Руководство по развертыванию VMware Workspace ONE с VMware Identity Manager

Сентябрь 2018 г.
VMware Workspace ONE

vmware®

Актуальная техническая документация доступна на веб-сайте VMware:

https://docs.vmware.com/ru/

Также на веб-сайте VMware доступны последние обновления продуктов.

Все замечания по данной документации можно отправлять по адресу:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Россия
Россия, 125284, г. Москва
ул. Беговая, д.3, стр.1
Бизнес-центр "NORDSTAR TOWER" 30й этаж
Телефон: +7 495 212 29 00
www.vmware.com/ru

Содержание

О развертывании VMware Workspace ONE

В руководстве по развертыванию VMware Workspace™ ONE™ с VMware Identity Manager содержатся сведения об интеграции VMware Identity Manager™ с VMware Workspace ONE UEM™ с помощью AirWatch, благодаря чему можно настроить единый вход в Workspace ONE, управление устройствами в Workspace ONE UEM и VMware Workspace ONE в качестве каталога приложений.

После интеграции Workspace ONE UEM с VMware Identity Manager пользователи зарегистрированных устройств Workspace ONE UEM могут безопасно входить во включенные приложения без необходимости вводить несколько паролей.

Целевая аудитория

Эти сведения предназначены для администраторов, которые уже работали со службами Workspace ONE UEM и VMware Identity Manager.

Версия за сентябрь 2018 г. применяется к облачной версии VMware Identity Manager (сентябрь 2018 г.), VMware Identity Manager 3.3 и Workspace ONE UEM 9.7.

Введение в Workspace ONE

1

VMware Workspace® ONE® — это безопасная корпоративная платформа, предоставляющая возможность работы с устройствами с iOS, Android и Windows 10, а также возможность управления ими. На платформе Workspace ONE предусмотрено управление удостоверениями, приложениями и корпоративной мобильной средой.

За счет интеграции VMware Workspace ONE UEM® с VMware Identity Manager™ вы получаете каталог Workspace ONE с приложениями и службами управления доступом к мобильным устройствам.

Службы VMware Identity Manager предоставляют компоненты, связанные с удостоверениями, включая методы проверки подлинности для пользователей, которые используют для входа на ресурсы единый вход. Для управления доступом к этим устройствам создается набор политик, связанных с сетевыми подключениями и проверкой подлинности.

Службы Workspace ONE UEM предоставляют средства регистрации устройств, распространения приложений и проверки соответствия нормативным требованиям, чтобы обеспечить соответствие устройств с удаленным доступом корпоративным стандартам безопасности. С зарегистрированных устройств Workspace ONE UEM пользователи могут безопасно выполнять вход в активированные приложения без ввода нескольких паролей.

В эту главу входят следующие разделы:

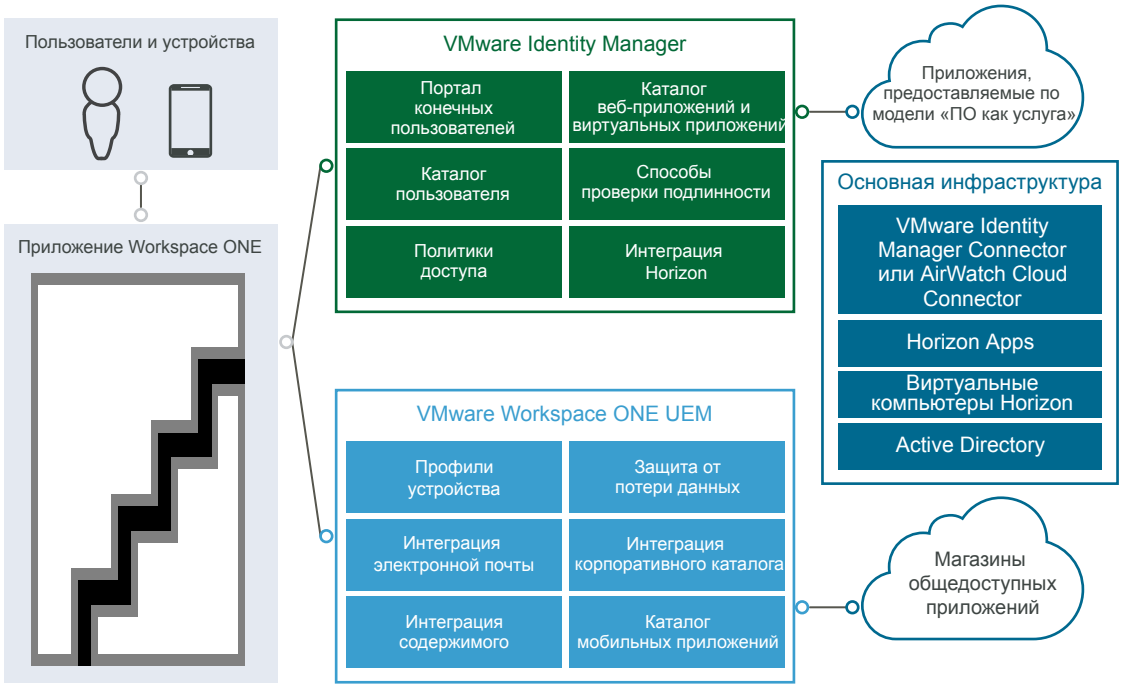
Обзор архитектуры Workspace ONE

Workspace ONE обеспечивает безопасный доступ пользователей к облачным и мобильным приложениям, а также к приложениям для Windows из единого каталога. К родному приложению Workspace ONE можно получить доступ с устройств с iOS, Android и Windows 10.

При развертывании Workspace ONE нужно внедрить следующие службы VMware Identity Manager и Workspace ONE UEM.

- Можно настроить либо компонент соединителя VMware Identity Manager, либо компонент AirWatch Cloud Connector.
- Выполните интеграцию корпоративной версии Active Directory с VMware Identity Manager или Workspace ONE UEM Cloud Connector для синхронизации пользователей и групп Active Directory со службой Workspace ONE.
- Настройте VMware Identity Manager с ключами API-интерфейса Workspace ONE UEM и корневым сертификатом администратора, а также включите каталог Workspace ONE, проверку соответствия нормативным требованиям и проверку подлинности пользователя с помощью пароля в Workspace ONE UEM.

Рис. 1-1. Обзор архитектуры **Workspace ONE**



Требования

Ниже указаны системные требования для Workspace ONE.

Таблица 1-1. Системные требования для Workspace ONE

Требования для Workspace ONE	Сведения
Active Directory	Windows Server 2008 и 2008 R2 Windows Server 2012 и 2012 R2
Веб-браузер для доступа к консоли VMware Identity Manager и Workspace ONE	Internet Explorer 11 для Windows Google Chrome 4.0 и более поздних версий Mozilla Firefox 4.0 и более поздних версий Safari 6.2.8 и более поздних версий
VMware Identity Manager Connector или AirWatch Cloud Connector установлены.	Windows Server 2008 R2 Windows Server 2012 или 2012 R2 .NET Framework 4.6.2 Руководство по установке соединителя VMware Identity Manager см. в центре документации по VMware Identity Manager. Руководство по установке AirWatch Cloud Connector см. в центре документации по Workspace ONE UEM.

Сведения о компонентах Workspace ONE

Ниже описаны основные компоненты Workspace ONE

Собственные мобильные приложения Workspace ONE

Пользователи могут установить приложение Workspace ONE на мобильном устройстве и использовать корпоративные учетные данные для единого входа в корпоративные, облачные и мобильные устройства.

Каталог приложений с возможностью самообслуживания для веб-ресурсов, а также ресурсов Horizon и Citrix

Workspace ONE обеспечивает доступ пользователей к облачным и мобильным приложениям, а также к приложениям для Windows из единого каталога. Каталог содержит приложения, опубликованные в VMware Identity Manager и VMware Workspace ONE UEM. Поддерживаются внутренние веб-приложения, приложения, предоставляемые по модели «ПО как услуга», собственные приложения, приложения, разработанные собственными силами, старые и новые версии приложений для Windows, приложения Horizon 7, VMware Horizon Cloud Service™, опубликованные приложения Citrix и пакеты ThinApp. В магазине приложений также есть виртуализированные настольные компьютеры.

Запуск веб-приложений и виртуальных приложений с использованием единого входа

Workspace ONE предоставляет возможность мобильного единого входа — реализацию входа в мобильные приложения одним касанием. Возможность единого входа на мобильные устройства доступна для устройств с Android, iOS и Windows 10.

Условный доступ и соответствие устройства политикам

С помощью Workspace ONE можно применить условный доступ с учетом диапазона сети, платформы и критериев проверки подлинности для конкретного приложения. Прежде чем предоставить право на использование приложения, нужно убедиться в соответствии устройства правилам безопасности. В VMware Identity Manager предусмотрен параметр политики доступа, с помощью которого на сервере Workspace ONE UEM можно инициировать проверку состояния соответствия устройства, когда пользователи входят в систему с такого устройства.

Многофакторная аутентификация

В Workspace ONE предусмотрена возможность многофакторной проверки подлинности через приложение VMware Verify. При попытке доступа к каталогу Workspace ONE или к любому приложению, требующему строгой проверки подлинности, VMware Verify отправляет уведомление на телефон пользователя. Чтобы подтвердить право на доступ к Workspace ONE при попытке его получения, пользователю нужно провести пальцем по параметру «Принять» для открытия приложения.

Адаптивное управление

Для приложений, требующих базового уровня защиты, пользователям не нужно регистрировать устройства в Workspace ONE UEM Mobile Device Management™. Пользователи могут загрузить мобильное приложение Workspace ONE и выбрать приложения, которые следует установить. Для приложений, требующих более высокого уровня защиты, пользователи могут зарегистрировать свои устройства в Workspace ONE UEM непосредственно из мобильного приложения Workspace ONE.

Начало работы с мастером Workspace ONE

Мастер начальной настройки Workspace ONE поможет настроить параметры для интеграции служб Workspace ONE UEM и VMware Identity Manager с целью создания среды Workspace ONE.

Мастер начальной настройки не заменяет возможности настройки и изменения отдельных параметров. Он лишь автоматизирует значительную часть процедур начальной настройки для большинства пользователей.

С помощью мастера начальной настройки Workspace ONE можно настроить следующие компоненты.

- Enterprise Connector и Directory. Мастер помогает настроить VMware Enterprise System Connector и подключение Active Directory в Workspace ONE UEM Cloud Connector для импорта пользователей и групп из каталога компании. Сведения о настройке Enterprise Connector см. в руководстве по быстрой настройке VMware Workspace ONE.

- Автоматическое обнаружение. Чтобы пользователям было проще получить доступ к порталу приложений из приложения Workspace ONE, можно запустить мастер, чтобы зарегистрировать домен электронной почты в службе автоматического обнаружения. Затем вместо URL-адреса организации конечные пользователи могут вводить свой адрес электронной почты.
- Каталог Workspace ONE. Мастер настройки каталога Workspace ONE поможет настроить каталог Workspace ONE. На этапе настройки фирменной символики в Workspace ONE можно добавить сведения о фирменной символике компании в каталог и приложение Workspace ONE. Сведения о настройке каталога Workspace ONE см. в руководстве по быстрой настройке VMware Workspace ONE.
- Адаптивное управление. Настройте адаптивное управление, чтобы ограничить доступ к определенным приложениям, которыми в этом случае можно будет воспользоваться, только если на устройстве пользователя установлен соответствующий профиль. Профиль гарантирует возможность удаления корпоративных приложений и данных по требованию. Кроме того, можно задать требование, в соответствии с которым управление общедоступными приложениями, а также их использование должны осуществляться отдельно. Для этого их нужно вручную загрузить из магазина приложений.

Мастер начальной настройки может оповестить о том, что в службе Workspace ONE UEM или VMware Identity Manager имеются потенциально конфликтные конфигурации. В этом случае, а также если в мастере начальной настройки выполнены не все действия, компоненты можно настроить вручную. Это руководство поможет вам вручную настроить службы Workspace ONE UEM и VMware Identity Manager для Workspace ONE.

Интеграция Workspace ONE UEM с VMware Identity Manager 2

Чтобы настроить службы Workspace ONE UEM для управления мобильными устройствами со службами VMware Identity Manager для управления единым входом и учетными записями пользователей, необходимо их интегрировать.

При интеграции Workspace ONE UEM с VMware Identity Manager пользователи зарегистрированных устройств Workspace ONE UEM могут входить в Workspace ONE и безопасно получать доступ к активированным для них приложениям, не вводя несколько паролей.

Мастер начальной настройки Workspace ONE поможет вам настроить и интегрировать Workspace ONE UEM с VMware Identity Manager. Сведения о работе с мастерами Workspace ONE см. в кратком руководстве по настройке VMware Workspace ONE.

В эту главу входят следующие разделы:

Настройка интеграции в консоли Workspace ONE UEM

Для интеграции со службами VMware Identity Manager настройте следующие параметры в консоли Workspace ONE UEM.

- Ключ REST API администратора для обмена данными со службой VMware Identity Manager
- Ключ REST API зарегистрированного пользователя для проверки подлинности с помощью пароля AirWatch Cloud Connector, созданный в той же самой организационной группе, в которой настроено решение VMware Identity Manager.

- Учетная запись администратора API для VMware Identity Manager и сертификата проверки подлинности, экспортированного из Workspace ONE UEM и добавленного к параметрам AirWatch консоли VMware Identity Manager.

Создание ключей REST API в Workspace ONE UEM

В консоли Workspace ONE UEM для интеграции VMware Identity Manager с Workspace ONE UEM должен быть включен доступ к API-интерфейсу администратора REST и доступ для зарегистрированных пользователей. При включении доступа API создается ключ API.

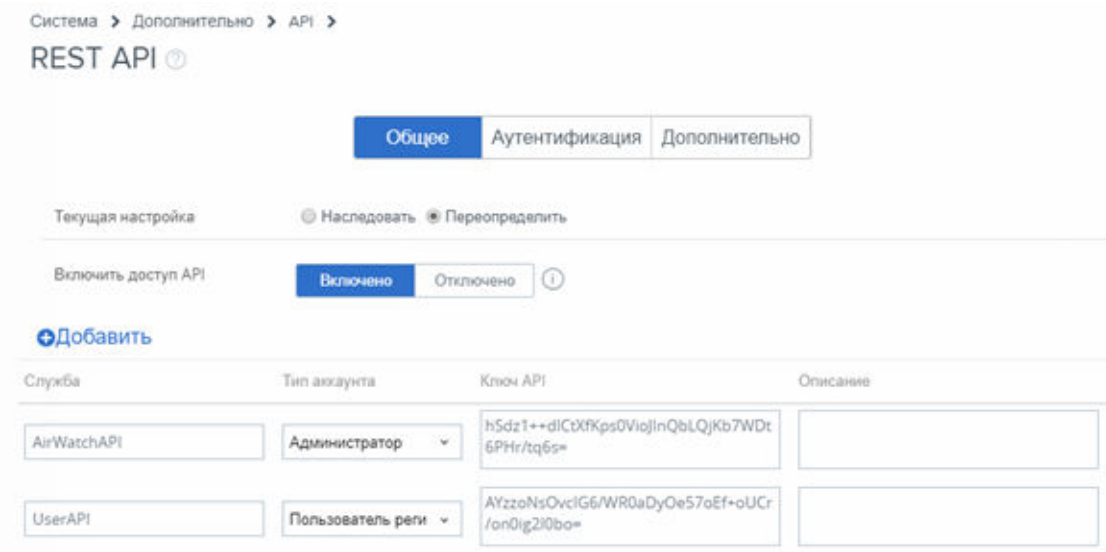
Процедура

1. В консоли Workspace ONE UEM укажите параметр «Глобально», а затем щелкните группу организации на уровне заказчика и выберите **Группы и настройки > Все настройки > Система > Дополнительно > API > REST API**.
2. На вкладке «Общие» нажмите кнопку **Добавить**, чтобы создать ключ API, который будет использоваться в службе VMware Identity Manager. Учетная запись должна принадлежать к типу **Администратор**.

   Введите уникальное имя службы. Добавьте описание, например **`AirWatchAPI для IDM`**.
3. Чтобы создать ключ API для зарегистрированного пользователя, нажмите кнопку **Добавить**.
4. В раскрывающемся меню «Тип учетной записи» выберите **Пользователь регистрации**.

   Введите уникальное имя службы. Добавьте описание, например **`UserAPI для IDM`**.
5. Скопируйте ключи API и сохраните их в файл.

   Добавьте эти ключи во время настройки Workspace ONE UEM (AirWatch) в консоли VMware Identity Manage.



6. Нажмите кнопку **Сохранить**.

Экспорт корневого сертификата администратора VMware Workspace ONE UEM

После создания ключа API для администратора можно добавить учетную запись администратора и настроить проверку подлинности с помощью сертификата в консоли Workspace ONE UEM.

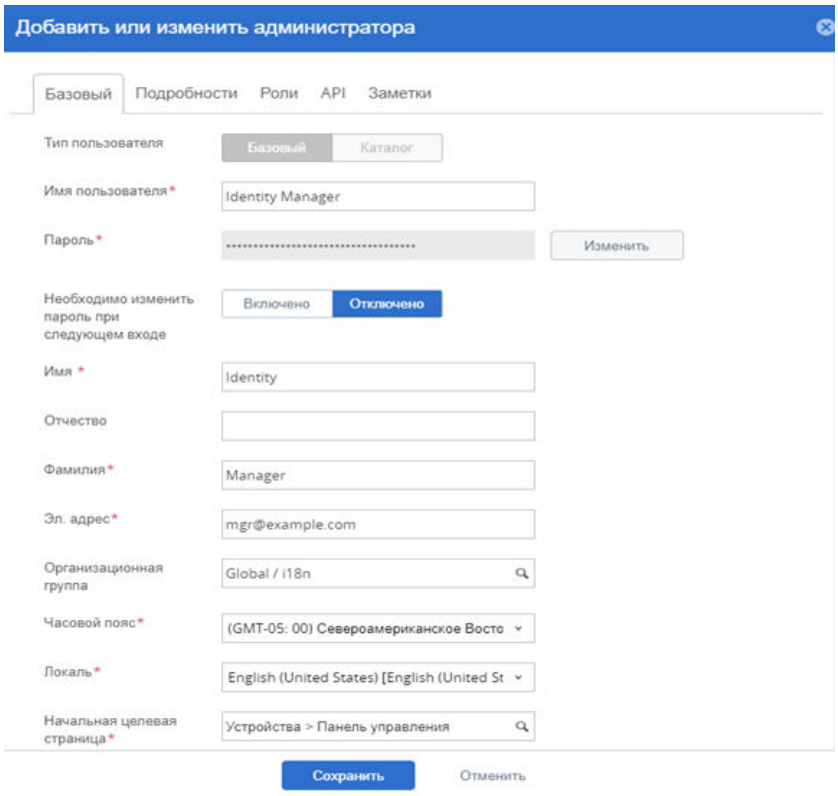
Для проверки подлинности с помощью сертификата REST API в консоли Workspace ONE UEM создается сертификат уровня пользователя. При этом используется самозаверяющий сертификат Workspace ONE UEM, созданный на основе корневого сертификата администратора Workspace ONE UEM.

Необходимые условия

Создан ключ API администратора Workspace ONE UEM REST.

Процедура

1. В консоли Workspace ONE UEM выберите параметр «Глобально», а затем щелкните группу организации на уровне заказчика и выберите **Учетные записи > Администраторы > Список**.
2. Щелкните **Добавить > Добавить админа**.
3. На вкладке «Базовый» введите в соответствующих текстовых полях имя пользователя администратора сертификата и его пароль.

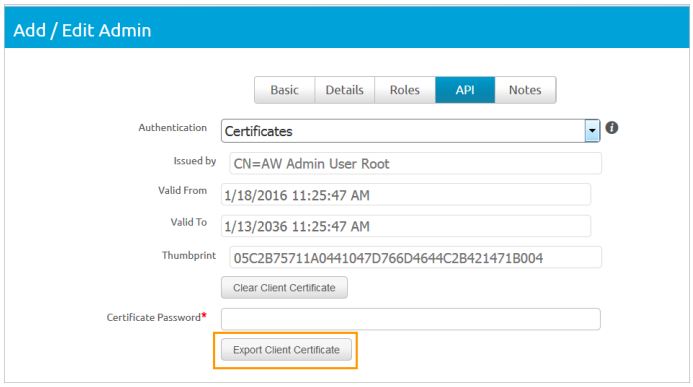


4. Перейдите на вкладку «Роли», выберите текущую организационную группу, щелкните второе текстовое поле и выберите **Администратор AirWatch**.

5. Выберите вкладку API, а затем в текстовом поле «Аутентификация» выберите **Сертификаты**.
6. Введите пароль сертификата. Это тот же пароль, который введен для администратора на вкладке «Базовый».
7. Нажмите кнопку **Сохранить**.

   В результате будет создана новая учетная запись администратора и сертификат клиента.
8. На странице «Список» выберите созданного администратора и откройте вкладку «API» снова.

   На странице сертификаты отображаются сведения о сертификате.
9. Введите пароль, заданный в текстовом поле «Пароль сертификата», щелкните **Экспортировать клиентские сертификаты** и сохраните файл.



Сертификат клиента сохраняется в виде файла типа P12.

Следующие шаги

Настройте параметры URL-адреса Workspace ONE UEM в консоли VMware Identity Manager.

Настройка экземпляра **Workspace ONE UEM** в **VMware Identity Manager**

После настройки параметров в консоли Workspace ONE UEM введите URL-адрес Workspace ONE UEM, значения ключей API и сертификат на странице «Управление учетными данными и доступом» в консоли VMware Identity Manager. После настройки параметров Workspace ONE UEM можно включить параметры, доступные для Workspace ONE.

Добавление параметров **Workspace ONE UEM** в **VMware Identity Manager**

Настройте параметры Workspace ONE UEM в VMware Identity Manager для интеграции Workspace ONE UEM с VMware Identity Manager и включите параметры интеграции компонента Workspace ONE UEM. Для авторизации VMware Identity Manager в Workspace ONE UEM необходимо добавить ключ API-интерфейса Workspace ONE UEM и сертификат.

Необходимые условия

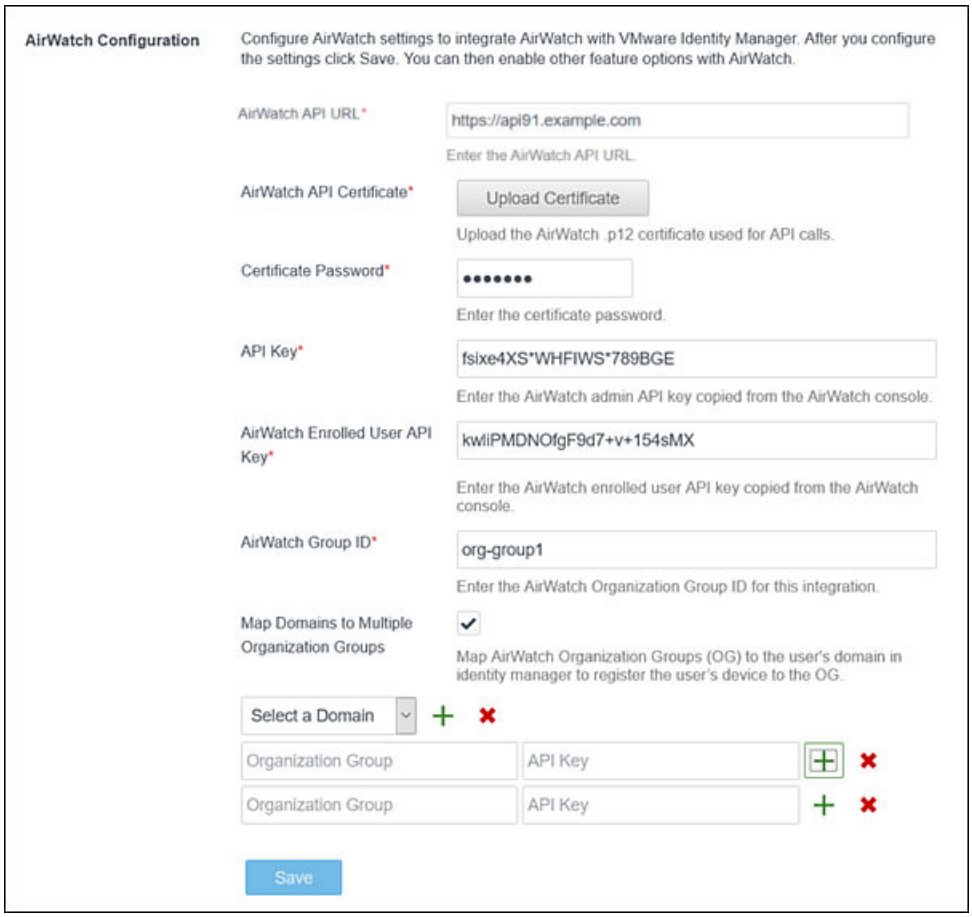
- URL-адрес сервера Workspace ONE UEM, который использует администратор, чтобы войти в консоль Workspace ONE UEM.
- Ключ API-интерфейса администратора Workspace ONE UEM, с помощью которого выполняются запросы API от VMware Identity Manager к серверу Workspace ONE UEM для настройки интеграции.
- Файл сертификата Workspace ONE UEM, используемый для выполнения вызовов API-интерфейса, и пароль сертификата. У файла сертификата должен быть формат P12.
- Ключ API-интерфейса зарегистрированного пользователя Workspace ONE UEM.
- Идентификатор группы Workspace ONE UEM для арендатора, который является идентификатором арендатора в Workspace ONE UEM.

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» щелкните **Настройка > AirWatch**.
2. Введите параметры интеграции Workspace ONE UEM в следующих полях.

Поле	Описание
URL-адрес API-интерфейса AirWatch	Введите URL-адрес Workspace ONE UEM. Например, **`https://myco.ws1uem.com`**
Сертификат API-интерфейса AirWatch	Передайте файл сертификата, используемый для выполнения вызовов API-интерфейса.
Пароль сертификата	Введите пароль сертификата.
Ключ API-интерфейса администратора AirWatch	Введите значение ключа API-интерфейса администратора. Пример значения ключа API-интерфейса: `FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc +jveeYs=`
Ключ API-интерфейса зарегистрированного пользователя AirWatch	Введите значение ключа API-интерфейса зарегистрированного пользователя.
Идентификатор группы AirWatch.	Введите идентификатор группы Workspace ONE UEM для организационной группы, в которой созданы ключ API-интерфейса и учетная запись администратора.

3. Нажмите кнопку **Сохранить**.



Следующие шаги

Включите параметр функции «Каталог Workspace ONE», чтобы объединить приложения, установленные в каталоге Workspace ONE UEM, с каталогом Workspace ONE.

- Для проверки соответствия устройств под управлением Workspace ONE UEM политикам Workspace ONE UEM включите проверку соответствия.

См. раздел Включение проверки соответствия для управляемых устройств Workspace ONE UEM.

Сопоставление доменов **VMware Identity Manager** с несколькими организационными группами в **Workspace ONE UEM**

При настройке пользователей и устройств в Workspace ONE UEM для группировки пользователей и настройки разрешений используются организационные группы Workspace ONE UEM. При интеграции Workspace ONE UEM с VMware Identity Manager ключи REST API администратора и регистрирующегося пользователя настраиваются в организационной группе Workspace ONE UEM типа «Заказчик».

В средах Workspace ONE UEM с настроенной поддержкой нескольких арендаторов для пользователей и устройств создается несколько организационных групп. Устройства регистрируются в организационных группах. В среде с поддержкой нескольких арендаторов организационные группы можно настроить в уникальных конфигурациях, например организационные группы по отдельным географическим регионам, отделам или примерам использования.

Для управления регистрацией устройства в Workspace ONE можно связать домены, настроенные в VMware Identity Manager, с отдельными организационными группами в Workspace ONE UEM. При входе пользователя в Workspace ONE в VMware Identity Manager инициируется событие регистрации устройства. Во время регистрации устройства в Workspace ONE UEM отправляется запрос на получение приложений, которые может использовать определенный пользователь на конкретном устройстве.

При интеграции Workspace ONE UEM с VMware Identity Manager следует идентифицировать организационные группы устройств, чтобы диспетчер Identity Manager смог найти пользователя и успешно зарегистрировать устройство в соответствующей организационной группе.

При настройке параметров Workspace ONE UEM в службе VMware Identity Manager можно ввести идентификаторы и ключи API организационных групп устройства для сопоставления нескольких организационных групп с доменом. Когда пользователь входит в Workspace ONE со своего устройства, выполняется проверка записей об этом пользователе и регистрация устройства в соответствующей организационной группе в Workspace ONE UEM.

Дополнительные сведения о настройке нескольких организационных групп см. в разделе Стратегии развертывания для настройки нескольких организационных групп Workspace ONE UEM.

Примечание При интеграции Workspace ONE UEM с VMware Identity Manager и настройке нескольких организационных групп Workspace ONE UEM глобальный каталог Active Directory нельзя настроить для использования вместе со службой VMware Identity Manager.

Включение каталога **Workspace ONE** для **Workspace ONE UEM**

При настройке VMware Identity Manager с помощью экземпляра Workspace ONE UEM можно включить каталог Workspace ONE, чтобы добавить приложения из каталога Workspace ONE UEM. На портале Workspace ONE конечные пользователи могут просматривать все приложения, на доступ к которым у них есть права.

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» щелкните **Настройка > AirWatch** и перейдите в раздел каталога Workspace ONE.

2. Чтобы добавить приложения из каталога AirWatch к приложениям в каталоге Identity Manager, включите параметры **Получить из IDM** и **Получить из Airwatch**.

   При использовании каталога Workspace ONE на мобильных устройствах без настроенной службы VMware Identity Manager выберите только параметр **Получить из AirWatch**.

   Параметр **Получить из IDM** включен по умолчанию.

3. Нажмите кнопку **Сохранить**.

Следующие шаги

Конечных пользователей Workspace ONE UEM следует уведомить о том, как можно получить доступ к каталогу и просматривать портал Workspace ONE.

Включение проверки соответствия для управляемых устройств Workspace ONE UEM

Когда пользователи регистрируют устройства, устанавливается расписание, по которому отправляются образцы данных, используемые для оценки соответствия нормативным требованиям. Оценка этого образца данных позволяет убедиться в том, что устройство отвечает требованиям к соответствию, которые установил администратор в консоли Workspace ONE UEM (UEM). Если устройство не соответствует нормативным требованиям, будут предприниматься определенные действия, настроенные в консоли UEM.

В службе VMware Identity Manager предусмотрен параметр политики доступа, который можно настроить для проверки состояния соответствия устройства на сервере Workspace ONE UEM, когда пользователи входят в систему с такого устройства. Проверка соответствия гарантирует, что пользователям будут запрещены вход в приложение или использование единого входа на портал Workspace ONE, если устройство не соответствует нормативным требованиям. Когда устройство снова будет соответствовать нормативным требованиям, возможность войти будет восстановлена.

Если устройство скомпрометировано, приложение Workspace ONE автоматически выполняет выход из системы и блокирует доступ к приложениям. Если устройство зарегистрировано с помощью адаптивного управления, через консоль UEM будет отправлена команда очистки корпоративных данных для отмены регистрации устройства и удаления с устройства всех управляемых приложений. Неуправляемые приложения не будут удалены.

Дополнительные сведения о политиках соответствия Workspace ONE UEM см. в руководстве по VMware Workspace ONE UEM Mobile Device Management на странице документации по VMware Workspace ONE UEM.

Включение проверки подлинности с помощью пароля пользователя с использованием Workspace ONE UEM

Чтобы внедрить проверку подлинности с помощью AirWatch Cloud Connector, необходимо включить проверку подлинности с помощью пароля, используя функцию Workspace ONE UEM.

Необходимые условия

- Выполнена настройка Workspace ONE UEM в VMware Identity Manager.
- Установка и активация AirWatch Cloud Connector.
- Интеграция служб каталогов Workspace ONE UEM с Active Directory.

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» щелкните **Настройка > AirWatch**
2. В разделе «Проверка подлинности с помощью пароля пользователя на платформе AirWatch» щелкните **Включить**.
3. Нажмите кнопку **Сохранить**.

Следующие шаги

Для получения дополнительных сведений об использовании проверки подлинности AirWatch Cloud Connector см. Проверка подлинности с помощью AirWatch Cloud Connector.

Настройка правил проверки соответствия

Если проверка соответствия включена, создайте правило политики доступа, для которого требуется проверка подлинности и проверка соответствия для устройств, управляемых Workspace ONE UEM.

Правило политики проверки соответствия работает вместе с системой единого входа для мобильных устройств с iOS, единого входа для мобильных устройствах с Android и развертыванием сертификатов в облачной среде. При настройке правила метод проверки подлинности необходимо настраивать перед методом проверки соответствия устройства.

Необходимые условия

Методы проверки подлинности настроены и связаны со встроенным поставщиком данных.

Проверка соответствия включена на странице VMware Identity Manager AirWatch.

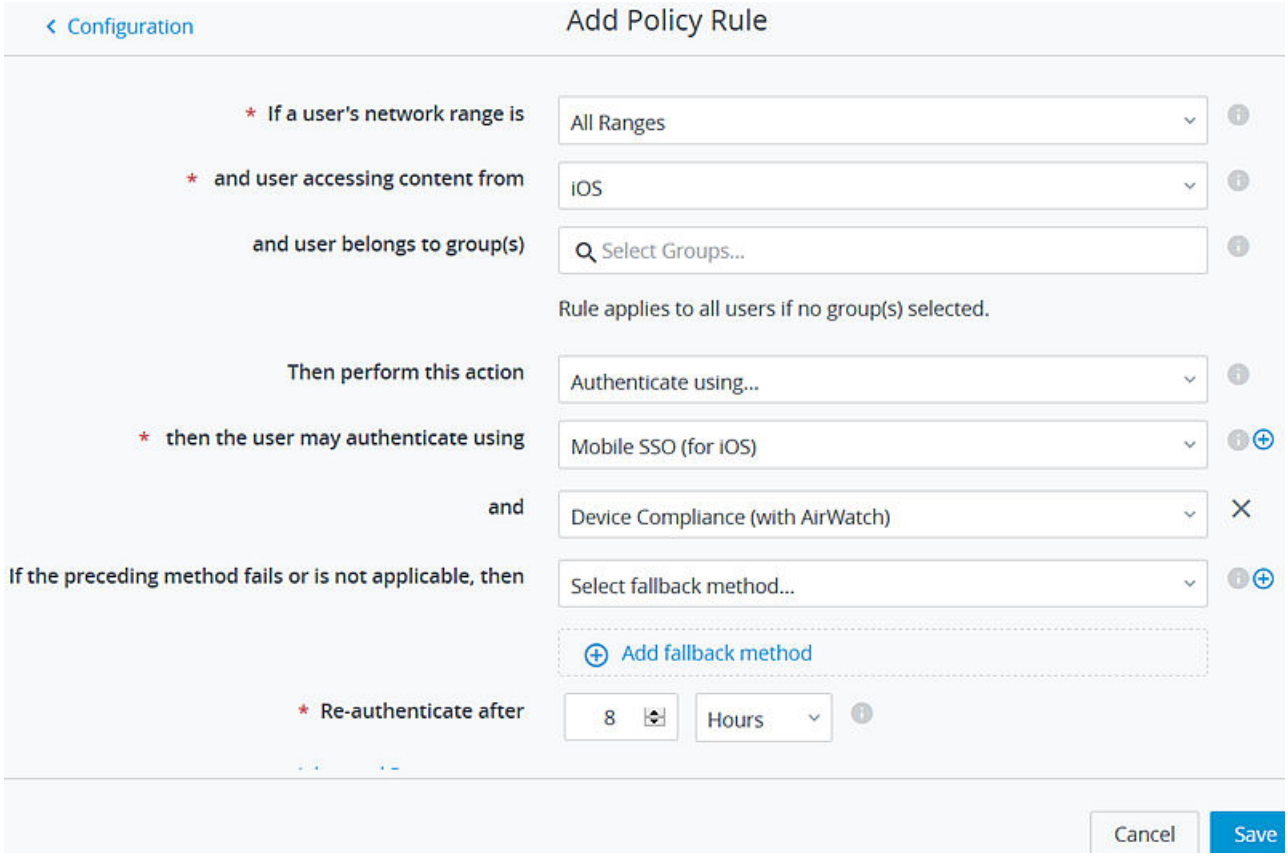
Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» выберите **Управление > Политики**.
2. Щелкните **Редактировать политику по умолчанию**.
3. Нажмите кнопку **Далее**.

4. Щелкните **Добавить правило политики** для добавления правила или выберите правило для изменения.

Параметр	Описание
Если сетевой диапазон для пользователя составляет	Убедитесь в правильности сетевого диапазона, при добавлении правила выберите сетевой диапазон.
и пользователи получают доступ к содержимому из	Выберите тип мобильного устройства.
и пользователи принадлежат к группам	Если это правило доступа применяется к определенным группам, выберите группы в поле поиска. Если не указана группа, политика доступа применяется ко всем пользователям.
Затем выполните следующее действие	Выберите **Проверка подлинности с помощью...**
затем пользователь может выполнить проверку подлинности с помощью	Выберите метод проверки подлинности мобильного устройства, чтобы применить его. Щелкните + и в раскрывающемся меню выберите пункт **Соответствие устройства (с AirWatch)**.
Если предыдущие методы не выполняются или не применяются, то	При необходимости настройте резервный метод проверки подлинности.
Выполните повторную проверку подлинности через	Выберите продолжительность сеанса, после которого пользователи должны выполнять повторную проверку подлинности.

5. Нажмите кнопку **Сохранить**.



Обновление **VMware Identity Manager** после обновления **Workspace ONE UEM**

При обновлении Workspace ONE UEM до новой версии необходимо обновить параметры каталога Workspace ONE и проверки подлинности пользователя с помощью пароля на странице конфигурации AirWatch в консоли VMware Identity Manager.

При сохранении этих параметров после обновления Workspace ONE UEM параметры AirWatch в службе VMware Identity Manager обновляются до новой версии Workspace ONE UEM.

Процедура

1. После обновления Workspace ONE UEM войдите в консоль VMware Identity Manager.
2. На вкладке «Управление учетными данными и доступом» щелкните **Настройка > AirWatch**.
3. Прокрутите страницу вниз до раздела **Каталог Workspace ONE** и нажмите кнопку **Сохранить**.
4. Прокрутите страницу вниз до раздела **Проверка подлинности с помощью пароля пользователя на платформе AirWatch** и нажмите кнопку **Сохранить**.

Конфигурация Workspace ONE UEM обновляется до новой версии в службе VMware Identity Manager.

Проверка подлинности с помощью AirWatch Cloud Connector

Компонент AirWatch Cloud Connector (ACC) решения VMware Enterprise Systems Connector интегрирован с VMware Identity Manager для проверки подлинности пользователя с помощью пароля в Workspace ONE.

Примечание Компонент ACC устанавливается и настраивается в Workspace ONE UEM. Сведения о том, как установить и настроить AirWatch Cloud Connector, см. в руководстве по установке и настройке VMware Enterprise Systems Connector. После установки настройки ACC необходимо интегрировать службы каталогов Workspace ONE UEM с Active Directory. Сведения о включении служб каталогов см. в руководстве по использованию служб каталогов VMware Workspace ONE UEM.

Чтобы внедрить проверку подлинности с помощью AirWatch Cloud Connector для Workspace ONE, свяжите метод проверки подлинности с помощью пароля (Workspace ONE UEM Connector) со встроенным поставщиком удостоверений в консоли VMware Identity Manager.

Вы можете включить поддержку моментальной регистрации в Workspace ONE UEM, чтобы добавлять в каталог VMware Identity Manager новых пользователей при их первом входе в систему. При этом пользователю не приходится ждать следующей запланированной синхронизации данных с сервера Workspace ONE UEM для доступа к Workspace ONE. Новые пользователи могут просто войти на портал Workspace ONE с устройства iOS или Android либо настольного компьютера, используя имя пользователя и пароль Active Directory. Служба VMware Identity Manager проверяет подлинность учетных данных Active Directory с помощью AirWatch Cloud Connector и добавляет профиль пользователя в каталог.

Связав методы проверки подлинности во встроенном поставщике удостоверений, необходимо создать политики доступа, которые будут применяться к методу проверки подлинности.

Примечание Имя пользователя и проверка подлинности пароля интегрируются в среду AirWatch Cloud Connector. Для поверки подлинности пользователей другими методами, которые поддерживает VMware Identity Manager, нужно настроить соединитель VMware Identity Manager.

Управление сопоставлением атрибутов пользователя

Между каталогами Workspace ONE UEM и VMware Identity Manager можно настроить сопоставление атрибутов пользователей.

На странице «Атрибуты пользователя» в VMware Identity Manager, на вкладке «Управление учетными данными и доступом» будут перечислены атрибуты по умолчанию для каталога, который отмечен для атрибутов каталога Workspace ONE UEM. Обязательные атрибуты отмечены звездочкой. Пользователи, у которых отсутствует какой-либо обязательный атрибут в профиле, не синхронизируются со службой VMware Identity Manager.

Таблица 2-1. Сопоставление с атрибутами каталога Workspace ONE UEM по умолчанию

Имя атрибута пользователя VMware Identity Manager	Сопоставление по умолчанию с атрибутом пользователя Workspace ONE UEM
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
domain	Домен
отключено (внешний пользователь отключен)	отключен
phone	telephoneNumber
lastName	lastname*
firstName	firstname*
email	Эл. почта*
userName	username*

Синхронизация пользователей и групп из каталога Workspace ONE UEM в каталоге VMware Identity Manager

Можно настроить параметры VMware Identity Manager в консоли Workspace ONE UEM, чтобы установить подключение между экземпляром организационной группы каталога Workspace ONE UEM и VMware Identity Manager. Это подключение используется для синхронизации пользователей и групп в каталоге, созданном в службе VMware Identity Manager.

Пользователи и группы изначально синхронизируются с каталогом VMware Identity Manager вручную. Расписание синхронизации Workspace ONE UEM определяет частоту синхронизации пользователей и групп с каталогом VMware Identity Manager.

При добавлении либо удалении пользователя или группы на сервере Workspace ONE UEM соответствующие изменения немедленно отражаются в службе VMware Identity Manager.

Необходимые условия

- Имя локального администратора и пароль VMware Identity Manager.
- Определите значения атрибутов для сопоставления из каталога Workspace ONE UEM. См. раздел Управление сопоставлением атрибутов пользователя.

Процедура

1. В консоли Workspace ONE UEM в разделе «Группы и параметры» на странице «Все параметры» выберите «Глобальные», а затем укажите группу организации на уровне заказчика и щелкните **Система > Интеграция предприятий** > **VMware Identity Manager**.

2. В разделе «Сервер» щелкните **Настройка**.

   Примечание Кнопка настройки доступна, только если служба каталога настроена для той же группы организации. Если кнопка «Настроить» не отображается, при входе была выбрана неправильная группа организации. Группу организации можно изменить в раскрывающемся меню Global (Глобальные).

3. Введите параметры VMware Identity Manager.

Параметр	Описание
URL-адрес	Введите URL-адрес арендатора VMware. Например, `https://myco.identitymanager.com`.
Имя пользователя администратора	Введите имя локального администратора VMware Identity Manager.
Пароль администратора	Введите пароль пользователя администратора VMware Identity Manager.

4. Нажмите кнопку **Далее**.
5. Включите настраиваемое сопоставление, чтобы настроить сопоставление атрибутов пользователя служб Workspace ONE UEM и VMware Identity Manager.
6. Чтобы проверить, правильно ли настроены параметры, щелкните **Проверить подключение**.
7. Чтобы вручную синхронизировать данные всех пользователей и групп со службой VMware Identity Manager, щелкните **Синхронизировать**.

   Примечание Синхронизацию вручную можно выполнить только через четыре часа после предыдущей синхронизации. Это необходимо, чтобы контролировать системную нагрузку.

Каталог Workspace ONE UEM создается в службе VMware Identity Manager, пользователи и группы синхронизируются в каталоге VMware Identity Manager.

Следующие шаги

Проверьте, синхронизированы ли имена пользователей и групп, на вкладке «Пользователи и группы» в консоли VMware Identity Manager.

Управление конфигурацией проверки подлинности с помощью пароля для Workspace ONE UEM

Можно просматривать конфигурацию пароля (AirWatch Connector), выполненную при установке Workspace ONE UEM и добавленную к службе VMware Identity Manager, а также управлять ею.

Метод проверки подлинности с помощью пароля (AirWatch Connector) настраивается на странице «Управление учетными данными и доступом» > «Методы проверки подлинности». Он связан со встроенным поставщиком удостоверений на странице «Поставщики удостоверений».

Важно! Если программное обеспечение AirWatch Cloud Connector обновлено, также обновите конфигурацию Workspace ONE UEM на странице AirWatch в консоли VMware Identity Manager.

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» выберите **Методы проверки подлинности**.
2. В разделе **Пароль (AirWatch Connector)** в столбце «Настроить» щелкните значок карандаша.
3. Просмотрите конфигурацию.

Параметр	Описание
Включить проверку подлинности с помощью пароля AirWatch	Этот флажок позволяет выполнять проверку подлинности Workspace ONE UEM с помощью пароля.
URL-адрес консоли администрирования AirWatch	Заполняется автоматически URL-адресом Workspace ONE UEM.
Ключ API-интерфейса AirWatch	Заполняется автоматически ключом API-интерфейса администратора Workspace ONE UEM.
Сертификат, используемый для проверки подлинности	Заполняется автоматически сертификатом Workspace ONE UEM Cloud Connector.
Пароль для сертификата	Заполняется автоматически паролем для сертификата Workspace ONE UEM Cloud Connector.
Идентификатор группы AirWatch	Заполняется автоматически организацией группы ID.
Разрешенное количество попыток проверки подлинности	Введите максимально допустимое число неудачных попыток входа в систему при использовании проверки подлинности с помощью пароля в Workspace ONE UEM. После достижения этого числа попытки входа в систему будут запрещены. Служба VMware Identity Manager попытается использовать резервный метод проверки подлинности, если он настроен. По умолчанию дается пять попыток.
JIT включена	Если параметр JIT не включен, установите этот флажок, чтобы динамически включать моментальную регистрацию пользователей в службе VMware Identity Manager при первом входе.

4. Нажмите кнопку **Сохранить**.

Настройка встроенных поставщиков удостоверений

Можно настроить несколько встроенных поставщиков удостоверений и связать с ними методы проверки подлинности, которые были настроены на странице «Управление учетными данными и доступом» > «Методы проверки подлинности».

Процедура

1. На вкладке «Управление учетными данными и доступом» выберите **Управление > Поставщики удостоверений**.

2. Щелкните **Добавить поставщика удостоверений** и выберите **Создать встроенного поставщика удостоверений**.

Параметр	Описание
Имя поставщика удостоверений	Введите имя этого экземпляра встроенного поставщика удостоверений.
Пользователи	Выберите пользователей, для которых необходимо выполнить проверку подлинности. Отобразится список настроенных каталогов.
Сеть	Перечисляются существующие сетевые диапазоны, настроенные в службе. Выберите диапазоны сетевых адресов для пользователей на основе IP-адресов, трафик с которых необходимо направлять в этот экземпляр поставщика удостоверений для проверки подлинности.
Способы проверки подлинности	Отобразятся методы проверки подлинности, которые настроены в службе. Установите флажок для методов проверки подлинности, которые необходимо связать со встроенным поставщиком удостоверений. Включите соответствующий параметр на странице конфигурации AirWatch, чтобы активировать параметры «Соответствие устройства (с Workspace ONE UEM)» и «Пароль (AirWatch Connector)».

3. Нажмите кнопку **Добавить**.

Следующие шаги

Настройте правило политики доступа по умолчанию, чтобы добавить политику проверки подлинности в правило. См. Настройка правил проверки соответствия.

Внедрение проверки подлинности с помощью единого входа для мобильных устройств с iOS под управлением Workspace ONE UEM

3

Чтобы проверить подлинность на устройствах с iOS, в VMware Identity Manager используется поставщик удостоверений, встроенный в службу VMware Identity Manager, который обеспечивает доступ к механизму проверки подлинности с помощью системы единого входа на мобильных устройствах.

Для проверки подлинности на устройствах с iOS с помощью этого метода используется центр распространения ключей (Key Distribution Center, KDC) без применения соединителя или систем других производителей. Проверка подлинности с помощью Kerberos предоставляет пользователям, которые успешно вошли в свой домен, возможность получать доступ к порталу приложений Workspace ONE, не получая дополнительные запросы на ввод учетных данных.

В эту главу входят следующие разделы:

Обзор внедрения для настройки единого входа на мобильных устройствах с iOS

Чтобы внедрить проверку подлинности с помощью единого входа на мобильных устройствах iOS 9 или более поздних версий под управлением Workspace ONE UEM, необходимо выполнить следующие действия.

- Загрузите сертификат издателя, чтобы настроить систему единого входа для мобильных устройств с iOS.
  - Если используется служба сертификации Active Directory, настройте шаблон центра сертификации для распространения сертификатов Kerberos в службах сертификации Active Directory. Затем настройте Workspace ONE UEM, чтобы использовать центр сертификации Active Directory. Добавьте шаблон сертификата в консоли Workspace ONE UEM. Скачайте сертификат издателя, чтобы настроить систему единого входа для мобильных устройств с iOS.
  - Если вы используете центр сертификации Workspace ONE UEM, включите сертификаты на странице «Интеграции» в VMware Identity Manager. Скачайте сертификат издателя, чтобы настроить систему единого входа для мобильных устройств с iOS.
- Подключитесь к необходимому центру распространения ключей (KDC).
- Настройте профиль устройства с iOS и включите единый вход в консоли Workspace ONE UEM.
- Настройте метод проверки подлинности единого входа для мобильных устройств с iOS.
- В консоли VMware Identity Manager настройте встроенный поставщик удостоверений и укажите проверку подлинности для единого входа на мобильных устройствах с iOS.

Настройка центра сертификации Active Directory в Workspace ONE UEM

Чтобы настроить проверку подлинности при входе на мобильные устройства iOS 9 под управлением Workspace ONE UEM, можно установить доверительные отношения между Active Directory и Workspace ONE UEM, а затем включить метод проверки подлинности для единого входа на мобильных устройствах iOS в VMware Identity Manager.

Настроив центр сертификации и шаблон сертификата для распространения сертификатов Kerberos в службах сертификации Active Directory, нужно разрешить Workspace ONE UEM запрашивать сертификат, использованный для проверки подлинности, и добавить центр сертификации в консоль Workspace ONE UEM.

Процедура

1. В главном меню консоли Workspace ONE UEM выберите **Устройства > Сертификаты > Центры сертификации**.
2. Нажмите кнопку **Добавить**.

3. На странице центра сертификации настройте следующее.

Примечание Прежде чем начать заполнять эту форму, убедитесь, что в качестве типа центра сертификации выбран Microsoft AD CS.

Параметр	Описание
Имя	Введите имя нового центра сертификации.
Тип центра сертификации	Убедись, что выбран тип **Microsoft AD CS**.
Протокол	В качестве протокола выберите **ADCS**.
Имя узла сервера	Введите URL-адрес этого сервера. Введите имя узла в формате `https://{servername.com}/certsrv.adcs/`. Тип транспорта сайта в зависимости от настроек: http или https. URL-адрес должен заканчиваться `/`. **Примечание** Если при тестировании URL-адреса подключиться не удается, удалите http:// или https:// из строки адреса и проверьте подключение еще раз.
Имя центра сертификации	Введите имя центра сертификации, к которому подключено конечное устройство AD CS. Это имя можно найти, запустив приложение центра сертификации на сервере центра сертификации.
Проверка подлинности	Убедись, что выбран тип **Служебный аккаунт**.
Имя пользователя и пароль	Введите имя пользователя и пароль учетной записи администратора AD CS с соответствующими правами доступа, чтобы разрешить Workspace ONE UEM запрашивать и выдавать сертификаты.

4. Нажмите кнопку **Сохранить**.

Следующие шаги

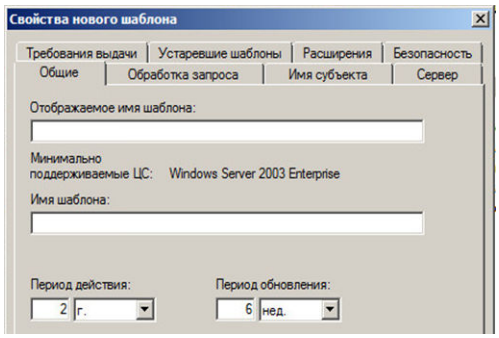
Настройте шаблон сертификата в Workspace ONE UEM.

Настройка Workspace ONE UEM для использования центра сертификации Active Directory

Шаблон центра сертификации для распространения сертификатов Kerberos должен быть настроен надлежащим образом. В службах сертификации Active Directory (AD CS) можно дублировать существующий шаблон проверки подлинности Kerberos для настройки нового шаблона центра сертификации для проверки подлинности iOS с использованием Kerberos.

При копировании шаблона проверки подлинности Kerberos из AD CS в диалоговом окне «Свойства нового шаблона» необходимо настроить следующие сведения.

Рис. 3-1. Диалоговое окно «Свойства нового шаблона» служб сертификации Active Directory



- Вкладка **Общие**. Введите отображаемое имя и имя шаблона. Например, iOSKerberos. Это имя, которое отображается в оснастке шаблонов сертификатов и центра сертификации.
- Вкладка **Обработка запроса**. Включите параметр **Разрешить экспортировать закрытый ключ**.
- Вкладка **Имя субъекта**. Установите переключатель **Предоставляется в запросе**. Когда Workspace ONE UEM запрашивает сертификат, Workspace ONE UEM предоставляет имя субъекта.
- Вкладка **Расширения**. Определите политики приложений.
  - Выберите политики приложений и нажмите кнопку «Изменить», чтобы добавить новую политику приложений. Присвойте этой политике имя «Клиентская проверка подлинности Kerberos».
  - Добавьте такой идентификатор объекта (OID): 1.3.6.1.5.2.3.4. Не изменяйте его.
  - В списке «Описание политик приложений» удалите все политики, кроме политики «Клиентская проверка подлинности Kerberos» и «Проверка подлинности с помощью смарт-карты».
- Вкладка **Безопасность**. Добавьте учетную запись Workspace ONE UEM в список пользователей, которые могут использовать сертификат. Установите разрешения для учетной записи. Установите параметр «Полное управление», чтобы позволить субъекту безопасности изменять все атрибуты шаблона сертификата, в том числе разрешения для шаблона сертификата. В противном случае установите разрешения в соответствии с требованиями организации.

Сохраните изменения. Добавьте шаблон в список шаблонов, используемых центром сертификации Active Directory.

В Workspace ONE UEM настройте центр сертификации и добавьте шаблон сертификата.

Добавление шаблона сертификата в Workspace ONE UEM

При добавлении шаблона сертификата выполняется привязка к центру сертификации, используемому для создания сертификатов пользователей.

Необходимые условия

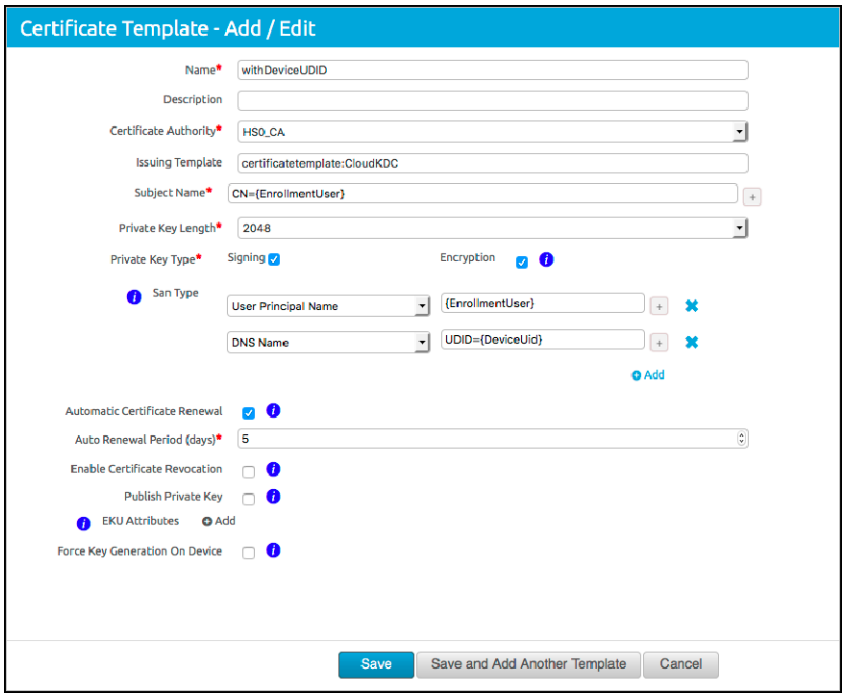
Настройте центр сертификации в Workspace ONE UEM.

Процедура

1. В консоли Workspace ONE UEM последовательно выберите элементы **Система > Интеграция предприятия > Центры сертификации**.
2. Перейдите на вкладку **Шаблон запроса** и щелкните **Добавить**.
3. На странице шаблона сертификата настройте следующие параметры.

Параметр	Описание
Имя	Введите имя нового шаблона запроса в Workspace ONE UEM.
Центр сертификации	В раскрывающемся меню выберите созданный центр сертификации.
Шаблон издателя	Введите точное имя шаблона ЦС Microsoft, созданного в службе сертификатов Active Directory. Например, `iOSKerberos`.
Имя субъекта	Введите имя субъекта в шаблоне. Можно нажать кнопку «+», чтобы выбрать значение подстановки в списке. Убедитесь в том, что значение введено после **CN =** в текстовом поле. Если выбрать тип поиска DeviceUid, необходимо ввести двоеточие (:) после значения и выбрать значение подстановки в списке. Например, **CN={DeviceUid}:{lookupvalue}**, где текстовое поле {} — значение подстановки Workspace ONE UEM. Необходимо использовать двоеточие (:). Текст, введенный в этом поле, является субъектом сертификата, который может использоваться для определения того, кто или какое устройство получили сертификат.
Длина закрытого ключа	Длина закрытого ключа соответствует параметру шаблона сертификата, используемого службой сертификатов Active Directory. Как правило, она равняется 2048 символам.
Тип закрытого ключа	Установите флажки **Подписывание** и **Шифрование**.
Тип сети SAN	Нажмите кнопку **+Добавить**. В качестве альтернативного имени субъекта выберите **Имя участника-пользователя**. Оно должно иметь значение `{EnrollmentUser}`. Когда проверка совместимости устройства настроена с проверкой подлинности Kerberos, если не настроить DeviceUid как значение подстановки имени субъекта, то необходимо добавить альтернативный тип SAN, чтобы включать уникальный идентификатор устройства (UDID). Выберите **DNS-имя** в качестве типа сети SAN. Он должен иметь значение **UDID={DeviceUid}**.
Автоматическое обновление сертификата	Установите этот флажок, чтобы включить автоматическое продление сертификатов, использующих этот шаблон, перед окончанием срока их действия.
Период автоматического обновления (в днях)	Укажите период автоматического продления в днях.
Разрешить отзыв сертификатов	Установите этот флажок, чтобы включить автоматический отзыв сертификатов в случае отмены регистрации или удаления соответствующих устройств или удаления соответствующего профиля.
Публиковать закрытый ключ	Установите этот флажок, чтобы опубликовать закрытый ключ.
Назначение закрытого ключа	Служба каталога или настраиваемая веб-служба

4. Нажмите кнопку **Сохранить**.



Следующие шаги

В консоли VMware Identity Provider настройте для встроенного поставщика удостоверений единый вход в качестве метода проверки подлинности на мобильных устройствах iOS.

Использование центра сертификации Workspace ONE UEM для проверки подлинности Kerberos

Центр сертификации Workspace ONE UEM можно использовать вместо центра сертификации Active Directory для единого входа с помощью встроенного механизма проверки подлинности Kerberos на мобильных устройствах iOS 9 под управлением Workspace ONE UEM. Можно включить центр сертификации Workspace ONE UEM в консоли Workspace ONE UEM и экспортировать сертификат эмитента центра сертификации,для использования в службе VMware Identity Manager.

Центр сертификации Workspace ONE UEM рассчитан на использование простого протокола регистрации сертификата (Simple Certificate Enrollment Protocol, SCEP). Он используется для управляемых устройств Workspace ONE UEM, которые поддерживают SCEP. При интеграции VMware Identity Manager с Workspace ONE UEM центр сертификации Workspace ONE UEM используется для выдачи сертификатов для мобильных устройств iOS 9 в рамках профиля.

Корневой сертификат издателя центра сертификации Workspace ONE UEM также представляет собой сертификат подписи OCSP.

Включение и экспорт центра сертификации Workspace ONE UEM

Когда решение VMware Identity Manager включено в Workspace ONE UEM, можно создать корневой сертификат издателя Workspace ONE UEM и экспортировать этот сертификат для проверки подлинности с помощью единого входа на управляемых мобильных устройствах iOS 9.

Процедура

1. В консоли Workspace ONE UEM последовательно щелкните **Система > Интеграция предприятий** > **VMware Identity Manager**.

   Включить центр сертификации Workspace ONE UEM можно в том случае, если группа организации имеет тип «Заказчик».

Совет Чтобы просмотреть или изменить тип группы, перейдите к группам и параметрам, а затем щелкните **Группы > Организационные группы** > **Подробности организационных групп**.

2. Щелкните **Конфигурация**.
3. В разделе «СЕРТИФИКАТ» щелкните **Включить**.

   На странице отобразятся сведения о корневом сертификате издателя.
4. Щелкните **Экспорт** и сохраните файл.

Следующие шаги

В консоли VMware Identity Manager во встроенном поставщике удостоверений настройте проверку подлинности Kerberos и добавьте сертификат издателя центра сертификации.

Использование центра распространения ключей для выполнения проверки подлинности на устройствах с iOS

На устройствах iOS необходимо интегрировать службу с Kerberos. Проверка подлинности с помощью Kerberos позволяет пользователям, которые успешно вошли в свой домен, получать доступ к порталу приложений без дополнительных запросов учетных данных. Для проверки подлинности на устройствах с iOS с помощью этого метода используется центр распространения ключей (Key Distribution Center, KDC) без применения соединителя или систем других производителей.

Для арендаторов облачной версии VMware Identity Manager не требуется управлять центром KDC или настраивать его.

Для локальных развертываний предусмотрены два варианта службы KDC.

- Встроенный центр KDC. Для встроенного центра KDC необходимо инициализировать KDC на устройстве и создать общедоступные записи DNS, чтобы разрешить клиентам Kerberos выполнять поиск центра KDC. Дополнительные сведения о включении встроенного центра KDC см. в руководстве по администрированию VMware Identity Manager.

- Центр KDC как размещенная в облаке служба VMware Identity Manager. При использовании KDC в облаке необходимо выбрать соответствующее имя области на странице адаптера проверки подлинности iOS.

Примечание При установке и настройке VMware Identity Manager с помощью Workspace ONE UEM в среде Windows для использования облачной службы KDC VMware Identity Manager необходимо настроить метод проверки подлинности с использованием единого входа для мобильных устройств с iOS.

Использование облачной службы KDC

Решение VMware Identity Manager предоставляет облачную службу KDC для проверки подлинности Kerberos при выполнении единого входа с мобильных устройств iOS.

Службу KDC, размещенную в облаке, необходимо использовать при развертывании службы VMware Identity Manager в среде Windows с помощью Workspace ONE UEM.

Сведения о работе со службой KDC, управляемой на устройстве VMware Identity Manager, см. в разделе «Подготовка к использованию проверки подлинности Kerberos на устройствах с ОС iOS» в руководстве по *установке и настройке VMware Identity Manager*.

В процессе настройки единого входа с мобильных устройств iOS выполняется настройка имени области для облачной службы KDC. Область — это имя административной единицы, в которой хранятся данные проверки подлинности. При выборе команды «Сохранить» служба VMware Identity Manager будет зарегистрирована в облачной службе KDC. Данные, хранимые в службе KDC, зависят от конфигурации способа проверки подлинности при выполнении единого входа с мобильных устройств iOS, включая сертификат ЦС, сертификат подписи OCSP и данные конфигурации запроса OCSP.

Записи журнала хранятся в облачной службе. Персональные данные в записях журнала включают имя участника Kerberos, указанное в профиле пользователя, значения различающегося имени, основного имени пользователя и альтернативного имени для адреса электронной почты субъекта, идентификатор устройства, указанный в сертификате пользователя, а также полное доменное имя службы IDM, к которой пользователь осуществляет доступ.

Для работы со службой KDC, размещенной в облаке, необходимо настроить VMware Identity Manager следующим образом.

- Полное доменное имя службы VMware Identity Manager должно быть доступно по сети Интернет. Сертификат SSL/TLS, используемый VMware Identity Manager, должен быть открыто подписан.
- Служба VMware Identity Manager должна иметь доступ к порту 88 (UDP) исходящего запроса/отклика и порту 443 (HTTPS/TCP).
- Если включен OCSP, то ответчик OCSP должен быть доступен по сети Интернет.

Настройка проверки подлинности с помощью единого входа для мобильных устройств с iOS

На странице «Методы проверки подлинности» в консоли VMware Identity Manager настройте метод проверки подлинности для единого входа с мобильных устройств (iOS). Выберите метод проверки подлинности «Единый вход для мобильных устройств (iOS)» для использования во встроенном поставщике удостоверений.

Необходимые условия

- Для выдачи сертификатов пользователям в арендаторе Workspace ONE UEM используется файл PEM или DER центра сертификации.
- Есть сертификат подписи ответчика OCSP для проверки отзыва.
- Для службы KDC выберите соответствующее имя области службы. Если используется встроенная служба KDC, центр KDC нужно инициализировать. Дополнительные сведения о встроенной службе KDC см. в разделе «Установка и настройка VMware Identity Manager».

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» выберите **Управление > Методы проверки подлинности**.
2. В столбце «Настройка» для параметра **Единый вход для мобильных устройств (iOS)** щелкните значок карандаша.
3. Настройте метод проверки подлинности Kerberos.

Параметр	Описание
Включить проверку подлинности центра распространения ключей	Установите этот флажок, чтобы разрешить пользователям входить в систему с помощью устройств с iOS, поддерживающих проверку подлинности Kerberos.
Область	Для развертываний арендатора в облаке значение области доступно только для чтения. Отображаемое имя области — это имя области Identity Manager для арендатора. В локальных средах, если используется облачная служба KDC, введите поддерживаемое предварительно назначенное имя области. Это имя вводится полностью заглавными буквами, Например, OP.VMWAREIDENTITY.COM. Если используется встроенная служба KDC, отображается имя области, настроенное вами при запуске KDC.
Сертификат корневого и промежуточного центров сертификации	Передайте файл сертификата для эмитента центра сертификации. Формат файла может быть PEM или DER.
Загруженные различающиеся имена субъектов сертификата ЦС	Содержимое переданного файла сертификата отображается здесь. Передать можно несколько файлов сертификатов, каждый из которых будет добавлен в список.
Включить OCSP	Установите флажок, чтобы использовать протокол проверки состояния сертификатов (OCSP) и получить статус отзыва сертификата.

Параметр	Описание
Отправить специальный параметр OCSP	Установите флажок, чтобы отправлять в ответе уникальный идентификатор запроса OCSP.
Сертификат подписи ответчика OCSP	Передайте сертификат OCSP для ответчика. При использовании центра сертификации Workspace ONE UEM в качестве сертификата OCSP используется сертификат эмитента. На этом этапе также следует передать сертификат Workspace ONE UEM.
Различаемое имя субъекта сертификата подписи ответчика OCSP	Здесь указывается переданный файл сертификата OCSP.
Отменить сообщение	Дает возможность создать настраиваемое сообщение, которое отображается, если проверка подлинности при входе занимает слишком много времени. Если настраиваемое сообщение не создано, используется сообщение по умолчанию: `Attempting to authenticate your credentials`.
Активировать ссылку отмены	Дает пользователям возможность щелкнуть ссылку «Отмена», чтобы прекратить попытку проверки подлинности и отменить вход, если проверка подлинности занимает слишком много времени. Если ссылка отмены включена, в конце сообщения об ошибке проверки подлинности отображается слово «Отменить».
URL-адрес сервера управления устройствами предприятия	Введите URL-адрес сервера Mobile Device Management (MDM) для перенаправления пользователей, если доступ запрещен из-за того, что устройство не зарегистрировано в Workspace ONE UEM для управления MDM. Этот URL-адрес отображается в сообщении об ошибке проверки подлинности. Если не ввести URL-адрес здесь, отобразится универсальное сообщение об отказе в доступе.

4. Нажмите кнопку **Сохранить**.

Следующие шаги

- Свяжите метод проверки подлинности «Единый вход для мобильных устройств (iOS)» во встроенном поставщике удостоверений.

Настройка встроенного поставщика удостоверений для проверки подлинности на мобильных устройствах с iOS с помощью единого входа

При необходимости можно настроить встроенный поставщик удостоверений и связать с ним метод проверки подлинности «Единый вход для мобильных устройств (iOS)», параметры которого были заданы на странице «Управление учетными данными и доступом > Методы проверки подлинности».

Необходимые условия

Проверка подлинности с помощью единого входа для мобильных устройств с iOS настраивается на странице «Методы проверки подлинности».

Процедура

1. На вкладке «Управление учетными данными и доступом» выберите **Управление > Поставщики удостоверений**.
2. Щелкните **Добавить поставщика удостоверений** и выберите **Создать встроенного поставщика удостоверений**.

Параметр	Описание
Имя поставщика удостоверений	Введите имя этого экземпляра встроенного поставщика удостоверений.
Пользователи	Выберите пользователей, для которых необходимо выполнить проверку подлинности. Отобразится список настроенных каталогов.
Сеть	Перечисляются существующие сетевые диапазоны, настроенные в службе. Выберите диапазоны сетевых адресов для пользователей на основе IP-адресов, трафик с которых необходимо направлять в этот экземпляр поставщика удостоверений для проверки подлинности.
Способы проверки подлинности	Отобразятся методы проверки подлинности, которые настроены в службе. Установите флажок для метода проверки подлинности iOS, который необходимо связать со встроенным поставщиком удостоверений. Добавьте другие методы проверки подлинности. Если используются параметры «Совместимость устройств (с Workspace ONE UEM)» и «Пароль (Workspace ONE UEM Connector)», включите соответствующий параметр на странице конфигурации Workspace ONE UEM.

3. В разделе «Экспортировать сертификат KDC» щелкните **Загрузить сертификат**. Сохраните этот сертификат в файле, доступном с консоли Workspace ONE UEM.

   Этот сертификат передается при настройке профиля устройства iOS в Workspace ONE UEM.
4. Нажмите кнопку **Добавить**.

Следующие шаги

- Настройте правило политики доступа по умолчанию для проверки подлинности Kerberos на устройствах с iOS. Убедитесь, что этот метод проверки подлинности указан в правиле первым.
- Перейдите в консоль Workspace ONE UEM, настройте профиль устройства iOS в Workspace ONE UEM и добавьте сертификат эмитента для сертификата сервера KDC из VMware Identity Manager.

Настройка профиля Apple iOS в Workspace ONE UEM с помощью центра сертификации Active Directory и шаблона сертификата

Чтобы применить параметры поставщика удостоверений к устройству, создайте и разверните профиль устройства Apple iOS в Workspace ONE UEM. Этот профиль содержит информацию, необходимую для подключения устройства к поставщику удостоверений VMware и сертификат, который устройство использовало для проверки подлинности. Включите единый вход в систему, чтобы обеспечить беспрепятственный доступ без необходимости проверки подлинности в каждом приложении.

Необходимые условия

- Единый вход для мобильных устройств с iOS настраивается в VMware Identity Manager.
- Файл центра сертификации Kerberos для iOS хранится на компьютере, доступ к которому можно получить из консоли администрирования Workspace ONE UEM.
- В Workspace ONE UEM правильно настроен центр сертификации и шаблон сертификата.
- Список URL-адресов и идентификаторов пакетов приложений, которые используют единый вход для проверки подлинности на мобильных устройствах с iOS.

Процедура

1. В консоли Workspace ONE UEM выберите **Устройства > Профили и ресурсы > Профили**.
2. Выберите **Добавить > Добавить профиль**, а затем выберите **Apple iOS**.
3. Введите имя `iOSKerberos` и настройте параметры в разделе **Общие**.
4. В области переходов слева выберите **Учетные данные > Настроить**, чтобы настроить учетные данные.

Параметр	Описание
Источник учетных данных	Выберите в раскрывающемся меню **Определенный центр сертификации**.
Центр сертификации	Выберите в раскрывающемся меню центр сертификации.
Шаблон сертификата	Выберите в раскрывающемся меню шаблон запроса, который ссылается на центр сертификации. Этот шаблон сертификата создается в дополнение к шаблону сертификата в Workspace ONE UEM.

5. Щелкните **+** в правом нижнем углу страницы снова и создайте второй набор учетных данных.
6. В раскрывающемся меню **Источник учетных данных** выберите **Загрузить на сервер**.
7. Введите имя учетных данных.
8. Щелкните **Загрузить на сервер**, чтобы передать корневой сертификат сервера KDC, загруженный на странице «Управление учетными данными и доступом > Управление > Поставщики удостоверений > Встроенный поставщик удостоверений».

9. В области переходов слева выберите **Единый вход** и нажмите кнопку **Настроить**.

10. Введите сведения о подключении.

Параметр	Описание
Имя учетной записи	Введите учетные данные `Kerberos`.
Имя участника Kerberos	Щелкните **+** и выберите**{EnrollmentUser}**.
Область	Для развертываний арендатора в облаке введите имя области Identity Manager для арендатора. Текст в этом параметре должен быть написан с заглавной буквы. Например, `VMWAREIDENTITY.COM`. Для локальных развертываний введите имя области, которая использовалось при инициализации KDC на устройстве VMware Identity Manager. Например, `EXAMPLE.COM`
Сертификат продления	В раскрывающемся меню выберите пункт **Сертификат № 1**. Это сертификат ЦС Active Directory, который был настроен первым согласно учетным данным.
Префиксы URL-адресов	Введите соответствующие префиксы URL-адресов, чтобы использовать эту учетную запись для проверки подлинности Kerberos через HTTP. Для развертываний арендатора в облаке введите URL-адрес сервера VMware Identity Manager в формате `https://<tenant>.vmwareidentity.<region>`. В локальных развертываниях введите URL-адрес сервера VMware Identity Manager в формате `https://myco.example.com`.
Приложения	Введите список удостоверений приложений, которые разрешено использовать для такого входа. Для выполнения единого входа в систему с помощью Safari (встроенного браузера iOS) введите первый идентификатор пакета приложения в следующем формате: `com.apple.mobilesafari`. Затем введите идентификаторы пакетов приложений. Перечисленные приложения должны поддерживать проверку подлинности SAML.

11. Щелкните **Сохранить и опубликовать**.

Следующие шаги

Назначьте профиль устройства смарт-группе. Смарт-группы — это настраиваемые группы, определяющие устройства, платформы и пользователей, которые могут получить назначенное приложение, книгу, политику соответствия, профиль устройства или подготовку.

Настройка профиля Apple iOS в Workspace ONE UEM с помощью центра сертификации Workspace ONE UEM

Чтобы применить параметры поставщика удостоверений к устройству, создайте и разверните профиль устройства Apple iOS в Workspace ONE UEM. Этот профиль содержит информацию, необходимую для подключения устройства к поставщику удостоверений VMware и сертификат, который устройство использует для проверки подлинности.

Необходимые условия

- Встроенная система Kerberos, настроенная в VMware Identity Manager.

- Файл корневого сертификата сервера KDC для VMware Identity Manager, хранящийся на компьютере, который доступен из консоли Workspace ONE UEM.
- Сертификат, включенный и загруженный со страницы «Система» > «Интеграция предприятий» > VMware Identity Manager в консоли Workspace ONE UEM.
- Список URL-адресов и идентификаторов пакетов приложений, которые используют встроенный модуль проверки подлинности Kerberos на устройствах iOS.

Процедура

1. В консоли Workspace ONE UEM выберите **Устройства > Профили и ресурсы > Профиль > Добавить профиль** и укажите **Apple iOS**.
2. Настройте параметры профиля в разделе **Общие** и введите имя устройства `iOSKerberos`.
3. В области переходов слева выберите **SCEP > Настроить**, чтобы настроить учетные данные.

Параметр	Описание
Источник учетных данных	Выберите в раскрывающемся меню **Центр сертификации AirWatch**.
Центр сертификации	Выберите в раскрывающемся меню **Центр сертификации AirWatch**.
Шаблон сертификата	Выберите **Единый вход**, чтобы задать тип сертификата, выданного центром сертификации AirWatch.

4. Щелкните **Учетные данные > Настроить** и создайте второй набор учетных данных.
5. В раскрывающемся меню **Источник учетных данных** выберите **Загрузить на сервер**.
6. Введите имя учетных данных Kerberos для iOS.
7. Щелкните **Загрузить на сервер**, чтобы передать корневой сертификат сервера KDC для VMware Identity Manager, загруженный на странице «Управление учетными данными и доступом > Управление > Поставщики удостоверений > Встроенный поставщик удостоверений».
8. В области переходов слева выберите **Единый вход**.
9. Введите сведения о подключении.

Параметр	Описание
Имя учетной записи	Введите учетные данные `Kerberos`.
Имя участника Kerberos	Щелкните **+** и выберите**{EnrollmentUser}**.
Область	Для развертываний арендатора в облаке введите имя области VMware Identity Manager для арендатора. Текст в этом параметре должен быть написан с заглавной буквы. Например, `VMWAREIDENTITY.COM`. Для локальных развертываний введите имя области, которая использовалась при инициализации KDC на компьютере VMware Identity Manager. Например, `EXAMPLE.COM`.
Сертификат продления	На устройствах с iOS 8+ выберите сертификат, используемый для автоматической повторной проверки подлинности пользователя без его участия по истечении срока действия сеанса единого входа.

Параметр	Описание
Префиксы URL-адресов	Введите соответствующие префиксы URL-адресов, чтобы использовать эту учетную запись для проверки подлинности Kerberos через HTTP. Для развертываний арендатора в облаке введите URL-адрес сервера VMware Identity Manager в формате **`https://<арендатор>.vmwareidentity.<область>`**. В локальных развертываниях введите URL-адрес сервера VMware Identity Manager, например, **`https://myco.example.com`**.
Приложения	Введите список удостоверений приложений, которые разрешено использовать для такого входа. Для выполнения единого входа в систему с помощью Safari (встроенного браузера iOS) введите первый идентификатор пакета приложения **`com.apple.mobilesafari`**. Затем введите идентификаторы пакетов приложений. Перечисленные приложения должны поддерживать проверку подлинности SAML.

10. Щелкните **Сохранить и опубликовать**.

Когда профиль iOS будет передан на устройства пользователей, они смогут входить в VMware Identity Manager с помощью встроенного механизма проверки подлинности Kerberos без ввода учетных данных.

Следующие шаги

Назначьте профиль устройства смарт-группе. Смарт-группы — это настраиваемые группы, определяющие устройства, платформы и пользователей, которые могут получить назначенное приложение, книгу, политику соответствия, профиль устройства или подготовку.

Назначение профиля устройства Workspace ONE UEM

Создав профиль устройства, следует назначить этот профиль смарт-группе.

Смарт-группы — это настраиваемые группы, определяющие устройства, платформы и пользователей, которые могут получить назначенное приложение, политику соответствия, профиль устройства или подготовленное решение. Дополнительные сведения см. в руководстве по Workspace ONE UEM Mobile Device Management.

Процедура

1. В консоли Workspace ONE UEM выберите **Устройства > Профили и ресурсы** >**Профили**.
2. Выберите профиль устройства, который следует назначить смарт-группе.
3. На вкладке «Общие» выберите текстовое поле **Назначенные группы** и **Создать группу назначения**.
4. На странице «Создание смарт-группы» введите имя смарт-группы.
5. Щелкните **Платформа и операционная система** и в раскрывающихся меню выберите соответствующую операционную систему и версию.
6. Щелкните **Сохранить и опубликовать**.

После назначения смарт-группы устройству пользователи смогут входить в Workspace ONE и использовать приложения из каталога.

Внедрение проверки подлинности для единого входа с мобильных устройств Android

4

Единый вход для мобильных устройств с Android — это реализация метода проверки подлинности с использованием сертификата для устройств с Android под управлением Workspace ONE UEM. Единый вход для мобильных устройств позволяет пользователям входить на устройства и получать безопасный доступ к приложениям Workspace ONE без повторного ввода пароля.

Мобильное приложение VMware Tunnel® устанавливается на устройство Android, чтобы добавить данные о сертификате и идентификаторе устройства в процесс проверки подлинности. В параметрах Tunnel в консоли Workspace ONE UEM Console настроен доступ к службе VMware Identity Manager для проверки подлинности, а служба извлекает сертификат с устройства для проверки подлинности.

В консоли Workspace ONE UEM Console можно также настроить следующие параметры.

- Профиль VPN для Android. Этот профиль используется для включения возможностей туннелирования отдельно для каждого приложения Android.
- Включение отдельной сети VPN для каждого приложения, когда для приложения в консоли Workspace ONE UEM Console используются возможности туннелирования.
- Создайте правила сетевого трафика со списком всех приложений, настроенных для использования отдельной сети VPN для каждого приложения, параметров прокси-сервера и URL-адреса VMware Identity Manager.

При реализации единого входа для мобильных устройств Android с помощью локальной службы VMware Identity Manager настройте службу прокси-сервера сертификата на компьютере VMware Identity Manager. После настройки службы прокси-сервера сертификата можно настроить проверку подлинности с помощью сертификата во встроенном поставщике удостоверений VMware Identity Manager с помощью консоли VMware Identity Manager.

При реализации единого входа на мобильных устройств Android с помощью службы VMware Identity Manager в облаке можно настроить проверку подлинности с помощью сертификата во встроенном поставщике удостоверений VMware Identity Manager с помощью консолиVMware Identity Manager. Служба прокси-сервера сертификата прокси-сервера управляется пользователем.

Дополнительные сведения по настройке единого входа для мобильных устройств Android см. в публикации *Единый вход для мобильных устройств Android для VMware Workspace One* в центре документации по Workspace ONE .

Поддерживаемые устройства Android

Поддерживается Android 5.1 или более поздней версии.

Приложения, доступные на устройстве Android, должны поддерживать SAML или другой поддерживаемый стандарт федерации для единого входа.

Прямая регистрация с помощью приложения Workspace ONE

5

Для прямой регистрации с помощью Workspace ONE требуется, чтобы пользователи зарегистрировали устройства, прежде чем смогут получить доступ к ресурсам в приложении Workspace ONE.

При прямой регистрации через приложение Workspace ONE можно сообщить всем пользователям, что им необходимо перейти в соответствующий магазин приложений, загрузить Workspace ONE, ввести адрес эл. почты и следовать инструкциям, чтобы начать работу на устройствах с помощью Workspace ONE.

Поддерживаемые устройства

- Apple iOS версии 9.0 и более новых версий
- Android Enterprise (прежнее название Android for Work) версии 5.1 и более новых версий
- Android Legacy версии 4.1 и более новых версий

  Устройство Android Legacy — это любое устройство Android, которое не поддерживает Android Enterprise, или устройство с поддержкой Android Enterprise, подключенное к экземпляру Workspace ONE UEM, на котором не включен Android Enterprise.

В эту главу входят следующие разделы:

Включение Workspace ONE для прямой регистрации

Включите прямую регистрацию устройства с помощью Workspace ONE для своей организационной группы в консоли Workspace ONE UEM на странице «Регистрация» > «Ограничение».

Если Workspace ONE включается для прямой регистрации, то при первом входе соответствующие устройства регистрируются напрямую. После регистрации в Workspace ONE устройствам, которые не подходят для прямой регистрации, предоставляется доступ только к управлению мобильными приложениями.

Процедура

1. В консоли Workspace ONE UEM выберите организационную группу, чтобы включить прямую регистрацию для Workspace ONE.
2. Перейдите в раздел **Группы и настройки > Все настройки > Устройства и пользователи > Общее > Регистрация** и выберите вкладку **Ограничения**.
3. При необходимости для параметра «Текущая настройка» установите **Переопределить**.
4. Прокрутите вниз до требований к управлению для Workspace ONE и задайте параметры конфигурации.

Параметр	Описание
Требовать MDM для Workspace ONE	При включении этого параметра соответствующим устройствам и пользователям предлагается пройти регистрацию сразу после входа в Workspace ONE.
Назначенная группа пользователей	По умолчанию установлена группа «Все пользователи». Можно выбрать конкретную группу пользователей для включения в процесс прямой регистрации.
iOS	Этот параметр предназначен для включения устройств iOS. Если этот параметр отключен, устройства iOS не смогут проходить прямую регистрацию. С отключенным параметром устройства по-прежнему можно зарегистрировать в Workspace ONE UEM в неуправляемом состоянии.
Android Legacy	Этот параметр предназначен для включения устройств Android Legacy. Если этот параметр отключен, прямая регистрация устройств Android Legacy недоступна. С отключенным параметром устройства по-прежнему можно зарегистрировать в Workspace ONE UEM в неуправляемом состоянии.
Android Enterprise	Функция предназначена для включения устройств Android Enterprise. Если этот параметр отключен, прямая регистрация устройств Android Enterprise недоступна. С отключенным параметром устройства по-прежнему можно зарегистрировать в Workspace ONE UEM в неуправляемом состоянии.

5. Нажмите кнопку **Сохранить**.
6. На вкладках регистрации настройте параметры регистрации для поддержки Workspace ONE. См. раздел Параметры конфигурации прямой регистрации с помощью Workspace ONE.

   Дополнительные сведения о настройке прямой регистрации для Workspace ONE см. в Руководстве по VMware AirWatch Mobile Device Management, глава о регистрации устройств.

Параметры конфигурации прямой регистрации с помощью Workspace ONE

Настройте прямую регистрацию с помощью Workspace ONE в консоли Workspace ONE UEM. Перейдите в раздел **Группы и настройки > Все настройки > Устройства и пользователи > Общее > Регистрация**. В таблице параметров регистрации устройств в Workspace ONE перечислены настраиваемые элементы меню.

На странице «Настройки регистрации» можно настроить параметры, относящиеся к регистрации устройств и пользователей. На странице расположены несколько вкладок. Их описание приведено ниже. Подробные сведения о настройке регистрации устройств см. в руководстве по VMware Workspace ONE UEM Mobile Device Management.

Рис. 5-1. Страница регистрации консоли **Workspace ONE UEM**

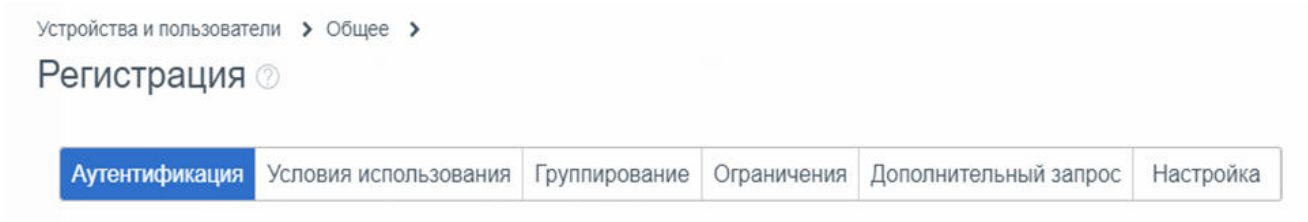


Таблица 5-1. Настраиваемые элементы меню для прямой регистрации с помощью **Workspace ONE**

Вкладка «Регистрация»	Настраиваемые элементы меню для прямой регистрации в Workspace ONE
Проверка подлинности	Поддерживаются пользователи каталогов. Кроме того, предоставляется быстрая поддержка пользователей, для которых выполняется проверка подлинности с использованием SAML и Active Directory. Пользователи, для которых выполняется проверка подлинности с использованием SAML без LDAP, поддерживаются, если запись пользователя существует в Workspace ONE UEM при первом входе в систему. Для модуля регистрации устройств поддерживается только **Открытая регистрация**. Функция «Только для зарегистрированных устройств» не поддерживается.
Условия использования	Можно создать условия использования, чтобы обязать пользователей принимать их до продолжения процесса прямой регистрации.
Группирование	Все параметры меню группирования совместимы с прямой регистрацией с помощью Workspace ONE. Параметр **синхронизации групп пользователей в режиме реального времени для Workspace ONE** включен по умолчанию. При регистрации устройства Workspace ONE UEM в режиме реального времени вызывает Active Directory для синхронизации групп пользователей конкретного пользователя. Если пользователь не существует в Workspace ONE UEM, в консоли Workspace ONE UEM сначала выполняется синхронизация пользователя, а затем групп пользователей в режиме реального времени. Если эта функция не включена, группы пользователей не синхронизируются в консоли Workspace ONE UEM. **Примечание** Эта функция сильно загружает ЦП. Если группы пользователей редко изменяются или уже существуют в Workspace ONE UEM, отключите этот параметр, чтобы повысить производительность и избежать проблем с задержкой при запуске приложения Workspace ONE. См. раздел, посвященный размещению устройств в правильной организационной группе, в Стратегии развертывания для настройки нескольких организационных групп Workspace ONE UEM.

Таблица 5-1. Настраиваемые элементы меню для прямой регистрации с помощью Workspace ONE (продолжение)

Вкладка «Регистрация»	Настраиваемые элементы меню для прямой регистрации в Workspace ONE

Ограничения	■ В разделе **Управление доступом пользователей** можно выбрать оба параметра «Ограничить регистрацию только известным пользователям» и «Ограничить регистрацию только настроенным группам».
	■ Поддерживается ограничение максимального количества устройств.
	■ **Настройка политики** поддерживается частично.
	  ■ **Разрешенные типы собственности**. В Workspace ONE отправляется запрос только для личных и корпоративно-личных устройств.
	
	  Примечание Тип регистрации Container Allow (с разрешения контейнера) не поддерживается.

Дополнительный запрос	Можно включить два дополнительных запроса: **Запросить тип собственности** и **Включить запрос инвентарного номера устройства**. Запрос на введение инвентарного номера появляется только для устройств с типом принадлежности «Корпоративное».
Настройка	Поддерживаются параметры меню настройки. ■ Целевой URL-адрес страницы после регистрации (только для iOS) ■ Сообщение MDM-профиля (только для iOS) ■ Использовать настраиваемые приложения MDM Можно включить параметр «Для каждой платформы использовать особый шаблон сообщения», но эти особые шаблоны сообщений Workspace ONE недоступны для Workspace ONE 3.2.

Удобство работы при прямой регистрации в Workspace ONE UEM с помощью Workspace ONE

При реализации управления мобильными устройствами через Workspace ONE пользователям необходимо загрузить приложение Workspace ONE, пройти проверку подлинности с помощью Workspace ONE UEM и зарегистрировать устройство. После регистрации устройства пользователи смогут использовать Workspace ONE для добавления и использования предоставленных ресурсов.

При использовании Workspace ONE процесс регистрации устройств iOS и Android Enterprise происходит одинаково. А устройства Android Legacy перенаправляются для регистрации в AirWatch Agent. AirWatch Agent автоматически передает управление обратно Workspace ONE после завершения регистрации. Пользователи могут получить доступ к Workspace ONE, воспользовавшись любым из этих способов.

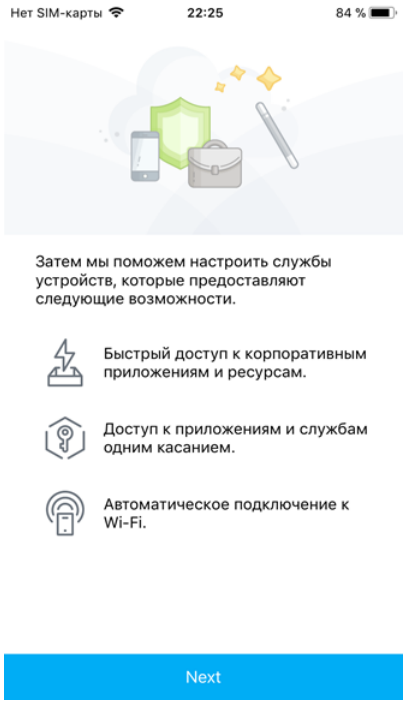
Прямая регистрация с помощью Workspace ONE на устройствах iOS

Сообщите пользователям, что им необходимо загрузить, установить и запустить приложение Workspace ONE из Apple App Store.

Процедура

1. Пользователям необходимо открыть приложение, ввести адрес эл. почты и URL-адрес сервера, а затем пройти проверку подлинности в соответствии с конфигурацией своей среды.
2. Отобразится окно **Требуется дополнительная настройка в компании**.

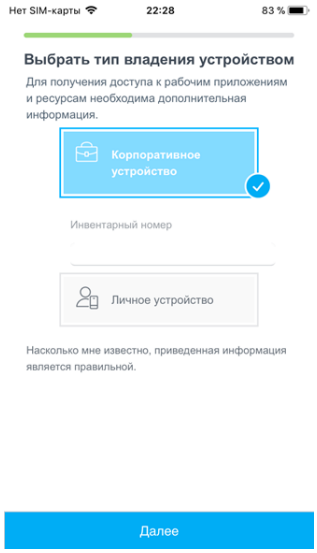
   Рис. **5-2.** Уведомление о настройке регистрации устройства



3. Если настроены условия использования, пользователям будет предложено принять их, прежде чем продолжить.

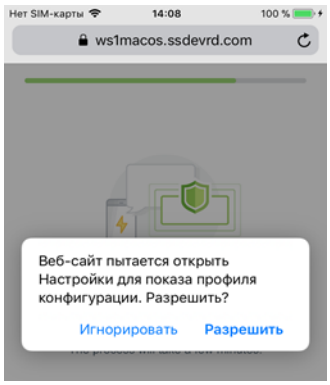
4. Если настроены дополнительный запрос на отображение типа собственности устройства и запрос на инвентарный номер устройства, отобразится соответствующая информация.

Рис. 5-3. Выбор собственности устройства



5. Пользователям необходимо открыть Safari и нажать кнопку **Разрешить**, чтобы открыть страницу настроек.

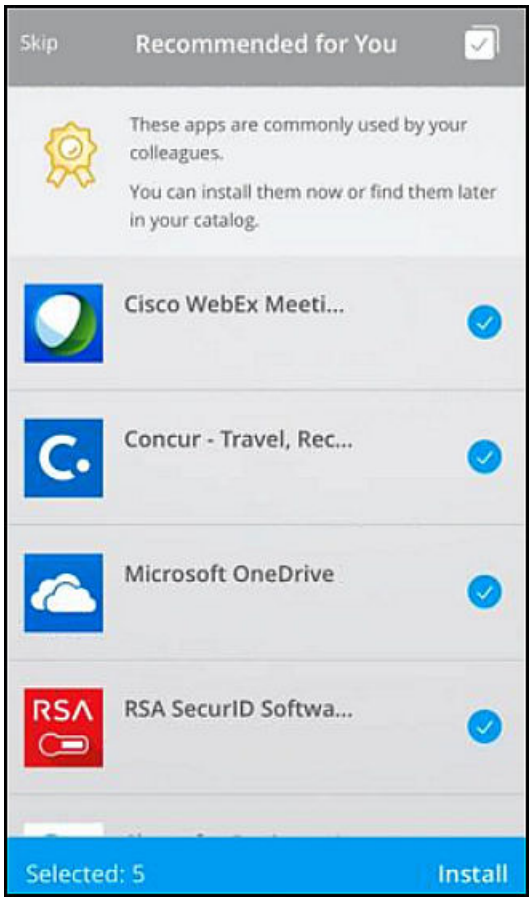
Рис. 5-4. Разрешить настройки профиля конфигурации



Теперь Workspace Services и профиль конфигурации настроены на устройстве.

Теперь устройство зарегистрировано в Workspace ONE UEM, и приложение Workspace ONE запущено. Появится окно «Рекомендованные для вас приложения».

Рис. 5-5. Окно «Рекомендуемые приложения»



6. Пользователи могут выбрать приложения для установки или пропустить этот шаг.

Теперь устройство находится под управлением Workspace ONE UEM MDM. Если рекомендованные приложения выбраны для установки, пользователи начнут получать push-уведомления для этих приложений.

Прямая регистрация с помощью Workspace ONE на устройствах Android Enterprise

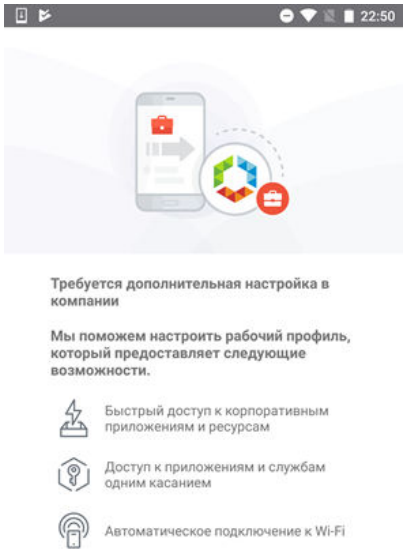
Сообщите пользователям, что им необходимо загрузить, установить и запустить приложение Workspace ONE из магазина приложений Google или репозитория.

Процедура

1. Пользователям необходимо ввести адрес эл. почты и URL-адрес сервера, а затем пройти проверку подлинности в соответствии с конфигурацией своей среды.

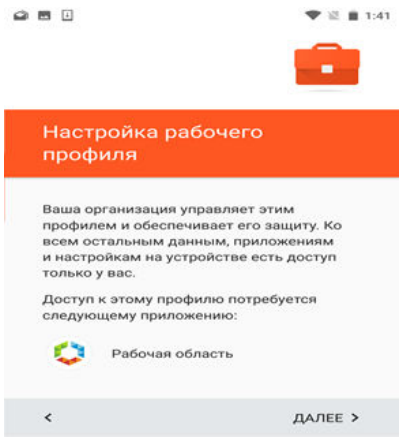
2. Отобразится окно **Требуется дополнительная настройка в компании**. Необходимо нажать кнопку **Продолжить**.

   Рис. 5-6. Уведомление о настройке регистрации устройства



3. Если настроены условия использования, пользователям будет предложено принять их, прежде чем продолжить.
4. Если настроены дополнительный запрос на отображение типа собственности устройства и запрос на инвентарный номер устройства, отобразится соответствующая информация.
5. Теперь Workspace Services и рабочий профиль настроены на устройстве.

   Рис. 5-7. Настройка уведомлений рабочего профиля

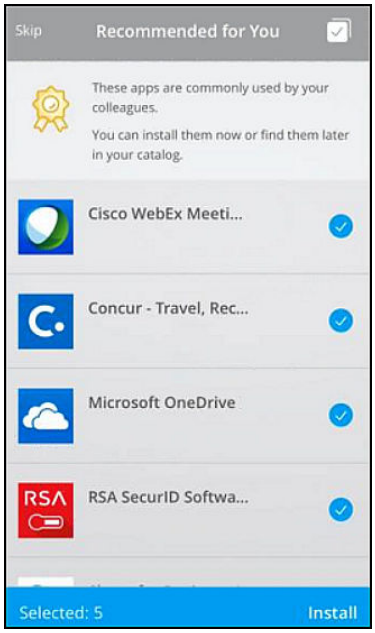


   Появится сообщение, описывающее управление устройством с помощью этого рабочего профиля. Следует нажать кнопку **ОК**.

   Теперь приложение Workspace ONE установлено и учетная запись Android for Work зарегистрирована.

6. Теперь устройство зарегистрировано в Workspace ONE UEM, и приложение Workspace ONE запущено. Появится окно «Рекомендованные для вас приложения».

   Рис. 5-8. Окно «Рекомендуемые приложения»



7. Пользователи могут выбрать приложения для установки или пропустить этот шаг.

Теперь устройство находится под управлением Workspace ONE UEM MDM. Если рекомендованные приложения выбраны для установки, они будут установлены со значком портфеля Android Enterprise.

Регистрация устройств Android Legacy

При регистрации устройств Android Legacy выполняется перенаправление к AirWatch Agent для регистрации. AirWatch Agent автоматически передает управление обратно в Workspace ONE после завершения регистрации.

Предложите пользователям перейти в магазин приложений для загрузки Workspace ONE.

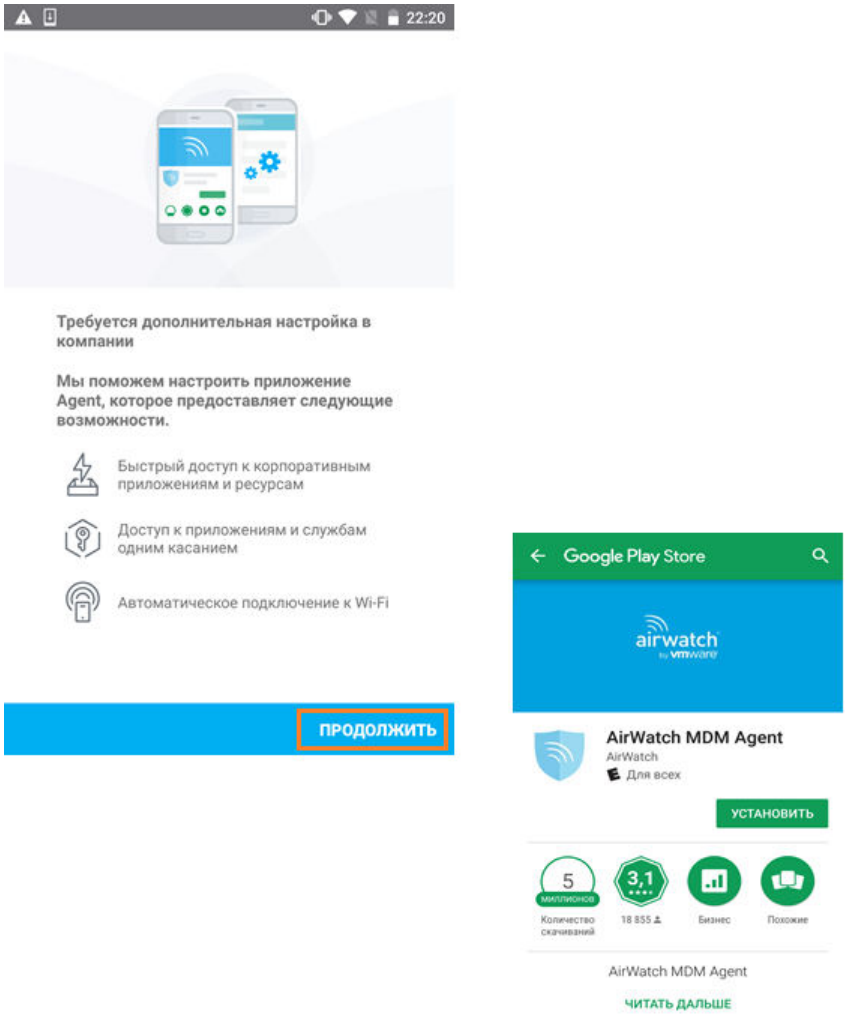
Процедура

1. Пользователям необходимо открыть приложение, указать URL-адрес сервера или адрес эл. почты, а затем ввести имя пользователя и пароль для входа систему.

   В этот момент приложение Workspace ONE может обнаружить, что устройство не поддерживается в Android Enterprise, а также определить, требуется ли прямая регистрация устройства перед получением доступа к ресурсам в Workspace ONE.

2. Отобразится окно **Требуется дополнительная настройка в компании**. Щелкнув **Продолжить**, пользователи будут перенаправлены к приложению AirWatch Agent в Google Play Store.

Рис. 5-9. Запрос загрузки приложения **AirWatch Agent**



3. Пользователям необходимо загрузить приложение AirWatch Agent.

Примечание Если приложение AirWatch Agent уже установлено на устройстве, Workspace ONE автоматически запустит его. Перенаправление в магазин приложений не производится.

Подробности проверки подлинности, указанные для Workspace ONE, передаются в приложение AirWatch Agent, чтобы не вводить эту информацию повторно.

Запускается приложение AirWatch Agent. Во время регистрации устройства с помощью AirWatch Agent пользователям следует выбрать тип владельца и ввести инвентарный номер устройства, если это необходимо.

4. При отображении окна **Разрешить Agent совершать телефонные звонки и управлять ими?** пользователи должны нажать кнопку **Разрешить**.

   AirWatch Agent проверяет регистрацию, выполняет проверку подлинности пользователей и предоставляет AirWatch разрешения на этом устройстве.

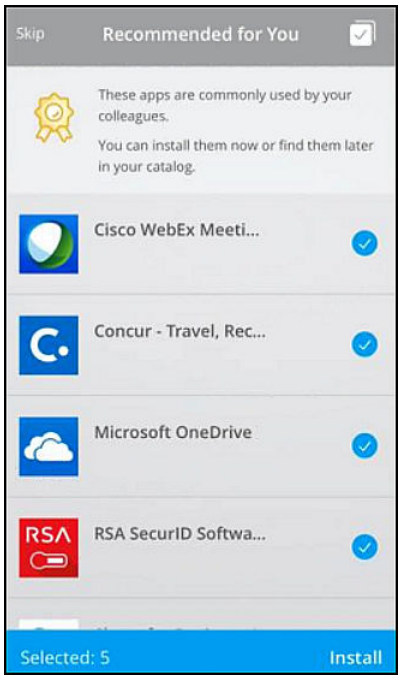
5. При отображении окна **Активировать приложение для администратора устройства?** пользователям необходимо щелкнуть **Активировать это приложение для администратора устройства**.

   Рис. 5-10. Активировать приложение для администратора устройства

6. У пользователей появится запрос на предоставление разрешения для доступа к различным возможностям устройства.

   Теперь устройство зарегистрировано в Workspace ONE UEM, и приложение Workspace ONE запущено. Появится окно «Рекомендуемые приложения».

Рис. 5-11. Окно «Рекомендуемые приложения»



7. Пользователи могут выбрать приложения для установки или пропустить этот шаг.

Теперь устройство находится под управлением Workspace ONE UEM MDM. Если рекомендованные приложения выбраны для установки, пользователи начнут получать уведомления для этих приложений.

Применение Workspace ONE для поддержки интеграции программы регистрации устройств Apple

6

Сценарии, в которых клиент использует SAML для проверки подлинности пользователя, не поддерживаются в программе регистрации устройств Apple (DEP). Тем не менее в Workspace ONE реализован уникальный способ поддержки для такого случая.

За счет промежуточной настройки устройства Workspace ONE UEM администраторы могут назначить устройство пользователю, обладающему правами на промежуточную настройку многопользовательских устройств, и разрешить Workspace ONE повторно назначать устройство соответствующему пользователю при входе в приложение Workspace ONE.

Приложение Workspace ONE должно быть установлено на устройстве в рамках регистрации пользователя для промежуточной настройки. При первом входе пользователя в Workspace ONE выполняется проверка подлинности Workspace ONE с помощью настроенного поставщика SAML. После проверки подлинности пользователя тип собственности устройства переключается с пользователя, обладающего правами на промежуточную настройку многопользовательских устройств, на пользователя, прошедшего проверку подлинности в каталоге.

Необходимое условие

При входе в приложение Workspace ONE пользователь каталога должен существовать в Workspace ONE UEM. Можно предварительно добавить пользователей в массовую загрузку в CSV-файл или применить следующий API-интерфейс для создания пользователей по мере необходимости.

Примечание Значение «Тип безопасности» должно быть как у каталога.

```
https://<API_SERVER_ADDRESS>/api/help/#!/apis/10006?!/User/User_AddUser
```

Процесс поддержки Workspace ONE для интеграции с программой DEP

Чтобы реализовать поддержку программы регистрации устройств Apple с помощью Workspace ONE, необходимо выполнить следующие задачи.

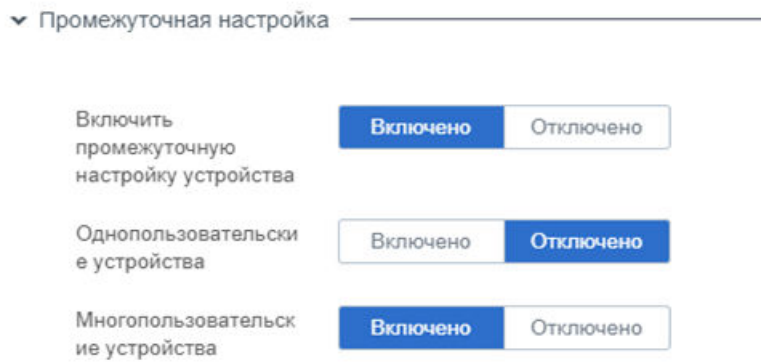
- Установите приложение Workspace ONE на устройствах iOS.

- Проверьте, что существует пользователь для промежуточной настройки со следующей промежуточной конфигурацией в консоли Workspace ONE UEM.

  а) Перейдите в раздел **Аккаунты > Пользователи > Список** и выберите для изменения учетную запись пользователя, для которого требуется включить промежуточную настройку устройства.

  б) На странице **Добавить или изменить пользователя** выберите вкладку **Дополнительно** . Прокрутите вниз до раздела **Промежуточная настройка** и включите параметры **Промежуточная настройка устройства** и **Многопользовательские устройства**.

  Рис. 6-1. Параметр «Многопользовательские устройства» в Workspace ONE UEM



- Назначьте устройство пользователю для промежуточной настройки на портале Apple DEP и предоставьте устройство конечному пользователю.

  Дополнительные сведения о программе регистрации устройств Apple см. в разделе руководства по Регистрации устройств Apple.

Реализация интеграции

При первом включении устройства оно регистрируется и назначается пользователю, обладающему правами на промежуточную настройку многопользовательских устройств. Пользователь запускает приложение Workspace ONE, доступное на домашнем экране, и входит в систему. Workspace ONE выполняет проверку подлинности пользователя с помощью настроенного поставщика SAML.

После проверки подлинности пользователя тип собственности устройства переключается с пользователя, обладающего правами на промежуточную настройку многопользовательских устройств, на пользователя, прошедшего проверку подлинности в каталоге. Приложения, профили и ресурсы, назначенные пользователю, прошедшему проверку подлинности, передаются на устройство.

Примечание Организационная группа устройства не изменяется. Эта функция не поддерживает сопоставление групп пользователей (или выбор пользователей вручную из раскрывающегося меню) в разделе «Параметр регистрации» консоли Workspace ONE UEM.

Развертывание мобильного приложения VMware Workspace ONE

7

При установке приложения VMware Workspace ONE на мобильных устройствах пользователи могут получить доступ к ресурсам, которые они уполномочены использовать.

Если удостоверениями управляет VMware Identity Manager, а пользователям предоставлены соответствующие права, они могут получить доступ к приложениям с помощью единого входа. Кроме того, они могут получить доступ к каталогу имеющихся приложений и добавить в него новые.

Интерфейс приложения Workspace ONE и его возможности выглядят одинаково на любом смартфоне, планшете и настольном компьютере.

Если устройство зарегистрировано в подсистеме Mobile Device Management (MDM), приложение Workspace ONE можно отправлять в качестве управляемого.

В эту главу входят следующие разделы:

Параметры управления устройствами в Workspace ONE UEM для общедоступных и внутренних приложений для Workspace ONE

Развертывание общедоступных и внутренних приложений можно настроить таким образом, чтобы оно выполнялось в зависимости от состояния управления устройством. Любое устройство может получить доступ к приложениям с открытым доступом. Доступ к приложениям с управляемым доступом могут получить только устройства, которым предоставлены разрешения (при включении в Workspace Services или регистрации с помощью агента).

В таблице представлены сведения для управляемых и неуправляемых устройств.

Тип доступа	Возможности	Описание	Рекомендуемые сценарии использования
Открытый доступ (неуправляемый)	■ Каталог приложений с возможностью самообслуживания для веб-ресурсов, а также ресурсов Horizon и Citrix ■ Запуск веб-приложений и виртуальных приложений путем единого входа ■ Защита приложений с помощью Touch ID и ПИН-кода ■ Обнаружение взлома на устройстве ■ Поддержка условного доступа VMware Identity Manager, включая политики проверки подлинности и блокировку устройств. ■ Доступ к родным приложениям. ■ Распределение внутренних приложений и приложений SDK.	Пользователям не приходится предоставлять администраторам разрешение на доступ к устройствам, чтобы получить доступ к ресурсам таких устройств. Доступ к приложениям с открытым доступом можно получить как на управляемых, так и на неуправляемых устройствах. Администраторы не могут систематически удалять родные приложения с открытым доступом.	■ Предоставление пользователям доступа к приложениям сразу же после входа без расширенных разрешений безопасности. ■ Рекомендуется использование приложения без его установки. Пользователи могут установить приложение на устройстве в любой удобный момент. ■ В приложениях нет конфиденциальных корпоративных данных и отсутствует доступ к защищенным корпоративным ресурсам. ■ Распространение приложений среди вспомогательного персонала без профиля MDM Workspace ONE UEM.
Управляемый доступ	■ Каталог приложений с возможностью самообслуживания для веб-ресурсов, а также ресурсов Horizon и Citrix ■ Запуск веб-приложений и виртуальных приложений путем единого входа ■ Защита приложений с помощью Touch ID и ПИН-кода ■ Обнаружение взлома на устройстве ■ Поддержка условного доступа VMware Identity Manager, включая политики проверки подлинности и блокировку устройств. ■ Управляемая и прямая установка родных приложений ■ Управление внутренними приложениями и приложениями SDK.	Пользователи устанавливают на своих устройствах профиль управления, чтобы предоставить администраторам разрешение на доступ к таким устройствам. Приложения с управляемым доступом можно использовать на устройствах, которыми управляет Workspace ONE UEM. Если Workspace ONE UEM не управляет устройством, Workspace ONE предлагает пользователю этого устройства зарегистрироваться в Workspace ONE UEM. Пользователь может использовать зарегистрированное устройство для доступа к приложениям с помощью Workspace ONE.	■ Удаление конфиденциальных корпоративных данных с устройств после увольнения пользователя из организации или потери устройства. ■ Туннелирование приложений для выполнения проверки подлинности и безопасного взаимодействия с внутренними конечными ресурсами при доступе приложений к интрасети. ■ Включение единого входа для приложений. ■ Отслеживание того, как пользователи внедряют и устанавливают приложения. ■ Автоматическое развертывание приложения после регистрации.

Тип доступа	Возможности	Описание	Рекомендуемые сценарии использования
	■ Поддержка настройки приложений ■ Отдельные сети VPN для приложений ■ Единый вход одним касанием для родных приложений с поддержкой SAML ■ Профили устройства ■ Модуль соответствия Workspace ONE UEM		

Дополнительные сведения о настройке параметров управляемого доступа для внутренних приложений и добавлении общедоступных приложений для развертывания с помощью Workspace ONE см. в руководстве по Workspace ONE UEM Mobile Application Management.

Поддерживаемые платформы для открытого и управляемого доступа

Настройте тип доступа для внутренних и общедоступных приложений с учетом платформы.

	Управляемый доступ	Открытый доступ
ВНУТРЕННИЕ ПРИЛОЖЕНИЯ		
Android	X	X
iOS	X	X
Windows 10 Desktop	X	-
Windows 10 Phone	X	-
ОБЩЕДОСТУПНЫЕ ПРИЛОЖЕНИЯ		
Android	X	X
iOS	X	X
Windows 10 Desktop	-	X
Windows 10 Phone	-	X

Управление доступом к приложениям

Пользователю может предоставляться право на открытый и управляемый доступ к родным приложениям. Благодаря адаптивному управлению пользователи могут использовать приложения с открытым доступом на неуправляемых устройствах. При запросе родного приложения, требующего управления, адаптивное управление обеспечивает дополнительную безопасность и контроль, необходимые для управления родным приложением.

Для установки и использования управляемых приложений пользователи должны включить службы Workspace. При отправке приложения в консоли Workspace ONE UEM в зависимости от конфигурации приложения для него отображается состояние доступа «Открыто» или «Под управлением». Например, если задан параметр **Отправить конфигурацию приложения**, для приложения задается состояние, требующее управления.

Приложения, требующие управления и находящиеся в неуправляемом состоянии, в каталоге обозначаются значком звездочки. Чтобы использовать приложения, пользователи должны включить службы Workspace в процессе адаптивного управления. При попытке загрузить приложения со звездочкой появится сообщение о том, что нужно включить службы Workspace. Если нужно прибегнуть к процессу адаптивного управления, можно просмотреть влияние на конфиденциальность личных сведений, выбрав ссылку на уведомление о конфиденциальности. При появлении уведомления о конфиденциальности автоматически отображаются параметры среды Workspace ONE UEM, в которой будет выполнена регистрация. Просмотрев сведения о параметрах конфиденциальности, можно перейти к включению служб Workspace или вернуться и продолжать использовать неуправляемое приложение Workspace ONE на своем устройстве. После включения служб Workspace значок звездочки удаляется со всех управляемых приложений.

Отключение доступа на управляемых устройствах

Пользователи могут отключить приложение Workspace ONE на управляемом устройстве с помощью параметра удаления учетной записи. При этом на устройстве выполняется очистка корпоративных данных, корпоративный доступ отключается и пользователь возвращается к экрану входа. Чтобы отключить службы Workspace ONE, администраторы могут очистить корпоративные данные в консоли Workspace ONE UEM.

При выполнении действия «Удалить учетную запись» на управляемом устройстве отзывается право доступа, предоставленное с помощью приложения Workspace ONE, а регистрация устройства в Workspace ONE UEM отменяется. Приложения, требующие управления, удаляются с устройства, а доступ к приложениям Workspace ONE UEM для повышения эффективности работы, например Boxer, Browser и Content Locker, аннулируется.

Обязательное принятие условий использования для доступа к каталогу Workspace ONE

Вы можете разработать собственные условия использования Workspace ONE для своей организации и настроить обязательное принятие этих условий пользователями для доступа к Workspace ONE.

Условия использования отображаются после того, как пользователь выполнит вход в Workspace ONE. Пользователи должны принять условия использования, прежде чем перейти к работе с каталогом Workspace ONE.

Для функции «Условия использования» предусмотрены следующие возможности конфигурации.

- Создание версий существующих условий использования.
- Изменение условий использования.

- Создание нескольких вариантов условий использования, которые будут отображаться в зависимости от типа устройства.
- Создание копий условий использования на различных языках.

Настроенные политики условий использования указаны на вкладке «Управление учетными данными и доступом». Можно внести изменения в существующую политику или создать новую версию политики. Новая версия условий использования заменяет существующие условия использования. При внесении изменений в политику новая версия условий использования не создается.

На странице «Условия использования» можно просмотреть количество пользователей, принявших или не принявших условия. Щелкните число, указывающее количество пользователей, которые приняли или не приняли условия использования, чтобы просмотреть список пользователей и их статус.

Настройка и активация условий использования

На странице «Условия использования» можно добавить политику условий использования, а также настроить параметры использования. После добавления условий использования необходимо активировать параметр «Условия использования». При входе в Workspace ONE пользователи должны принять условия использования, чтобы получить доступ к своим каталогам.

Необходимые условия

Текст политики условий использования в формате HTML для копирования и вставки в текстовое поле «Условия использования». Можно добавить условия использования на английском, немецком, испанском, французском, итальянском и голландском языках.

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» выберите **Настройка > Условия использования**.
2. Нажмите **Добавить условия использования**.
3. Укажите описательное имя условий использования.
4. Выберите значение **Все**, если политика условий использования предназначена для всех пользователей. Чтобы отображать политику условий использования на отдельных типах устройств, выберите **Выбранные платформы устройств**, а затем выберите типы устройств, на которых будет отображаться эта политика условий использования.
5. По умолчанию условия использования отображаются на том языке, который настроен для веб-браузера. В текстовом поле введите содержимое условий использования на том языке, который используется по умолчанию.

6. Нажмите кнопку **Сохранить**.

   Чтобы добавить политику условий использования на другом языке, нажмите **Добавить язык** и выберите нужный язык. Текстовое поле содержимого условий использования будет обновлено, после чего можно будет добавить текст.

   Можно перетащить названия языков, чтобы задать порядок отображения для условий использования на различных языках.

7. Чтобы начать применять условия использования, нажмите **Включить условия использования** на отобразившейся странице.

Следующие шаги

Если для отображения условий использования выбран конкретный тип устройства, можно создать дополнительные условия использования для других типов устройств.

Просмотр статуса принятия условий использования

Для политики условий использования, приведенной на странице «Удостоверения и управление» > «Условия использования», отображается количество пользователей, которые подтвердили или не подтвердили свое согласие с этой политикой.

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» выберите **Настройка > Условия использования**.

2. Щелкните число, указывающее количество принявших условия пользователей (слева в столбце «Принявшие/не принявшие»), или число, указывающее количество пользователей, которые не приняли условия (справа в этом столбце).

   На странице статуса отобразится выполненное действие (принятие или отклонение), имя пользователя, идентификатор устройства, версия просмотренной политики, используемая платформа, а также дата.

3. Нажмите **Отмена**, чтобы закрыть вид.

Получение и распространение приложения Workspace ONE

Пользователи могут загрузить приложение VMware Workspace ONE из магазина приложений на свое устройство сами, или администратор может настроить Workspace ONE UEM для отправки Workspace ONE на устройства в качестве управляемого приложения.

Приложение Workspace ONE развертывается из консоли Workspace ONE UEM для конкретных групп и пользователей в организации. После входа в приложение Workspace ONE на устройствах пользователи могут получить доступ к веб-приложениям и приложениям SaaS, для которых у них есть право доступа.

Далее представлена процедура отправки мобильного приложения Workspace ONE в качестве управляемого приложения из консоли Workspace ONE UEM. Кроме того, для отправки приложения можно воспользоваться мастером начальной настройки Workspace ONE.

Примечание Дополнительные сведения о настройке управляемых приложений в Workspace ONE UEM см. в руководстве по работе с VMware Workspace ONE UEM Mobile Application Management (MAM), которое доступно на портале ресурсов по адресу https://resources.air-watch.com.

Необходимые условия

Если планируется передать мобильное приложение Workspace ONE из консоли Workspace ONE UEM, подготовьте смарт-группы конечных пользователей, у которых есть права на доступ к приложению.

Процедура

1. В консоли Workspace ONE UEM последовательно выберите **Книги и приложения > Приложения** > **Список > Общедоступные**, а затем выберите **Добавить приложение**.
2. Выберите платформу (iOS, Android или Windows).
3. Выберите элемент **Поиск в магазине приложений** и в текстовом поле **Имя** введите `Workspace ONE` в качестве ключевого слова для поиска VMware Workspace ONE в магазине приложений.
4. Нажмите кнопку **Далее** и щелкните **Выбрать**, чтобы передать приложение Workspace ONE со страницы результатов магазина приложений.
5. Настройте следующие параметры назначения и развертывания для пользователей Workspace ONE на следующих вкладках:

Вкладка	Описание
Информация	Введите и просмотрите сведения о поддерживаемых моделях устройств, оценках и категориях.
Назначение	Назначьте мобильное приложение Workspace ONE смарт-группам конечных пользователей, которые могут использовать приложение на своем устройстве.
Развертывание	При необходимости настройте компоненты, отвечающие за доступность, и расширенные возможности управления корпоративной мобильной средой (Enterprise Mobility Management, EMM). Для автоматической настройки управляемых приложений включите **отправку конфигурации приложения** и задайте конфигурацию приложений в корпоративной среде для пар «ключ–значение». См. раздел Настройка приложения Workspace ONE UEM в корпоративной среде для использования пар «ключ–значение».
Условия использования	(Необязательно.) Включите параметр **Условия использования** для использования приложения Workspace ONE.

6. Выберите **Сохранить и опубликовать**, чтобы сделать приложение доступным для пользователей.

   Выполните эти действия для каждой поддерживаемой платформы.

Настройка приложения Workspace ONE UEM в корпоративной среде для использования пар «ключ–значение»

При развертывании приложения Workspace ONE в качестве управляемого приложения в Workspace ONE UEM и включении параметра отправки конфигураций приложения во время отправки приложения Workspace ONE из консоли Workspace ONE UEM можно предварительно задать параметры Workspace ONE, которые применяются, когда пользователи устанавливают и запускают приложение Workspace ONE.

Если приложение Workspace ONE отправляется в консоль Workspace ONE UEM в качестве управляемого мобильного приложения, можно настроить URL-адрес сервера VMware Workspace ONE, значение идентификатора UID устройства, а также обязательную проверку подлинности с помощью сертификата на устройствах Android.

Таблица 7-1. Параметры конфигурации управляемого устройства Workspace ONE в консоли Workspace ONE UEM

Платформа	Конфигурационный ключ	Тип значения	Конфигурационное значение	Объяснение
Все	`AppServiceHost`	String	**<URL-адрес сервера VMware Workspace ONE>**	Определяет URL-адрес сервера для VMware Workspace ONE на устройствах.
iOS	`deviceUDID`	String	**{DeviceUid}** Введите значение UID устройства. Не используйте функцию Insert Lookup Value.	Отслеживает устройства, используемые для проверки подлинности в среде VMware Identity Manager.

Таблица 7-1. Параметры конфигурации управляемого устройства Workspace ONE в консоли Workspace ONE UEM (продолжение)

Платформа	Конфигурационный ключ	Тип значения	Конфигурационное значение	Объяснение
iOS	SkipDiscoveryScreen	Логическое	**true**	Начиная с версии приложения Workspace ONE 3.1, можно настроить ключ конфигурации SkipDiscoveryScreen. При установке значения True Workspace ONE пытается пропустить экран с адресом электронной почты или URL-адресом сервера. При использовании с ключом конфигурации AppServiceHost пользователи автоматически переходят на экран проверки подлинности. Если также используется единый вход для мобильных устройств, администраторы могут создать для конечных пользователей более удобные условия работы, настроив загрузку приложения Workspace ONE при запуске Workspace ONE.
Android и iOS	RemoveAccountSignOut	Целое число	0 — отображается параметр «Удалить учетную запись» 1 — не отображается параметр «Удалить учетную запись» Если значение не задано, отображается параметр «Удалить учетную запись».	Если задано значение 1, параметр «Удалить учетную запись» не отображается на странице настроек Workspace ONE для пользователей. Пользователям не удается удалить учетную запись Workspace ONE со своих устройств.

Таблица 7-1. Параметры конфигурации управляемого устройства Workspace ONE в консоли Workspace ONE UEM (продолжение)

Платформа	Конфигурационный ключ	Тип значения	Конфигурационное значение	Объяснение
				Если установлено значение 0 или значение не задано, отобразится параметр «Удалить учетную запись». При нажатии кнопки «Удалить учетную запись» Workspace ONE UEM выполняет очистку корпоративных данных устройства и отменяет регистрацию устройства в Workspace ONE UEM.

Регистрация доменов электронной почты для автоматического обнаружения

Чтобы конечным пользователям было проще получить доступ к порталу приложений из приложения Workspace ONE, можно зарегистрировать домен электронной почты в службе автоматического обнаружения. Вместо URL-адреса организации конечные пользователи вводят свой адрес электронной почты.

Когда домен электронной почты организации регистрируется для автоматического обнаружения, чтобы получить доступ к порталу приложений, конечные пользователи вводят только адрес электронной почты на странице входа. Например, они должны ввести **username@myco.com**.

Если автоматическое обнаружение не используется, конечные пользователи должны указать полный URL-адрес организации при первом открытии приложения Workspace ONE. Например, они должны ввести **myco.vmwareidentity.com**.

Установка автоматического обнаружения в VMware Identity Manager

Для регистрации домена необходимо ввести домен электронной почты и адрес электронной почты на странице «Автоматическое обнаружение» в консоли VMware Identity Manager.

На адрес электронной почты в домене отправляется электронное сообщение с маркером активации. Для активации регистрации домена необходимо ввести маркер на странице «Автоматическое обнаружение» и убедиться в правильности зарегистрированного домена.

Примечание Чтобы настроить автоматическое обнаружение для локальных развертываний VMware Identity Manager, необходимо войти в консоль VMware Identity Manager от имени локального администратора. Введите идентификатор и пароль Workspace ONE UEM, созданные на странице веб-сайта Workspace ONE UEM https://secure.air-watch.com/register.

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» выберите **Настройка > Автоматическое обнаружение**.
2. (Только для локальных сред). Настройте URL-адрес автоматического обнаружения Workspace ONE UEM.

Параметр	Описание
URL-адрес автообнаружения	Введите URL-адрес, например https://discovery.awmdm.com.
Идентификатор AirWatch	Введите адрес электронной почты, зарегистрированный в Workspace ONE UEM, чтобы войти на соответствующий веб-сайт.
Пароль	Введите пароль, связанный с учетной записью Workspace ONE UEM.

3. В текстовом поле **Домен электронной почты** введите домен электронной почты организации, который нужно зарегистрировать.
4. В текстовом поле **Адрес эл. почты для подтверждения** введите адрес электронной почты в указанном домене электронной почты, чтобы получить маркер проверки.
5. Нажмите кнопку **ОК**.

   Для регистрации этого домена электронной почты будет задано состояние «Ожидание». Только один домен электронной почты может находиться в состоянии «Ожидание».
6. Откройте электронное сообщение и скопируйте маркер активации.
7. Вернитесь на страницу **Управление учетными данными и доступом > Автоматическое обнаружение** и вставьте маркер в текстовое поле «Код активации».
8. Щелкните **Проверить**, чтобы зарегистрировать домен.

Домен электронной почты зарегистрирован и добавлен в список зарегистрированных доменов электронной почты на странице «Автоматическое обнаружение».

Теперь конечные пользователи могут использовать для доступа к порталу приложений в приложении Workspace ONE свой адрес электронной почты.

Следующие шаги

При наличии нескольких доменов электронной почты добавьте другой домен электронной почты для регистрации.

Настройка проверки подлинности для сеанса

Служба VMware Identity Manager включает в себя политику доступа по умолчанию, управляющую доступом пользователей к ресурсам VMware Identity Manager.

Продолжительность сеанса проверки подлинности настраивается в правилах политик, которые определяют максимальное количество времени, которое есть у пользователей с момента последнего события проверки подлинности для доступа на страницу запуска приложений или для запуска определенного веб-приложения. По умолчанию — 8 часов. После проверки подлинности у пользователей есть восемь часов для запуска веб-приложения, если они не инициируют еще одно событие проверки подлинности, которое продлит срок.

Политику по умолчанию можно изменить для изменения продолжительности сеанса. Это можно сделать в консоли администрирования VMware Identity Manager на вкладке «Управление учетными данными и доступом» («Управление > Политики»). См. раздел «Управление политиками доступа» в руководстве по администрированию VMware Identity Manager.

Включение проверки соответствия для управляемых устройств Workspace ONE UEM

Когда пользователи регистрируют устройства, устанавливается расписание, по которому отправляются образцы данных, используемые для оценки соответствия нормативным требованиям. Оценка этого образца данных позволяет убедиться в том, что устройство отвечает требованиям к соответствию, которые установил администратор в консоли Workspace ONE UEM (UEM). Если устройство не соответствует нормативным требованиям, будут предприниматься определенные действия, настроенные в консоли UEM.

В службе VMware Identity Manager предусмотрен параметр политики доступа, который можно настроить для проверки состояния соответствия устройства на сервере Workspace ONE UEM, когда пользователи входят в систему с такого устройства. Проверка соответствия гарантирует, что пользователям будут запрещены вход в приложение или использование единого входа на портал Workspace ONE, если устройство не соответствует нормативным требованиям. Когда устройство снова будет соответствовать нормативным требованиям, возможность войти будет восстановлена.

Если устройство скомпрометировано, приложение Workspace ONE автоматически выполняет выход из системы и блокирует доступ к приложениям. Если устройство зарегистрировано с помощью адаптивного управления, через консоль UEM будет отправлена команда очистки корпоративных данных для отмены регистрации устройства и удаления с устройства всех управляемых приложений. Неуправляемые приложения не будут удалены.

Дополнительные сведения о политиках соответствия Workspace ONE UEM см. в руководстве по VMware Workspace ONE UEM Mobile Device Management на странице документации по VMware Workspace ONE UEM.

Стратегии развертывания для настройки нескольких организационных групп Workspace ONE UEM

Workspace ONE UEM использует организационные группы для идентификации пользователей и настройки разрешений. При интеграции Workspace ONE UEM с VMware Identity Manager ключи REST API администратора и регистрирующегося пользователя настраиваются в организационной группе Workspace ONE UEM типа «Заказчик».

При входе пользователя в Workspace ONE с устройства в VMware Identity Manager инициируется событие регистрации устройства. В Workspace ONE UEM отправляется запрос на получение любых приложений, право на использование которых есть как у пользователя, так и у устройства. Чтобы найти пользователя в Workspace ONE UEM и поместить устройство в подходящую организационную группу, запрос отправляется через REST API.

В VMware Identity Manager можно настроить два варианта управления организационными группами:

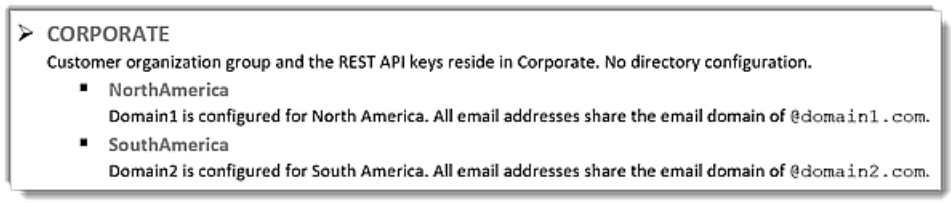
- включение автоматического обнаружения Workspace ONE UEM;
- сопоставление организационных групп Workspace ONE UEM с доменами в службе VMware Identity Manager.

Если не настроить ни один из них, Workspace ONE попытается найти пользователя в организационной группе, где создан ключ REST API. Это группа «Заказчик».

Использование автоматического обнаружения Workspace ONE UEM

Настройте автоматическое обнаружение, если для одного каталога в дочерней группе настроена организационная группа «Заказчик» или если в одной группе «Заказчик» настроено несколько каталогов с уникальными доменами электронной почты.

Рис. 7-1. Пример 1



В примере 1 домен электронной почты организации зарегистрирован для автоматического обнаружения. На странице входа Workspace ONE пользователи вводят только адрес электронной почты.

В данном примере, если пользователи в домене NorthAmerica входят в Workspace ONE, им нужно ввести полный адрес электронной почты в формате «пользователь1@домен1.com». Приложение ищет домен и проверяет, существует ли пользователь или можно ли его создать при вызове каталога в организационной группе NorthAmerica. После этого устройство можно зарегистрировать.

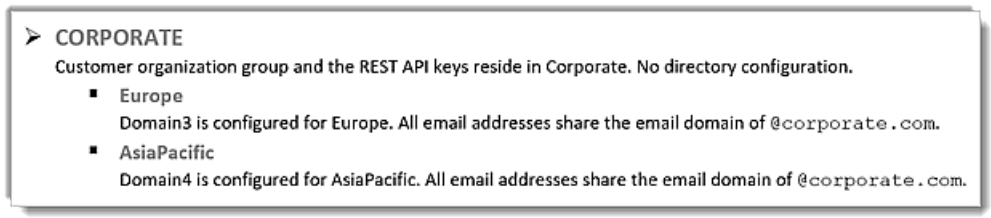
Использование сопоставления организационной группы **Workspace ONE UEM** с доменами **VMware Identity Manager**

Сопоставление службы VMware Identity Manager с организационной группой Workspace ONE UEM следует настроить, если в одном домене электронной почты настраивается несколько каталогов. Параметр **Сопоставление доменов с несколькими организационными группами** можно включить на странице конфигурации AirWatch в консоли VMware Identity Manager.

Если этот параметр «Сопоставление доменов с несколькими организационными группами» включен, домены, настроенные в VMware Identity Manager, можно сопоставить с идентификаторами организационных групп Workspace ONE UEM. Кроме того, вам потребуется ключ REST API администратора.

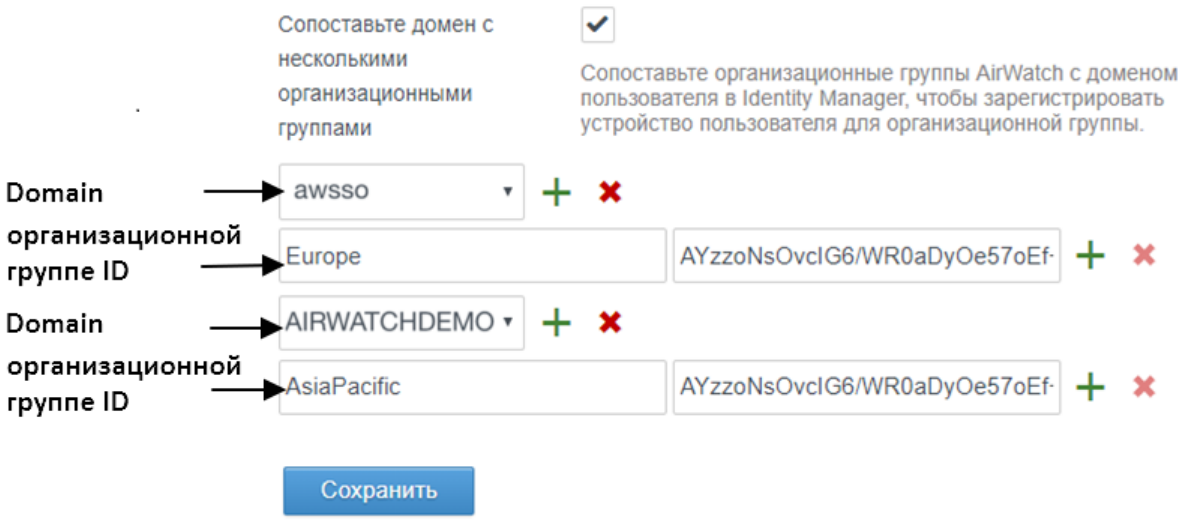
В примере 2 два домена сопоставляются с разными организационными группами. Вам потребуется ключ REST API администратора. Один ключ REST API администратора используется для обоих идентификаторов организационной группы.

Рис. **7-2.** Пример **2**



На странице конфигурации AirWatch в консоли VMware Identity Manager настройте определенный идентификатор организационной группы Workspace ONE UEM для каждого домена.

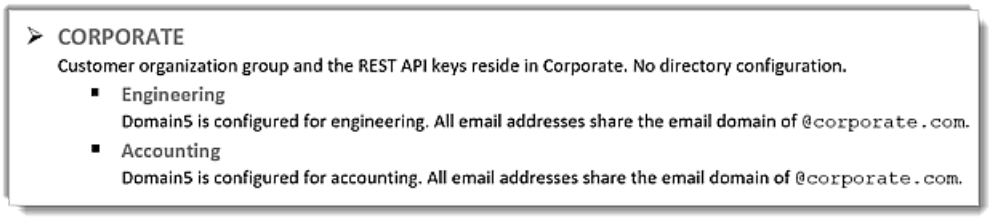
Рис. **7-3.** Пример **2.** Настройка организационной группы



С этой конфигурацией при входе пользователей в Workspace ONE с устройства в ходе запроса на регистрацию устройства осуществляется попытка найти пользователей из домена Domain3 в организационной группе «Europe» и домена Domain4 в организационной группе «AsiaPacific».

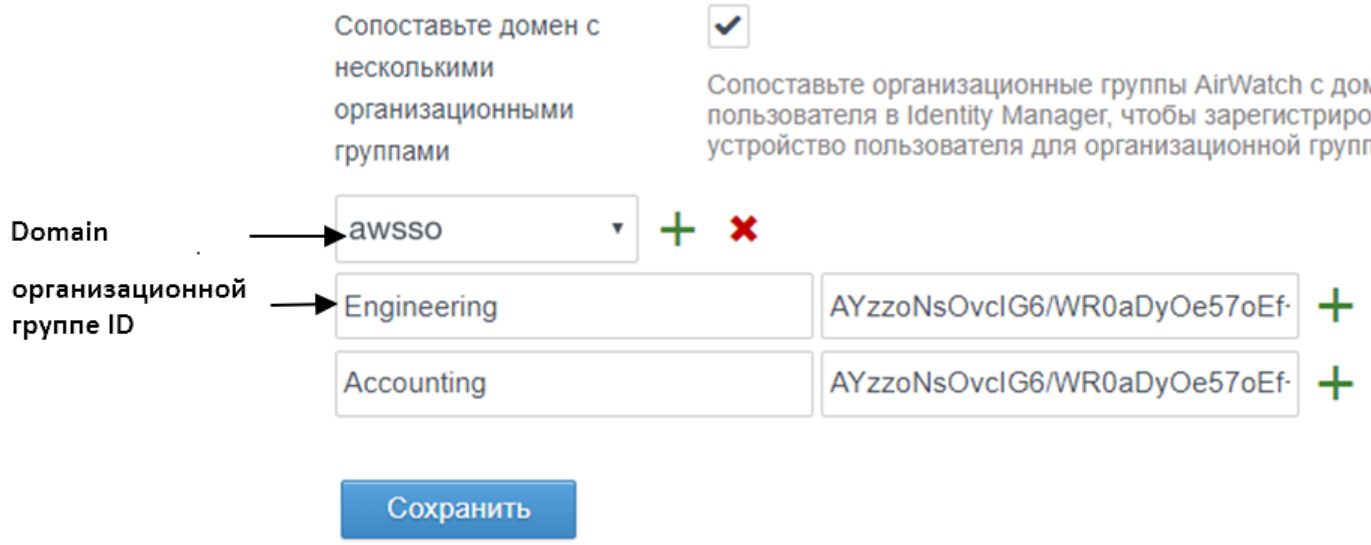
В примере 3 один домен сопоставляется с несколькими организационными группами Workspace ONE UEM. Оба каталога используют один и тот же домен электронной почты. Домен указывает на одну и ту же организационную группу Workspace ONE UEM.

Рис. 7-4. Пример 3



В этой конфигурации при входе в Workspace ONE приложение предлагает пользователю выбрать группу, в которой он желает зарегистрироваться. В этом примере пользователи могут выбрать только группу «Проектирование» или «Учет».

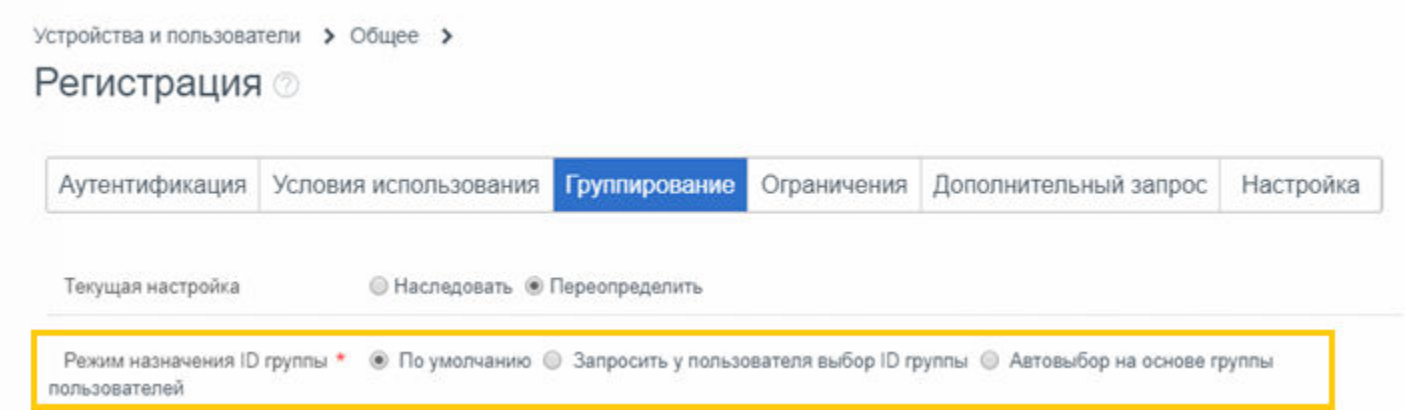
Рис. 7-5. Организационные группы, в которых каталоги используют один и тот же домен



Помещение устройств в соответствующую организационную группу

При обнаружении записи пользователя устройство добавляется в соответствующую организационную группу. Параметр регистрации в Workspace ONE UEM **Режим назначения ID группы** определяет организационную группу, в которую будет помещено. Этот параметр находится на странице «Параметры системы» > «Устройство и пользователи» > «Общие» > «Регистрация» > «Группирование»в консоли Workspace ONE UEM Console.

Рис. 7-6. Регистрация устройств в группах Workspace ONE UEM



В примере 4 все пользователи находятся на уровне организационной группы «Корпоративная».

Рис. 7-7. Пример 4

Размещение устройства зависит от конфигурации, выбранной для режима назначения идентификатора группы в организационной группе «Корпоративная».

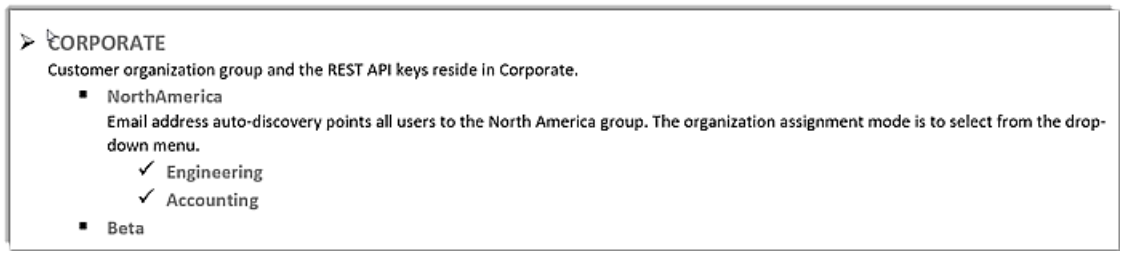
- Если выбрано значение «По умолчанию», устройство помещается в группу, в которой находится пользователь. В примере 4 устройство помещается в группу «Корпоративная».
- Если выбрано значение «Запросить у пользователя выбор ID группы», пользователям предлагается выбрать группу для регистрации устройства. В примере 4 в приложении Workspace ONE отображается раскрывающееся меню с вариантами «Проектирование» или «Учет».
- Если выбрано значение «Автовыбор на основе группы пользователей», устройства помещаются в группу «Проектирование» или «Учет» в соответствии с назначенной группой пользователей и сопоставлением в консоли Workspace ONE UEM.

Общие сведения о понятии «Скрытая группа»

В примере 4 пользователям предлагается выбрать организационную группу для регистрации. При этом они также могут ввести значение идентификатора группы, не указанной в приложении Workspace ONE. Именно такая группа и называется скрытой.

В примере 5 в структуру организационной группы «Корпоративная» входят группы North America и Beta.

Рис. 7-8. Пример 5



В примере 5 пользователи вводят адреса электронной почты в Workspace ONE. После проверки подлинности отображается список с группами «Проектирование» и «Учет» на выбор. Группа «Бета» не отображается. Если идентификатор организационной группы известен, можно вручную ввести группу «Бета» в текстовом поле выбора группы и зарегистрировать в ней устройство.

Работа на портале Workspace ONE

8

Если приложение Workspace ONE установлено на устройствах, пользователи могут войти в Workspace ONE, чтобы получить безопасный доступ к каталогу приложений, которые включила для них организация. Если в приложении настроен единый вход, пользователям не придется повторно вводить учетные данные для входа при запуске приложения.

Пользовательский интерфейс Workspace ONE на телефонах, планшетах и настольных компьютерах работает по схожему принципу. На странице «Каталог» в Workspace ONE отображаются ресурсы, опубликованные в Workspace ONE. Чтобы выполнить поиск приложения, добавить или обновить его, а также сделать для него закладку, можно коснуться или щелкнуть его. Чтобы удалить приложение со страницы закладок, можно щелкнуть его правой кнопкой мыши. Добавить ресурсы, к которым предоставлен доступ, можно на странице «Каталог».

В эту главу входят следующие разделы:

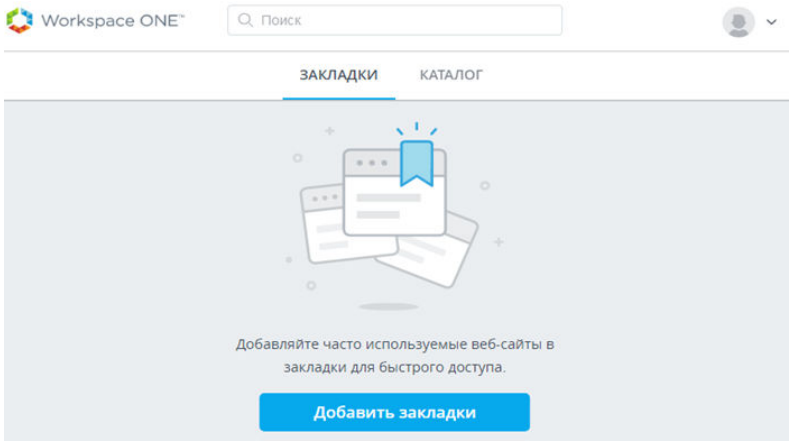
Работа с приложениями в Workspace ONE

Пользовательский портал Workspace ONE состоит из вкладок «Каталог» и «Закладки». При первом входе пользователей на портал Workspace ONE отображается вкладка «Каталог», если вкладка «Закладки» пуста.

После первого запуска открывается последняя использованная вкладка. Если нужно, чтобы при запуске отображалась вкладка «Каталог», можно воспользоваться представлением «Каталог».

На портале Workspace ONE можно скрыть вкладку «Каталог» или «Закладки» для удобства работы пользователей. В консоли VMware Identity Manager на странице «Каталог» > «Параметры» > «Конфигурация пользовательского портала» можно изменить конфигурацию портала.

Рис. 8-1. Исходное представление страницы «Закладки»



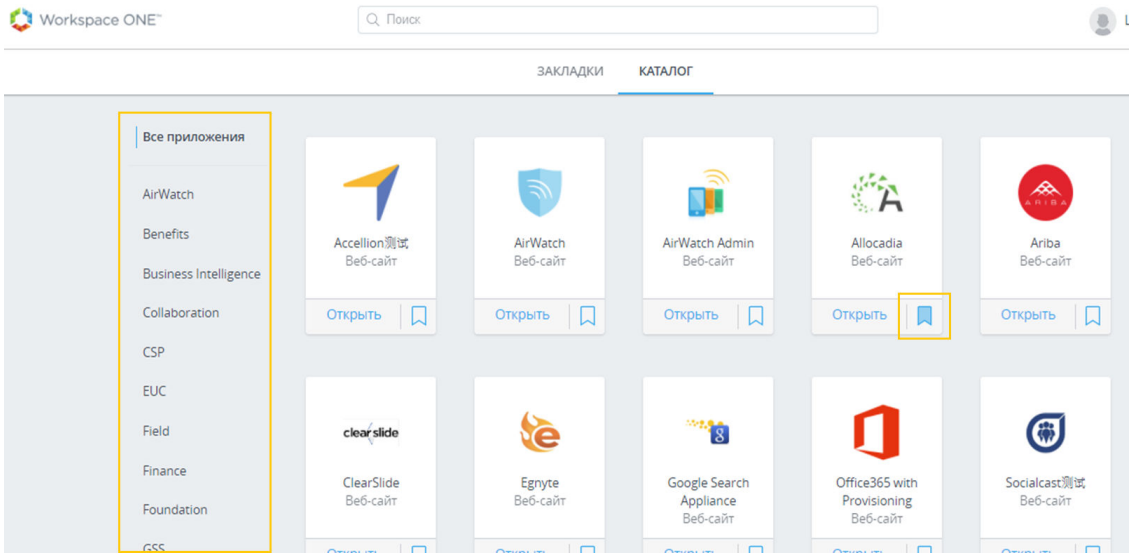
В каталоге можно открыть или установить веб-приложения, а также мобильные и виртуальные приложения, к которым пользователям предоставлен доступ. Виртуальные приложения и веб-приложения можно открывать непосредственно со страниц «Каталог» или «Закладки» в приложении Workspace ONE.

Нативные приложения, например iOS и Android, нельзя добавить в закладки или запустить со страниц Workspace ONE. Эти приложения запускаются со Springboard в iOS или Android.

На странице «Каталог» можно структурировать приложения по логическим категориям, чтобы упростить пользователям поиск необходимых ресурсов. Категория с названием «Рекомендовано» указывается по умолчанию. Определяя приложения в категорию «Рекомендовано», можно включить параметр **Показать рекомендуемые приложения на вкладке «Закладки»**, чтобы предварительно заполнить сведения об этих приложениях на странице «Закладки».

При использовании этой конфигурации пользователям при первом входе на портал Workspace ONE будет предложен быстрый доступ к рекомендованным приложениям.

Рис. 8-2. Страница «Каталог» приложения Workspace ONE



Примечание Мобильные приложения недоступны в браузерах для настольных компьютеров.

Для запуска веб-приложений можно воспользоваться следующими компонентами.

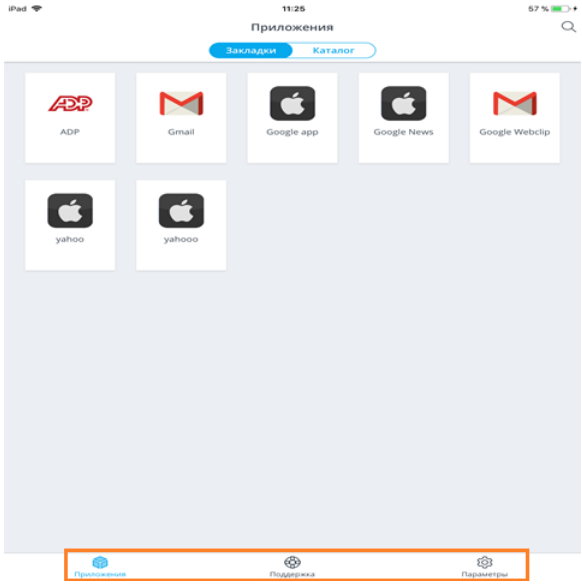
- Вкладка «Закладки». Чтобы запустить приложение, нужно щелкнуть его значок.
- Вкладка «Каталог». Чтобы открыть приложение, нужно щелкнуть поле со стрелкой.
- «Поиск в Spotlight» или «Поиск в Workspace ONE». В «Поиск в Spotlight» на устройстве с iOS нужно выбрать значок приложения в списке, а в области поиска в Workspace ONE — щелкнуть поле со значком стрелки, чтобы открыть приложение.

Для получения доступа к параметрам Workspace ONE пользователям нужно щелкнуть стрелку раскрывающегося меню рядом с названием приложения.

- Учетная запись. Сведения о профиле пользователя, включая имя, имя пользователя и адрес электронной почты.
- Устройства. Список устройств, с которых выполнен вход в приложение Workspace ONE, а также сведения о дате и времени последнего входа.
- Советы по работе с приложением. Советы по работе с Workspace ONE на устройстве пользователя.
- Описание. Сведения об авторском праве, патенте и лицензии Workspace ONE.
- Параметры. Параметры запуска по умолчанию при доступе к удаленным приложениям Horizon во время их просмотра из Horizon Client или браузера.

Чтобы войти на портал приложений, пользователям нужно коснуться значка приложения Workspace ONE. Если имеются приложения, добавленные в закладки, отобразится страница «Закладки». В приложении Workspace ONE на устройствах есть ссылки «Поддержка» и «Настройки».

Рис. 8-3. Представление портала **Workspace ONE** на устройстве



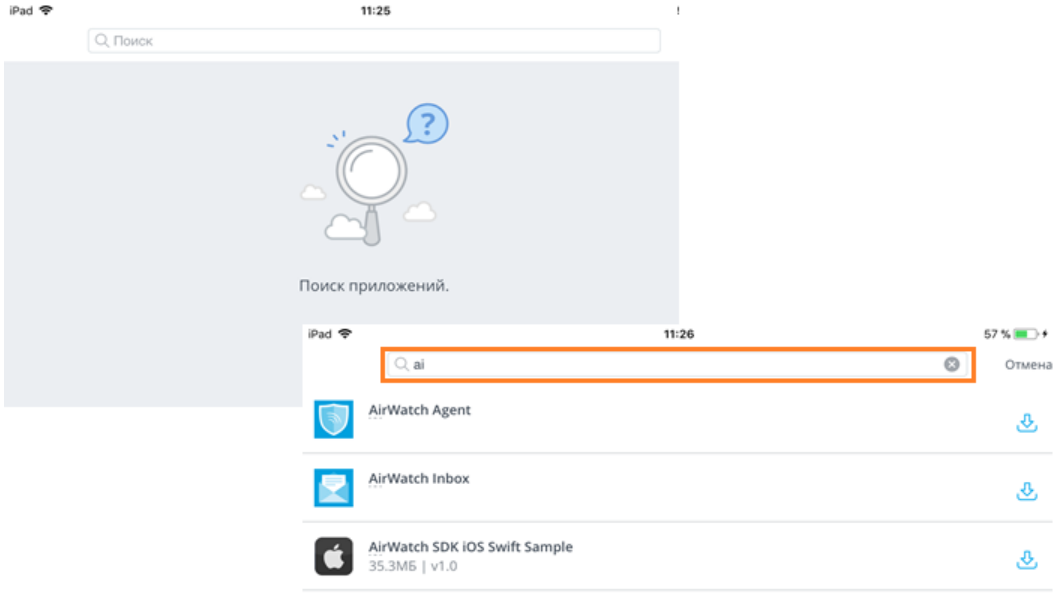
- На странице «Поддержка» отображаются ссылки «Устройства» и «Отправить отчет». На странице «Устройства» содержатся сведения о последнем входе. На странице отправки отчета пользователи могут отправить вам диагностические сведения или комментарии. Пользователи могут включить или отключить эту возможность в параметрах устройства.
- На странице «Настройки» представлена версия приложения Workspace ONE и политика конфиденциальности VMware Workspace. Пользователи могут удалить учетную запись на странице «Настройки», чтобы выйти из приложения Workspace ONE.

Использование поиска в **Workspace ONE**

С помощью функции писка пользователи могут искать в Workspace ONE приложения по имени или категории.

По мере ввода текста в поле поиска на экране появляются приложения, соответствующие введенному тексту.

Рис. 8-4. Поиск с результатами



Пользователи могут запускать веб-приложения или загружать родные приложения непосредственно из окна результатов поиска.

На устройствах с iOS для поиска приложений на портале Workspace ONE можно воспользоваться компонентом «Полезные сведения». Нужно коснуться главного экрана на устройстве с iOS и провести вниз, чтобы появилось поле поиска компонента «Полезные сведения». При вводе имени приложения на портале Workspace ONE открывается Workspace ONE и запускается приложение.

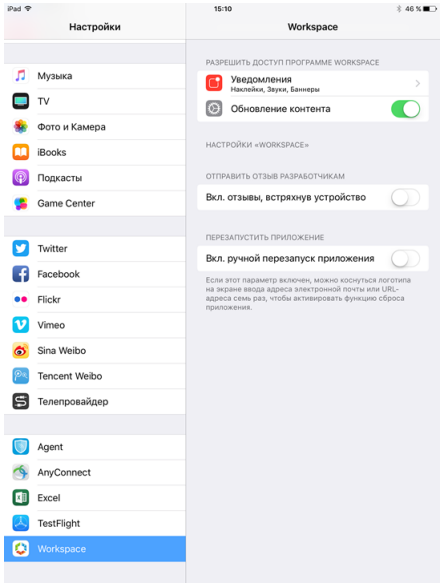
Помощь пользователям с отправкой отчетов о проблемах, возникающих на устройствах iOS

На устройствах с iOS компонент Rage Shake можно использовать для отправки журналов разработчикам приложений iOS.

Пользователь встряхивает устройство, которое, в свою очередь, записывает сведения о текущем состоянии и по умолчанию отправляет их в электронном сообщении разработчикам приложения Workspace ONE. Пользователи могут вручную ввести другой адрес электронной почты для отправки сведений.

Параметр «Включить отзыв» или компонент Shake можно включить на устройстве на странице «Настройки > Рабочая область». Компонент Rage Shake можно использовать для отправки отчета с любого экрана на портале Workspace ONE.

Рис. 8-5. Включение отзывов в компоненте **Shake**



Когда в устройстве с iOS появляется сообщение об ошибке примерно такого содержания: Это устройство зарегистрировано другим пользователем или в другой среде, можно использовать параметр «Сброс параметров приложения вручную» для полной очистки данных приложения, хранящихся на устройстве локально.

Настройка секретных кодов для приложения Workspace ONE

На устройствах пользователей должен быть включен компонент блокировки с помощью секретного кода. Если он не включен, при первом запуске приложения Workspace ONE для пользователей отображается запрос на создание секретного кода. Этот код необходимо вводить каждый раз, когда пользователи хотят получить доступ к Workspace ONE на устройстве.

Если компонент блокировки с помощью секретного кода не используется, при попытке получить доступ к приложению Workspace ONE для пользователей отображается запрос на создание секретного кода. Уровень, на котором устанавливается секретный код, зависит от платформы. Для устройств Android секретный код устанавливается на уровне приложений. Для компьютеров с Windows и устройств с iOS при использовании Workspace ONE 3.2 или более ранних версий секретный код устанавливается на уровне устройств.

Примечание Устройства с iOS и Android также поддерживают компонент сканера отпечатков пальцев Touch ID.

С помощью Workspace ONE можно обнаружить возможные проблемы безопасности на устройствах. Если пользователи отключили секретный код на устройстве, при следующем открытии приложения Workspace ONE им будет предложено установить секретный код перед входом в Workspace ONE. Если включен секретный код на уровне приложений, пользователи не смогут отключить его.

Секретные коды на уровне приложений на устройствах с iOS

Можно создать более сложные секретные коды, чем секретный код устройства с минимальным набором из четырех цифр. Секретный код на уровне приложений можно использовать совместно с другими приложениями повышения производительности, например, VMware Boxer.

Можно назначить требования к локальному секретному коду для приложения в консоли Workspace ONE UEM. Перейдите в раздел «Группы и настройки» > «Все настройки» > «Приложения» > «Параметры и политики» > «Политики безопасности» > «Тип проверки подлинности».

После настройки проверки подлинности с помощью секретного кода у пользователей появится запрос на задание секретного кода на уровне приложений, если не существует других приложений повышения производительности, или пользователей попросят ввести свой общий секретный код с остальными приложениями повышения производительности.

Если проверка подлинности с помощью секретного кода не настроена, для устройств с iOS потребуется секретный код устройства.

Добавление встроенных приложений

Встроенные приложения — это программы, которые разработаны для конкретного типа мобильных устройств. Пользователи могут просмотреть встроенные приложения для Workspace ONE UEM на странице «Каталог Workspace ONE». Например, если пользователь просматривает каталог с устройства iOS, отображаются только приложения iOS, на которые у него есть права.

Чтобы установить приложение на устройстве, на странице «Каталог» нажмите кнопку «Установить». После нажатия кнопки «Установить» отображается всплывающее окно, содержащее информацию о дальнейших действиях. Отображаемая информация зависит от типа приложения и платформы. Для приложений, на которых отображается значок блокировки, необходимо использовать устройство под управлением Workspace ONE UEM. Когда конечный пользователь пытается скачать приложение со значком блокировки, появляется следующее сообщение: `Installation of this app requires enablement of Workspace Services`.

Использование VMware Verify для проверки подлинности пользователей

Если служба VMware Verify включена в качестве второго способа двухфакторной проверки подлинности, пользователям, чтобы входить с устройства в Workspace ONE, нужно загрузить приложение VMware Verify из магазина приложений устройства.

При первом входе в приложение Workspace ONE появляется запрос на ввод имени пользователя и пароля. После проверки этих сведений пользователям будет предложено ввести номер телефона устройства для регистрации в службе VMware Verify.

Если щелкнуть **Регистрация**, номер телефона устройства регистрируется в службе VMware Verify. Если приложение VMware Verify не загружено, появляется запрос на его загрузку.

При установке приложения пользователю понадобится ввести номер телефона, введенный ранее, и выбрать способ уведомления для получения одноразового регистрационного кода. Регистрационный код вводится на странице закрепления регистрации.

После регистрации номера телефона устройства пользователи могут использовать одноразовый секретный код с ограниченным временем действия, отображаемый в приложении VMware Verify, для входа в Workspace ONE. Секретный код — это уникальный номер, который создается на устройстве и постоянно меняется.

Пользователи могут зарегистрировать несколько устройств. Секретный код VMware Verify автоматически синхронизируется со всеми зарегистрированными устройствами.

Отправка оповещений пользователям Workspace ONE

Администраторы могут уведомлять пользователей Workspace ONE о предстоящем простое системы, состоянии соответствия, а также требовать от них какие-либо действия или отправлять им оповещения. Уведомления отправляются через консоль Workspace ONE UEM.

Пользователи управляют способом получения уведомлений со своих устройств.

Работа с Workspace ONE на устройствах с Android

С помощью приложения Workspace ONE для Android можно активировать приложения перечисленных ниже типов.

- Веб-приложения
- Удаленные приложения, которые можно активировать в службе VMware Identity Manager. Например, виртуальные приложения Horizon, Citrix XenApp и ThinApp.
- Родные управляемые и неуправляемые приложения. Родные приложения — это приложения, разработанные для платформы Android. Бывают двух типов:
  - общедоступные (распространяются через магазин Google Play);
  - внутренние (распространяются в частном порядке через Workspace ONE UEM и недоступны в магазине Google Play).

  Веб-приложения открываются в браузере. Пользователи могут получить доступ к виртуальным приложениям с помощью VMware Horizon Client или Citrix Receiver.

Регистрация приложения Workspace ONE с устройств Android

Выполнив вход в приложение Workspace ONE с использованием действительного URL-адреса и учетных данных сервера, пользователи смогут получить доступ к единому каталогу Workspace ONE. В нем отображаются все назначенные им приложения.

Для доступа к приложениям пользователи должны зарегистрировать приложение Workspace ONE. После регистрации Workspace ONE пользователи могут использовать виртуальные и веб-приложения, активированные с помощью VMware Identity Manager, приложения Workspace ONE UEM для повышения эффективности работы и неуправляемые приложения SDK.

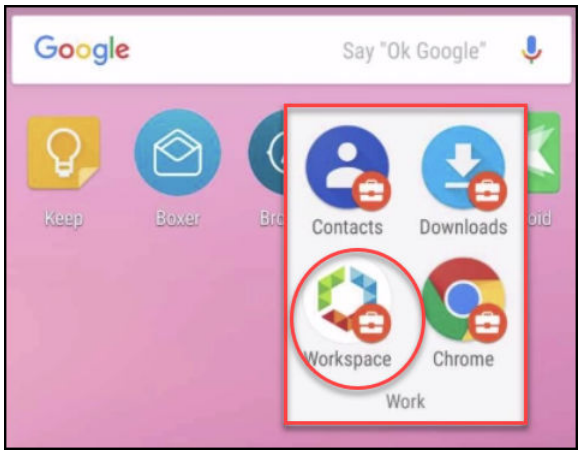
Примечание Приложения SDK находятся в контейнерах. Ими можно управлять с помощью SDK для Workspace ONE UEM даже на неуправляемых устройствах.

Пользователи могут включить адаптивное управление, благодаря которому на устройстве активируется Android for Work и обеспечивается улучшенное распространение приложений, а также поддержка профилей и политик.

Управление **Android for Work** с помощью **Workspace ONE**

При включении Android for Work на устройствах личные и рабочие данные разделяются на уровне операционной системы. Android for Work, в свою очередь, четко разграничивает рабочие и личные приложения. Android for Work создает приложения для работы, отмеченные соответствующим значком Android.

Рис. 8-6. Содержимое **Android for Work**



Прежде чем предоставлять доступ к приложению, администраторы определяют, какие из приложений в каталоге можно использовать только на управляемых устройствах. Если приложение в каталоге требует управления, рядом с кнопкой его загрузки отображается звездочка.

Если пользователь попытается загрузить такое приложение, отобразится сообщение о том, что приложение можно использовать только на управляемом устройстве. Появится экран с описанием возможностей и преимуществ управления устройством.

Рис. 8-7. Вводная страница **Workspace Services**

Когда пользователь согласится включить управление Android for Work, появятся пошаговые инструкции по его настройке. После настройки управления на устройстве создается контейнер Android for Work.

Использование каталога Workspace ONE

9

При интеграции Workspace ONE UEM с VMware Identity Manager каталог приложений Workspace ONE представляет собой репозиторий всех ресурсов, к которым можно предоставить доступ пользователям. Пользователи могут получить доступ к управляемым корпоративным приложениям в каталоге Workspace ONE в зависимости от настроенных параметров приложения.

Доступ к облачным и мобильным приложениям, а также к приложениям для Windows можно получить в каталоге. Конечным пользователям портала Workspace ONE можно предоставить доступ к разработанным своими силами встроенным приложениям или общедоступным приложениям из магазинов приложений.

На страницах каталога в Workspace ONE можно сделать следующее:

- Добавить новые ресурсы в свой каталог.
- Просмотреть ресурсы, к которым в данный момент можно предоставить право доступа пользователям.
- Получить доступ к сведениям о каждом ресурсе в каталоге.

Некоторые веб-приложения можно добавить в каталог напрямую на страницах каталога. Другие типы ресурсов требуют выполнения действий за пределами консоли администрирования. Сведения о настройке ресурсов см. в руководстве по настройке ресурсов VMware Identity Manager.

Управление ресурсами в каталоге

Чтобы предоставить пользователям право на конкретный ресурс, этот ресурс необходимо добавить в каталог. Используемый для этого метод зависит от типа ресурса.

Чтобы распространять ресурсы среди пользователей, предоставляя им соответствующие права, необходимо определить такие ресурсы в каталоге. Это могут быть веб-приложения, приложения для Windows, сохраненные в качестве пакетов VMware ThinApp, пулы виртуальных компьютеров Horizon Client, виртуальные приложения Horizon и приложения Citrix.

Чтобы интегрировать и активировать пулы виртуальных компьютеров и приложений Horizon Client, опубликованные ресурсы Citrix или пакетные приложения ThinApp, воспользуйтесь функцией коллекции виртуальных приложений в раскрывающемся меню на вкладке «Каталог».

Дополнительные сведения, требования, инструкции по установке и настройке этих ресурсов см. в документе *Настройка ресурсов в VMware Identity Manager*.

Добавление веб-приложения в каталог организации

Можно добавить веб-приложения в каталог, выбрав их из каталога облачных приложений или создав новые.

В каталоге облачных приложений содержатся часто используемые корпоративные веб-приложения. Эти приложения частично настроены, и пользователю необходимо предоставить недостающие сведения, чтобы заполнить запись приложения. Кроме того, чтобы выполнить другие обязательные действия по настройке веб-приложения, возможно, потребуется связаться с представителями VMware по работе с заказчиками.

Чтобы включить единый вход с помощью Workspace ONE для веб-приложения, во многих приложениях из каталога облачных приложений используется SAML 2.0 или 1.1 для обмена данными проверки подлинности и авторизации.

При создании приложения необходимо ввести все сведения о его конфигурации. Конфигурация зависит от типа добавляемого приложения. Для приложений, в которых не используется протокол федерации, требуется указать только целевой URL-адрес.

Приложения сторонних поставщиков удостоверений, настроенные в качестве источников приложений в VMware Identity Manager, добавляются в качестве новых приложений.

При добавлении приложения можно также выбрать политику доступа для управления доступом пользователей к приложению. Можно использовать политику доступа по умолчанию, а также можно создавать новые политики на странице «Управление учетными данными и доступом» > «Управление» > «Политики». Дополнительные сведения о политиках доступа см. в разделе *Администрирование VMware Identity Manager*.

Группировка ресурсов в категории

Ресурсы можно сгруппировать в логические категории, чтобы пользователям было удобнее искать необходимые ресурсы на портале Workspace ONE.

При создании категорий учитывайте структуру организации, функциональные обязанности ресурсов и тип последних. Ресурсу можно назначить несколько категорий. Например, можно создать категорию под названием «Продавец-консультант» и другую категорию под названием «Торговые ресурсы для персонала». Назначьте категорию «Продавец-консультант» всем ресурсам, связанным с продажами, в каталоге. Кроме того, назначьте категорию «Торговые ресурсы для персонала» определенным ресурсам, связанным с продажами, к которым предоставляется доступ только продавцам-консультантам.

После создания категории можно применить ее к любому из ресурсов в каталоге. Можно также применить несколько категорий к этому ресурсу.

При входе на портал Workspace ONE пользователи видят разрешенные для просмотра категории.

См. раздел «Управление каталогом» в руководстве по администрированию VMware Identity Manager.

Настройки корпоративного стиля для служб VMware Identity Manager

10

При необходимости можно настроить логотипы, шрифты и фон, которые отображаются в консоли VMware Identity Manager, на экранах входа в систему для пользователей и администратора, а также в веб-интерфейсе портала приложений Workspace ONE и самого приложения Workspace ONE на мобильных устройствах.

Чтобы в оформлении использовалась цветовая грамма, логотипы и корпоративный стиль компании, можно воспользоваться средством настройки.

В эту главу входят следующие разделы:

Настройка корпоративного стиля в службе VMware Identity Manager

Для консоли администрирования и пользовательского портала можно добавить в адресную строку название компании, название продукта и значок веб-сайта. Кроме того, можно настроить страницу входа таким образом, чтобы цвет фона соответствовал цветам и дизайну эмблемы вашей компании.

Процедура

1. В консоли VMware Identity Manager на вкладке «Управление учетными данными и доступом» выберите **Настройка > Пользовательский корпоративный стиль**.
2. Измените следующие параметры в форме так, как это необходимо.

Поле формы	Описание
	Вкладка «Названия и логотипы»
Название компании	Название компании применяется как для настольных компьютеров, так и для мобильных устройств. Название компании можно добавить в качестве заголовка, который будет отображаться на вкладке браузера. Чтобы изменить название, введите название компании вместо текущего.
Название продукта	Название продукта применяется как для настольных компьютеров, так и для мобильных устройств. Название продукта отображается на вкладке браузера после названия компании.

Поле формы	Описание
Значок веб-сайта	Значок веб-сайта — это связанный с URL-адресом значок, который отображается в адресной строке браузера. Максимальный размер значка веб-сайта — 16 x 16 пикселей. Поддерживаются форматы JPEG, PNG и GIF и ICO. Щелкните **Загрузить на сервер**, чтобы загрузить новое изображение вместо текущего значка веб-сайта. Отобразится запрос на подтверждение изменения. Изменение произойдет немедленно.
	Вкладка «Экран входа»
Логотип	Щелкните **Загрузить на сервер**, чтобы загрузить новый логотип и заменить текущий на экранах входа. При нажатии кнопки **Подтвердить** изменения применяются незамедлительно. Минимальный рекомендуемый размер передаваемого изображения — 350 x 100 пикселей. Если передать изображения, размер которых превышает 350 x 100 пикселей, они масштабируются до этого размера. Поддерживаются форматы JPEG, PNG и GIF.
Фоновый цвет	Это цвет фона экрана входа. Чтобы его изменить, перезапишите шестизначный шестнадцатеричный код цвета новым значением.
Цвет фона поля	Цвет рамки экрана входа можно настроить. Перезапишите шестизначный шестнадцатеричный код цвета новым.
Цвет фона кнопки входа	Цвет кнопки входа в систему можно настроить. Перезапишите шестизначный шестнадцатеричный код цвета новым.
Цвет шрифта кнопки входа	Цвет текста, который отображается на кнопке входа в систему, можно настроить. Перезапишите шестизначный шестнадцатеричный код цвета новым.

При настройке экрана входа в систему перед сохранением изменений можно просмотреть их в области предварительного просмотра.

3. Нажмите кнопку **Сохранить**.

Обновления фирменной символики организации в консоли VMware Identity Manager и на страницах входа применяются в течение пяти минут после нажатия кнопки «Сохранить».

Следующие шаги

Проверьте изменения корпоративного стиля в различных интерфейсах.

Обновите внешний вид портала Workspace ONE и интерфейса для мобильных устройств и планшетов. См. Настройка корпоративного стиля для пользовательского портала.

Настройка корпоративного стиля для пользовательского портала

Вы можете добавить эмблему, изменить цвет фона, а также добавить изображения для настройки портала Workspace ONE.

Процедура

1. На вкладке «Каталоги» в консоли VMware Identity Manager выберите **Параметры > Фирменная символика пользовательского портала**.
2. Измените параметры в форме так, как это необходимо.

Элемент формы	Описание
Логотип	Добавьте основной логотип, который будет использоваться в качестве баннера в верхней части консоли VMware Identity Manager и на веб-страницах портала Workspace ONE. Максимальный размер изображения — 220 x 40 пикселей. Поддерживаются форматы JPEG, PNG и GIF.
	Портал
Основной цвет фона	Чтобы его изменить, перезапишите шестизначный шестнадцатеричный код основного цвета фона новым значением. При вводе нового кода цвет фона будет автоматически меняться на экране предварительного просмотра портала приложений.
Основной цвет текста	Чтобы его изменить, перезапишите шестизначный шестнадцатеричный код цвета текста, который отображается в основной области, новым значением.
Фоновый цвет	Это цвет фона экрана веб-портала. Чтобы его изменить, перезапишите шестизначный шестнадцатеричный код цвета новым значением. При вводе нового кода цвет фона будет автоматически меняться на экране предварительного просмотра портала приложений. Выберите **Выделение фона цветом**, чтобы подчеркнуть цвет фона. Если параметр «Световой эффект фона» включен, а браузер поддерживает несколько фоновых изображений, в средстве запуска и на страницах каталога фоновые изображения накладываются друг на друга. Выберите **Фоновый рисунок**, чтобы использовать в качестве фона стандартный узор в виде треугольников соответствующего цвета.
Цвет фона значка	Введите шестизначный шестнадцатеричный цветовой код для изменения цвета фона, окружающего значки приложений.
Прозрачность фона значка	Для того чтобы настроить прозрачность, переместите ползунок.
Имя и цвет значка	При необходимости можно выбрать цвет текста для имен, которые отображаются под значками на страницах портала приложений. Чтобы изменить цвет шрифта, перезапишите шестнадцатеричный код цвета новым значением.
Эффект надписи	Выберите тип эффекта, который будет использоваться для текста на экранах портала Workspace ONE.
Выделение фона цветом	Если функция включена, в браузерах с поддержкой нескольких фоновых изображений наложение фона отображается на страницах закладок и каталога.
Фоновый рисунок	Если функция включена, в браузерах с поддержкой нескольких фоновых изображений наложения фона отображаются на страницах закладок и каталога.
Изображение (необязательно)	Чтобы вместо цветной заливки использовать на экране портала приложений фоновое изображение, загрузите это изображение.

3. Нажмите кнопку **Сохранить**.

Обновление пользовательского корпоративного стиля на пользовательском портале выполняется каждые 24 часа. Чтобы изменения отобразились раньше, администратор может открыть новую вкладку и ввести этот URL-адрес, подставив свое доменное имя вместо myco.example.com: `https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true`.

Следующие шаги

Просмотрите изменения корпоративного стиля в различных интерфейсах.

Доступ к другим документам

11

Во время настройки Workspace ONE может понадобиться справочная документация по VMware Identity Manager и VMware Workspace ONE UEM.

Дополнительную документацию можно найти в следующих центрах документации

- VMware Workspace ONE
- VMware Workspace ONE UEM
- VMware Identity Manager