтобы его виртуальные устройства синхронизировали время с ним. Если решение XClarity Management Hub настроено для синхронизации с источником, отличным от его хоста, синхронизацию времени между виртуальным устройством XClarity Management Hub и его хостом необходимо отключить.

- Для ESXi следуйте инструкциям в разделе Веб-страница «VMware — отключение синхронизации времени».

Процедура

Для установки даты и времени в XClarity Management Hub выполните следующие действия.

Шаг 1. В строке меню XClarity Management Hub нажмите **Администрирование (⚙) → Дата и время**, чтобы открыть карту Дата и время.



Шаг 2. Выберите часовой пояс, в котором находится хост для XClarity Management Hub.

Если в выбранном часовом поясе действует переход на летнее время (DST), время автоматически корректируется с учетом летнего времени.

Шаг 3. Укажите имя хоста или IP-адрес для каждого сервера NTP в вашей сети. Можно определить до четырех серверов NTP.

Шаг 4. Нажмите **Применить**.

Управление сертификатами безопасности Lenovo XClarity Management Hub для пограничных клиентских устройств

Lenovo XClarity Management Hub использует сертификаты SSL для установления безопасных доверенных соединений между Lenovo XClarity Management Hub и его управляемыми устройствами, а также соединений пользователей с Lenovo XClarity Management Hub и соединений с различными службами. По умолчанию Lenovo XClarity Management Hub и XClarity Orchestrator используют сертификаты, созданные в XClarity Orchestrator, которые являются самозаверяющими и подписаны во внутреннем центре сертификации.

Перед началом работы

Этот раздел предназначен для администраторов, которые имеют общее представление о стандартах SSL и сертификатах SSL и принципах управления ими. Общие сведения о сертификатах с открытым ключом см. в разделах Веб-страница X.509 в Wikipedia и Веб-страница сертификата инфраструктуры открытых ключей X.509 в Интернете и профиля списка отзыва сертификатов (RFC5280).

Об этой задаче

Сертификат сервера по умолчанию, который создается уникально в каждом экземпляре Lenovo XClarity Management Hub, обеспечивает достаточный уровень безопасности для многих сред. Можно разрешить Lenovo XClarity Management Hub управлять сертификатами за вас или взять на себя более активную роль, настроив или заменив сертификаты серверов. Lenovo XClarity Management Hub предоставляет параметры для настройки сертификатов для вашей среды. Доступные варианты:

- Создать новую пару ключей, воссоздав внутренний центр сертификации и (или) сертификат конечного сервера, использующий определенные для вашей организации значения.
- Создать запрос подписи сертификата (CSR), который может быть отправлен в центр сертификации на ваш выбор для подписи пользовательского сертификата, который затем можно отравить в Lenovo XClarity Management Hub для использования в качестве сертификата конечного сервера для всех размещенных сервисов.
- Скачать сертификат сервера в свою локальную систему, чтобы иметь возможность импортировать этот сертификат в список доверенных сертификатов веб-браузера.

Lenovo XClarity Management Hub предоставляет несколько сервисов, принимающих входящие подключения SSL/TLS. Если какой-либо клиент (например, веб-браузер) подключается к одной из этих служб, Lenovo XClarity Management Hub предоставляет ему свой *сертификат сервера* для идентификации клиентом, который пытается подключиться. В клиенте должен храниться список сертификатов, которым он доверяет. Если сертификат сервера Lenovo XClarity Management Hub отсутствует в списке клиента, клиент отключается от Lenovo XClarity Management Hub во избежание обмена конфиденциальными данными безопасности с ненадежным источником.

При взаимодействии с управляемыми устройствами и внешними службами Lenovo XClarity Management Hub выступает в качестве клиента. В этом случае управляемое устройство или внешняя служба предоставляет Lenovo XClarity Management Hub свой сертификат сервера на проверку. Lenovo XClarity Management Hub сохраняет список доверенных сертификатов. Если *доверенный сертификат*, предоставляемый управляемым устройством или внешней службой, в этом списке отсутствует, Lenovo XClarity Management Hub отключается от управляемого устройства или внешней службы во избежание обмена конфиденциальными данными безопасности с ненадежным источником.

Следующая категория сертификатов используется службами Lenovo XClarity Management Hub, поэтому любой подключающийся клиент предположительно должен доверять этим сертификатам.

- **Сертификат сервера**. Во время начальной загрузки создаются уникальный ключ шифрования и самозаверяющий сертификат. Они используются в качестве корневого центра сертификации по умолчанию, которым можно управлять на странице «Центр сертификации» в параметрах безопасности Lenovo XClarity Management Hub. Нет необходимости в повторном создании этого корневого сертификата, если ключ шифрования не был скомпрометирован или если организация использует политику периодической замены всех сертификатов (см. Повторное создание самозаверяющего сертификата сервера XClarity Management Hub для пограничных клиентских устройств).Кроме того, во время первоначальной настройки генерируется отдельный ключ и создается сертификат сервера, подписанный внутренним центром сертификации. Этот сертификат используется в качестве сертификата сервера Lenovo XClarity Management Hub по умолчанию. Он автоматически заново создается каждый раз, когда Lenovo XClarity Management Hub обнаруживает изменение сетевых адресов (IP или DNS), чтобы гарантировать наличие в сертификате правильных адресов для сервера. Его можно настроить и создать по требованию (см. Повторное создание самозаверяющего сертификата сервера XClarity Management Hub для пограничных клиентских устройств).

  Вместо самозаверяющего сертификата сервера по умолчанию можно использовать сертификат сервера, подписанный сторонним центром. Для этого нужно создать запрос подписи сертификата, подписать этот запрос частным или коммерческим корневым центром сертификации, а затем импортировать всю цепочку сертификатов в Lenovo XClarity Management Hub (см. раздел Установка доверенного сертификата сервера, подписанного сторонним центром сертификации, для XClarity Management Hub для пограничных клиентских устройств).

  Если вы решите использовать самозаверяющий сертификат сервера по умолчанию, рекомендуется импортировать сертификат сервера в веб-браузер как доверенный корневой ЦС, чтобы избежать появления сообщений об ошибке сертификата в браузере (см. раздел Импорт сертификата сервера в веб-браузер для Lenovo XClarity Management Hub для пограничных клиентских устройств).
- **Сертификат развертывания ОС**. Чтобы установщик операционной системы мог безопасно подключаться к службе развертывания во время развертывания, служба развертывания операционной системы использует отдельный сертификат. Если ключ шифрования взломан, его можно создать повторно путем перезагрузки Lenovo XClarity Management Hub.

Повторное создание самозаверяющего сертификата сервера XClarity Management Hub для пограничных клиентских устройств

Можно создать новый сертификат сервера для замены текущего самозаверяющего сертификата сервера Lenovo XClarity Management Hub или восстановить сертификат, созданный XClarity Management Hub, если XClarity Management Hub в настоящее время использует настраиваемый сертификат сервера, подписанный сторонним центром сертификации. XClarity Management Hub использует новый самозаверяющий сертификат сервера для доступа через HTTPS.

Перед началом работы

Внимание: При повторном создании сертификата сервера XClarity Management Hub с использованием нового корневого ЦС XClarity Management Hub теряет подключение к управляемым устройствам, и необходимо выполнить повторное управление устройствами. При повторном создании сертификата сервера XClarity Management Hub без изменения корневого ЦС (например, если истек срок действия сертификата), нет необходимости выполнять повторное управление устройствами.

Об этой задаче

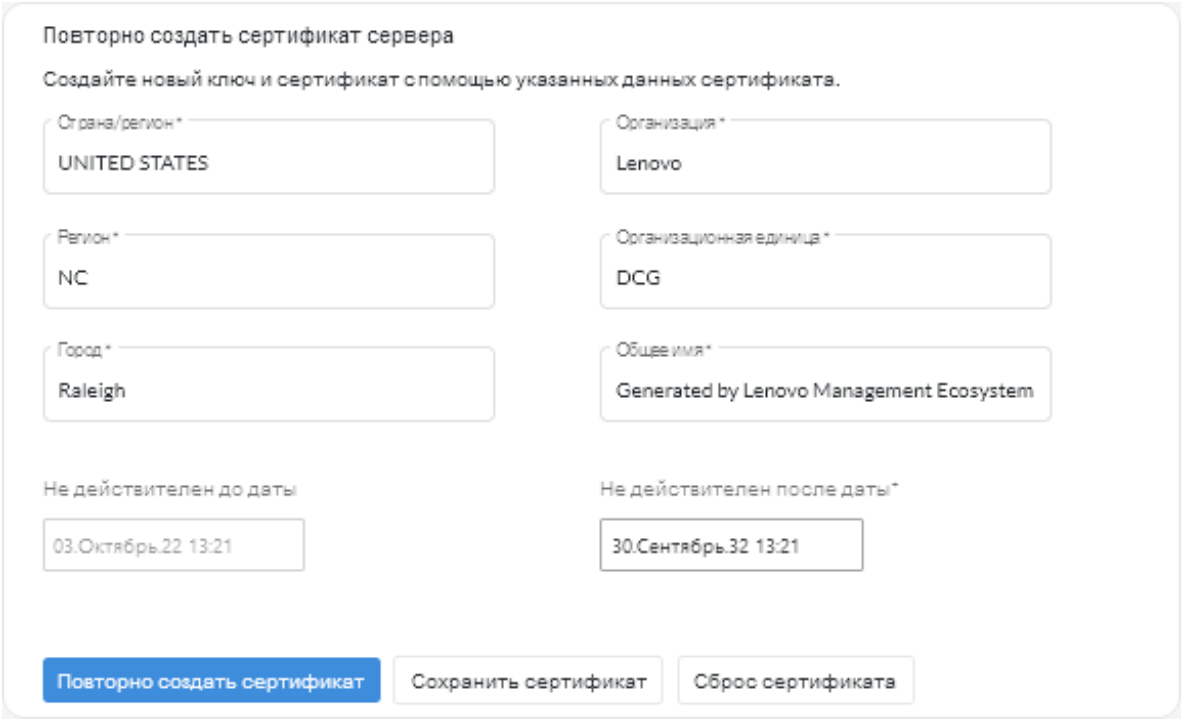
Используемый в настоящее время самозаверяющий сертификат сервера или сертификат сервера, подписанный сторонним центром сертификации, будет использоваться до создания, подписи и установки нового сертификата сервера.

Важно: При изменении сертификата сервера концентратор управления перезапускается и все сеансы пользователей завершаются. Для продолжения работы в веб-интерфейсе пользователи должны снова войти в систему.

Процедура

Чтобы создать самозаверяющий сертификат сервера XClarity Management Hub, выполните следующие действия.

Шаг 1. В строке меню XClarity Management Hub нажмите **Безопасность** (⚙) → **Сертификат сервера**, чтобы открыть карту **Повторно создать самозаверяющий сертификат сервера**.



Шаг 2. На карте **Повторно создать самозаверяющий сертификат сервера** заполните поля для запроса.

- Код страны или региона происхождения согласно ISO 3166, состоящий из двух букв, который будет связан с организацией сертификата (например, US для США).
- Полное название штата или провинции, которое будет связано с сертификатом (например, Калифорния или Нью-Брансуик).
- Полное название города, которое будет связано с сертификатом (например, Сан-Хосе). Длина значения не должна превышать 50 символов.
- Организация (компания), которой будет принадлежать сертификат. Как правило, это официально зарегистрированное название компании. Название должно включать имеющиеся суффиксы, такие как Ltd., Inc. или Corp (например, ACME International Ltd.). Длина этого значения не должна превышать 60 символов.
- (Необязательно) Организационная единица, которой будет принадлежать сертификат (например, ABC Division). Длина этого значения не должна превышать 60 символов.

- Общее имя владельца сертификата. Как правило, это полное доменное имя (FQDN) IP-адрес сервера, использующего сертификат (например, `www.domainname.com` или `192.0.2.0`). Длина этого значения не должна превышать 63 символа.

  Примечание: В настоящее время этот атрибут не влияет на сертификат.

- Дата и время прекращения срока действия сертификата сервера.

  Примечание: В настоящее время эти атрибуты не влияют на сертификат.

Примечание: Изменить альтернативные имена субъекта при повторном создании сертификата сервера нельзя.

Шаг 3. Нажмите **Повторно создать самозаверяющий сертификат сервера**, чтобы повторно создать самозаверяющий сертификат, затем нажмите **Повторно создать сертификат** для подтверждения.Концентратор управления перезапустится, и все установленные сеансы пользователей завершатся.

Шаг 4. Снова войдите в веб-браузер.

После завершения

На карте Повторно создать самозаверяющий сертификат сервера можно выполнить следующие действия.

- Сохранить текущий сертификат сервера в локальной системе в формате PEM, нажав **Сохранить сертификат**.
- Повторно создать сертификат сервера с использованием параметров по умолчанию, нажав **Сбросить сертификат**. При появлении соответствующего запроса нажмите Ctrl+F5, чтобы обновить браузер, а затем снова установите подключение к веб-интерфейсу.

Установка доверенного сертификата сервера, подписанного сторонним центром сертификации, для XClarity Management Hub для пограничных клиентских устройств

Можно выбрать использование доверенного сертификата сервера, который был подписан частным или коммерческим центром сертификации (ЦС). Чтобы использовать сертификат сервера, подписанный сторонним центром, создайте запрос подписи сертификата (CSR) и импортируйте полученный сертификат сервера для замены существующего сертификата сервера.

Перед началом работы

Внимание:

- При установке сертификата сервера Lenovo XClarity Management Hub, подписанного сторонним центром сертификации, с использованием нового корневого ЦС XClarity Management Hub теряет подключение к управляемым устройствам, и необходимо выполнить повторное управление устройствами. При установке сертификата сервера Lenovo XClarity Management Hub, подписанного сторонним центром сертификации, без изменения корневого ЦС (например, если истек срок действия сертификата), нет необходимости выполнять повторное управление устройствами.
- Если новые устройства добавляются после создания CSR и перед импортом подписанного сертификата сервера, эти устройства необходимо перезапустить для получения нового сертификата сервера.

Об этой задаче

Рекомендуется всегда использовать подписанные сертификаты v3.

Сертификат сервера, подписанный сторонним центром, должен быть создан на основе последнего запроса подписи сертификата, созданного с помощью кнопки **Создать файл CSR**.

Сертификат сервера, подписанный сторонним центром, должен быть набором сертификатов, содержащим всю цепочку подписания ЦС, включая корневой сертификат ЦС, все промежуточные сертификаты и сертификат сервера.

Если новый сертификат сервера не подписан сторонним доверенным центром сертификации, при следующем подключении к Lenovo XClarity Management Hub веб-браузер выведет сообщение о безопасности и диалоговое окно с предложением разрешить новый сертификат для браузера. Чтобы избежать появления сообщений о безопасности, можно импортировать сертификат сервера в список доверенных сертификатов веб-браузера (см. раздел Импорт сертификата сервера в веб-браузер для Lenovo XClarity Management Hub для пограничных клиентских устройств).

XClarity Management Hub начинает использовать новый сертификат сервера, не завершая текущий сеанс. Новые сеансы создаются с использованием нового сертификата. Для использования нового используемого сертификата перезагрузите свой веб-браузер.

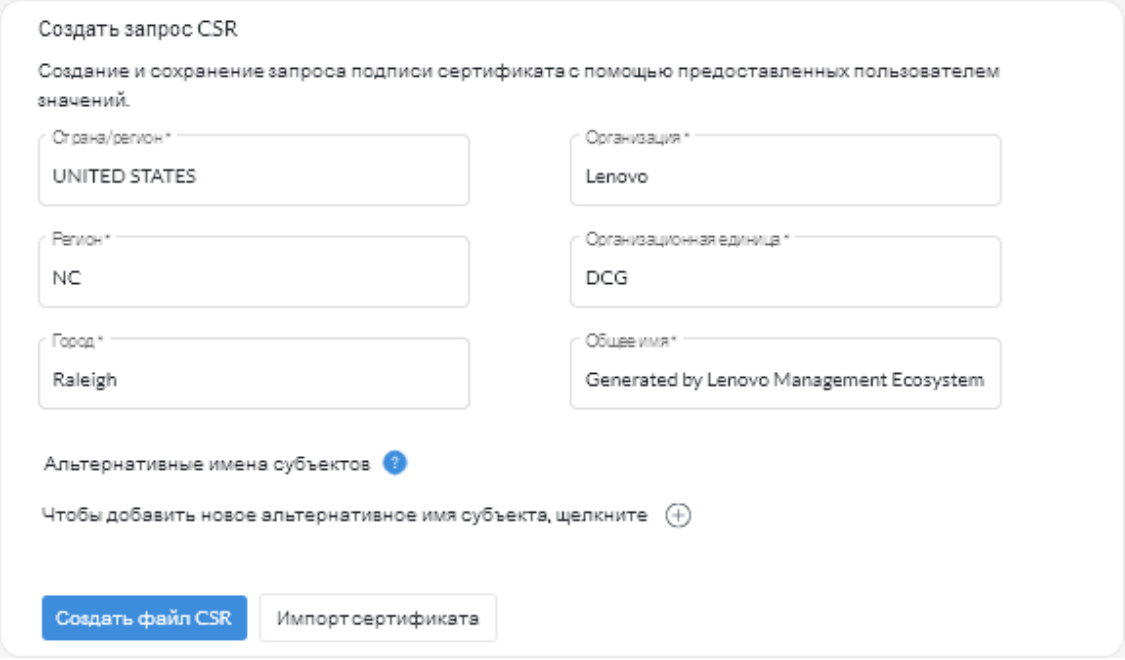
Важно: При изменении сертификата сервера все установленные сеансы пользователей должны принять новый сертификат, обновив браузер с помощью сочетания клавиш Ctrl+F5, а затем снова установить подключение к XClarity Management Hub.

Процедура

Чтобы создать и установить сертификат сервера, подписанный сторонним центром, выполните следующие действия.

Шаг 1. Создайте запрос подписи сертификата и сохраните файл в локальной системе.

1. В строке меню XClarity Management Hub нажмите **Безопасность** ( ) → **Сертификат сервера**, чтобы открыть карту Создание запроса подписи сертификата.



2. Заполните поля для запроса на карте «Создать запрос CSR».
   - Код страны или региона происхождения согласно ISO 3166, состоящий из двух букв, который будет связанный с организацией сертификата (например, US для США).

- Полное название штата или провинции, которое будет связано с сертификатом (например, Калифорния или Нью-Брансуик).
- Полное название города, которое будет связано с сертификатом (например, Сан-Хосе). Длина значения не должна превышать 50 символов.
- Организация (компания), которой будет принадлежать сертификат. Как правило, это официально зарегистрированное название компании. Название должно включать имеющиеся суффиксы, такие как Ltd., Inc. или Corp (например, ACME International Ltd.). Длина этого значения не должна превышать 60 символов.
- (Необязательно) Организационная единица, которой будет принадлежать сертификат (например, ABC Division). Длина этого значения не должна превышать 60 символов.
- Общее имя владельца сертификата. Это должно быть имя хоста сервера, который использует сертификат. Длина этого значения не должна превышать 63 символа.

  Примечание: В настоящее время этот атрибут не влияет на сертификат.
- (Необязательно) Альтернативные имена субъектов, настроенные, удаленные или добавленные в расширение X.509 «subjectAltName» при создании CSR. Указанные альтернативные имена субъектов проверяются (на основе указанного типа) и добавляются в файл CSR только после создания CSR. По умолчанию XClarity Management Hub автоматически определяет альтернативные имена субъектов (SAN) для CSR на основании IP-адреса и имени хоста, обнаруженных сетевыми интерфейсами гостевой операционной системы XClarity Management Hub.

  Внимание: Альтернативные имена субъектов должны включать полное доменное имя (FQDN) или IP-адрес концентратора управления, а имя субъекта должно быть задано равным FQDN концентратора управления. Перед началом процесса CSR проверьте, что эти обязательные поля присутствуют и содержат правильные значения, чтобы гарантировать, что полученный сертификат будет полным. Отсутствие данных сертификата может привести к установке недоверенных соединений при попытке подключить концентратор управления к Lenovo XClarity Orchestrator.

  Указываемое имя должно быть допустимым для выбранного типа.
  - **DNS** (используйте FQDN, например hostname.labs.company.com)
  - **IP-адрес** (например, 192.0.2.0)
  - **Адрес электронной почты** (например, example@company.com)

Шаг 2. Отправьте CSR в доверенный центр сертификации (ЦС). Центр сертификации подпишет CSR и вернет сертификат сервера.

Шаг 3. Импортируйте сертификат сервера, подписанный сторонним центром, и сертификат ЦС в XClarity Management Hub и замените текущий сертификат сервера.

1. На карте «Создать запрос CSR» нажмите **Импортировать сертификат**, чтобы открыть диалоговое окно Импорт сертификата.
2. Скопируйте сертификат сервера и сертификат ЦС в формате PEM. Необходимо указать всю цепочку сертификатов, начиная с сертификата сервера и заканчивая корневым сертификатом ЦС.
3. Нажмите **Импорт**, чтобы сохранить сертификат сервера в доверенном хранилище XClarity Management Hub.

Шаг 4. Примите новый сертификат, нажав Ctrl+F5 для обновления браузера, а затем снова установите подключение к веб-интерфейсу. Это необходимо сделать для всех установленных сеансов пользователей.

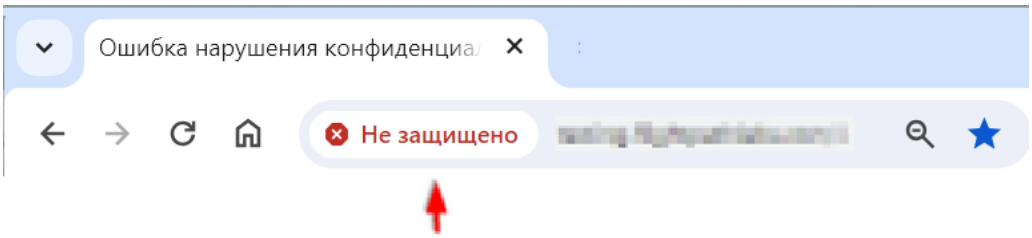
Импорт сертификата сервера в веб-браузер для Lenovo XClarity Management Hub для пограничных клиентских устройств

Можно сохранить копию текущего сертификата сервера в формате PEM в свою локальную систему. Затем можно импортировать сертификат в список доверенных сертификатов веб-браузера или в другие приложения во избежание появления предупреждающих сообщений о безопасности в веб-браузере при доступе к Lenovo XClarity Management Hub.

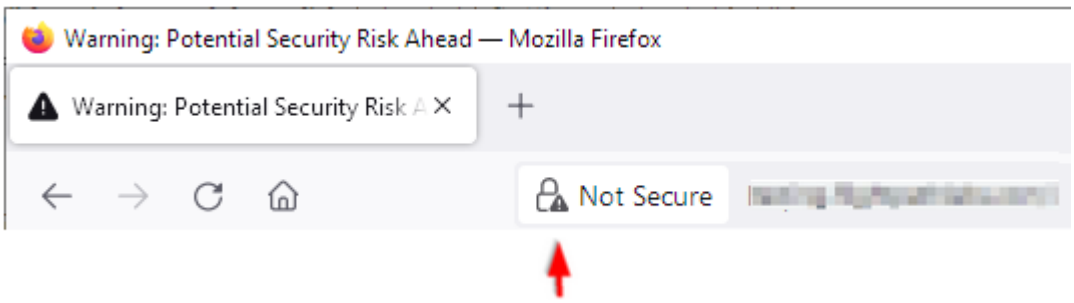
Процедура

Чтобы импортировать сертификат сервера в веб-браузер, выполните следующие действия.

- **Chrome**
  1. Экспортируйте сертификат сервера Lenovo XClarity Management Hub.
     a. Щелкните значок предупреждения «Не безопасно» в верхней адресной строке, например:



     b. Нажмите **Сертификат недопустим**, чтобы открыть диалоговое окно «Сертификат».
     c. Перейдите на вкладку **Сведения**.
     d. Нажмите кнопку **Экспорт**.
     e. Укажите имя и расположение файла сертификата, а затем нажмите кнопку **Сохранить**, чтобы экспортировать сертификат.
     f. Закройте диалоговое окно «Средство просмотра сертификатов».
  2. Импортируйте сертификат сервера Lenovo XClarity Management Hub в список доверенных корневых сертификатов ЦС для своего браузера.
     a. В браузере Chrome щелкните три точки в правом верхнем углу окна и выберите **Параметры**, чтобы открыть страницу Параметры.
     b. Нажмите **Конфиденциальность и безопасность** и выберите **Безопасность**, чтобы отобразить страницу Безопасность.
     c. Прокрутите до раздела **Дополнительные параметры** и нажмите **Управление сертификатами устройств**.
     d. Нажмите **Импорт**, а затем щелкните **Далее**.
     e. Выберите файл сертификата, который вы экспортировали ранее, и нажмите **Далее**.
     f. Выберите место хранения сертификата и нажмите **Далее**.
     g. Нажмите **Готово**.
     h. Закройте и снова откройте браузер Chrome, а затем откройте Lenovo XClarity Management Hub.
- **Firefox**
  1. Экспортируйте сертификат сервера Lenovo XClarity Management Hub.
     a. Щелкните значок предупреждения «Не безопасно» в верхней адресной строке, например:



b. Нажмите **Подключение не защищено** и выберите **Дополнительная информация**.

c. Нажмите **Просмотр сертификата**.

d. Прокрутите вниз до раздела **Разное** и перейдите по ссылке **PEM (серт)**, чтобы сохранить файл в локальной системе.

2. Импортируйте сертификат сервера Lenovo XClarity Management Hub в список доверенных корневых сертификатов ЦС для своего браузера.
   a. Откройте браузер, нажмите **Инструменты → Параметры**, а затем щелкните **Конфиденциальность и безопасность**.
   b. Прокрутите вниз до раздела **Безопасность**.
   c. Нажмите **Просмотреть сертификаты**, чтобы отобразить диалоговое окно Диспетчер сертификатов.
   d. Перейдите на вкладку **Ваши сертификаты**.
   e. Нажмите **Импорт** и перейдите в папку, куда был загружен сертификат.
   f. Выберите сертификат и нажмите **Открыть**.
   g. Закройте диалоговое окно Диспетчер сертификатов.

Подключение XClarity Management Hub для пограничных клиентских устройств к XClarity Orchestrator

После регистрации (подключения) Lenovo XClarity Management Hub в Lenovo XClarity Orchestrator можно начать управление устройствами и их мониторинг.

Перед началом работы

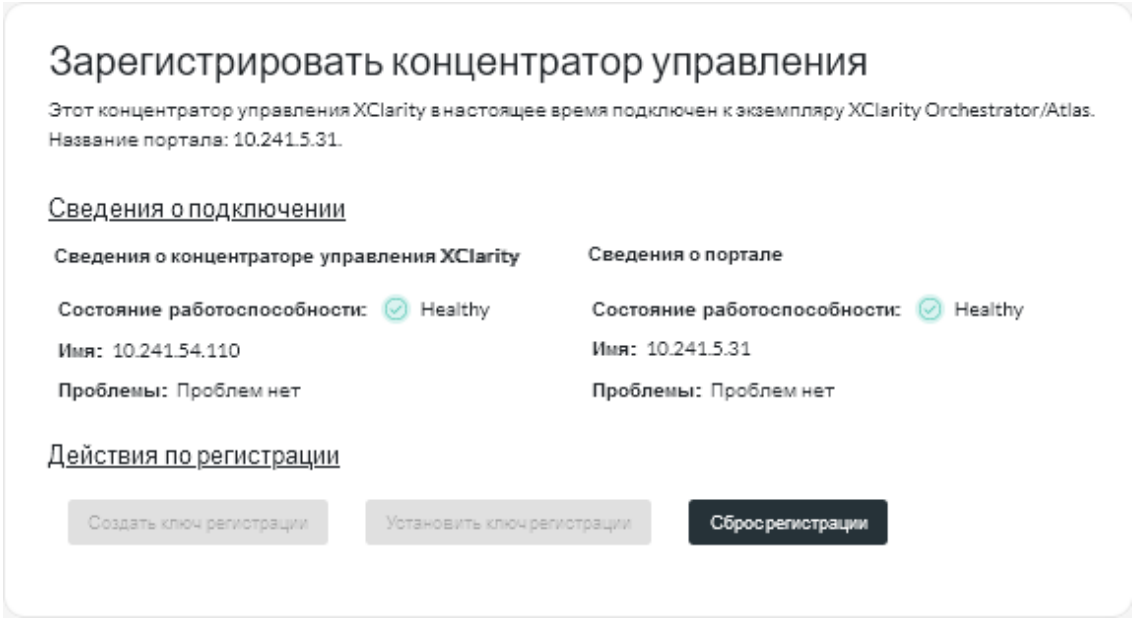
Убедитесь, что решение XClarity Management Hub доступно по сети из XClarity Orchestrator и что решение XClarity Orchestrator доступно по сети из XClarity Management Hub.

Процедура

Чтобы зарегистрировать XClarity Management Hub, выполните следующие действия.

Шаг 1. Создайте ключ регистрации концентратора управления.

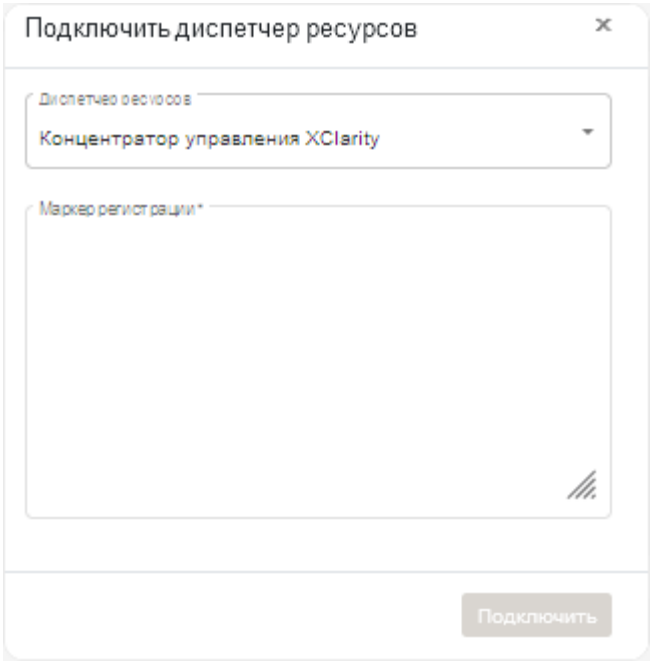
1. В строке меню Management Hub нажмите **Регистрация**, чтобы открыть страницу Регистрация.



2. Нажмите **Создать ключ регистрации**.
3. Нажмите **Копировать в буфер обмена**, чтобы скопировать ключ регистрации, и закройте диалоговое окно.

Шаг 2. Добавьте ключ регистрации концентратора управления в XClarity Orchestrator.

1. В строке меню XClarity Orchestrator нажмите **Ресурсы( ) → Диспетчеры ресурсов**, чтобы открыть карту Диспетчеры ресурсов.
2. Нажмите значок **Подключить** ( ), чтобы открыть диспетчер ресурсов. Диалоговое окно Подключить диспетчер ресурсов.



3. Выберите **XClarity Management Hub** в качестве диспетчера ресурсов.
4. Скопируйте ключ регистрации в поле **Маркер регистрации**.

5. Нажмите **Подключить**, чтобы открыть диалоговое окно Подключить диспетчер ресурсов, которое содержит ключ регистрации XClarity Orchestrator.
6. Нажмите **Копировать в буфер обмена**, чтобы скопировать ключ регистрации, и закройте диалоговое окно.

Шаг 3. Добавьте ключ регистрации XClarity Orchestrator в концентратор управления.

1. В строке меню Management Hub нажмите **Регистрация**, чтобы открыть страницу «Регистрация».
2. Нажмите **Установить ключ регистрации**.
3. Скопируйте ключ регистрации в поле **Маркер регистрации**.
4. Нажмите **Подключить**.

После завершения

- Управляйте устройствами с помощью концентратора управления (см. раздел Управление устройствами ThinkEdge Client в документации по XClarity Orchestrator в Интернете).
- Удалите текущий ключ регистрации концентратора управления, нажав **Сброс регистрации**.

Глава 3. Удаление XClarity Management Hub для пограничных клиентских устройств

Выполните эти действия, чтобы удалить виртуальное устройство XClarity Management Hub.

Процедура

Чтобы удалить виртуальное устройство XClarity Management Hub, выполните указанные ниже действия.

Шаг 1. Удалите все устройства, которые в настоящее время находятся под управлением XClarity Management Hub

Шаг 2. Для удаления XClarity Management Hub выполните указанные ниже действия в зависимости от операционной системы.

- **ESXi**
  1. Подключитесь к хосту с помощью VMware vSphere Client.
  2. Нажмите правой кнопкой мыши виртуальную машину и выберите **Питание → Выключить питание**.
  3. Снова нажмите правой кнопкой мыши виртуальную машину и выберите **Удалить с диска**.

Lenovo