ESET SECURE AUTHENTICATION

Руководство пользователя

(предназначено для версии продукта 2.6)

ENJOY SAFER TECHNOLOGY™

ESET SECURE AUTHENTICATION

Служба поддержки клиентов: www.eset.com/support

Версия от 04.04.2017

Содержание

1. Обзор

ESET Secure Authentication (ESA) добавляет двухфакторную аутентификацию (Two Factor Authentication (2FA)) в доменах Microsoft Active Directory, то есть создается либо одноразовый пароль (OTP), который нужно указать вместе с обычным именем пользователя и паролем, либо push-уведомление, которое пользователь должен подтвердить на своем мобильном телефоне под управлением ОС Android после успешной аутентификации с помощью обычных учетных данных для доступа.

Для работы push-уведомлений требуется ОС Android 2.3 или более поздней версии, а также службы Google Play.

Продукт ESA состоит из следующих компонентов.

- Подключаемый модуль ESA Web Application обеспечивает двухфакторную аутентификацию (2FA) в различных веб-приложениях Microsoft (Microsoft Web Applications).
- Подключаемый модуль ESA Remote Desktop обеспечивает двухфакторную аутентификацию (2FA) для протокола удаленного рабочего стола (Remote Desktop Protocol).
- Сервер ESA RADIUS Server добавляет двухфакторную аутентификацию (2FA) в аутентификацию VPN.
- Служба ESA Authentication Service включает в себя интерфейс API, который основан на архитектуре REST и с помощью которого можно добавлять двухфакторную аутентификацию (2FA) в пользовательские приложения.
- ESA Management Tools:
  - Подключаемый модуль управления пользователями ESA User Management для средства Active Directory Users and Computers (ADUC) (Пользователи и компьютеры Active Directory) используется для управления пользователями.
  - Консоль управления ESA (ESA Management Console), которая называется ESET Secure Authentication Settings, используется для настройки ESA.

Для ESA требуется инфраструктура Active Directory, поскольку это решение хранит данные в хранилище данных Active Directory. Это означает, что дополнительные политики резервного копирования не требуются, так как данные ESA автоматически добавляются в резервные копии Active Directory.

2. Требования

Для установки ESET Secure Authentication требуется домен Active Directory. Минимальный поддерживаемый функциональный уровень домена Active Directory — это Windows 2000 Native. Поддерживается только Windows DNS.

Программа установки всегда автоматически выбирает компоненты Authentication Service (Служба аутентификации) и Management Tools (Средства управления). Если пользователь выбирает компонент, который нельзя установить, установщик сообщает о конкретных обязательных условиях, которые не выполнены.

2.1 Поддерживаемые операционные системы

Компоненты ESET Secure Authentication Services и Management Tools проверены и поддерживаются в следующих операционных системах.

Серверные операционные системы (SOS)

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Small Business Server 2008
- Windows Small Business Server 2011
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials
- Windows Server 2016
- Windows Server 2016 Essentials

Клиентские операционные системы (COS)

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10 (в том числе юбилейное обновление)

Компонент Management Tools (Средства управления) поддерживается также в клиентских операционных системах (начиная с Windows 7).

ПРИМЕЧАНИЕ.: После установки RADIUS Server в Windows Small Business Server 2008 или 2011 номер порта NPS по умолчанию необходимо изменить с 1812 на 1645. Перед установкой ESA убедитесь, что на порту 1812 нет никаких прослушивающих процессов. Для этого выполните следующую команду: *C:\> netstat -a -p udp | more*

2.2 Поддерживаемые веб-приложения

Решение ESET Secure Authentication добавляет 2FA в следующие продукты Microsoft:

- Microsoft Exchange 2007
  - Outlook Web Access - Exchange Client Access Server (CAS)
- Microsoft Exchange 2010
  - Outlook Web App - Exchange Mailbox Server Role (MBX)
  - Панель управления Exchange
- Microsoft Exchange 2013
  - Outlook Web App - Exchange Mailbox Server Role (MBX)
  - Центр администрирования Exchange
- Microsoft Exchange 2016
  - Outlook Web App - Exchange Mailbox Server Role (MBX)
  - Центр администрирования Exchange
- Microsoft Dynamics CRM 2011
- Microsoft Dynamics CRM 2013
- Microsoft Dynamics CRM 2015
- Microsoft Dynamics CRM 2016
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016
- Microsoft SharePoint Foundation 2010
- Microsoft SharePoint Foundation 2013
- Веб-доступ к удаленному рабочему столу Microsoft
- Веб-доступ к службам терминалов Microsoft
- Удаленный веб-доступ Microsoft

2.3 Поддерживаемые операционные системы мобильных телефонов

Приложение ESET Secure Authentication Mobile совместимо со следующими мобильными операционными системами:

- с iPhone iOS 6 по iOS 10;
- с Android™ 2.3 по Android 7.0 (Android N);
- с Windows Phone 7 по Windows 10 Mobile;
- Windows Mobile 6
- с BlackBerry® 4.3 по 7.1;
- BlackBerry® 10
- Symbian®: все версии, поддерживающие J2ME;
- все телефоны с поддержкой J2ME.

2.4 Требования для установки

Для безопасной установки требуется исходящее подключение к esa.eset.com на TCP-порте 443. Программу установки должен запустить участник группы безопасности Domain Administrators (Администраторы домена). Также требуется наличие установленного пакета .NET Framework Version 4 (Full Install). Если пакет .NET 4 не установлен, установщик автоматически попытается его установить.

ESA поддерживает установку компонентов в распределенной среде, когда все компоненты устанавливаются на компьютеры, объединенные в один домен Windows.

Исключения файервола Windows, от которых зависит нормальная работа решения ESET Secure Authentication, добавляются автоматически в рамках установки. Если вы используете другой файервол, сведения о важных исключениях, которые нужно будет создать, см. в разделе Исключения файервола.

Ниже приведены обязательные условия для установки каждого компонента.

- Authentication Service:
  - Windows 2003 Server SP2 или более поздняя версия операционной системы сервера из списка поддерживаемых операционных систем.
  - Когда Authentication Service впервые устанавливается в домене, установщик должен быть запущен от имени пользователя, который принадлежит к группе безопасности «Schema Admins».
- Management Tools:
  - Windows7 или более поздняя версия операционной системы клиента из списка поддерживаемых операционных систем, Windows 2003 Server SP2 или более поздняя версия операционной системы сервера из списка поддерживаемых операционных систем
  - .NET Framework версии 3.5.
  - Windows Remote Server Administration Tools, компонент Active Directory Domain Services (RSAT AD DS).
  - **ПРИМЕЧАНИЕ.** Компонент RSAT раньше назывался так: Remote Administration Pack (adminpack). Его можно загрузить с сайта Microsoft. В Windows Server 2008 и более новых версиях этот компонент можно установить с помощью мастера добавления компонентов (Add Feature) в диспетчере серверов (Server Manager). Во всех контроллерах доменов эти компоненты уже установлены.
- RADIUS Server:
  - Windows 2003 Server SP2 или более поздняя версия операционной системы сервера из списка поддерживаемых операционных систем.
- Подключаемый модуль Web App для Microsoft Exchange Server.
  - Microsoft Exchange Server 2007 или более новая версия (только 64-разрядные варианты) с установленной ролью «Client Access» (Outlook Web App / Outlook Web Access).
  - .NET Framework версии 3.5.
  - Internet Information Services 7 (IIS7) или более поздняя версия.
- Подключаемый модуль Web App для Microsoft SharePoint Server.
  - Microsoft SharePoint Server 2010 или 2013 (только 64-bit версии).
  - .NET Framework версии 3.5.
- Подключаемый модуль Web App для Microsoft Dynamics CRM.
  - Microsoft Dynamics CRM 2011, 2013 или 2015.
  - .NET Framework версии 3.5.
- Подключаемый модуль Web App для Microsoft Terminal Services Web Access.
  - Роль служб терминалов (Terminal Services) с установленной службой роли Terminal Services в ОС Windows Server 2008.
  - .NET Framework версии 3.5.
- Подключаемый модуль Web App для Microsoft Remote Desktop Services Web Access.

- Роль служб удаленных рабочих столов (Remote Desktop Services) с установленной службой роли Remote Desktop Web Access в ОС Windows Server 2008 R2 или в более поздней версии операционной системы сервера из списка поддерживаемых операционных систем
- .NET Framework версии 3.5.

- Подключаемый модуль Web App для Microsoft Remote Web Access.
  - Служба роли Remote Web Access (Удаленный веб-доступ), установленная в ОС Windows SBS 2008 , где она называется Remote Web Access, Windows SBS 2011, Windows Server 2012 Essentials и Windows Server 2012 Essentials R2
  - .NET Framework версии 3.5.
- Remote Desktop Protection:
  - Windows Server 2008 R2 или более поздняя версия операционной системы сервера из списка поддерживаемых операционных систем.
  - Microsoft Windows 7 или более поздняя версия операционной системы клиента из списка поддерживаемых операционных систем.
  - Поддерживаются только 64-разрядные операционные системы.
- Windows login protection:
  - Windows Server 2008 R2 или более поздняя версия операционной системы сервера из списка поддерживаемых операционных систем.
  - Windows 7 или более поздняя версия операционной системы клиента из списка поддерживаемых операционных систем.
- ADFS 3.0 protection:
  - Windows Server 2012 R2

Требования для .NET:

- Все компоненты: .NET 4 или 4.5 (Full Install).
- Core Server: .NET 4 или 4.5 (Full Install).
- RADIUS Server: .NET 4 или 4.5 (Full Install).
- Management Tools: .NET 3.5 (4 для Windows Server 2012).
- Подключаемый модуль Web App: .NET 3.5

ПРИМЕЧАНИЕ.: Компоненты Authentication Service (служба аутентификации) и RADIUS Server (сервер Radius) совместимы с Windows7 и более поздней версией операционной системы клиента из списка поддерживаемых операционных систем, но не будут поддерживаться в таких клиентских системах.

2.5 Поддерживаемые среды Active Directory

ESET Secure Authentication поддерживает среды Active Directory как с одним доменом, так и с несколькими. Разница между средами и требованиями к установке описана ниже.

Один домен, один лес

Эта самая простая конфигурация, поэтому программу установки можно запустить с правами любого администратора домена. Программа ESET Secure Authentication доступна всем пользователям в домене.

Несколько доменов, один лес

В этом развертывании родительский домен, например `example.corp`, имеет несколько поддоменов, например `branch1.example.corp` и `branch2.example.corp`. Решение ESET Secure Authentication можно развернуть в нескольких доменах леса, но между установками не будет взаимосвязи. Для каждой установки потребуется отдельная лицензия ESET Secure Authentication.

Чтобы установить ESET Secure Authentication в поддомене, программу установки нужно запустить в домене высшего уровня с правами администратора домена.

Рассмотрим пример с использованием приведенных выше доменов.

Чтобы установить ESET Secure Authentication в домене `server01.branch1.example.corp`, войдите на сервер `server01` с помощью имени пользователя `example.corp\Administrator` (или с помощью учетной записи одного из администраторов домена `example.corp`). После установки решение ESET Secure Authentication будет доступно любому пользователю в рамках домена `branch1.example.corp`.

Несколько доменов, несколько лесов

Как и в предыдущей среде, решения ESET Secure Authentication, установленные в разных лесах, не видят друг друга.

2.6 Исключения файервола

Исключения файервола Windows, от которых зависит нормальная работа решения ESET Secure Authentication, добавляются автоматически в рамках установки. Если используется другой файервол, в нем нужно вручную задать следующие исключения:

Имя исключения: ESET Secure Authentication Core Service

Область: все

Протокол: TCP

Локальный порт: 8000

Удаленные порты: все

Имя исключения: Интерфейс API для ESET Secure Authentication

Область: все

Протокол: TCP

Локальный порт: 8001

Удаленные порты: все

Имя исключения: служба ESET Secure Authentication RADIUS

Область: все

Протокол: UDP

Локальный порт: 1812

Удаленные порты: все

Имя исключения: служба ESET Secure Authentication RADIUS (альтернативный порт)

Область: все

Протокол: UDP

Локальный порт: 1645

Удаленные порты: все

2.7 Политики

В процессе установки решение ESA добавляет пользователя ESA_<имя_компьютера> в сущность Log on as a service (Вход в качестве службы), которая находится здесь: Local Security Policies > Local Policies > User Rights Assignments (Локальные политики безопасности > Локальные политики > Назначения прав пользователей). При этом переменная <имя_компьютера> заменяется именем компьютера, на который устанавливается решение ESA. Это необходимо для запуска службы ESET Secure Authentication Service, который происходит автоматически при запуске операционной системы.

Если вы используете групповую политику (Group Policy) с заданным параметром Log on as service (Group Policy Management > <Forest> > Domains > <domain> > Default Domain Policy > Settings > Computer Configuration > Policies > Windows Settins > Security Settings > Local Policies), следует добавить пользователя ESA_<имя_компьютера> в сущность Log on as a service или вообще не задавать параметр Log on as a service.

Чтобы узнать имя компьютера, на который устанавливается решение ESA, выполните следующие действия:

- нажмите одновременно клавиши **Windows** и **E**, чтобы открыть окно **проводника**;
- в области справа щелкните правой кнопкой мыши **Этот компьютер** или **Компьютер** и выберите пункт **Свойства**.

В новом окне отобразится **имя компьютера**.

3. Установка

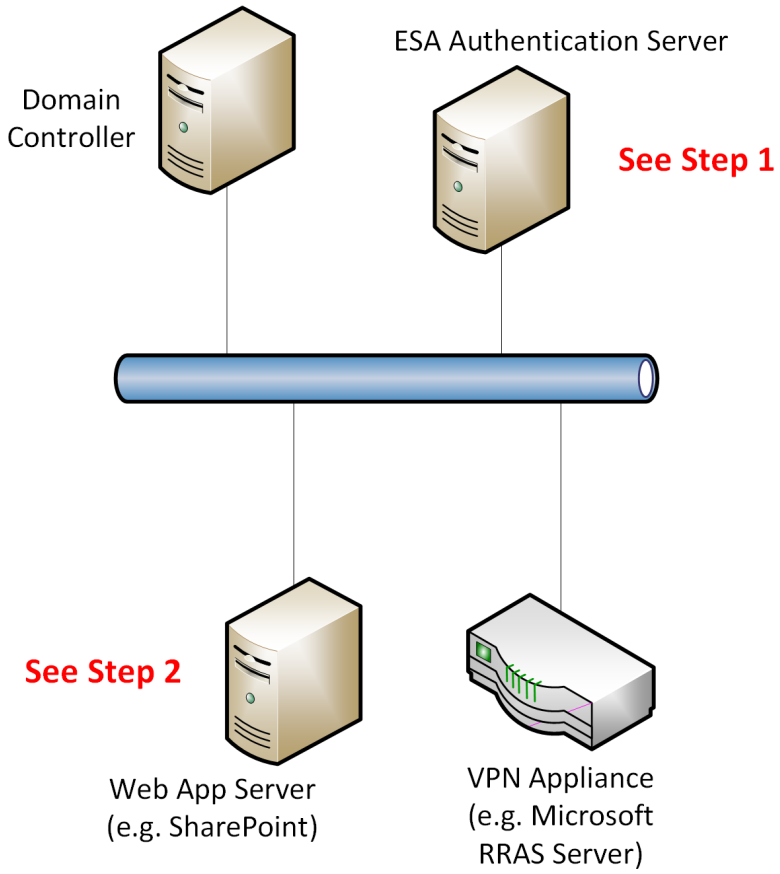
Ниже перечислены компоненты, которые обязательны для первой установки ESA.

- Как минимум один экземпляр Authentication Server.
- Как минимум один экземпляр средств управления (Management Tools).
- Как минимум одна конечная точка аутентификации (API, Web Application, Remote Desktop, или RADIUS).

Все эти компоненты могут быть установлены на одном компьютере либо на нескольких компьютерах в распределенной среде. В случае с распределенными системами существует множество сценариев установки.

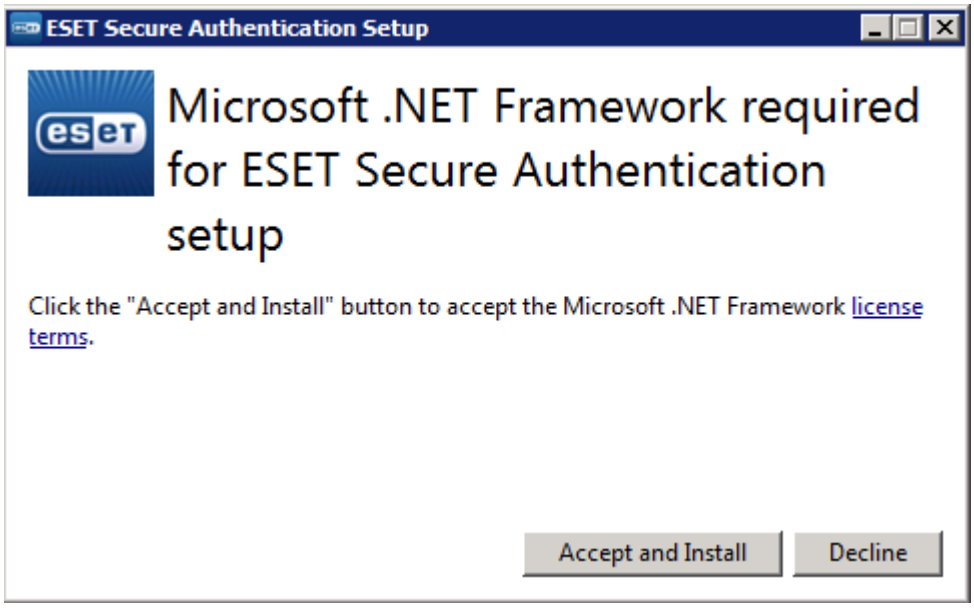
Нет необходимости устанавливать основные компоненты ESA (Authentication Server, Management Tools) непосредственно на контроллере домена, их можно установить на любом другом компьютере в сети Active Directory.

Пример ниже представляет собой стандартный сценарий установки, на который можно в основном ориентироваться при работе с другими сценариями развертывания. Пример установки состоит из двух последовательностей. После выполнения обеих ваше развертывание будет соответствовать приведенному ниже рисунку.

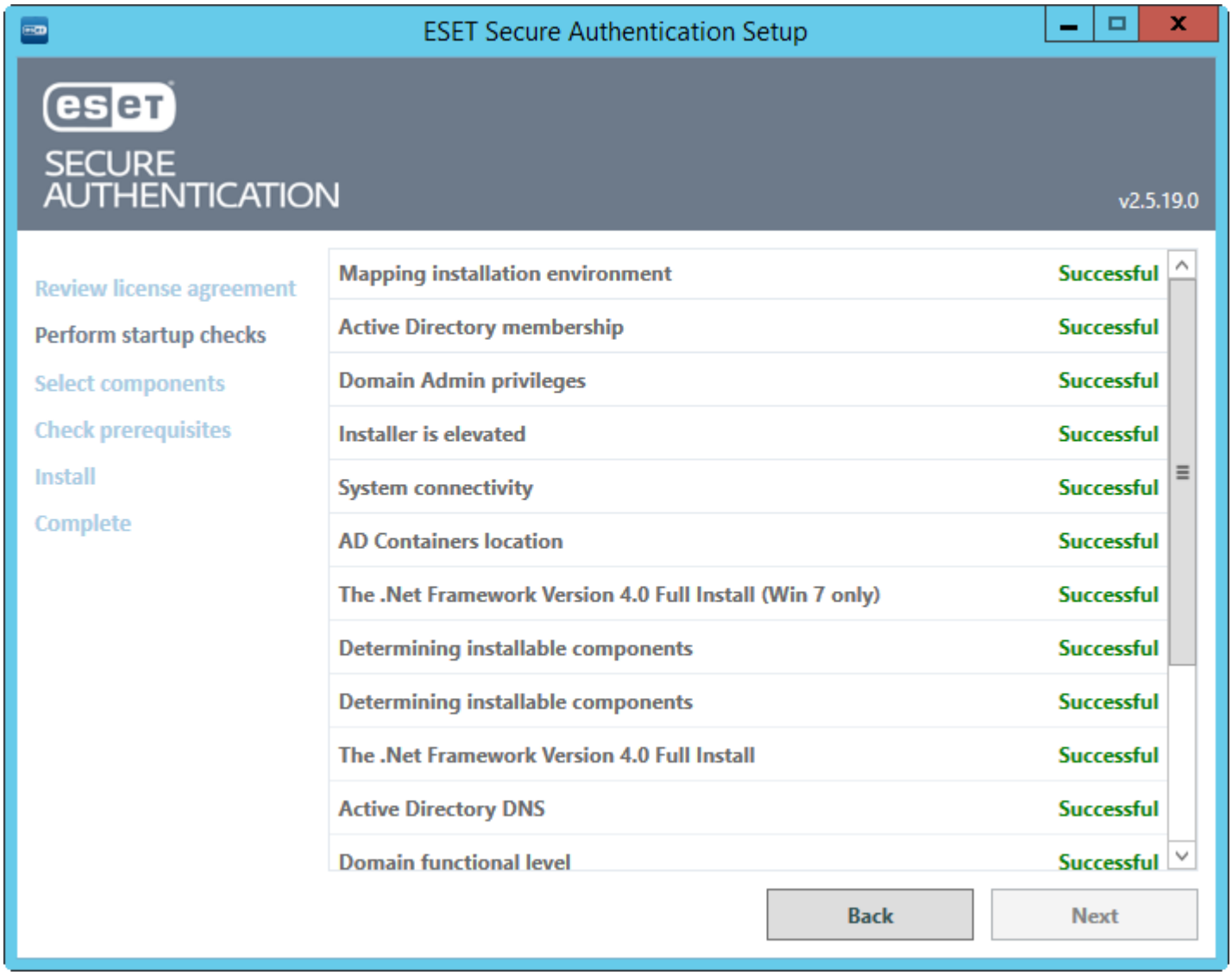


3.1 Установка компонентов Core

Запустите полученный файл с расширением *.exe*, чтобы начать установку основных компонентов на компьютере, на котором будет размещена служба ESA Authentication Service. Если платформа NET Framework версии 4.0 не будет обнаружена, она будет установлена автоматически.

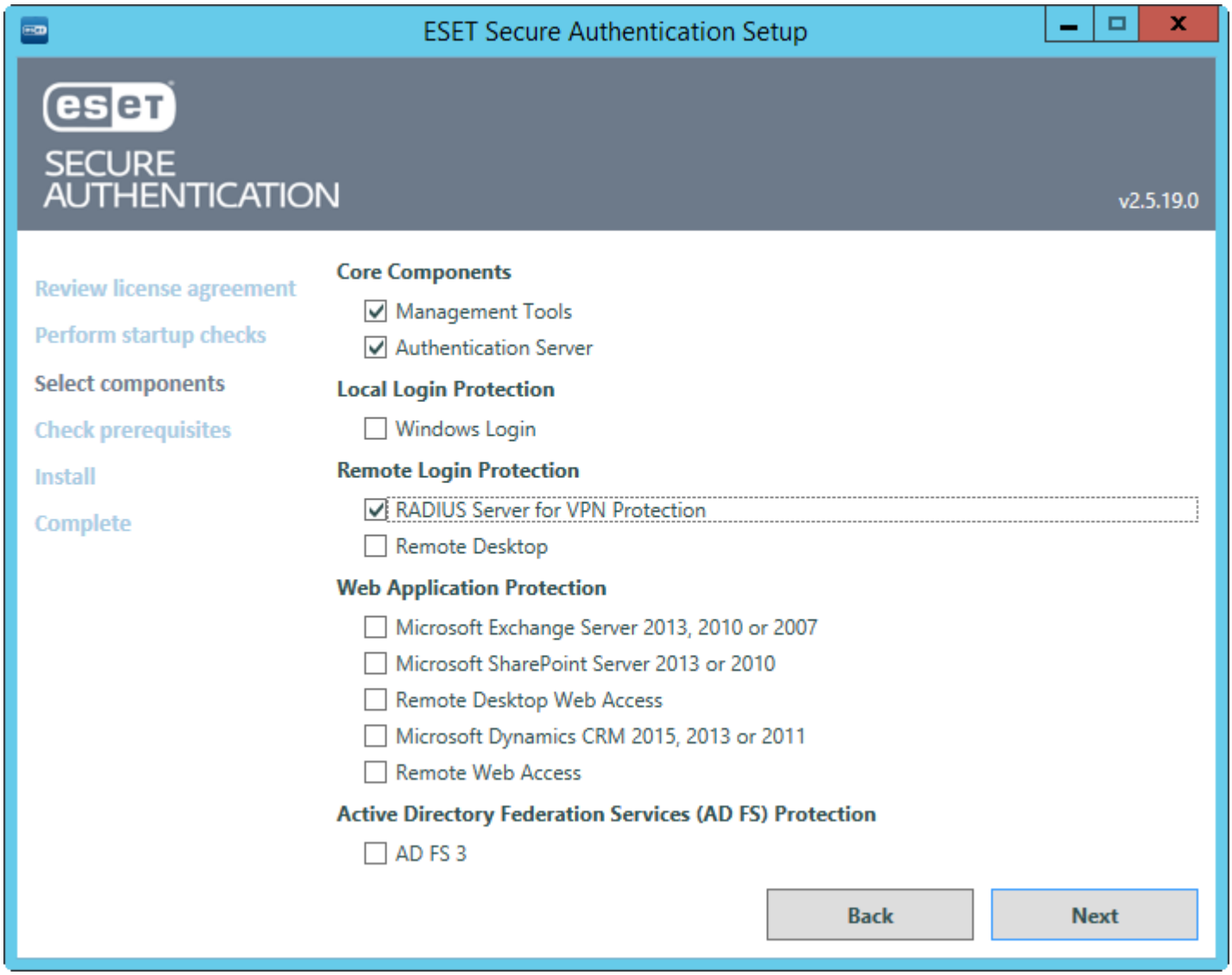


Чтобы убедиться в работоспособности домена и в том, что установка ESA возможна, будет выполнено несколько предварительных проверок. Для продолжения установки все ошибки должны быть исправлены. После успешного выполнения всех необходимых условий установка продолжится.



Если кнопка **Next** (Далее) не станет активной через 5 секунд, прокрутите окно вниз, чтобы просмотреть, какие требования остались невыполненными.

При появлении запроса выберите компоненты **Management Tools** (Средства управления), **Authentication Server** (Сервер аутентификации) и **RADIUS Server for VPN Protection** (Сервер RADIUS для защиты VPN) (см. рисунок ниже).



Если порт 1812 уже используется в вашей сети, выберите другой порт для сервера RADIUS. Если вы предпочитаете использовать прозрачный прокси-сервер, выберите **Use proxy** (Использовать прокси-сервер) и введите соответствующие значения. Нажмите кнопку **Next** (Далее).

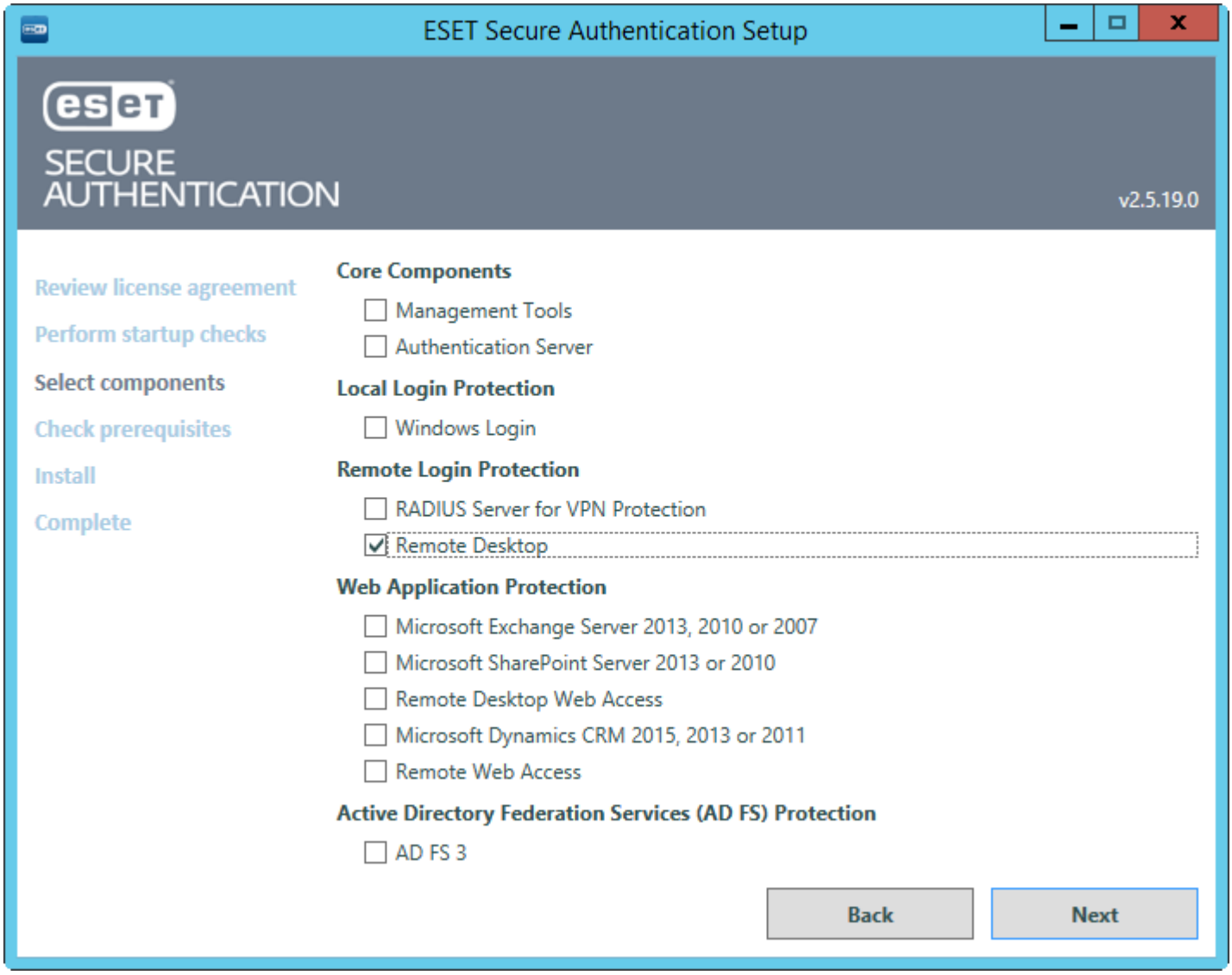
В следующем окне **Check prerequisites** (Проверка обязательных условий) будет отображена информация о том, используется выбранный порт или нет.

Выполните остальные шаги, следуя подсказкам установщика, и закройте его, когда установка будет завершена.

3.2 Установка подключаемого модуля удаленного рабочего стола

На компьютере, к которому вы подключились через Remote Desktop Access и который должен быть защищен, запустите полученный exe-файл, чтобы начать установку. Установщик выполнит несколько предварительных проверок, как во время установки компонентов Core.

На рисунке ниже показан экран выбора компонентов для установки подключаемого модуля Remote Desktop.

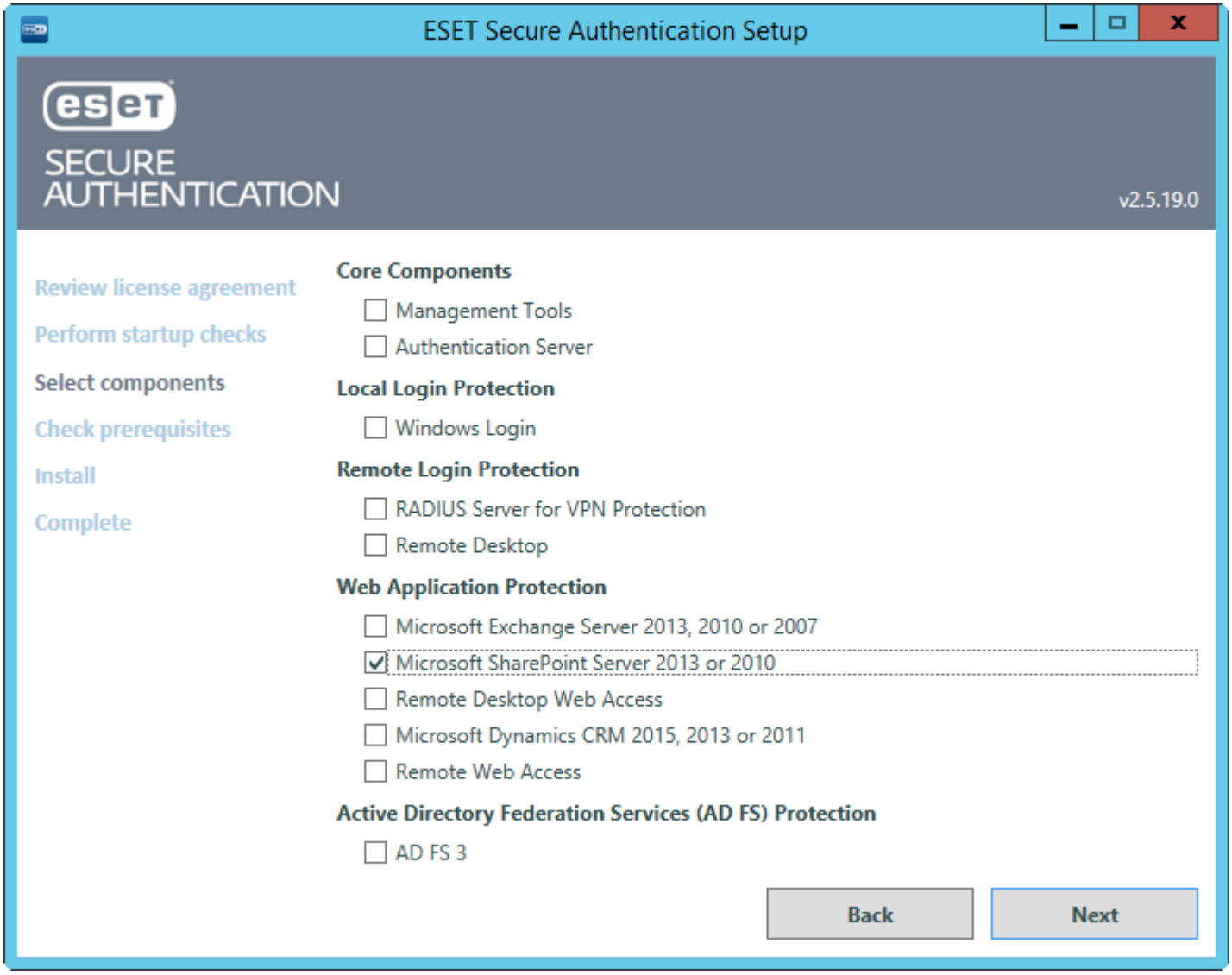


Для проверки возможности установки подключаемого модуля ESA Remote Desktop будут выполнены необходимые проверки. Для продолжения установки все ошибки должны быть исправлены. Выполните остальные шаги, следуя подсказкам установщика, и закройте его, когда установка будет завершена.

3.3 Установка подключаемого модуля веб-приложений

На компьютере, на котором открыто Web App, которое нужно защитить, запустите полученный *.exe*-файл, чтобы начать установку. Установщик выполнит несколько предварительных проверок, как во время установки компонентов Core.

Когда появится запрос, выберите компонент для соответствующего Web App. На рисунке ниже показан экран выбора компонентов для установки подключаемого модуля SharePoint Server.



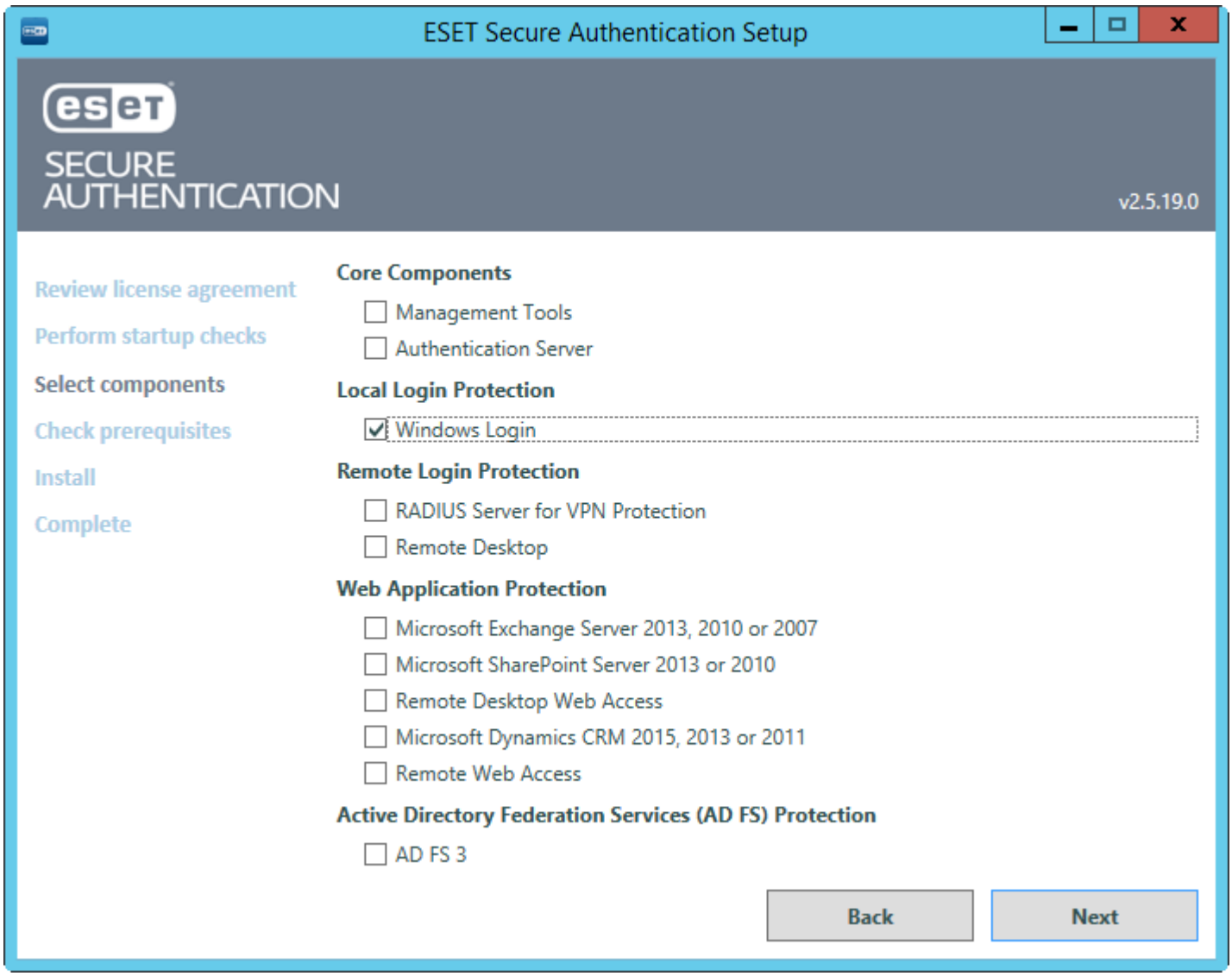
Программа проверит возможность установки подключаемого модуля ESA Web App, а также, запущено ли на сервере Web App. Для продолжения установки все ошибки должны быть исправлены.

Выполните остальные шаги, следуя подсказкам установщика, и закройте его, когда установка будет завершена.

ПРИМЕЧАНИЕ. Если вы используете установочный файл с расширением MSI для установки защиты 2FA для Microsoft SharePoint Server, веб-доступа к удаленному рабочему столу или Microsoft Dynamics CRM, запустите установщик с повышенными правами.

3.4 Установка подключаемого модуля входа в Windows

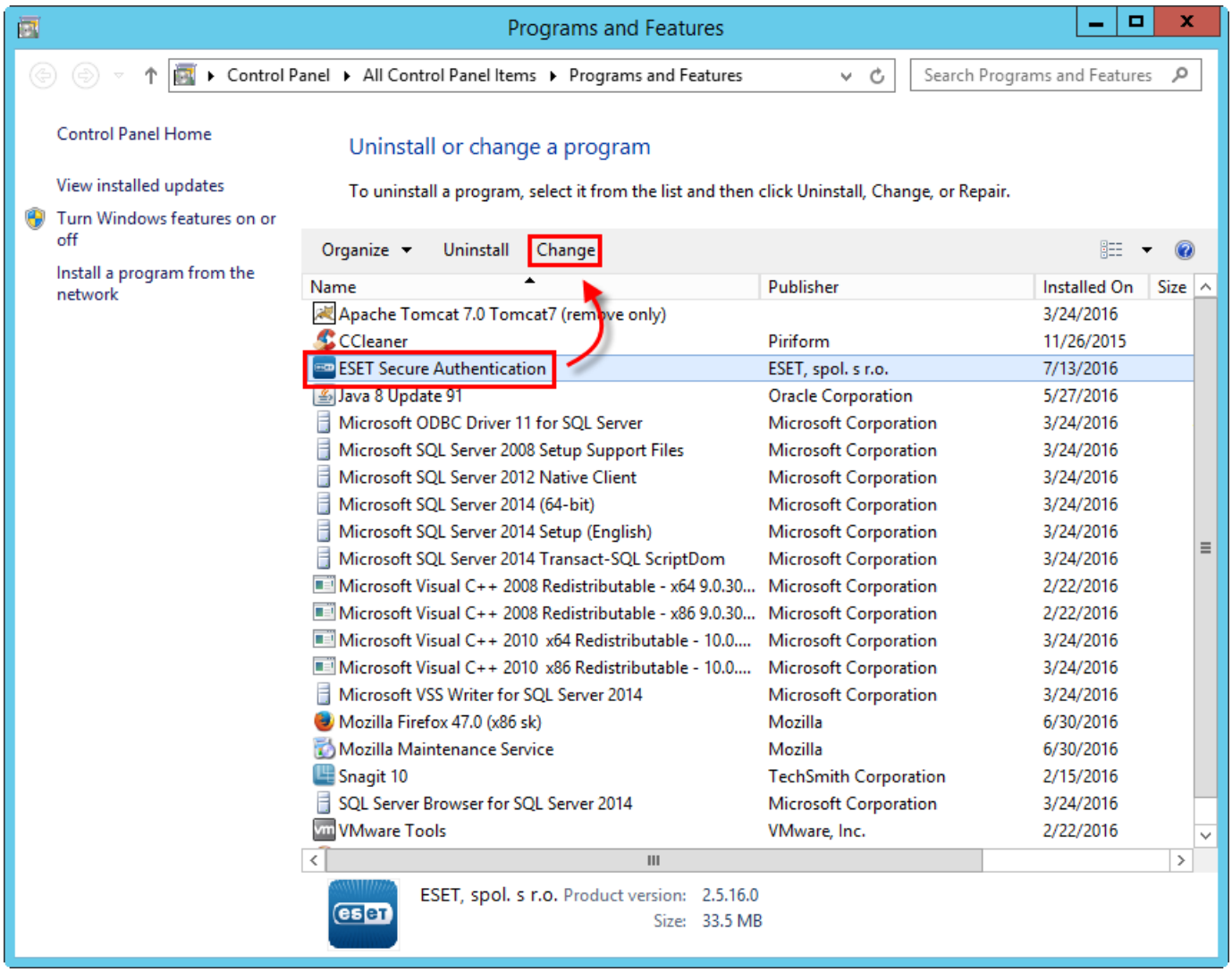
При установке ESA на компьютер под управлением Windows, который необходимо защитить с помощью двухфакторной аутентификации (2FA), убедитесь, что выбран компонент **Windows Login** (Вход в Windows) на странице **Select components** (Выбор компонентов) мастера установки.



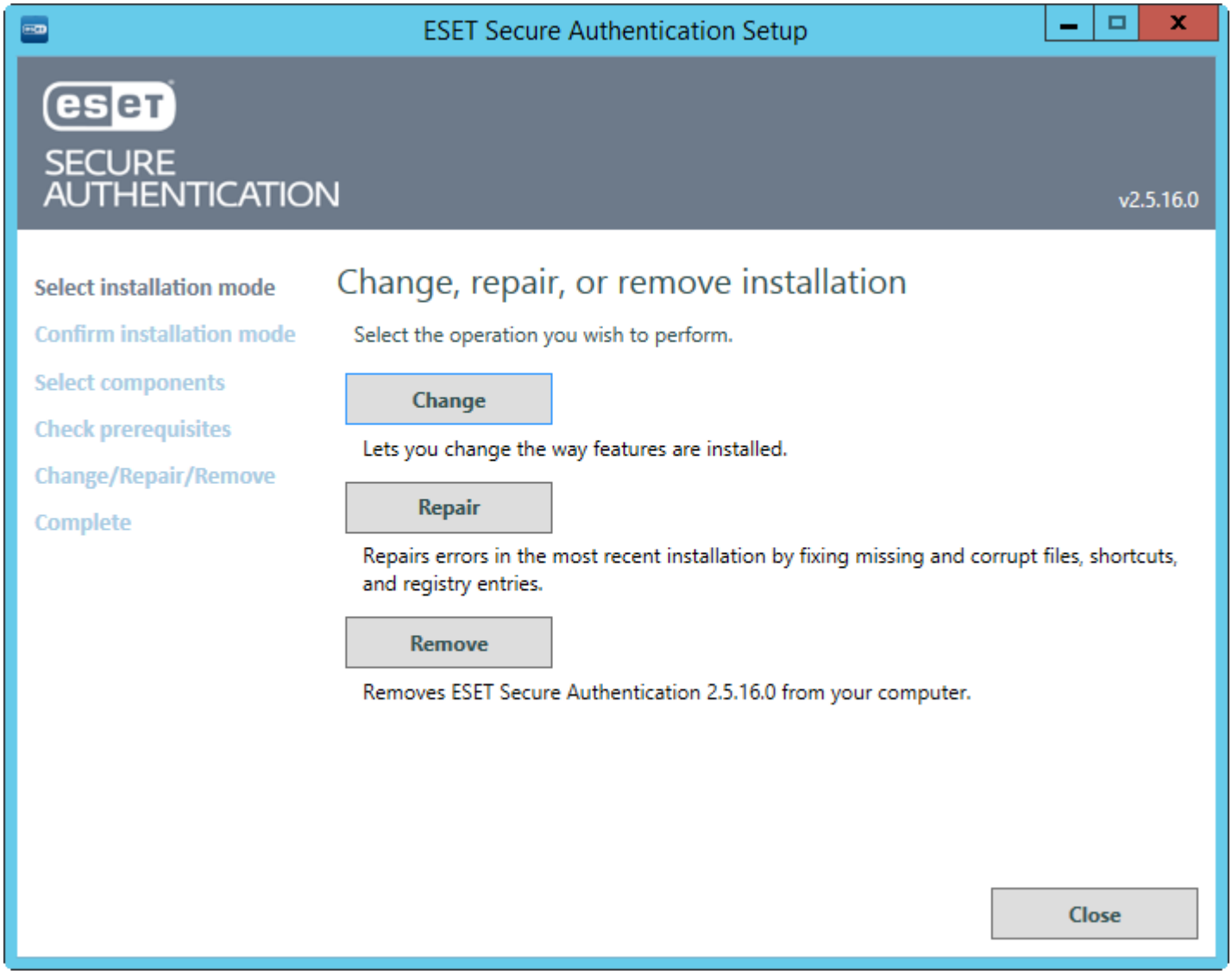
ПРИМЕЧАНИЕ.: Не требуется устанавливать компонент **Management Tools** (Средства управления) на каждый компьютер, который вы хотите защитить с помощью двухфакторной аутентификации (2FA) (этот компонент требуется только на основном сервере ESA). Защита **Windows Login** (Вход в Windows) работает только в среде домена, а это означает, что конкретный компьютер и учетная запись пользователя должны относиться к домену, основанному доменными службами Active Directory Domain Services.

3.5 Изменение, восстановление или удаление установки

Чтобы добавить или удалить компоненты решения ESA, удалить либо восстановить приложение, следует повторно запустить установщик. Кроме того, можно открыть окно **Programs and Features** (Программы и компоненты) в ОС Windows, выбрать ESET Secure Authentication и нажать кнопку **Change** (Изменить).



На экране **ESET Secure Authentication Setup** нажмите кнопку **Change** (Изменить), чтобы выбрать с помощью флажков новые компоненты, которые нужно установить, либо снять флажки для существующих компонентов, которые следует удалить.



Выполните остальные шаги, следуя подсказкам установщика, и закройте его, когда установка будет завершена.

При удалении ядра ESA в окне **Additional configuration** (Дополнительная настройка) можно выбрать параметр удаления всех данных и настроек приложения ESET Secure Authentication. Этот параметр недоступен, если ядро ESA core не является последним в конкретном домене Active Directory, который вы собираетесь удалить, или у вас нет прав администратора домена, в том числе прав на удаление.

Выберите параметр **Remove all program and user data including product configuration** (Удалить все данные программы и пользователя, в том числе конфигурацию продукта), если вы не желаете повторно устанавливать приложение ESET Secure Authentication на этом же компьютере или желаете использовать этот компьютер для другого домена Active Directory, в котором будет использоваться ESET Secure Authentication. Этот параметр доступен в виде строки **AUTHENTICATION_SERVER_CLEAN_DATA** при выполнении автоматического удаления с помощью MSI-пакета:

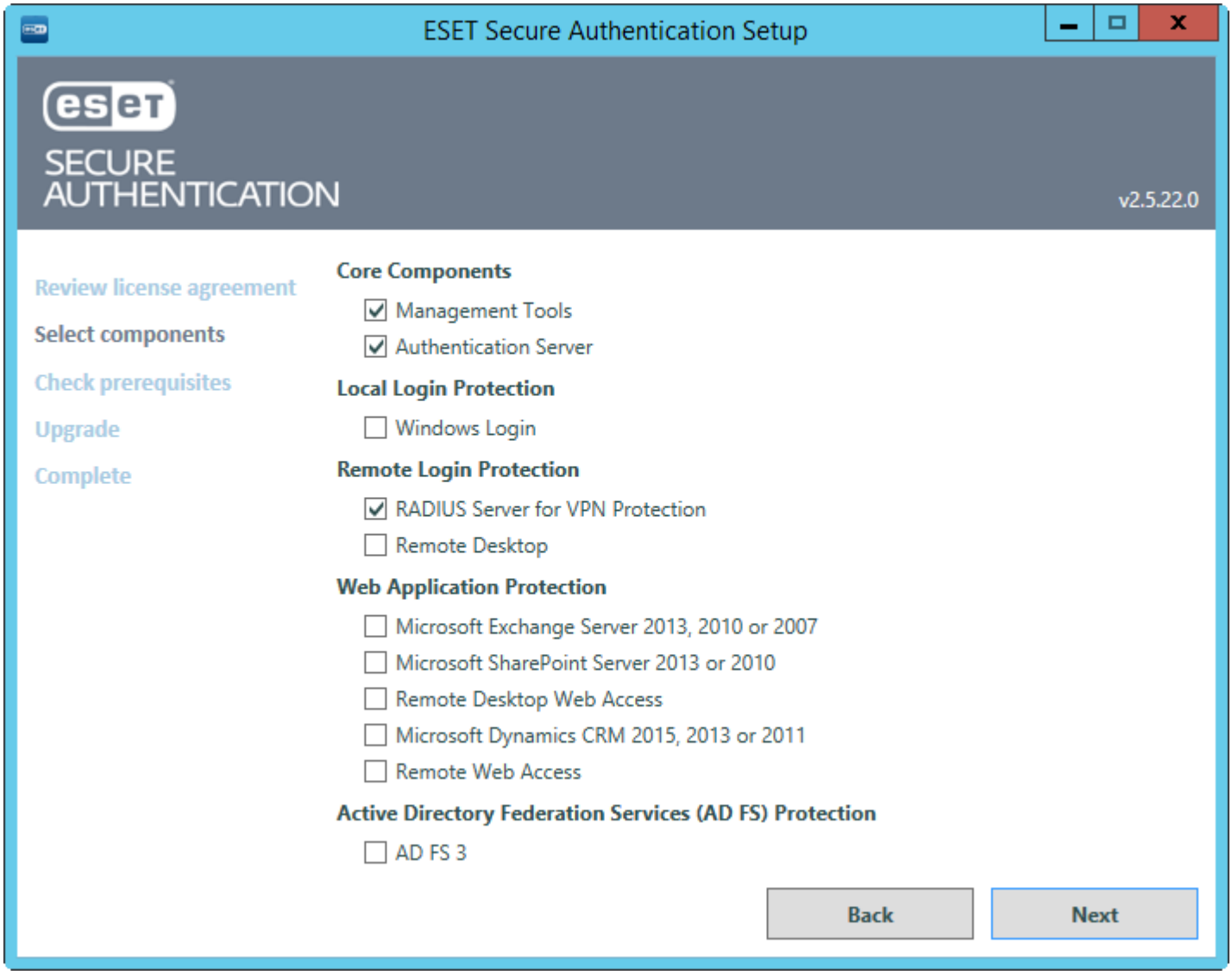
```
msiexec /x ESA.msi /qn AUTHENTICATION_SERVER_CLEAN_DATA=1
```

ПРИМЕЧАНИЕ.: Если ядро ESA было установлено в поддомене с использованием прав администратора домена, вы не сможете выполнить полное удаление с использованием прав администратора поддомена.

3.6 Установка обновлений

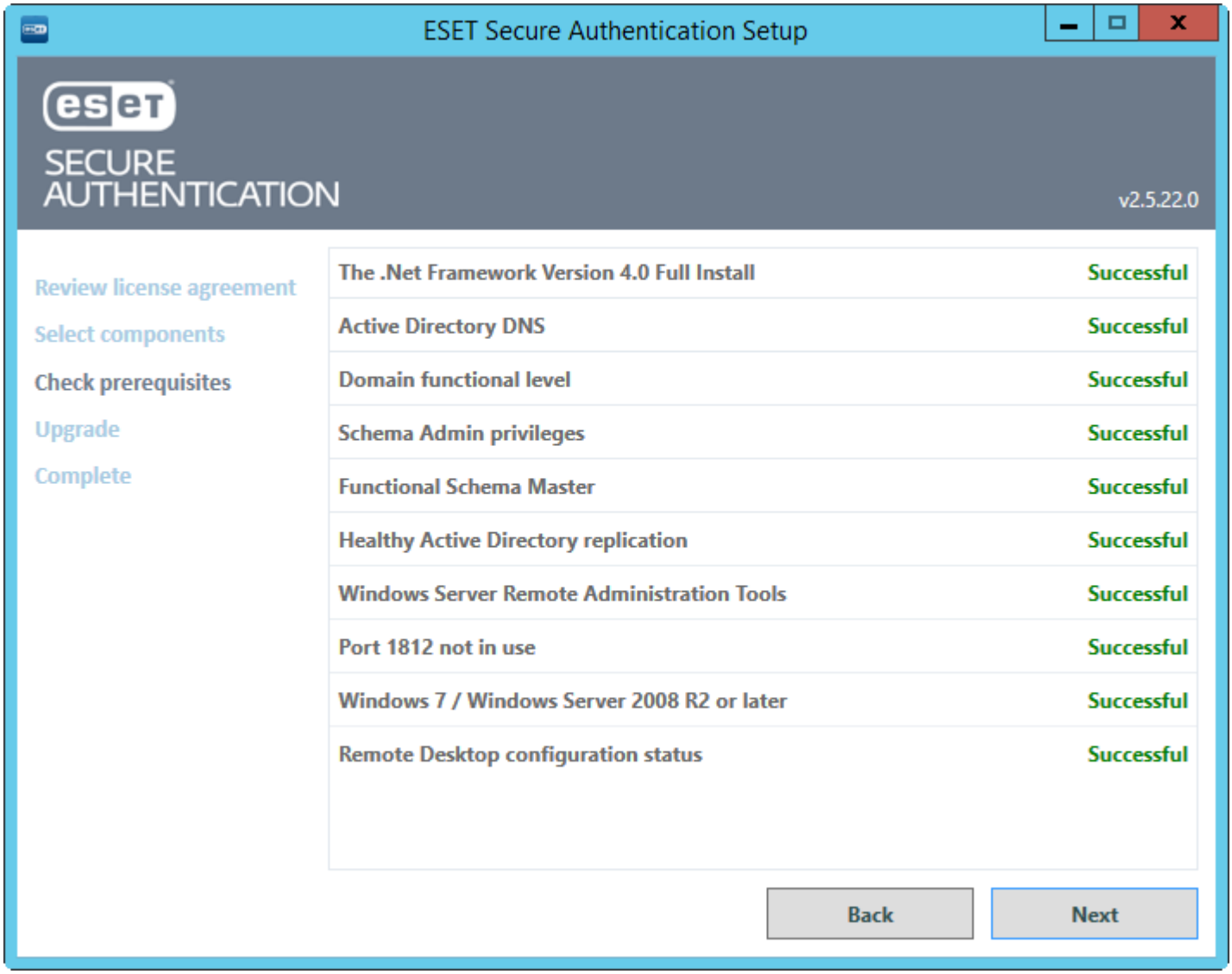
В ESET Secure Authentication 2.5.X и более поздних версий вы можете обновить ESA, запустив установщик. Предыдущую версию не нужно удалять вручную.

Устанавливаемые компоненты выбираются автоматически. Вы можете выбрать дополнительные компоненты для установки или отменить выбор существующих для удаления. Нажмите кнопку **Next** (Далее).



Экран **Advanced configuration** (Расширенная настройка) можно пропустить, щелкнув **Next** (Далее), если вам не нужно настроить прокси-сервер для сервера аутентификации или изменить порт сервера RADIUS.

После успешной проверки необходимых для установки условий нажмите кнопку **Next** (Далее), чтобы обновить выбранные компоненты.



Завершите обновление с помощью установщика и закройте установщик.

3.7 Установка защиты входа в Windows и защиты RDP с помощью GPO

Необходимые условия

❑ Сервер (или главный компьютер), на котором установлены основные компоненты ESET Secure Authentication (ESA):

- должен принадлежать к тому же домену Active Directory (AD), что и клиентские компьютеры, на которых будет установлена защита входа в Windows и защита RDP.
- На сервере должна быть установлена консоль управления групповыми политиками Microsoft (GPMC). Чтобы получить инструкции по установке GPMC, щелкните здесь.
- Компьютер, на котором будет установлена защита входа в Windows, необходимо добавить к службам EsaServices помощью интерфейса Active Directory для управления пользователями и компьютерами..

❑ Клиентские компьютеры:

- На клиентском компьютере должен быть установлен компонент .NET Framework 4.0 или более поздней версии.

- Членство в Active Directory — компьютер должен принадлежать к тому же домену AD, что и сервер (главный компьютер), на котором установлены основные компоненты ESA.
- Права администратора домена — установщик должен запускаться участником группы безопасности «Администраторы домена».
- Windows 7/Windows Server 2008 R2 или более поздней версии — компьютер должен работать под управлением ОС Windows 7 (или более поздней версии) либо Windows Server 2008 R2 (или более поздней версии).

❑ Дополнительные условия для защиты RDP:

- Необходимо включить подключение к удаленному рабочему столу на конкретном компьютере (*Пуск > Панель управления > Свойства системы > Удаленный доступ*).

Добавление компьютера к службам EsaServices

1. Откройте средство управления **Пользователи и компьютеры Active Directory**.
2. Щелкните **Вид** > **Расширенные функции**.
3. Перейдите к разделу **<ваш_домен_active_directory>** > **ESET Secure Authenitcation**, щелкните правой кнопкой мыши элемент **EsaServices** и выберите пункт **Свойства**.
4. Щелкните вкладку **Участники** и последовательно выберите элементы **Добавить...** > **Типы объектов** > **Компьютеры** > **ОК**.
5. В поле **Введите имена объектов для выбора** введите имя компьютера, на котором нужно установить защиту входа в Windows, и щелкните **Проверить имена**, чтобы проверить, правильно ли указано имя компьютера.
6. Если имя компьютера указано правильно, нажмите кнопку **ОК**, а затем еще раз нажмите кнопку **ОК**.

Получение MSI-файла установки

Если ключевые компоненты ESA установлены с помощью установщика с расширением *.exe*, то установщики с расширением *.msi* создаются автоматически в папке *C:\Program Files\ESET Secure Authentication\msi* (в 32-разрядной ОС используется путь *C:\Program Files (x86)\ESET Secure Authentication\msi*).

Получить установщик можно и иным способом. Для этого выполните следующие действия.

1. Загрузите EXE-файл установки для ESA со страницы https://www.eset.com/us/products/secure-authentication/.
2. Извлеките MSI-файл установки (с именем ESET Secure Authentication x64.msi или ESET Secure Authentication x86.msi) из загруженного EXE-файла.
3. Выгрузите полученный *MSI*-файл установки в общую папку на сервере (главном компьютере), к которой есть доступ у членов вашего домена AD.

Далее выполните один из следующих вариантов развертывания:

- сценарий входа;
- задача установки программного обеспечения.

3.7.1 Сценарий входа

Подготовка сценария входа (BAT-файл) с необходимыми параметрами

1. Нажмите клавиши **Windows + R**, введите **notepad.exe** в диалоговое окно **Выполнить** и нажмите клавишу **ВВОД**.
2. Когда откроется Блокнот, введите следующий код:

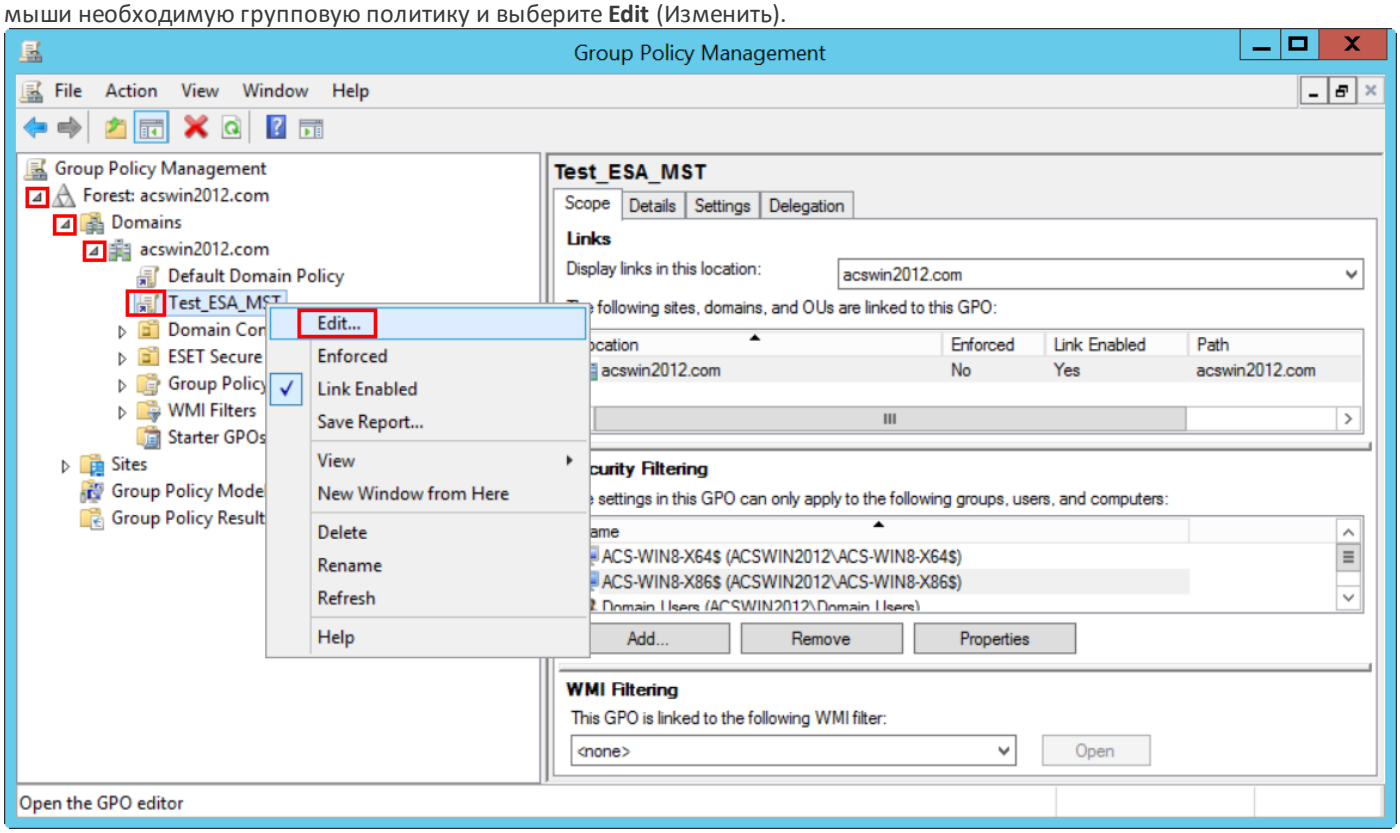
   ```
   msiexec /i "<путь_к_файлу_msi>" NO_DOMAIN_ADMIN_MODE=1
   ADDLOCAL="Credential_Provider,Win_Credential_Provider" /qn /L*v "c:\esa_install_log.txt"
   ```

   где вместо `<путь_к_файлу_msi>` следует указать действительный UNC-путь (сетевой путь) к общему пакету установщика (например, *\\файловый_сервер\общая_папка\имя_файла*). Код необходимо ввести в одной строке.

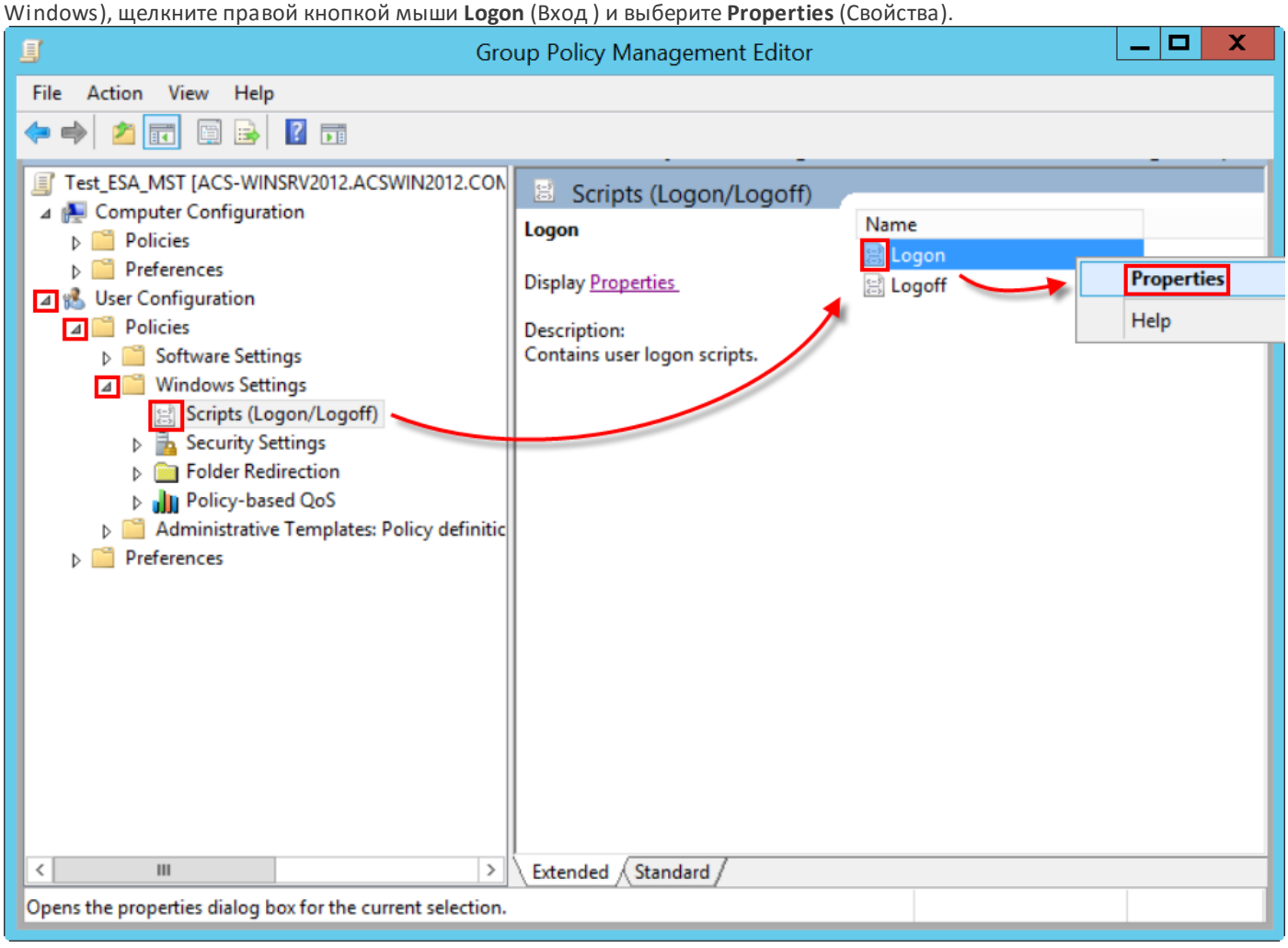
   ПРИМЕЧАНИЕ.: `Credential_Provider` означает защиту входа в RDP, а `Win_Credential_Provider` — защиту входа в Windows. Для получения дополнительных сведений см. раздел Аргументы MSI.
3. В Блокноте щелкните **File > Save As**, выберите **All Files** в раскрывающемся меню **Save as type** и введите имя файла **esainstall.bat**.

Развертывание сценария входа

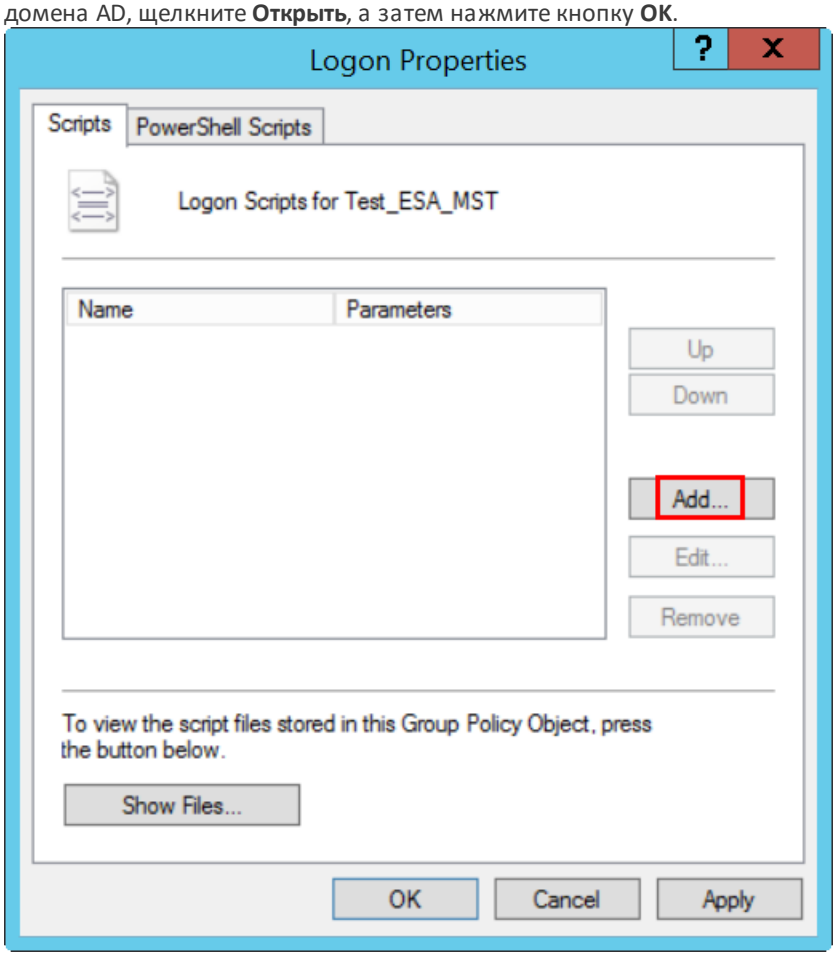
1. Откройте **Group Policy Management** (Управление групповыми политиками), найдите свой домен, щелкните правой кнопкой мыши необходимую групповую политику и выберите **Edit** (Изменить).



2. В окне **Group Policy Management Editor** (Редактор управления групповыми политиками) для политики вашего домена разверните **User Configuration** (Конфигурация пользователя) **> Policies** (Политики) **> Windows Settings** (Параметры Windows), щелкните правой кнопкой мыши **Logon** (Вход) и выберите **Properties** (Свойства).



3. Щелкните **Add...** (Добавить) > **Обзор...** и найдите файл **esainstall.bat**, который был скопирован в общую папку вашего домена AD, щелкните **Открыть**, а затем нажмите кнопку **OK**.



4. Нажмите кнопку **OK**, чтобы применить изменения и закрыть окно **Logon Properties** (Свойства входа).

3.7.2 Задача «Установка программного обеспечения»

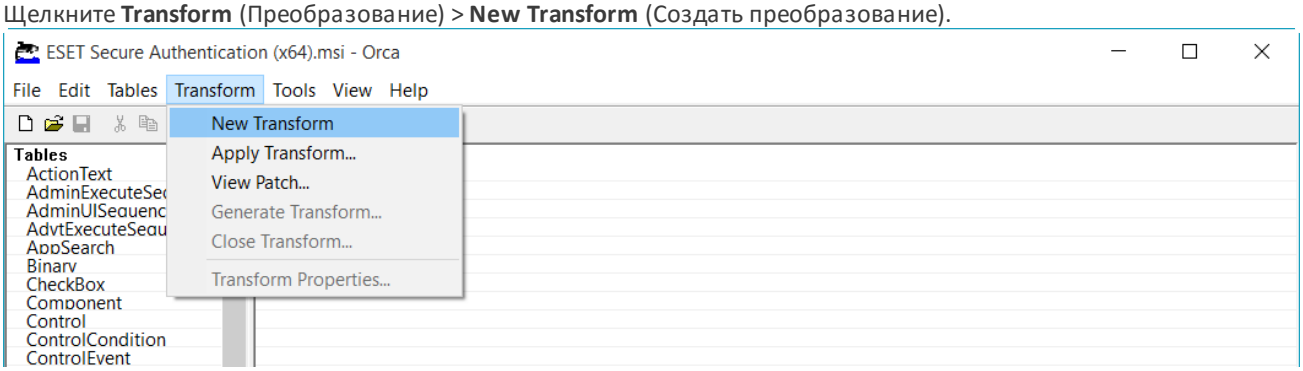
Прежде чем создавать задачу **Установка программного обеспечения** с помощью **GPO**, необходимо создать *MST*-файл преобразования.

Необходимое условие

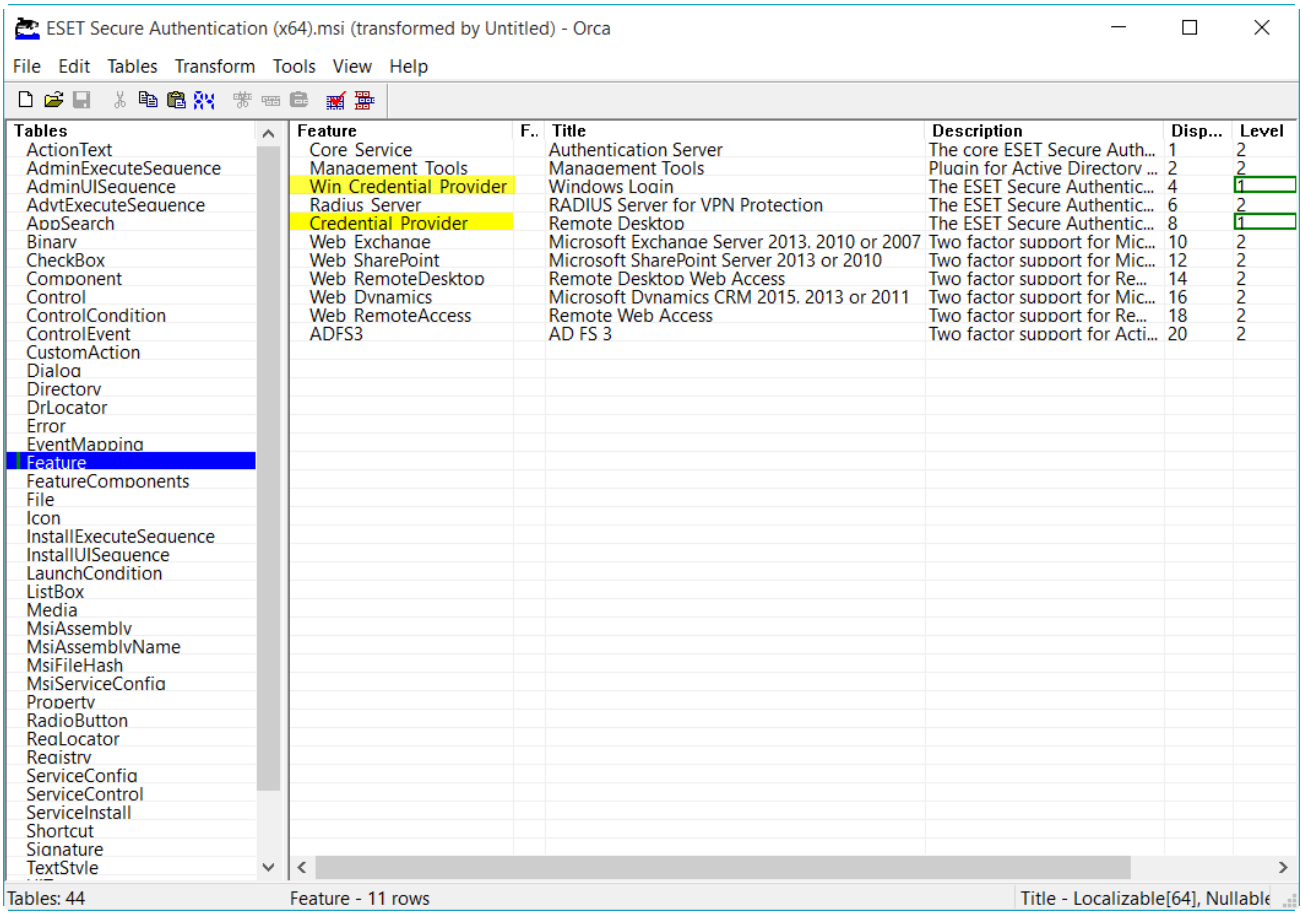
- Установите средство редактирования баз данных Orca на компьютер. Средство Orca — это часть Windows SDK. Инструкции по загрузке и установке Orca см. в статье базы знаний Майкрософт Использование редактора базы данных Orca для редактирования файлов установщика Windows.

Создание MST-файла преобразования

1. Щелкните **Пуск** > **Все программы** > **Orca**, чтобы запустить редактор базы данных Orca.
2. Выберите последовательно элементы **Файл** > **Открыть**. Перейдите в папку с *MSI*-файлом установщика, к которому вы хотите применить файл преобразования, выберите файл и нажмите кнопку **Открыть**.
3. Щелкните **Transform** (Преобразование) > **New Transform** (Создать преобразование).

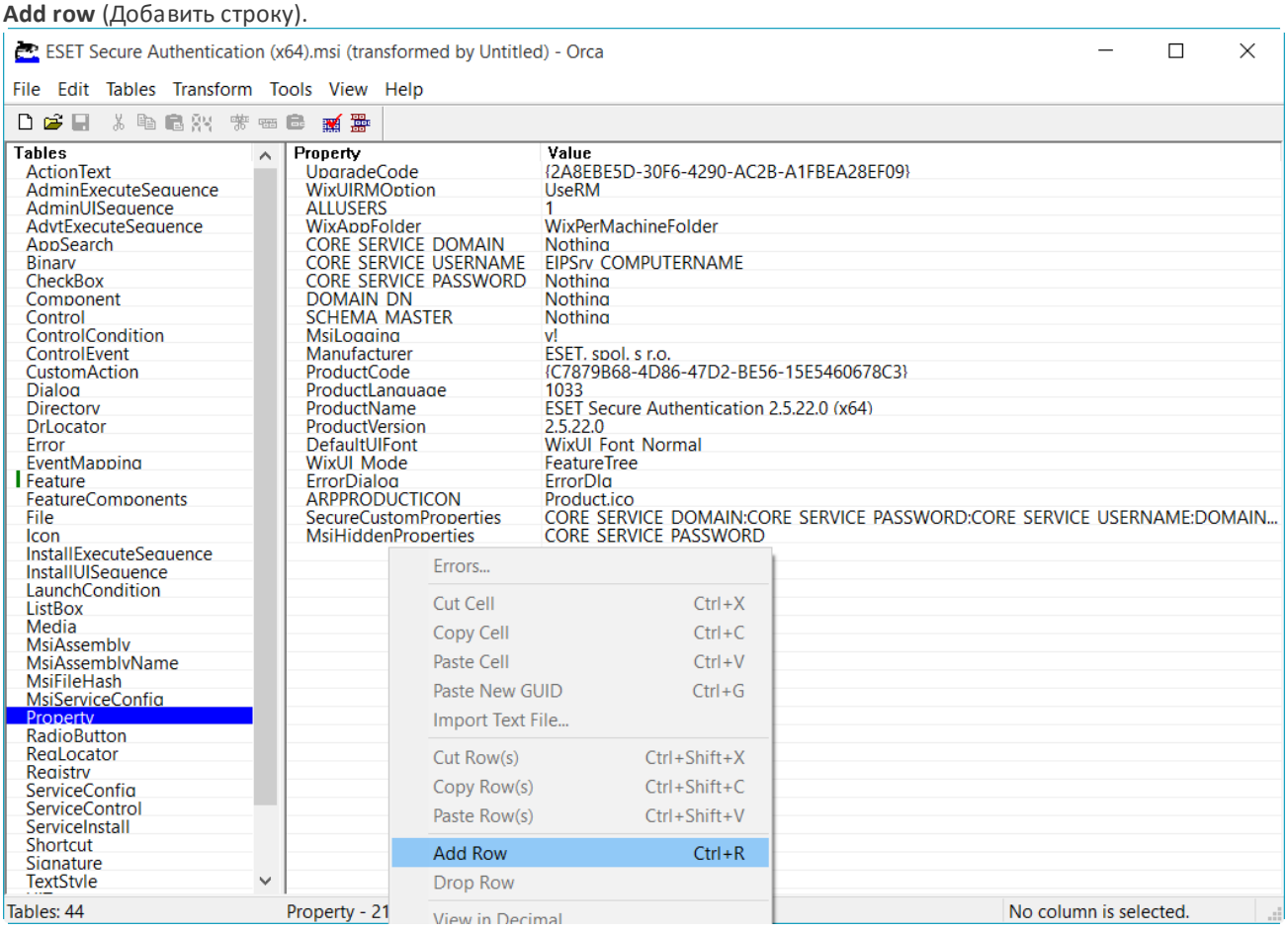


4. Выберите **Features** (Компоненты) в столбце **Tables** (Таблицы), затем выберите **Windows Login** (Вход в Windows) и задайте для параметра **Level** (Уровень) значение 1. Затем выберите **Remote Desktop** (Удаленный рабочий стол) и задайте для параметра **Level** (Уровень) значение **1**.

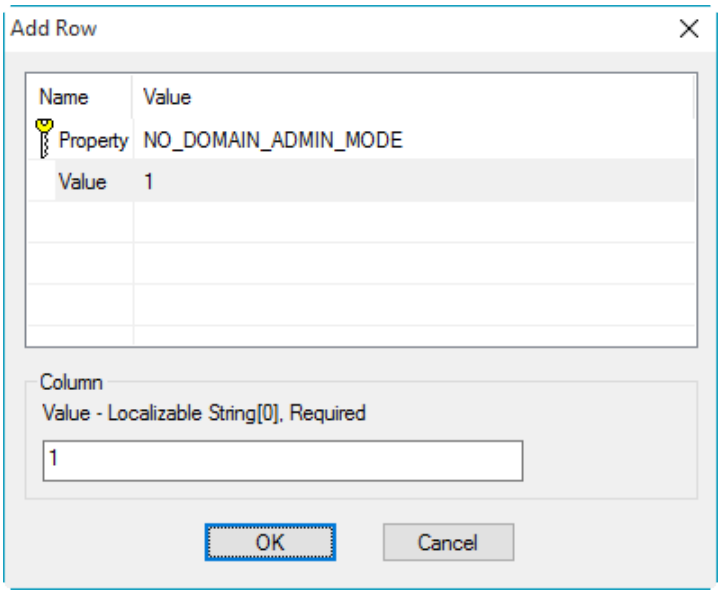


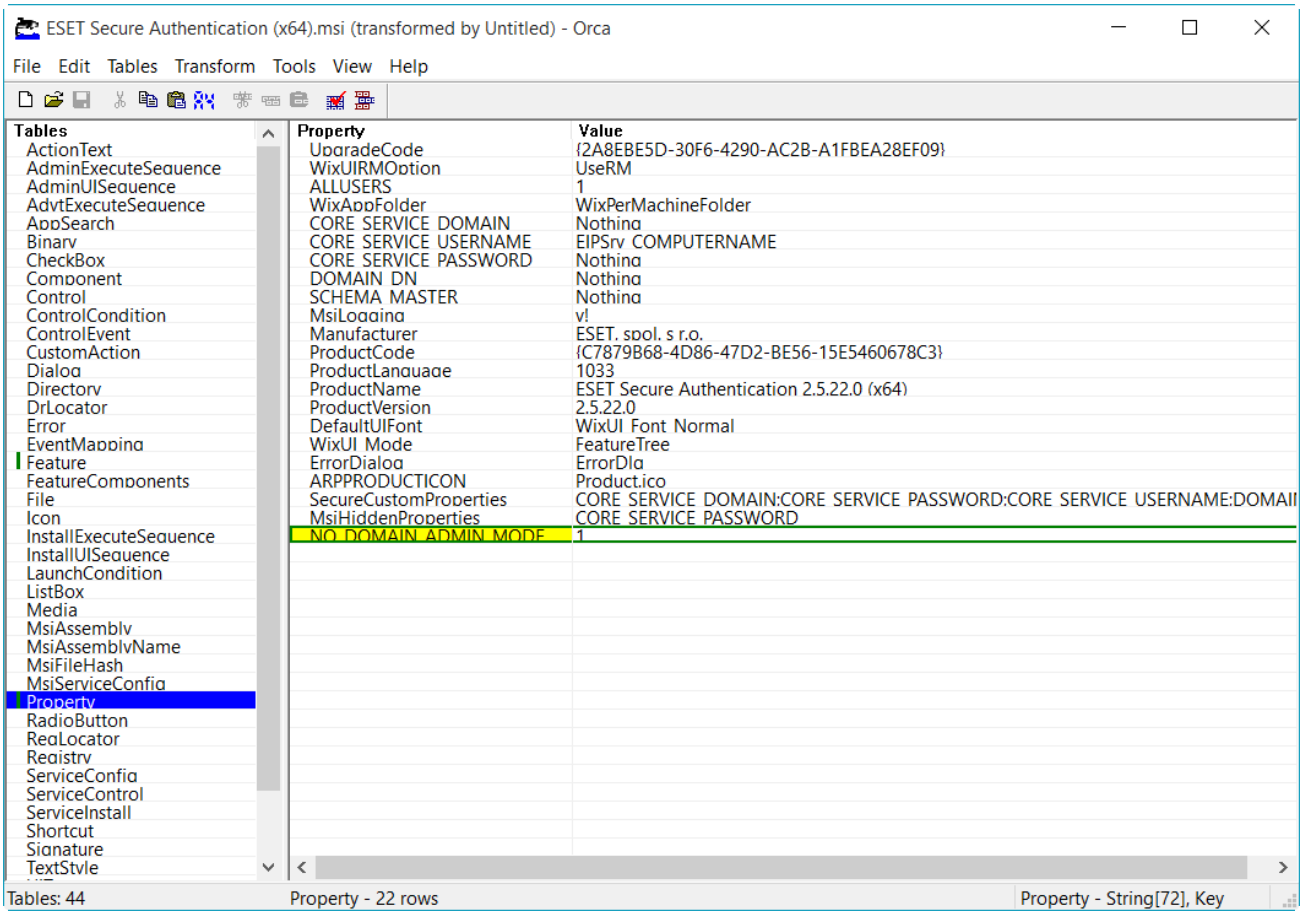
ПРИМЕЧАНИЕ. Все изменения выделены зеленым цветом.

5. Выберите **Property** (Свойство) в столбце **Tables** (Таблицы), щелкните правой кнопкой мыши пустую строку и выберите **Add row** (Добавить строку).

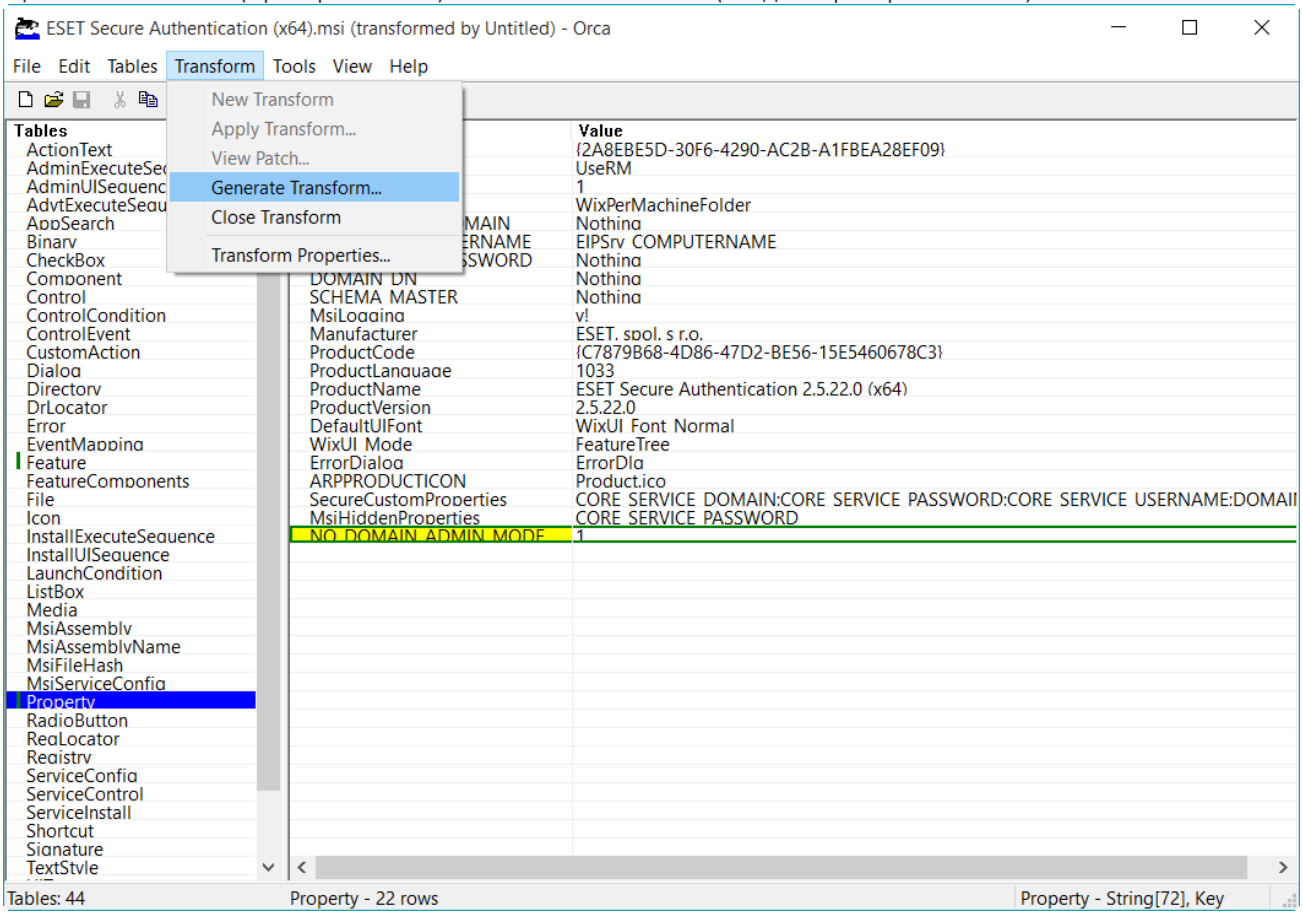


6. В диалоговом окне **Add Row** (Добавить строку) введите **NO_DOMAIN_ADMIN_MODE** в поле **Property** (Свойство), задайте для поля **Value** (Значение) значение **1** и нажмите кнопку **OK**.


Add Row
Name
Value
Property
NO_DOMAIN_ADMIN_MODE
Value
1
Column
Value - Localizable String[0], Required
1
OK
Cancel


ESET Secure Authentication (x64).msi (transformed by Untitled) - Orca
File Edit Tables Transform Tools View Help
Tables
ActionText
AdminExecuteSequence
AdminUISequence
AdvtExecuteSequence
AppSearch
Binary
CheckBox
Component
Control
ControlCondition
ControlEvent
CustomAction
Dialog
Directory
DrLocator
Error
EventMapping
Feature
FeatureComponents
File
Icon
InstallExecuteSequence
InstallUISequence
LaunchCondition
ListBox
Media
MsiAssembly
MsiAssemblyName
MsiFileHash
MsiServiceConfig
Property
RadioButton
RegLocator
Registry
ServiceConfig
ServiceControl
ServiceInstall
Shortcut
Signature
TextStyle
Property
Value
UpgradeCode {2A8EBE5D-30F6-4290-AC2B-A1FBEA28EF09}
WixUIRMOption UseRM
ALLUSERS 1
WixAppFolder WixPerMachineFolder
CORE_SERVICE_DOMAIN Nothing
CORE_SERVICE_USERNAME EIPSrv COMPUTERNAME
CORE_SERVICE_PASSWORD Nothing
DOMAIN_DN Nothing
SCHEMA_MASTER Nothing
MsiLogging v!
Manufacturer ESET, spol. s r.o.
ProductCode {C7879B68-4D86-47D2-BE56-15E5460678C3}
ProductLanguage 1033
ProductName ESET Secure Authentication 2.5.22.0 (x64)
ProductVersion 2.5.22.0
DefaultUIFont WixUI_Font_Normal
WixUI_Mode FeatureTree
ErrorDialog ErrorDlg
ARPPRODUCTICON Product.ico
SecureCustomProperties CORE_SERVICE_DOMAIN:CORE_SERVICE_PASSWORD:CORE_SERVICE_USERNAME:DOMAI
MsiHiddenProperties CORE_SERVICE_PASSWORD
NO_DOMAIN_ADMIN_MODE 1
Tables: 44
Property - 22 rows
Property - String[72], Key

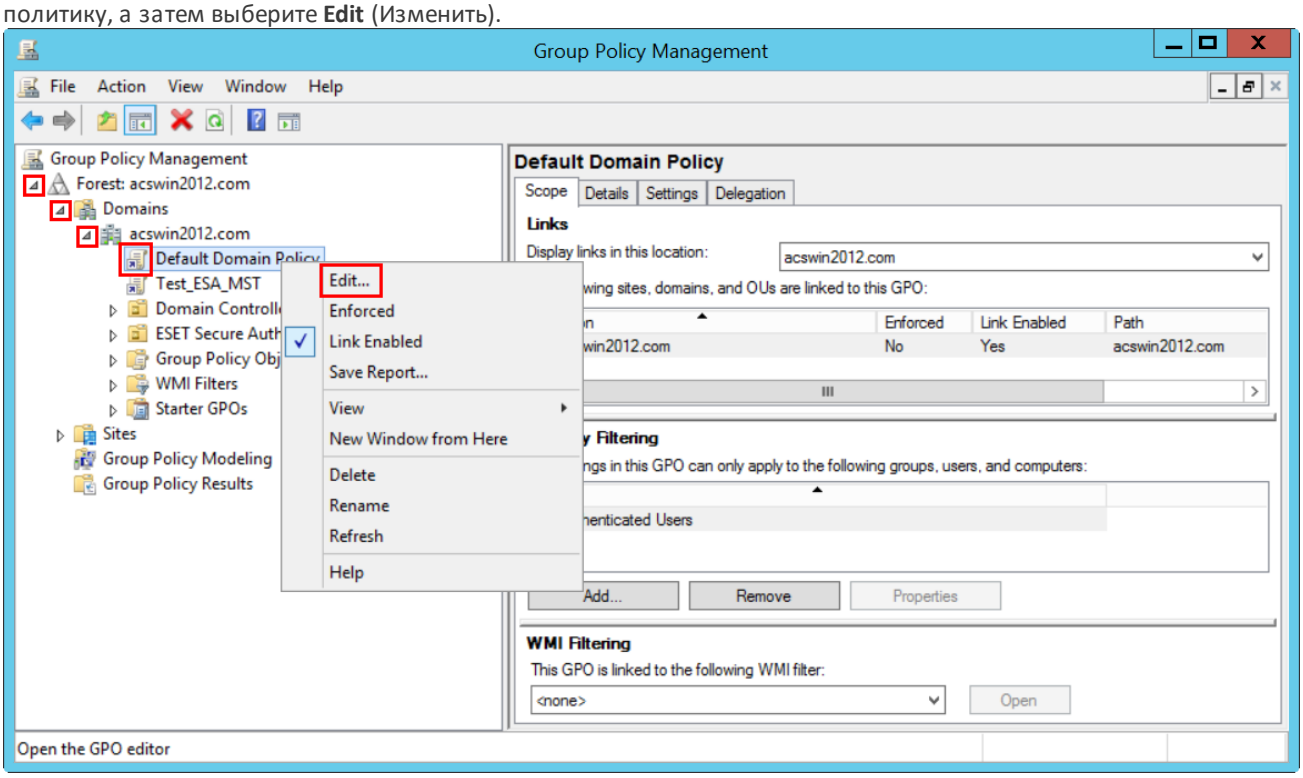
7. Щелкните **Transform** (Преобразование) > **Generate Transform...** (Создать преобразование...).



Создание задачи «Установка программного обеспечения» с помощью GPO

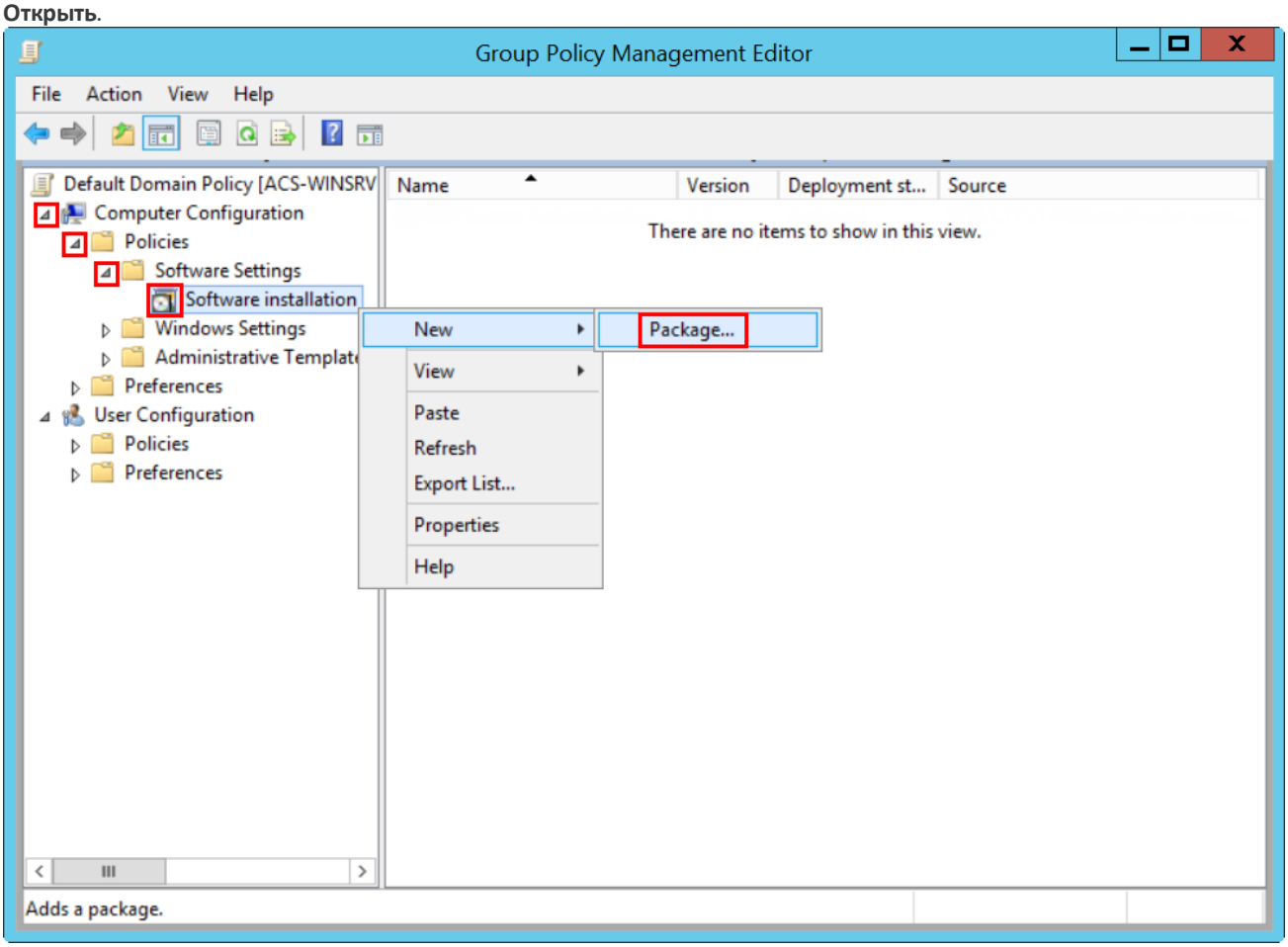
Следующие действия демонстрируются на примере Microsoft Server 2012 R2.

1. Откройте **Group Policy Management** (Управление групповыми политиками), найдите свой домен, щелкните правой кнопкой мыши **Default Domain Policy** (Политика домена по умолчанию) или созданную вами пользовательскую политику, а затем выберите **Edit** (Изменить).

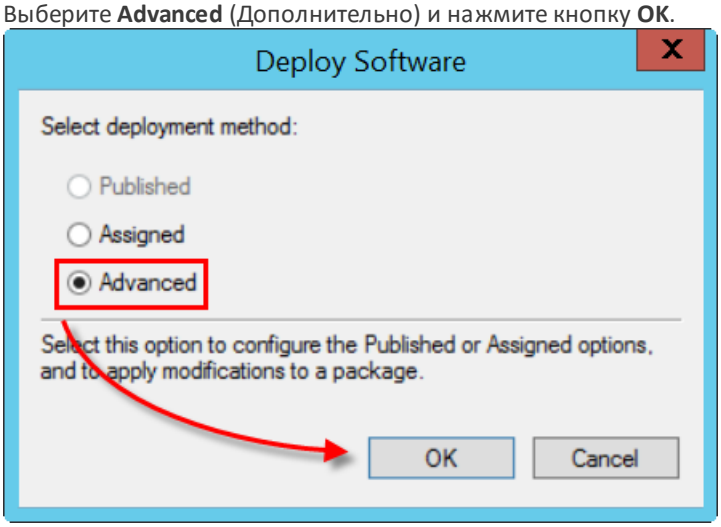


2. В окне **Group Policy Management Editor** (Редактор управления групповыми политиками) для политики вашего домена разверните **Computer Configuration** (Конфигурация компьютера) > **Policies** (Политики) > **Software Settings** (Параметры программного обеспечения).

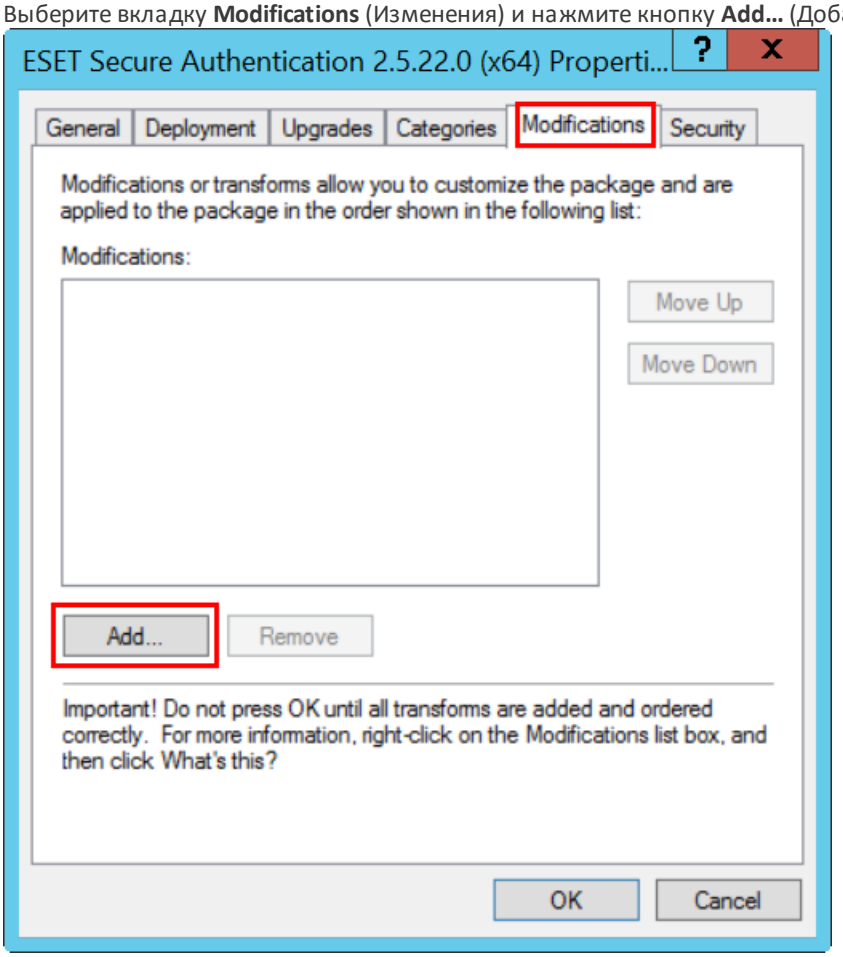
3. Щелкните правой кнопкой мыши **Software installation** (Установка программного обеспечения), выберите **New** (Создать) > **Package** (Пакет) и перейдите в папку, в которой сохранен установщик ESA с расширением *.msi*. Введите UNC-путь общего пакета установщика (например, \\файловый_сервер\общая_папка\имя_файла.msi) и нажмите кнопку **Открыть**.



4. Выберите **Advanced** (Дополнительно) и нажмите кнопку **OK**.

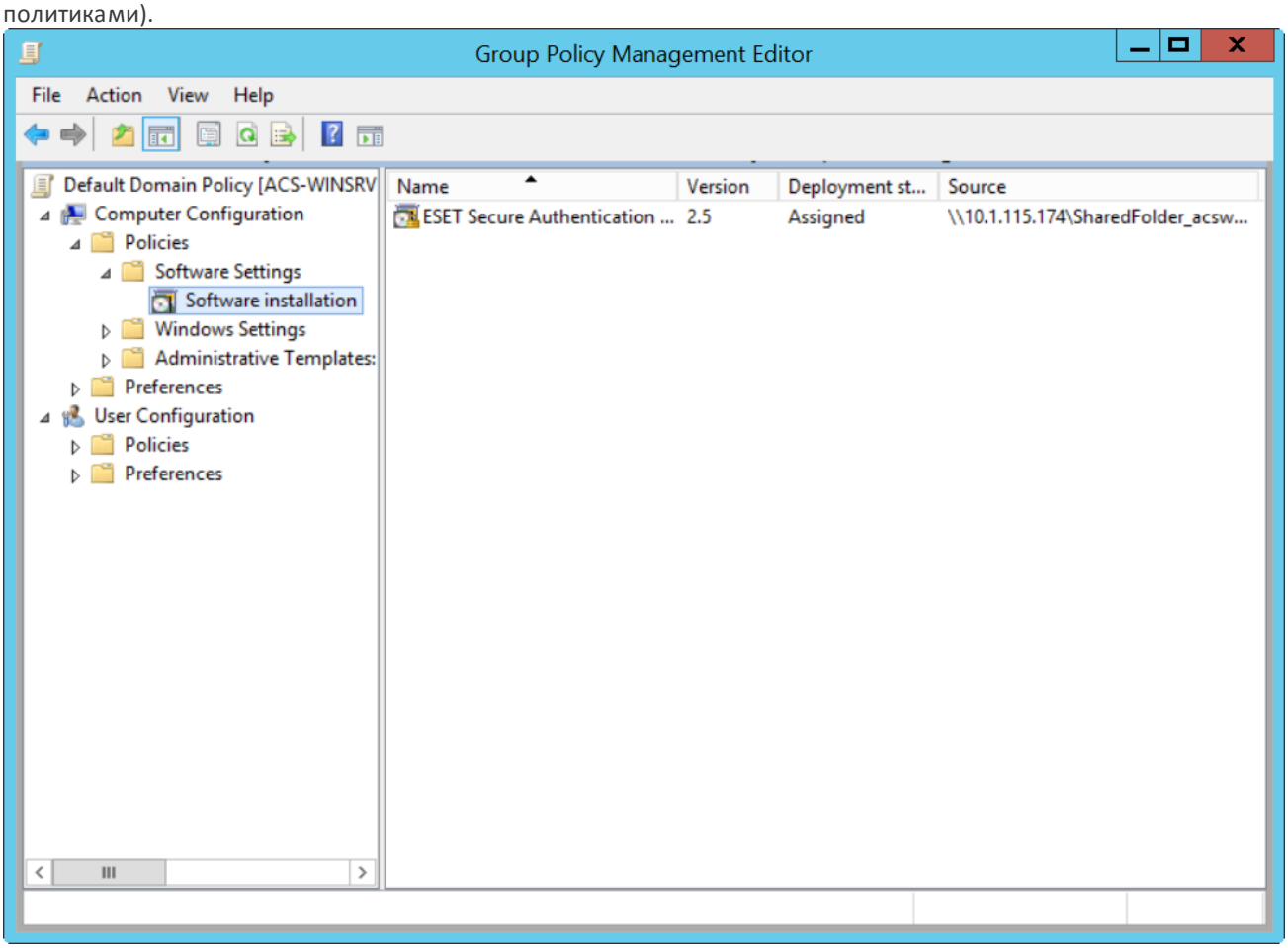


5. Выберите вкладку **Modifications** (Изменения) и нажмите кнопку **Add...** (Добавить).



6. Откройте файл преобразования установщика ESA (в той же папке, которую вы указали на шаге 3), введите UNC-путь *MST*-файла (например, \\файловый_сервер\общая_папка\имя_файла.mst) и нажмите кнопку **Открыть**.

7. Нажмите кнопку **OK**. Пакет отобразится в окне **Group Policy Management Editor** (Редактор управления групповыми политиками).



8. Пакет будет установлен на все клиентские компьютеры, к которым применяется измененная групповая политика.

См. статью базы данных Майкрософт об использовании групповой политики для удаленной установки программного обеспечения в ОС Windows Server 2003 и 2008.

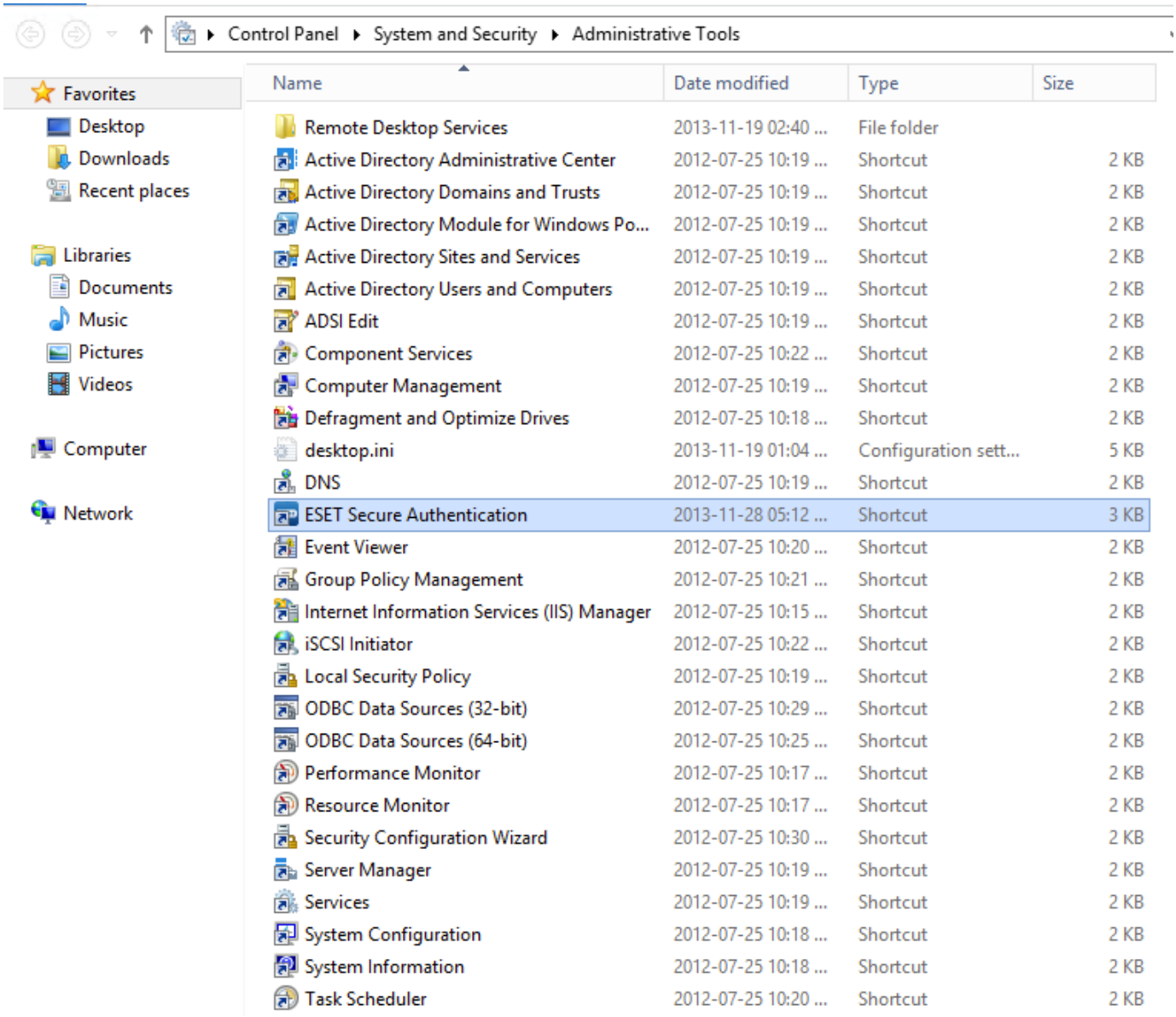
3.7.3 Аргументы MSI

При использовании *MSI-установщика* в качестве сценария входа или задачи установки можно использовать несколько аргументов.

- Для указания устанавливаемых компонентов используется аргумент `ADDLOCAL` . Ниже приведены возможные значения.
  `Credential_Provider` — компонент защиты удаленного рабочего стола.
  `Win_Credential_Provider` — компонент защиты входа в Windows.
  `Radius_Server`
  `Web_Exchange`, `Web_SharePoint`, `Web_RemoteDesktop`, `Web_Dynamics`, `Web_RemoteAccess`
  `Management_Tools` — консоль управления.
  `ADFS3`
  `Core_Service` — сервер аутентификации.
- Чтобы задать пользовательский порт RADIUS или указать данные прокси-сервера, который необходимо использовать, применяются нижеследующие аргументы. Задайте соответствующие значения.
  `ESA_CONFIG_RADIUS_PORT`
  `ESA_CONFIG_PROXY_SERVER`, `ESA_CONFIG_PROXY_PORT`, `ESA_CONFIG_PROXY_USER`, `ESA_CONFIG_PROXY_PASSWORD`
- Полезные аргументы `MSIEXEC` .
  `/L*v "c:\esa_install_log.txt"` — для создания файла журнала установки с именем *esa_install_log.txt* в каталоге *C*.
  `/qn` — режим автоматической установки, который означает, что установка выполняется в фоновом режиме без взаимодействия с пользователем, выполнившим вход.
- Чтобы установить или удалить компоненты ESA без администратора домена, используйте `NO_DOMAIN_ADMIN_MODE=1`.
- Для полного удаления основных компонентов ESA, в том числе данных конфигурации, хранящихся в Active Directory, используйте `AUTHENTICATION_SERVER_CLEAN_DATA=1`.

3.8 Основная настройка

После установки обязательных компонентов необходимо выполнить основную настройку. Все настройки системы ESA выполняются в ESA Management Console. The ESA Management Console добавляется как оснастка в стандартную консоль MMC. ESA Management Console можно открыть из раздела «Средства администрирования», как показано на рисунке ниже.



Сначала необходимо активировать систему ESA с помощью лицензии ESA. Лицензию можно получить у дистрибьютора ESET. Также можно воспользоваться демонстрационной лицензией (в файле *License.txt*), которая поставляется вместе с установщиком.

Чтобы активировать ESA Server, выполните следующие действия.

1. Откройте ESA Management Console.
2. Перейдите в узел домена.
3. Введите имя пользователя и пароль для своей лицензии ESA.
4. ESA Server автоматически получит лицензию и отобразит текущую информацию о ней.

После активации лицензии настройте в разделе «Basic Settings» имя маркера. Это имя маркера вашей компании, которое будет отображаться в Mobile Application на телефонах пользователей.

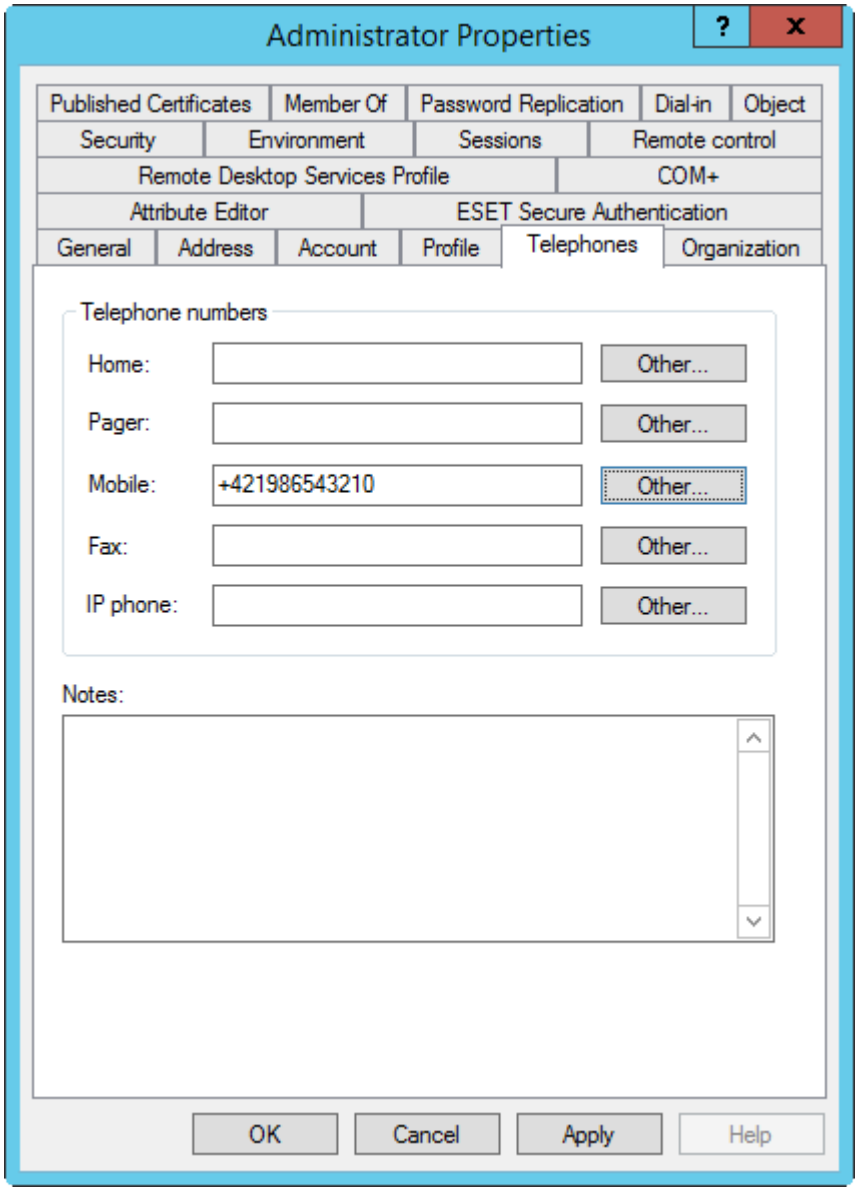
Если вы хотите настроить веб-приложение (Web Application), перейдите к главе Защита веб-приложений. Сведения о настройке 2FA в VPN приведены в главе Защита VPN. Сведения о настройке 2FA для Remote Desktop см. в главе Защита удаленного рабочего стола.

4. Управление пользователями — подготовка

Управление пользователями осуществляется в интерфейсе управления Active Directory Users and Computers. В поле **Mobile** (Мобильный) на вкладке **Telephones** (Телефоны) для каждого пользователя ESA должен быть указан действительный номер мобильного телефона.

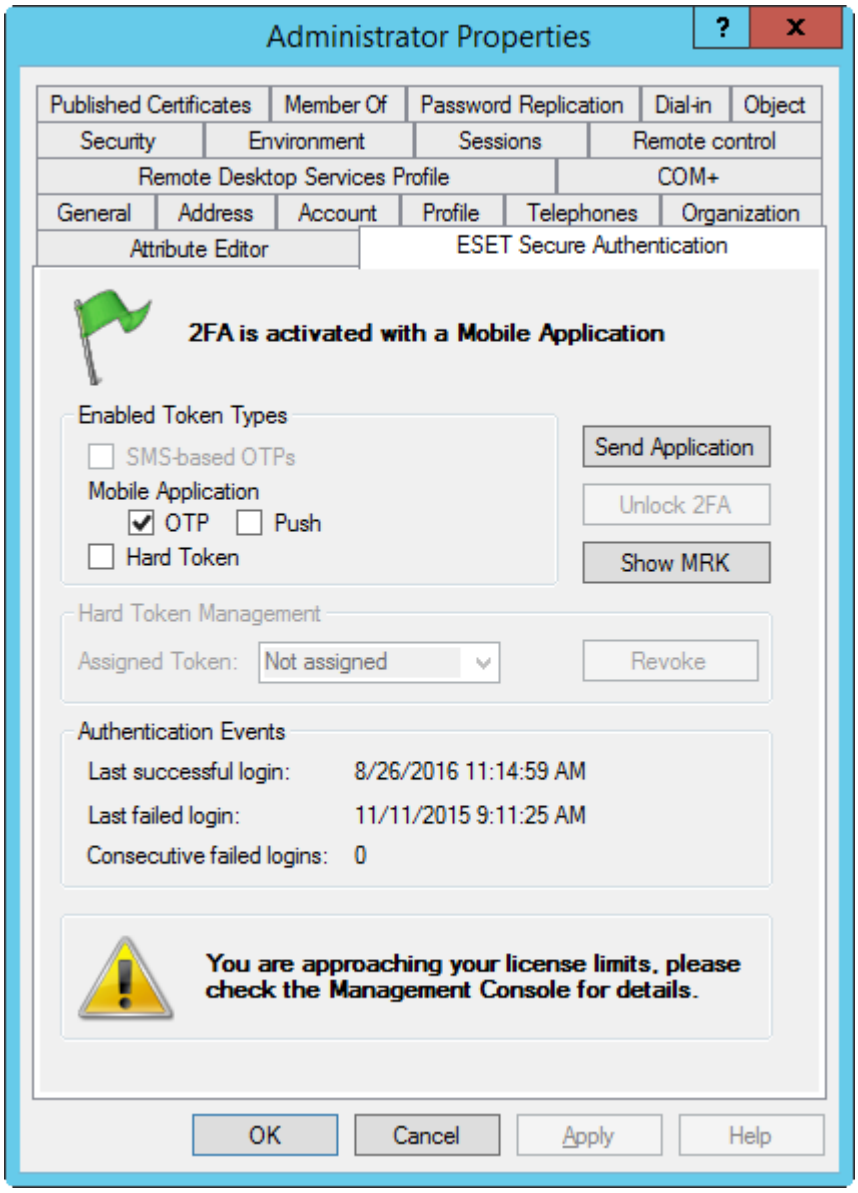
Для подготовки нового Mobile App выполните следующие действия.

1. Откройте обычное представление пользователей ADUC.
2. Щелкните **User** (Пользователь) правой кнопкой мыши и выберите пункт **Properties** (Свойства).
3. В поле **Mobile** (Мобильный) введите номер мобильного телефона пользователя.



ПРИМЕЧАНИЕ. Мобильный номер должен содержать только цифры (например, 421987654321, где 421 — это код страны).

Чтобы изменить настройки ESET Secure Authentication для того или иного пользователя, откройте вкладку ESET Secure Authentication.



Чтобы настроить для определенного пользователя использование OTP, созданных программным маркером, выполните следующие действия.

1. Установите флажок **OTP** (Одноразовый пароль) и/или **Push**-уведомление.
2. Нажмите кнопку **Send Application** (Отправить приложение).
3. Пользователь получит SMS-сообщение, содержащее ссылку для установки приложения.

Инструкции по установке и использованию мобильных приложений (выберите мобильную ОС, чтобы перейти к соответствующей статье):

- Android
- BlackBerry
- iPhone
- Windows Phone

5. Соединение

В ESET Secure Authentication предусмотрено несколько вариантов аутентификации пользователей для доступа к определенным компьютерам или службам, защищенным двухфакторной аутентификацией.

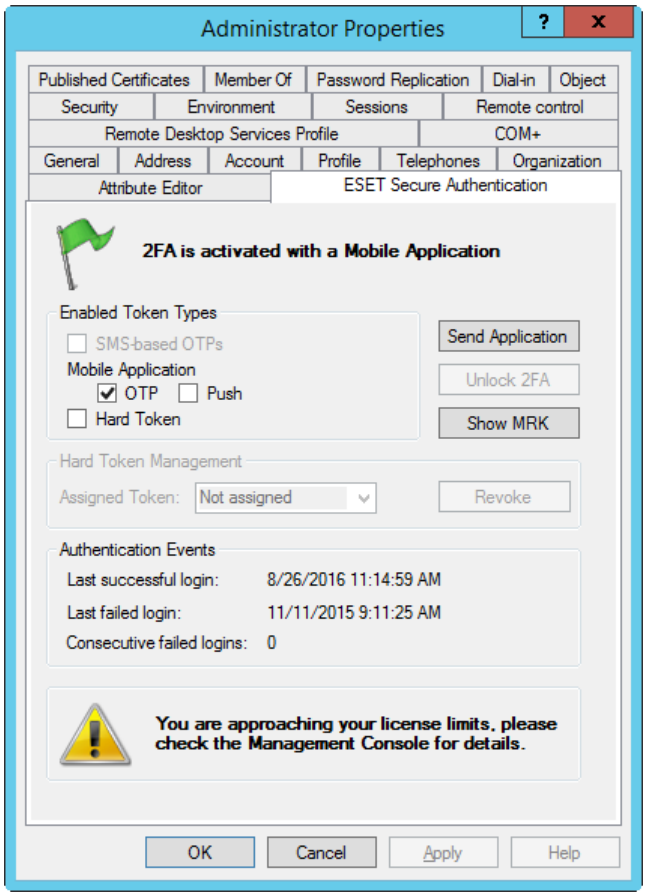
- Одноразовый пароль (OTP), полученный посредством SMS.
- Одноразовый пароль, созданный в мобильном приложении ESA.
- Аутентификация с помощью push-уведомлений.
- Маркеры оборудования.
- Одноразовый пароль, полученный с помощью пользовательских вариантов доставки.

Из-за технической природы SMS-сообщений, которые обычно доставляются локальными операторами телекоммуникационных услуг, компания ESET не может гарантировать надежность доставки SMS-сообщений на мобильные телефоны конечных пользователей.

5.1 Аутентификация с помощью push-уведомлений

Метод аутентификации с помощью push-уведомлений, в котором используются push-уведомления на мобильных устройствах, впервые появился в приложении ESET Secure Authentication версии 2.5.X и был доступен только для Android-устройств. В приложении ESET Secure Authentication 2.6.X добавлена возможность аутентификации с помощью push-уведомлений для iOS-устройств.

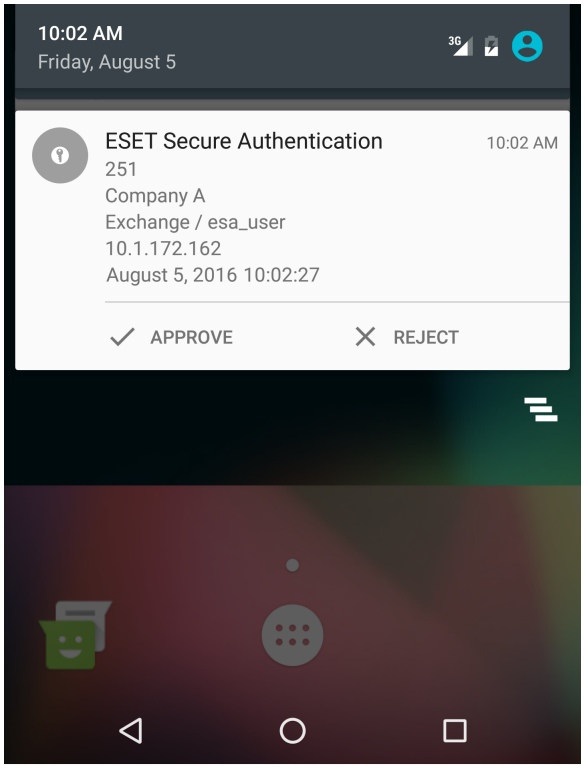
Пользователь может включить оба метода аутентификации (**OTP** (Одноразовый пароль) и **Push**-уведомления) в интерфейсе управления ADUC .



Чтобы включить push-уведомления на iOS-устройствах, нажмите **Allow** (Разрешить), когда появится запрос. На Android-устройствах уведомления включены автоматически.

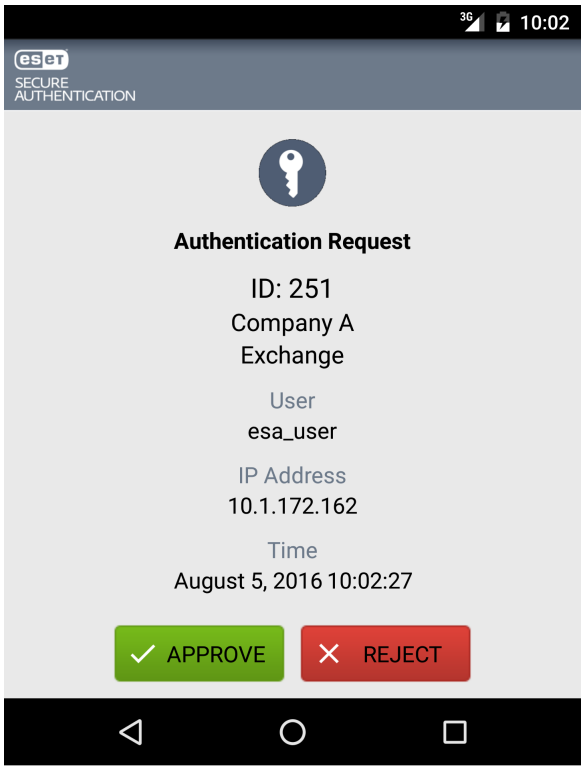
ПРИМЕЧАНИЕ.: Работа push-уведомлений может начаться с некоторой задержкой после подготовки телефона пользователя или включения push-уведомлений в консоли управления.

Пользователь может утвердить или отклонить запрос на аутентификацию непосредственно в области уведомлений своего мобильного устройства.



Android **iOS**

Коснитесь уведомления, не нажимая кнопок **Approve** (Подтвердить) и **Reject** (Отклонить), чтобы открыть мобильное приложение Mobile application, в котором можно подтвердить или отклонить запрос аутентификации.



Android **iOS**

Запросами аутентификации с помощью push-уведомлений можно управлять также на смарт-часах, которые работают под управлением ОС Android или iOS.

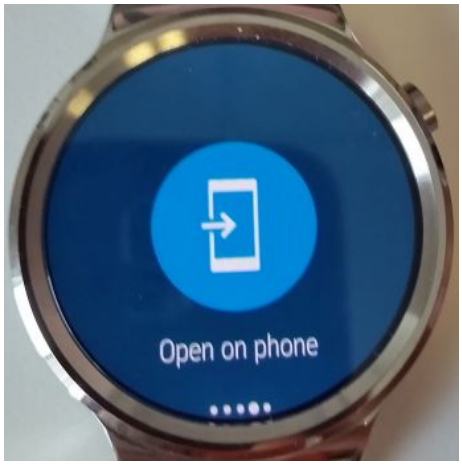
Каждое push-уведомление содержит идентификатор, который соответствует идентификатору экрана запроса на аутентификацию.

Смарт-часы Android

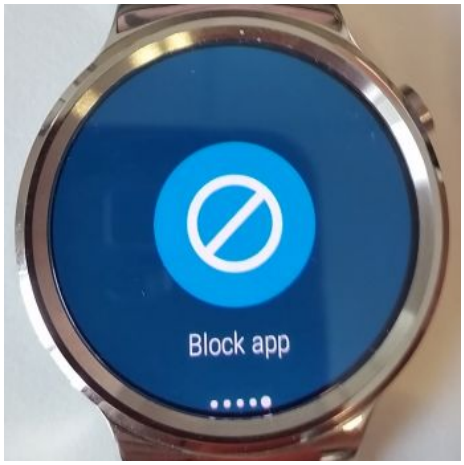
Когда отобразится уведомление, проведите вправо или влево по экрану, чтобы отобразились доступные варианты.

Утвердить запрос на аутентификацию

Отклонить запрос на аутентификацию



Открыть запрос на аутентификацию в мобильном приложении



Отключить уведомление на смарт-часах

Если используемое мобильное приложение Mobile Application защищено PIN-кодом, отобразится сообщение **Approve on phone** (Подтвердить на телефоне)

Apple Watch

Когда уведомление появляется на часах Apple, прокрутите вниз, чтобы увидеть кнопки **Approve** (Подтвердить) и **Reject** (Отклонить) .

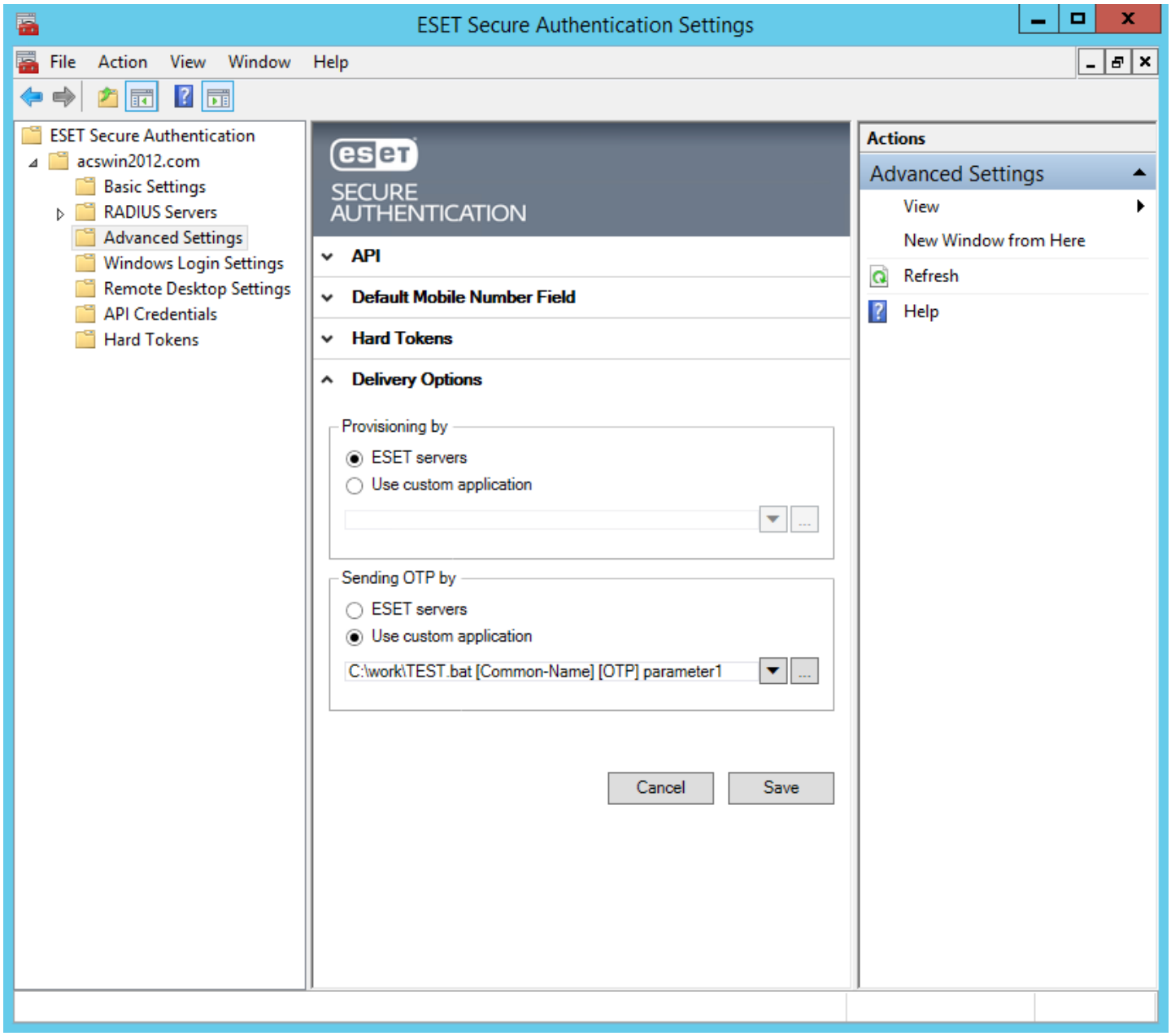
Уведомление пришло **Прокрутите вниз до кнопок**

Если вы используете защищенное PIN-кодом мобильное приложение (Mobile Application), после прокрутки уведомления вниз доступна только кнопка **Reject** (Отклонить).

5.2 Пользовательские параметры доставки

Используемые по умолчанию параметры доставки пароля OTP (SMS, мобильное приложение) превосходно подходят большинству пользователей. При этом в решении ESA можно использовать также пользовательские параметры доставки.

Откройте консоль управления ESA (ESA Management Console) на главном компьютере, перейдите к узлу домена (в нашем примере это **acswin2012.com**), щелкните **Advanced Settings** (Дополнительные настройки), а затем щелкните **Delivery Options** (Параметры доставки).



Здесь можно указать путь к пользовательскому сценарию (или найти его, нажав кнопку ...), с помощью которого вы хотите выполнить подготовку или доставку пароля OTP. Щелкните ▼, чтобы отобразить список параметров, которые можно передать в пользовательский сценарий. Например, для доставки одноразового пароля (OTP) нужно использовать параметр [OTP]. Кроме того, в сценарий можно передать пользовательскую строку, которую для этого нужно указать (см. **parameter1** на снимке экрана выше).

Образец сценария — доставка пароля OTP по электронной почте

Обязательные условия:

- нужно знать параметры SMTP шлюза электронной почты, с помощью которого нужно отправить электронное письмо, содержащее пароль OTP;
- нужен пользовательский сценарий отправки электронных писем;

- нужен пользовательский сценарий в формате BAT (.bat), к которому задается путь в консоли управления ESA (ESA Management Console) (см. снимок экрана выше) и который вызывает наш пользовательский сценарий, отправляющий электронное письмо;
- для каждого пользователя, для которого включена двухфакторная аутентификация (2FA) и который получает одноразовые пароли (OTP passwords) по электронной почте, нужно указать адрес электронной почты в поле **E-mail** (Электронная почта) на вкладке **General** (Общие) при просмотре сведений о таких пользователях в интерфейсе управления Active Directory Users and Computers (Пользователи и компьютеры Active Directory).

Образец сценария Python для отправки электронной почты: мы назвали этот файл **sendmail.py**:

```
import sys, smtplib

server = smtplib.SMTP('smtpserver:port')

server.starttls()

server.login('username','password')

server.sendmail(sys.argv[1] , sys.argv[1], 'Subject: OTP is '+sys.argv[2])

server.quit()
```

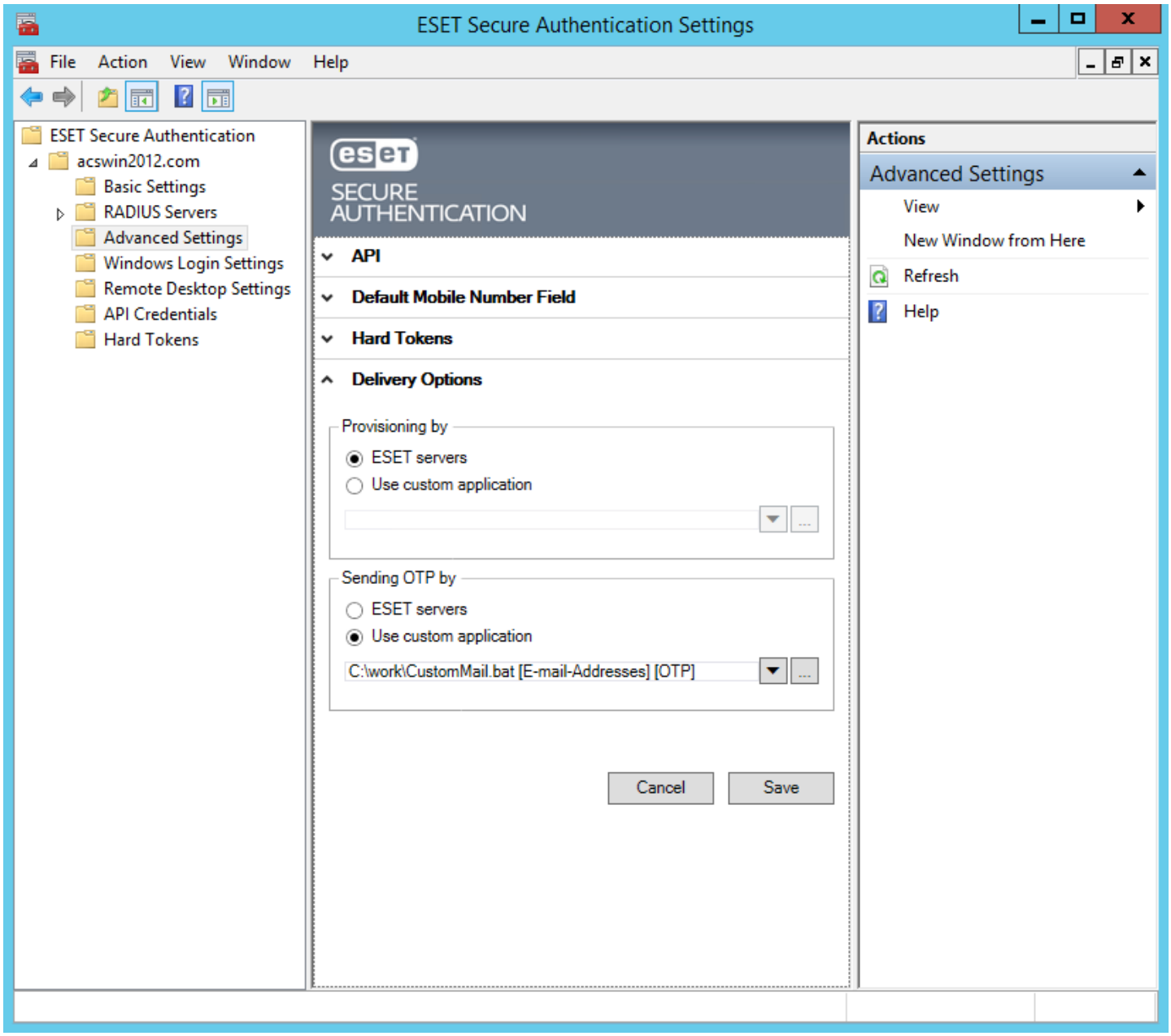
ПРИМЕЧАНИЕ. В образце сценария Python, приведенном выше, параметры smtpserver:port, username и password следует заменить соответствующими параметрами SMTP .

Образец сценария .bat для вызова сценария sendmail.py и передачи ему необходимых параметров: мы назвали этот файл **CustomMail.bat**:

```
c:\Python\python.exe c:\work\sendmail.py %1 %2
```

ПРИМЕЧАНИЕ. Для работы с этим образцом сценария нужно установить библиотеку Python на основном компьютере (на котором установлено решение ESA Core component) и знать путь к файлу python.exe.

В поле **Sending OTP by** (Путь отправки OTP) мы указываем путь, ведущий к нашему сценарию **CustomMail.bat**, выбираем необходимые параметры, например [E-mail-Addresses] (Адреса электронной почты) и [OTP], а затем щелкаем **Save** (Сохранить).

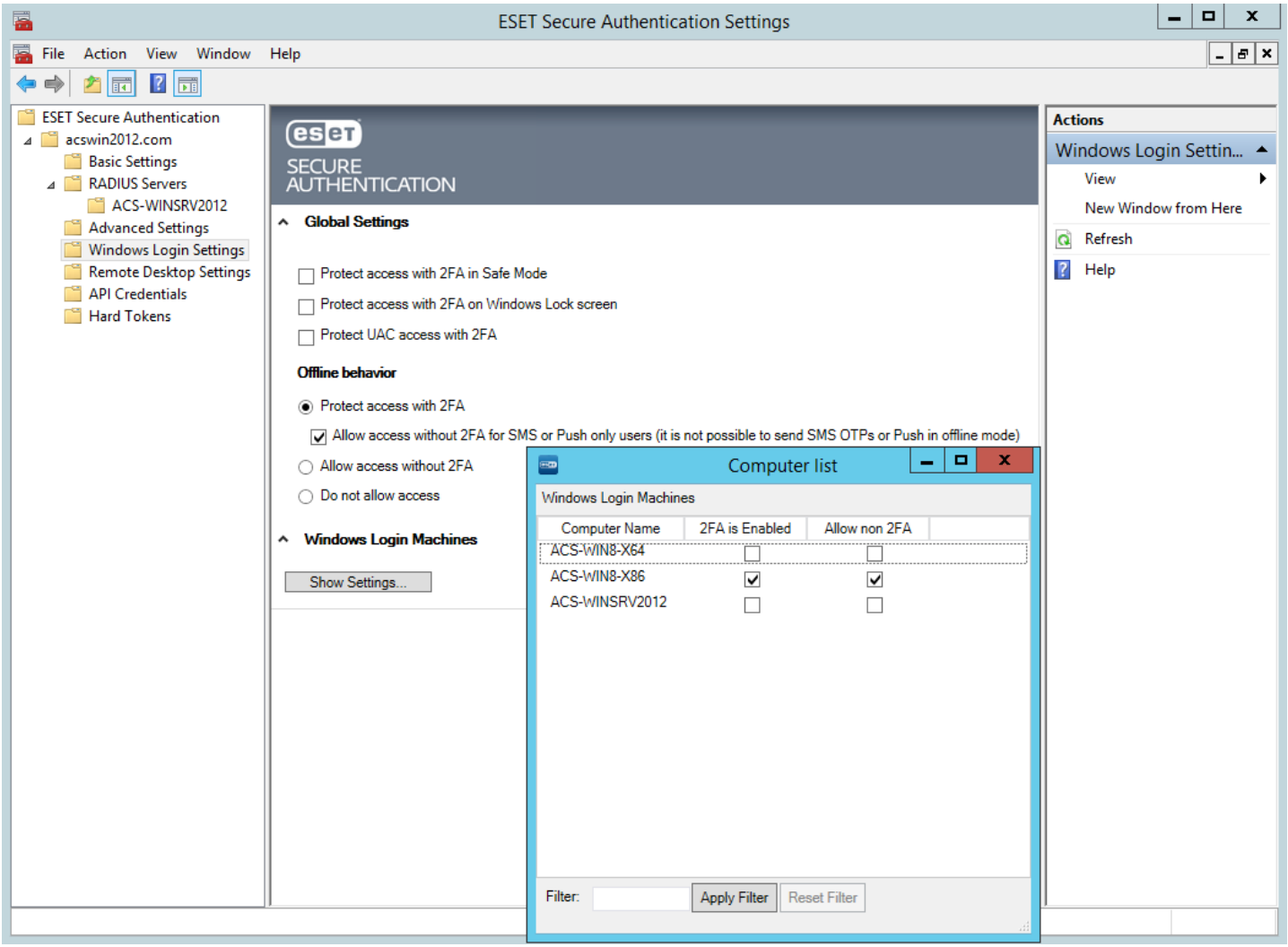


Подготовку (доставку мобильного приложения) можно настроить таким же образом с помощью необходимых параметров [PHONE] (Телефон) и [URL] (URL-адрес).

ПРИМЕЧАНИЕ.: По сравнению с доставкой SMS (или использованием подготовленного мобильного приложения) выполнять распределение паролей OTP с помощью электронной почты не так безопасно, так как электронное письмо можно прочитать на любом устройстве пользователя. С помощью этого метода нельзя подтвердить, что целевой получатель владеет зарегистрированным телефоном (номером телефона).

6. Защита входа в Windows

В ESA доступна защита локального входа в ОС Windows в доменной среде, установленной с помощью доменных служб Active Directory (Active Directory Domain Services). Чтобы использовать эту функцию, необходимо включить компонент **Windows Login** (Вход в Windows) во время установки ESA. По завершении установки откройте консоль управления ESA (ESA Management Console) на главном компьютере, перейдите в узел своего домена (в нашем примере — acswin2012.com) и щелкните **Windows Login Settings** (Параметры входа в Windows).



В этом окне вы увидите разные варианты применения двухфакторной аутентификации (2FA,), в том числе ее (2FA) применение для безопасного режима, экрана блокировки Windows и контроля учетных записей (UAC). Щелкните **Show Settings...** (Показать параметры), чтобы открыть список компьютеров, на которых установлен компонент **Windows Login** (Вход в Windows) решения ESA, и включить двухфакторную аутентификацию (2FA) для необходимых компьютеров. Если список компьютеров слишком длинный, введите в поле **Фильтр** имя конкретного компьютера, чтобы найти его.

Если компонент **Windows Login** (Вход в Windows) решения ESA версии 2.6 и выше удален с определенного компьютера, этот компьютер будет автоматически удален из раздела Computer list консоли управления ESA. В консоли управления также можно вручную удалить запись компьютера. Щелкните правой кнопкой мыши запись компьютера и нажмите **Delete Selected** (Удалить выбранные). Если запись компьютера удалена из консоли управления, но компонент **Windows Login** (Вход в Windows) не удален с конкретного компьютера, этот компьютер снова появится в консоли управления с настройками по умолчанию.

Если компьютер, на котором установлен компонент **Windows Login** (Вход в Windows) решения ESA, иногда должен работать в автономном режиме и на нем будут работать пользователи, для которых включена аутентификация с помощью SMS, вы можете включить параметр **Allow access without 2FA for SMS or Push only users** (Разрешить доступ без двухфакторной аутентификации для пользователей SMS, если компьютер в автономном режиме).

Если пользователь, использующий доставку одноразовых паролей (OTP) с помощью SMS-сообщений, хочет запросить повторную отправку одноразового пароля (OTP), ему нужно закрыть окно ввода одноразового пароля (OTP) и через 30 секунд ввести свои имя пользователя и пароль AD, чтобы получить новый одноразовый пароль (OTP).

Защиту, которую обеспечивает двухфакторная аутентификация (2FA), не может обойти ни один злоумышленник, даже если он знает имя пользователя и пароль AD, поэтому эта функция обеспечивает более надежную защиту конфиденциальных данных. Конечно, предполагается, что жесткий диск не доступен злоумышленникам или что содержимое диска зашифровано.

Рекомендуем сочетать защиту 2FA с шифрованием всего диска, чтобы уменьшить риск нарушения конфиденциальности, если злоумышленник получит физический доступ к диску.

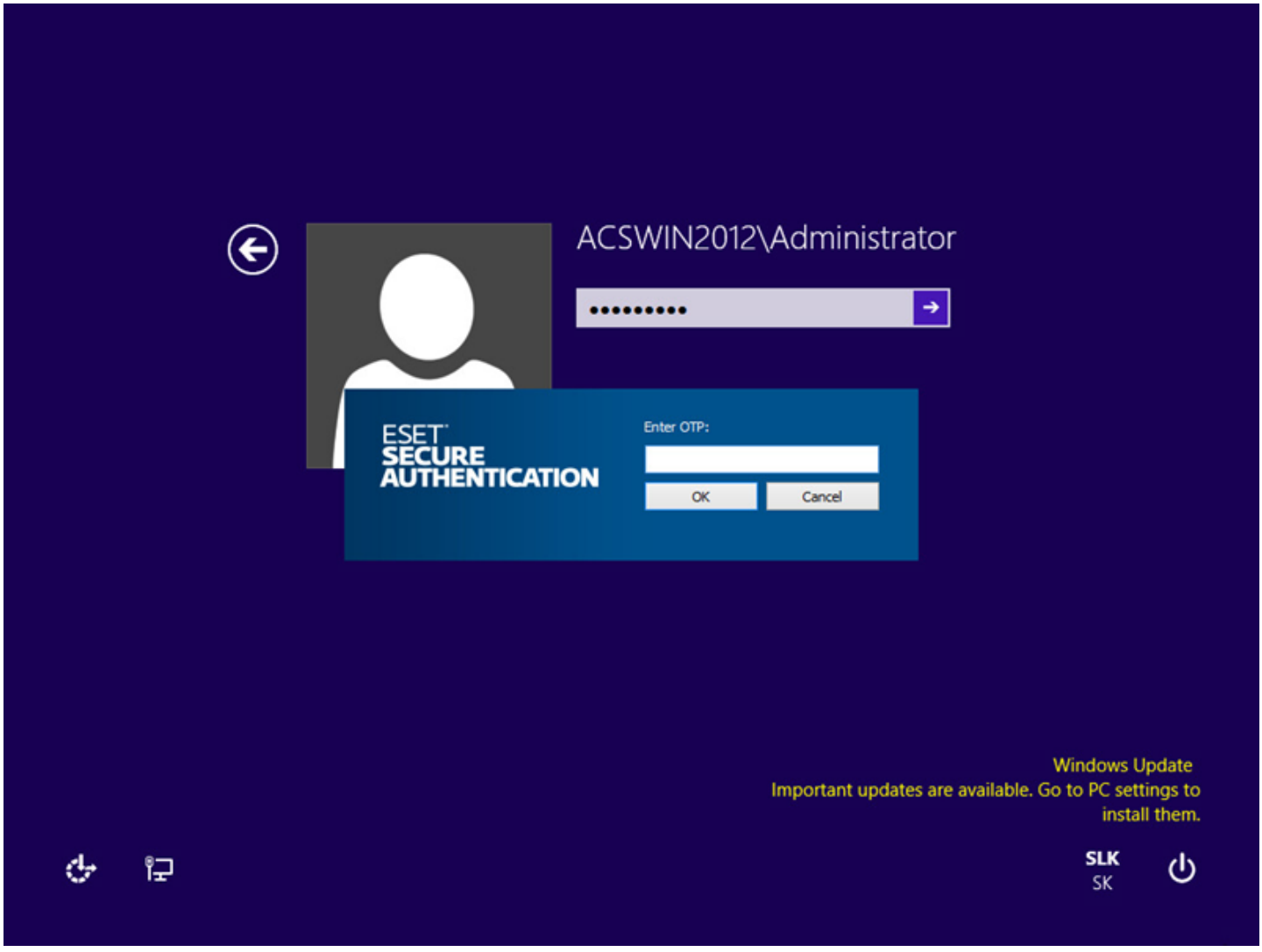
ПРИМЕЧАНИЕ. Если защита 2FA включена для автономного режима, все пользователи, учетные записи которых защищены с помощью метода 2FA и которые хотят использовать компьютер, защищенный с помощью 2FA, должны ввести имя пользователя и пароль только при первом входе на этот компьютер, когда он подключен к сети. Терминonlineозначает, что главный компьютер, на котором установлены ключевые компоненты службы ESA и на котором работает служба *ESET Secure Authentication Service* отвечает на запросы проверки связи, отправляемые с компьютера, защищенного с помощью метода 2FA.

Если компонент Windows Login установлен на том же компьютере, на котором установлены ключевые компоненты ESA Core Components и для безопасного режима на этом компьютере включена защита 2FA , а автономный режим для этого компьютера выключен (выбран параметр*Do not allow access when offline* (Не разрешать доступ в автономном режиме)), пользователь сможет войти в безопасном режиме (локально) без ввода пароля OTP.

В автономном режиме можно войти в систему 20 раз, используя каждый раз действительный пароль OTP. Если это ограничение превышено, компьютер должен быть подключен к сети во время попытки входа на него. Если компьютер подключен к сети во время попытки входа, счетчик ограничения сбрасывается.

Чтобы разрешить конкретным пользователям входить только на конкретные компьютеры, настройте политику Запретить вход локально.

Вход в Windows 8, защищенный с помощью решения ESA, — после ввода правильных имени пользователя и пароля AD пользователи должны ввести одноразовый пароль (OTP).



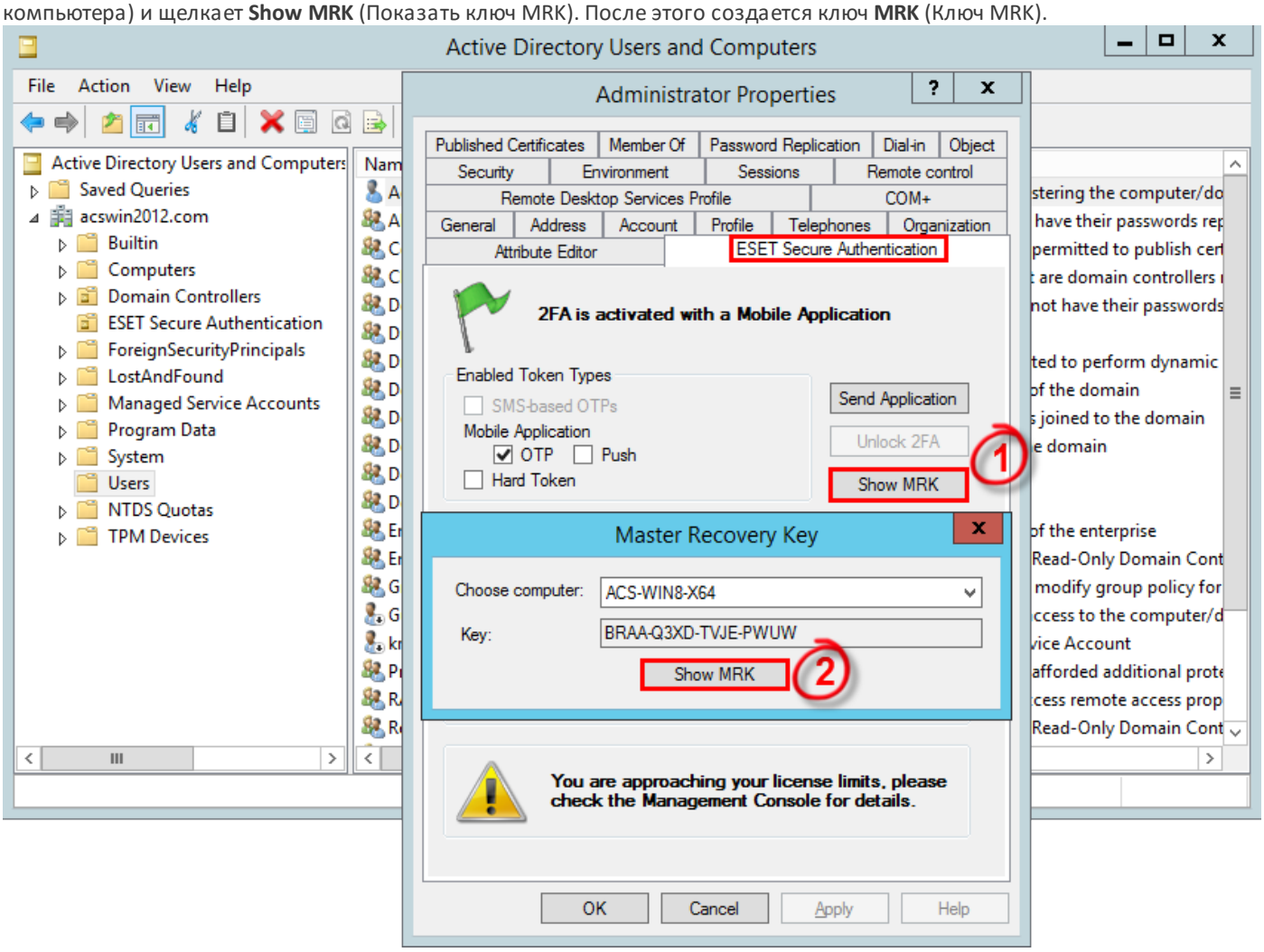
6.1 Главный ключ восстановления

Главный ключ восстановления (MRK) — это альтернативный пароль OTP, с помощью которого можно войти в компьютер под управлением Windows, защищенный двухфакторной аутентификацией (2FA), в ситуациях, когда пользователь не может ввести правильный пароль OTP. Например, пользователь потерял телефон, на котором установлено мобильное приложение ESA. Ключ MRK является уникальным для пользователя и компьютера, то есть у пользователей User1 и User2 будут разные ключи MRK для компьютера PC1. Доступ с помощью MRK возможен как при подключении к Интернету, так и в автономном режиме. Автономное использование MRK доступно, только если автономный режим для данного компьютера включен в консоли управления ESA (ESA Management Console) в разделе Параметры входа в Windows. Если включен автономный режим, ключ MRK хранится также локально на компьютере в зашифрованном и защищенном кэше.

Можно использовать ключ MRK версии 2.6 и выше для других модулей защиты ESA.

Использование ключа MRK для аутентификации:

1. Пользователь не может получить одноразовый пароль OTP и обращается к администратору.
2. Администратор открывает ADUC, переходит к соответствующему имени домена Active Directory (в нашем примере — *acswin2012.com*), выбирает **Users** (Пользователи), дважды щелкает имя конкретного пользователя, выбирает вкладку **ESET Secure Authentication**, нажимает кнопку **Show MRK** (Показать ключ MRK), выбирает конкретный модуль защиты из списка **Choose component** (Выбор компонента), затем выбирает конкретный компьютер из списка **Choose computer** (Выбор компьютера) и щелкает **Show MRK** (Показать ключ MRK). После этого создается ключ **MRK** (Ключ MRK).



3. Администратор предоставляет полученный ключ MRK пользователю, который сможет использовать для входа ключ MRK вместо пароля OTP.

Когда компьютер находится в автономном режиме, ключ MRK можно использовать для входа на конкретный Windows-компьютер несколько раз.

После первого успешного подключения к ядру ESA созданный ранее ключ MRK становится недействительным и больше не может использоваться, даже если он еще ни разу не использовался.

Ключ MRK, созданный для других модулей защиты ESA, имеет срок действия не более 1 часа или до повторного создания.

7. Защита VPN

Система ESA поставляется с отдельным сервером RADIUS, который используется для аутентификации подключений к VPN. После установки сервера ESA RADIUS служба запустится автоматически. Убедитесь, что она запущена. Для этого проверьте ее статус в консоли служб Windows.

Хотя служба ESA RADIUS используется в большинстве конфигураций, не обязательно использовать исключительно ее для защиты VPN. Дополнительные сведения см. в разделе Модули PAM RADIUS в Linux/Mac.

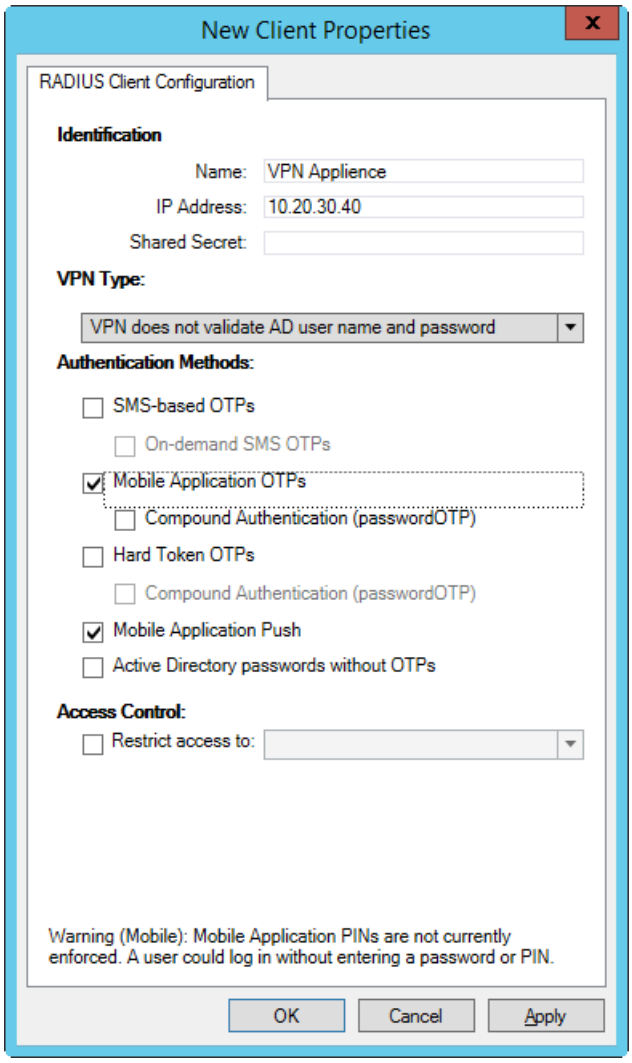
7.1 Настройка

Чтобы настроить двухфакторную аутентификацию (2FA) для сети VPN, устройство VPN сначала нужно добавить в качестве клиента RADIUS. Для этого выполните следующие действия:

1. В ESA Management Console выберите **RADIUS Servers** (Серверы RADIUS), затем имя домена Active Directory, щелкните пустую область правой кнопкой мыши и выберите **Add Client** (Добавить клиент).
2. Выберите новый клиент и выберите в списке доступных действий **Properties** (Свойства).
3. Присвойте клиенту RADIUS запоминающееся имя.
4. Настройте для Client IP Address и **Shared Secret** (Общий секрет). Они должны соответствовать конфигурации устройства VPN. IP-адрес — это внутренний IP-адрес устройства. Общий секрет — это общий секрет RADIUS для внешнего аутентификатора, который вы будете настраивать на устройстве.
5. В качестве метода аутентификации выберите «Mobile Application». Оптимальный метод аутентификации зависит от марки и модели устройства VPN. Дополнительные сведения см. в соответствующем ESA VPN Integration Guide. Руководства по интеграции VPN доступны в базе знаний ESET.
6. При необходимости можно разрешить всем пользователям, у которых не включена двухфакторная аутентификация (non-2FA), использовать VPN.

ПРИМЕЧАНИЕ. Если для ограничения доступа не использовать группы безопасности и разрешить пользователям non-2FA входить в VPN, все пользователи в домене смогут входить в систему через VPN. Использовать такую конфигурацию не рекомендуется.

7. При желании предоставьте доступ к VPN только существующей группе безопасности Active Directory.
8. После внесения всех изменений нажмите кнопку **OK**.
9. Перезапустите сервер RADIUS .
    a. Найдите ESA RADIUS Service в службах Windows. Для этого последовательно щелкните **Control Panel** (Панель управления) - **Administrative Tools** (Администрирование) - **View Local Services** (Просмотр локальных служб).
    b. Щелкните службу ESA Radius Service правой кнопкой мыши и выберите пункт **Restart** (Перезапустить) from the context menu.



ПРИМЕЧАНИЕ.: Если метод аутентификации Mobile Application Push (Push-уведомления в мобильном приложении) включен, задайте срок действия аутентификации VPN-сервера больше 2,5 минут.

Доступны указанные ниже варианты типа VPN (**VPN Type**):

- **VPN does not validate AD user name and password**
- **VPN validates AD user name and password**
- **Use Access-Challenge feature of RADIUS**

Следующие клиенты RADIUS поддерживают функцию запроса доступа RADIUS:

- Junos Pulse (VPN)
- модуль Linux PAM.

Следующие клиенты RADIUS не следует использовать с функцией запроса доступа:

- Microsoft RRAS.

Если в вашем клиенте VPN требуется, чтобы атрибут Filter-Id отправлялся сервером ESA RADIUS, необходимо в файле *C:\Program Files\ESET Secure Authentication\EIP.Radius.WindowsService.exe.config* добавить фрагмент кода, аналогичный следующему:

```
<appSettings>
    <add key="RadiusFilterIdValue" value="any_value_expected_by_your_VPN_server" />
</appSettings>
```

Если тег `<appSettings>` уже присутствует, не копируйте его, а просто добавьте код `<add key.... >` под ним.

7.2 Использование

После конфигурации клиента RADIUS, прежде чем менять конфигурацию устройства VPN, рекомендуется проверить возможность подключения к RADIUS с помощью служебной программы тестирования, например NTRadPing. После проверки возможности подключения к RADIUS вы можете настроить в устройстве использование сервера ESA RADIUS в качестве внешнего аутентификатора пользователей VPN.

Поскольку оптимальные метод аутентификации и использование зависят от марки и модели устройства, ознакомьтесь с руководством по интеграции ESET Secure Authentication и VPN в базе знаний ESET.

8. Модули PAM RADIUS в Linux/Mac

Компьютеры под управлением Linux/Mac могут использовать ESA для двухфакторной аутентификации (2FA), применяя модуль Pluggable Authentication Module (PAM), который будет выполнять функцию клиента RADIUS, обменивающегося данными с сервером ESA RADIUS.

В целом любую службу, использующую RADIUS, можно настроить на использование сервера ESA RADIUS.

PAM — это набор динамических библиотек C (.so), которые используются для добавления пользовательских уровней в процесс проверки подлинности. Они могут выполнять дополнительные проверки, а затем разрешить или запретить доступ. В этом случае мы используем модуль PAM, который запрашивает у пользователя пароль OTP на компьютере под управлением Linux или Mac, присоединенном к домену Active Directory, и сравнивает этот пароль OTP с данными на сервере ESA RADIUS.

В этом руководстве компонент FreeRADIUS использует модуль проверки подлинности и учета The PAM. Вы можете также использовать другие клиенты RADIUS PAM.

Основная конфигурация, описанная здесь, использует функцию запроса доступа (Access-Challenge) RADIUS, которую поддерживают и сервер ESA RADIUS, и используемый клиент RADIUS PAM. Существуют другие конфигурации, которые не используют метод запроса доступа. См. их краткое описание в разделе Другие конфигурации RADIUS этого руководства.

Сначала настройте клиент Linux/Mac RADIUS в ESA Management Console. Type the IP address of your Linux/Mac computer. Введите IP-адрес своего компьютера под управлением Linux/Mac в поле **IP Address** (IP-адрес). Выберите параметр **Use Access-Challenge feature of RADIUS** f (Использовать функцию запроса доступа RADIUS) в раскрывающемся меню **VPN Type** drop-down menu (Тип VPN).

Выполнив эти действия, настройте свой компьютер под управлением Linux или Mac, следуя инструкциям в следующих подразделах.

8.1 Mac OS — конфигурация

Описанные ниже действия были выполнены в ОС OS X - Yosemite 10.10.5.

Примечание. Если вы включите защиту 2FA с помощью инструкций из этого руководства, то по умолчанию не принадлежащие к вашему домену AD локальные пользователи не смогут выполнить вход. Чтобы разрешить вход для локальных пользователей в случаях, когда защита 2FA включена, выполните дополнительные действия, описанные в разделе *Другие конфигурации RADIUS* — см. раздел *Пользователи без двухфакторной аутентификации (учетные записи пользователей, в которых не используется двухфакторная аутентификация)*.

Чтобы развернуть двухфакторную аутентификацию (2FA) на компьютере Mac, убедитесь, что ваш компьютер добавлен в домен Active Directory. Вы можете настроить его в разделе *Системные настройки… > Пользователи и группы > Параметры входа*. Щелкните *Присоединить…* рядом с элементом *Сервер сетевых учетных записей* и введите свои учетные данные для Active Directory.

Модуль аутентификации PAM

1. Загрузите PAM RADIUS tar.gz со страницы http://freeradius.org/pam_radius_auth/.
2. Создайте библиотеку в формате SO, выполнив следующие команды в окне терминала:

   ```
   ./configure
   make
   ```

3. Скопируйте созданную библиотеку в модули PAM.

   ```
   cp pam_radius_auth.so /usr/lib/pam
   ```

В ОС OS X El Capitan и более поздних версиях это расположение защищено с помощью компонента System Integrity Protection (Защита целостности системы). Чтобы использовать его, необходимо отключить его для команды копирования.

4. Создайте файл конфигурации сервера с именем *server* в папке */etc/raddb/*. В этом файле введите данные сервера RADIUS в следующем формате:
   `<radius сервер>:<порт> <общий секрет> <время ожидания в секундах>`

   Например,
   1.1.1.1 test 30

Рекомендации по безопасности для файла конфигурации см. в разделе УСТАНОВКА, а параметры, которые можно передать в библиотеку, — в разделе ИСПОЛЬЗОВАНИЕ. Например, для выявления потенциальных проблем можно использовать параметр debug.

Включение модуля PAM

Модули PAM можно включать в процессы входа различных типов, например login, sshd, su, sudo и т. д. Список типов входа доступен в каталоге */etc/pam.d/*.

Измените соответствующий файл в каталоге */etc/pam.d/*, чтобы включить модуль PAMRADIUS в те или иные типы входа.

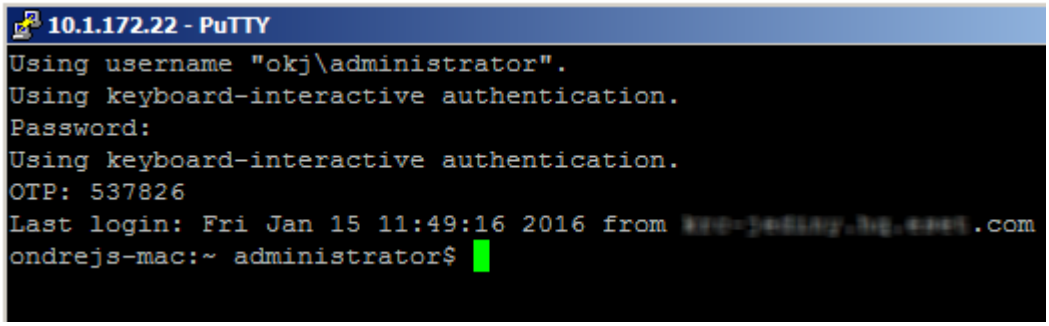
Включение модуля PAM в SSH

Чтобы включить модуль PAM в SSH, измените файл /etc/pam.d/sshd и добавьте в конец этого файла следующую строку:

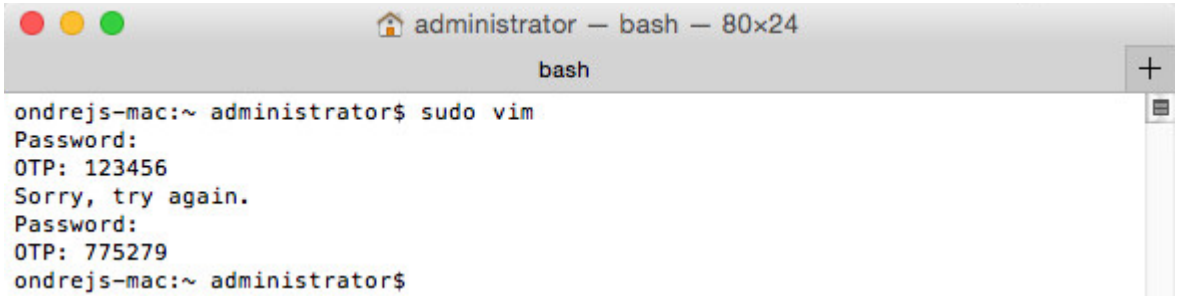
```
auth required /usr/lib/pam/pam_radius_auth.so
```

Затем активируйте SSH в OS X. В разделе *Системные настройки… > Общий доступ* включите параметр **Удаленный вход**.

Ниже приведен пример входа в SSH с помощью решения ESA (модуля PAM, включенного в файл /etc/pam.d/sshd).



Ниже приведен пример входа в sudo с помощью решения ESA (модуля PAM, включенного в файл /etc/pam.d/sudo).

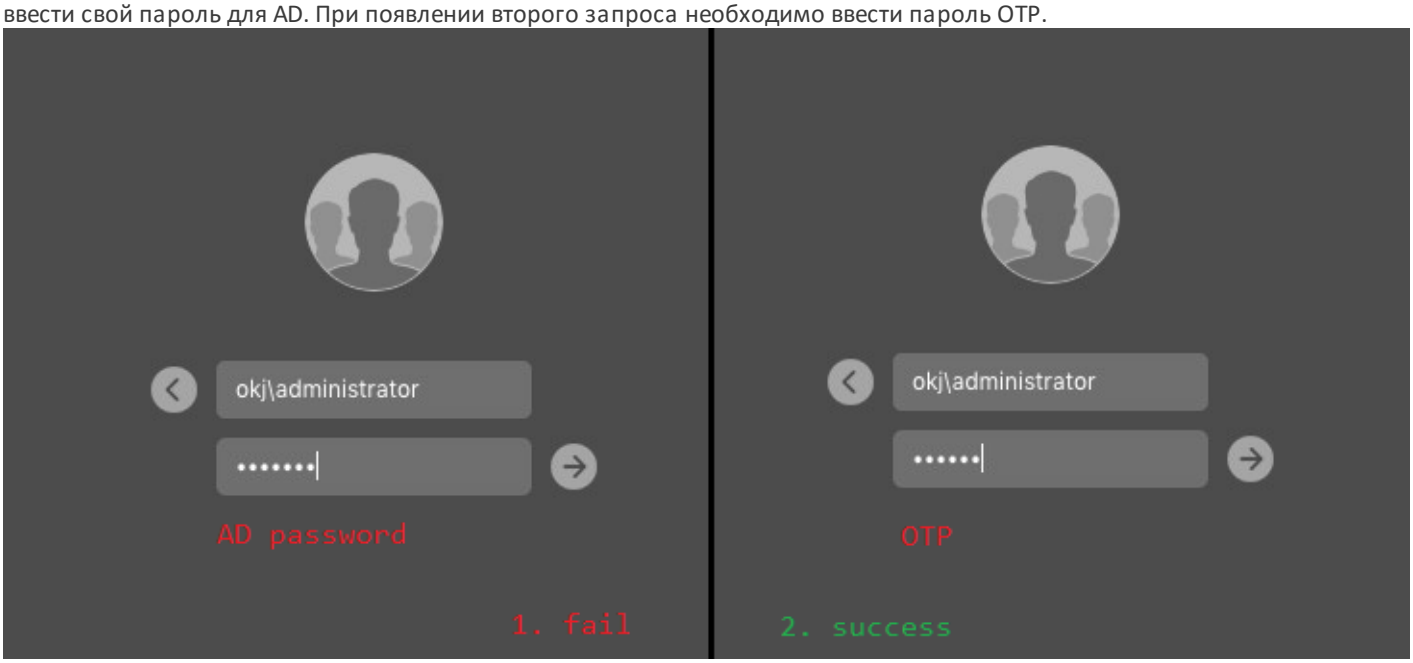


Включение модуля PAM в процесс входа в настольный компьютер

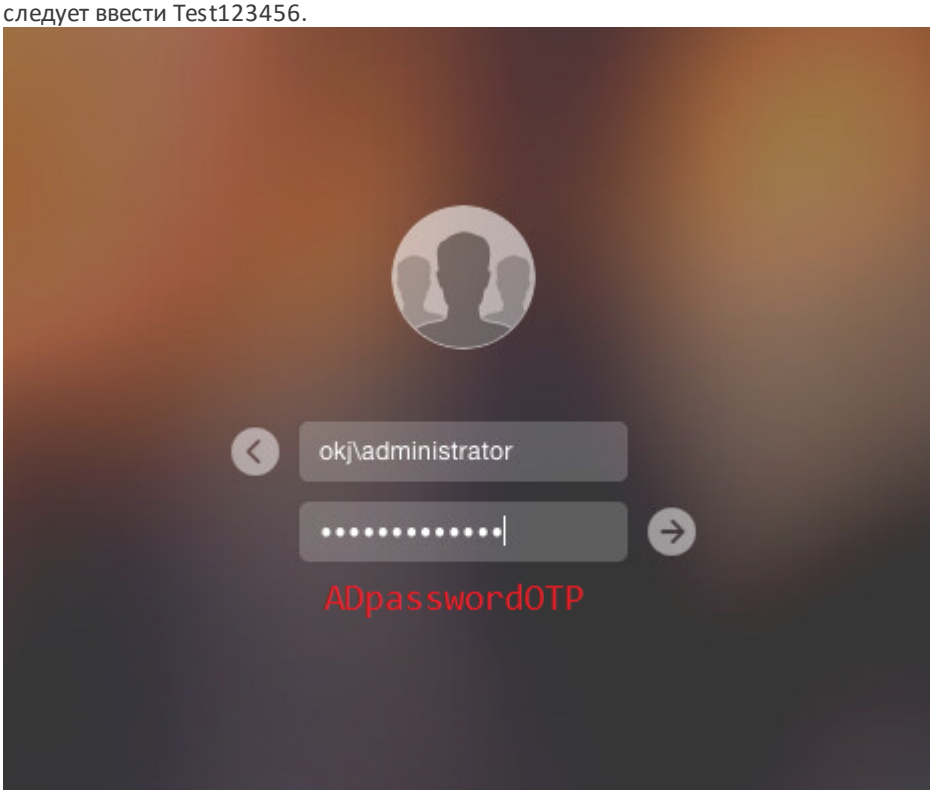
Для входа в настольный компьютер нельзя использовать запрос доступа Radius (RADIUS Accept-Challenge) подобно типу VPN (VPN Type) при настройке клиента RADIUS в средстве управления ESA (ESA Management Tool). Конфигурация клиента RADIUS должна быть такой, как показано в разделе **VPN Type - VPN does not validate AD username and password** (Тип VPN — VPN не проверяет имя пользователя и пароль AD) главы Другие конфигурации RADIUS, а модуль PAM должен быть включен в файл */etc/pam.d/authorization*.

Используйте следующие параметры:

- Пароль OTP (OTP is) доставляется с помощью SMS — при появлении первого запроса на ввод пароля пользователь должен ввести свой пароль для AD. При появлении второго запроса необходимо ввести пароль OTP.



- Одноразовый пароль OTP другого типа (сложная аутентификация) — введите пароль для AD и одноразовый пароль OTP одновременно в формате ADpasswordOTP. Например, если ваш пароль для AD — Test, а полученный пароль OTP — 123456, следует ввести Test123456.



8.2 Linux — конфигурация

Действия, описанные здесь, были выполнены в выпуске OpenSUSE Leap 42.1.

Примечание. Если вы включите защиту 2FA с помощью инструкций из этого руководства, то по умолчанию не принадлежащие к вашему домену AD локальные пользователи не смогут выполнить вход. Чтобы разрешить вход для локальных пользователей в случаях, когда защита 2FA включена, выполните дополнительные действия, описанные в разделе Другие конфигурации RADIUS — см. раздел *Пользователи без двухфакторной аутентификации (учетные записи пользователей, в которых не используется двухфакторная аутентификация)*.

Убедитесь, что ваш компьютер под управлением Linux присоединен к домену Active Directory. Перейдите в раздел *YaST > Оборудование > Параметры сети > Имя хоста/DNS* и введите IP-адрес компьютера Domain Controller (DC, контроллер домена) и имя домена Active Directory. Затем перейдите в раздел *YaST > Сетевые службы > Членство в домене Windows*.

Введите имя домена *AD*, к которому следует присоединить компьютер под управлением Linux, в поле *Домен или рабочая группа* и нажмите кнопку *ОК*. Появится запрос на ввод имени пользователя и пароля администратора домена.

ПРИМЕЧАНИЕ. Процесс присоединения к домену отличается в разных дистрибутивах Linux.

PAM Модуль аутентификации

1. Загрузите PAM RADIUS tar.gz со страницы http://freeradius.org/pam_radius_auth/.
2. Создайте библиотеку в формате SO (.so), выполнив следующие команды в окне терминала:

   ```
   ./configure
   make
   ```

   В зависимости от результатов выполнения команды `configure` может потребоваться установить зависимости.

   ```
   sudo zypper install gcc make pam-devel
   ```

3. Скопируйте созданную библиотеку в модули PAM.

   ```
   sudo cp pam_radius_auth.so /lib/security/
   ```

4. Создайте в папке */etc/raddb/* файл конфигурации сервера с именем *server.* В этом файле введите данные сервера RADIUS в следующем формате:
   `<radius сервер>:<порт> <общий секрет> <время ожидания в секундах>`

   Например,
   1.1.1.1 test 30

Рекомендации по безопасности для файла конфигурации см. в разделе УСТАНОВКА, а параметры, которые можно передать в библиотеку, — в разделе ИСПОЛЬЗОВАНИЕ. Например, для выявления потенциальных проблем можно использовать параметр debug.

Включение модуля PAM

Модули PAM могут отличаться в зависимости от дистрибутива Linux. Сценарии включения также зависят от среды настольного ПК, используемой на конкретном компьютере под управлением Linux. В этом примере среда Xfce используется на компьютере под управлением OpenSUSE, поэтому модуль PAM включен в каталог */etc/pam.d/xdm* (см. примеры ниже). Возможно, некоторые модули не будут запрашивать второй фактор, как показано в примере ниже.

Включение модуля PAM в SSH в Linux выполняется так же, как и в Mac OS, — см.Включение модуля PAM в SSH в Mac OS (раздел о конфигурации). Однако строка кода, которую следует добавить в файл /etc/pam.d/sshd, отличается:

```
auth required /lib/security/pam_radius_auth.so
```

Включение модуля PAM в процесс входа в консоль

Чтобы включить модуль PAM в процесс входа в консоль, измените файл */etc/pam.d/login* и добавьте в конец этого файла следующую строку:

```
auth required /lib/security/pam_radius_auth.so
```

Ниже приведен пример входа в консоль с защитой посредством решения ESA .

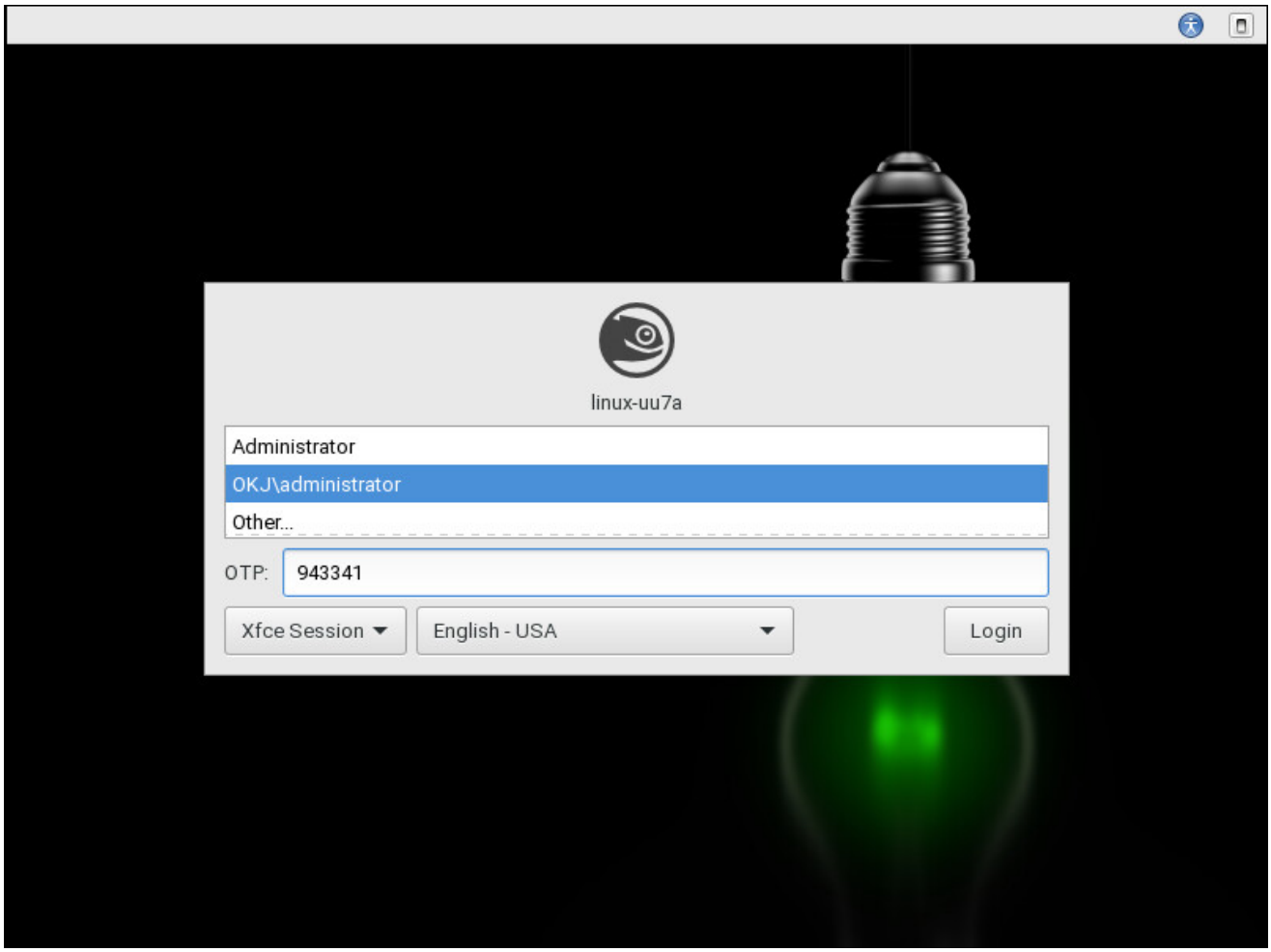
```
[    2.552437] sd 0:0:0:0: [sda] Assuming drive cache: write through
[    8.922390] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!

Welcome to openSUSE Leap 42.1 - Kernel 4.1.13-5-default (tty1).


linux-uu7a login: okj\administrator
Password:
OTP: 421219
Last login: Mon Jan 18 09:34:43 from console
Have a lot of fun...
OKJ\administrator@linux-uu7a:~> _
```

Включение модуля PAM в процесс входа Xfce в настольный компьютер

Чтобы включить модуль PAM в процесс входа в Xfce настольный компьютер, необходимо изменить файл */etc/pam.d/xdm* и добавить в его конец следующую строку:

```
auth required /lib/security/pam_radius_auth.so
```

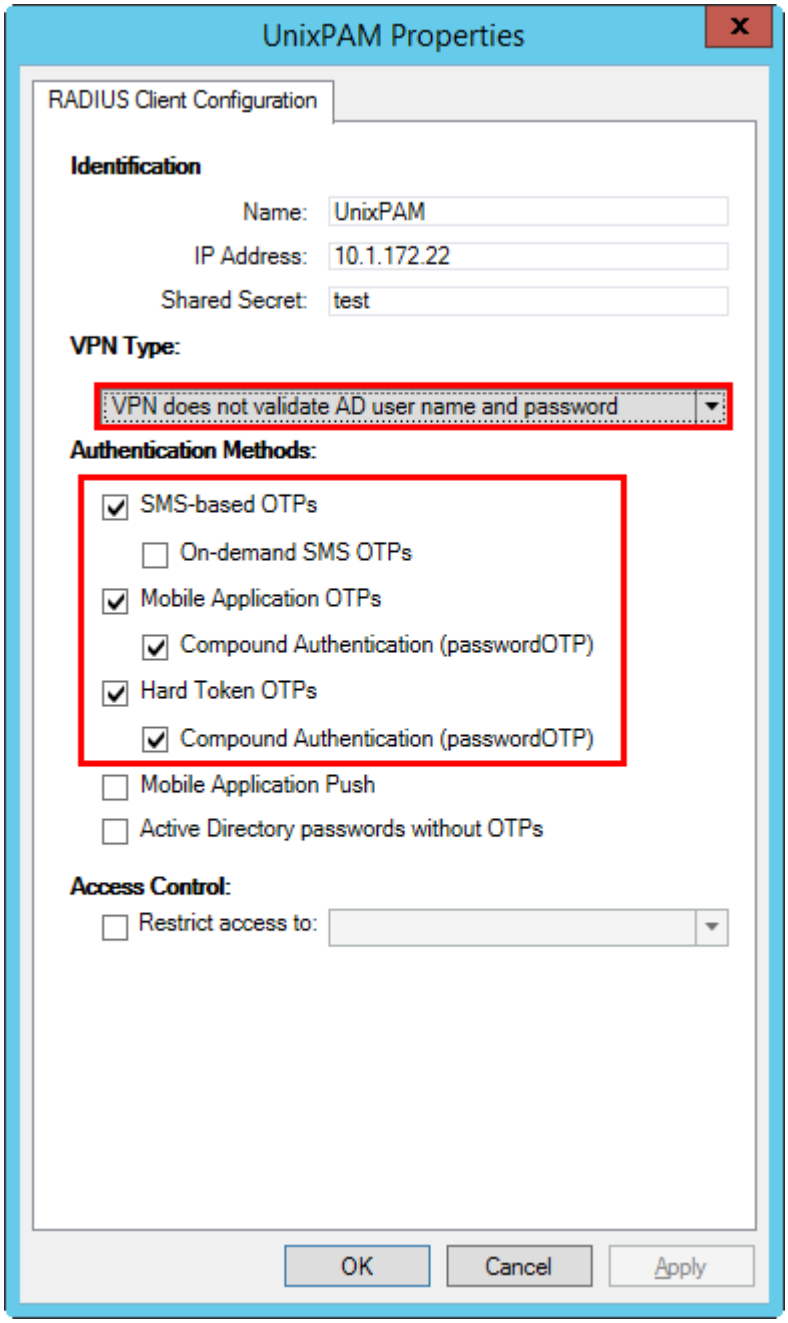
Ниже приведен пример входа в настольный компьютер Xfce с защитой посредством решения ESA.



8.3 Другие конфигурации RADIUS

VPN Type - VPN does not validate AD username and password

Если во время настройки клиента RADIUS в средстве управления ESA (ESA Management Tool) вы укажете для параметра **VPN Type** (Тип VPN) значение **VPN does not validate AD username and password** (VPN не проверяет имя пользователя и пароль AD), решение ESA будет проверять оба фактора (имя пользователя AD в качестве первого фактора и пароль OTP в качестве второго фактора).



Затем в **/etc/pam.d/sshd** (или другой интеграции) добавьте строку

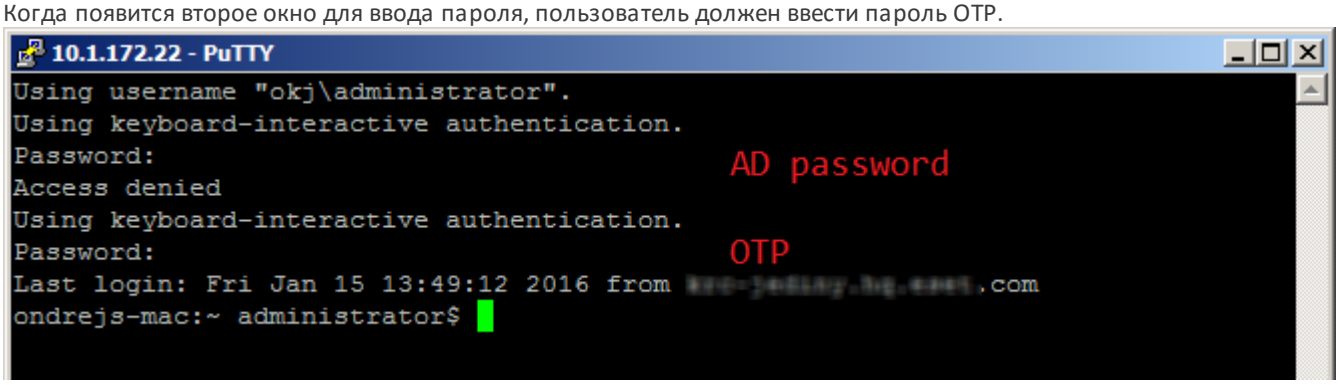
```
auth required /usr/lib/pam/pam_radius_auth.so
```

и закомментируйте (поместите тег # вначале) все остальные строки `auth`.

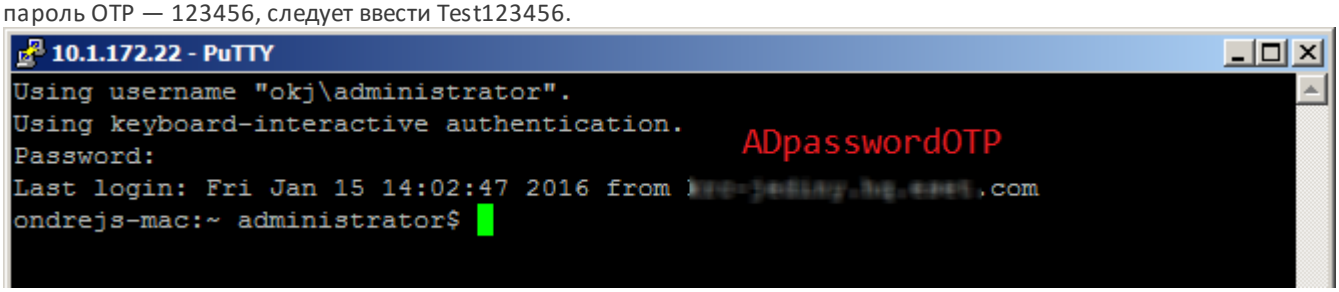
ПРИМЕЧАНИЕ. Администратор домена должен проверить, подходит ли этот сценарий, который отключает все остальные модули, для развертывания.

В этом случае вход в SSH будет выполняться, как описано ниже.

- Доставка SMS с паролем OTP — когда появится первый запрос на ввод пароля, пользователь должен ввести пароль AD. Когда появится второе окно для ввода пароля, пользователь должен ввести пароль OTP.

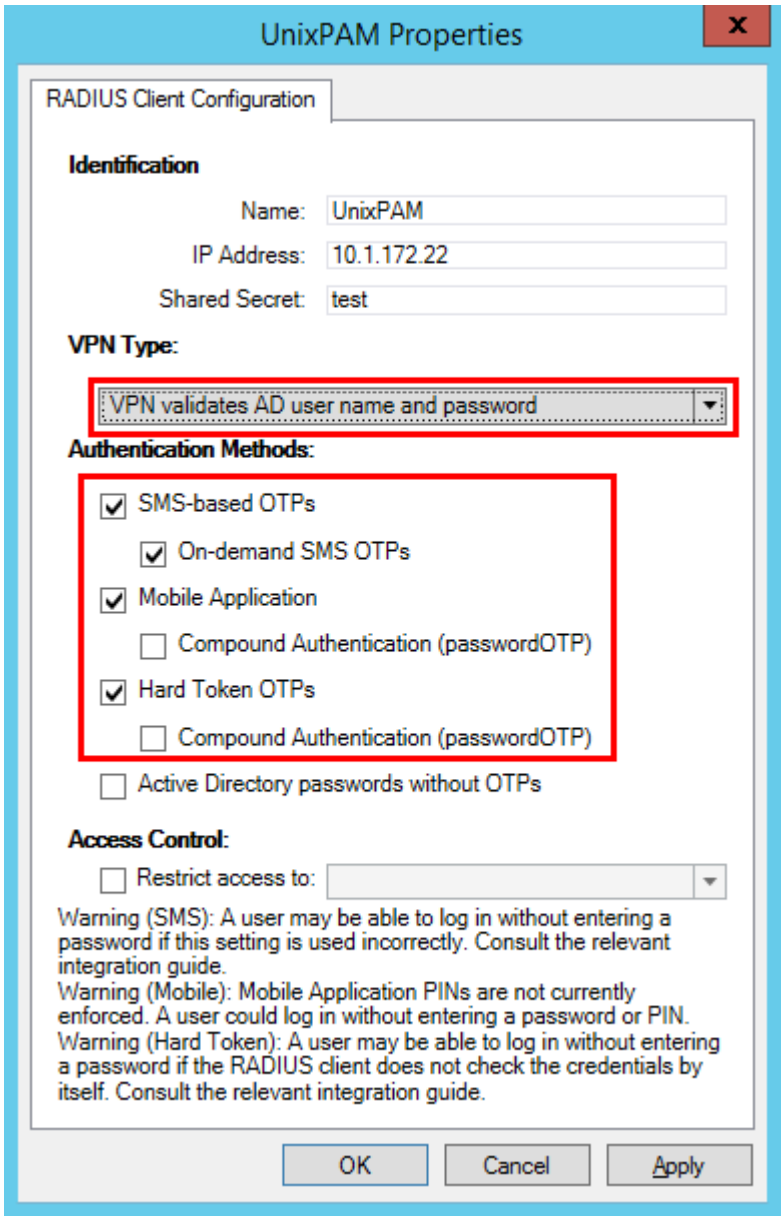


- Другой тип одноразового пароля OTP (сложная аутентификация) — пользователь должен ввести одновременно и пароль AD, и одноразовый пароль OTP в качестве ADpasswordOTP. Например, если ваш пароль для AD — Test, а полученный пароль OTP — 123456, следует ввести Test123456.



Тип VPN — VPN проверяет имя пользователя и пароль AD

Если во время настройки клиента RADIUS в средстве управления ESA (ESA Management Tool) вы укажете для параметра **VPN Type** (Тип VPN) значение **VPN validates AD username and password** (VPN проверяет имя пользователя и пароль AD), первый фактор (имя пользователя и пароль AD) будет проверяться другим модулем PAM.



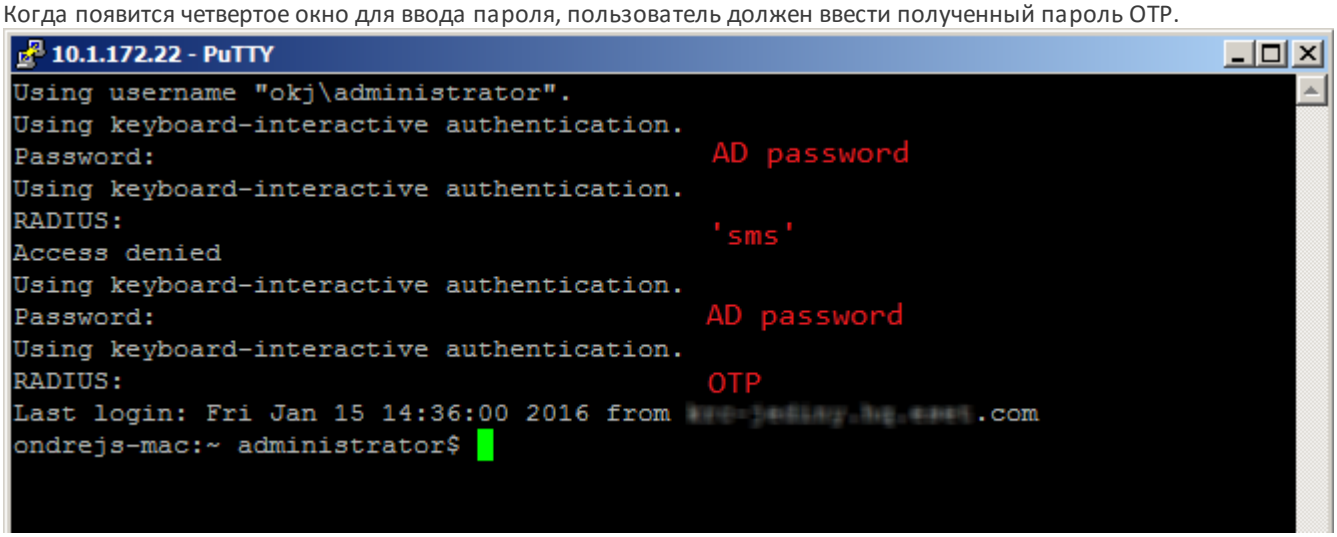
Если вы настраиваете RADIUS таким образом, добавьте следующую строку в **/etc/pam.d/sshd** (или соответствующую интеграцию):

```
auth required /usr/lib/pam/pam_radius_auth.so force_prompt prompt=RADIUS
```

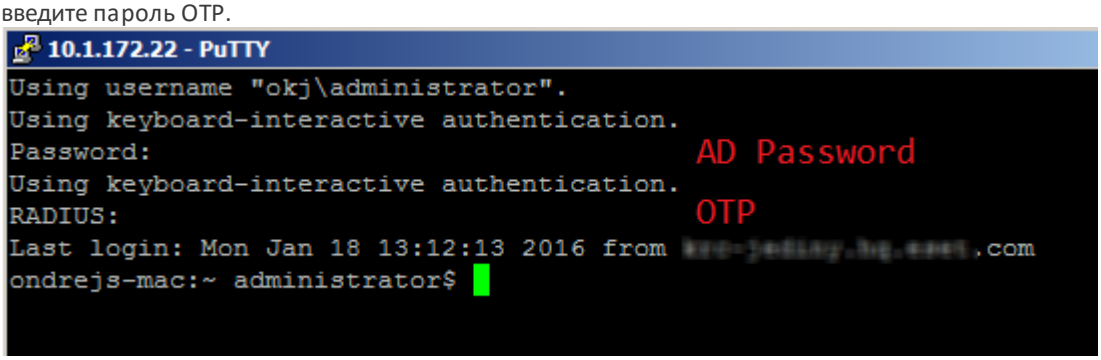
В этом случае вход в SSH будет выполняться, как описано ниже.

- Запросы, которые начинаются со строки **Password:**, будут обрабатываться другими модулями PAM. Запросы, которые начинаются со строки **RADIUS:**, будут обрабатываться нашим модулем PAM. См. аргумент **prompt=RADIUS** в примере кода ниже.
- SMS — во время первого запроса пользователь должен ввести свой пароль AD. Во время второго запроса пользователь должен ввести текст **sms** (без кавычек). Когда появится третье окно запроса, пользователь должен ввести свой пароль AD.

Когда появится четвертое окно для ввода пароля, пользователь должен ввести полученный пароль OTP.



- Другой тип пароля OTP (пароль OTP, полученный с помощью мобильного приложения или маркера оборудования (hard token)) — введите пароль AD, когда появится первый запрос на ввод пароля. Когда появится второе окно для ввода пароля, введите пароль OTP.



Non-2FA Пользователи (учетные записи пользователей, в которых не используется двухфакторная аутентификация)

Во время настройки модуля PAM для ESA не забудьте создать процедуру входа для пользователей, которые не используют двухфакторную аутентификацию (non-2FA), например локальных пользователей Linux или Mac, а не пользователей домена.

Linux

Используя эту конфигурацию, сервер RADIUS не сможет аутентифицировать локальных пользователей, пока вы не добавите следующий код (или соответствующий код для вашей системы) в файл */etc/pam.d/sshd* (или соответствующий файл для вашего модуля PAM):

```
auth sufficient pam_unix.so try_first_pass
```

После этого изменения для входа будет достаточно аутентификации Unix, поэтому любой локальный пользователь сможет войти в систему после ввода локального пароля. Чтобы разрешить вход пользователям домена, учетные записи которых не защищены двухфакторной аутентификацией (2FA), включите параметр **Active Directory Passwords without OTPs** (Пароли Active Directory без одноразовых паролей) во время настройки клиента RADIUS в консоли управления ESA (ESA Management Console).

Mac

В отличие от ОС Linux, для ОС Mac нет стандартного модуля PAM, который выполняет аутентификацию локальных пользователей (см. выше). Поэтому для аутентификации нужно использовать другой модуль PAM. В этом руководстве мы решили загрузить коллекцию модулей для PAM, а затем собрать модуль, запустив следующие команды в окне терминала:

```
./configure --disable-pgsql --disable-mysql --disable-ldaphome
make
make install
```

Следующие шаги зависят от того, как будет использоваться интеграция двухфакторной аутентификации (2FA): для входа на компьютер или для входа в другие системы (например, ssh).

Интеграция для входа в другие системы Mac:

- в файле конкретной интеграции /etc/pam.d/ добавьте следующую строку перед pam_radius_auth.so:

```
auth sufficient /usr/local/lib/security/pam_regex.so sense=allow regex=^user$
```

В этой строке **user** — это локальное имя пользователя (**username**), которому мы хотим разрешить вход без ввода пароля OTP.

- Не забудьте определить модули Mac (которые мы не добавляли) как required (обязательные) или requisite (базовые), чтобы добавленный модуль sufficient (достаточный) не позволил пользователю войти, если он введет неправильный первый фактор.
- Вы также можете использовать все модули, кроме pam_regex, из коллекции модулей для PAM. Например, вы можете использовать модуль pam_groupmember, чтобы разрешить вход группам пользователей вместо одиночных пользователей.

Интеграция для входа в компьютер Mac.

- Измените файл /etc/pam.d/authorization, чтобы он выглядел так:

```
# authorization: auth account
auth     sufficient /usr/lib/pam/pam_radius_auth.so
auth     requisite /usr/local/lib/security/pam_regex.so sense=allow regex=^user$
auth        optional       pam_krb5.so use_first_pass use_kcminit
auth        optional       pam_ntlm.so use_first_pass
auth        required       pam_opendirectory.so use_first_pass nullok
account     required       pam_opendirectory.so
```

Последствия этих изменений.

1. Наш модуль RADIUS PAM будет первым в списке и будет определен как sufficient (достаточный).
2. Наш модуль regex PAM будет вторым в списке и будет определен как requisite (базовый).
3. Остальные модули в файле будут следовать за ними.

9. Защита веб-приложений

Модуль ESA Web Application Protection автоматически добавляет 2FA в процесс аутентификации всех поддерживаемых Web Applications. После установки ESA модуль загрузиться при следующей попытке доступа к защищенному Web Application.

Пользователи будут входить, используя обычный процесс аутентификации для Web Application. Когда аутентификация в Web Application пройдена, пользователь перенаправляется на веб-страницу ESA, на которой появляется запрос на ввод OTP или утверждение push-уведомления. Доступ к веб-приложению (Web Application) будет предоставлен только после ввода действительного одноразового пароля (OTP) или подтверждения push-уведомления.

Сеанс 2FA будет оставаться активным, пока пользователь не выйдет из Web Application или не закроет браузер.

9.1 Настройка

Интеграцию Web Application можно настроить на странице «Basic Settings» вашего домена в консоли управления ESET Secure Authentication.

Параметры для подключаемых модулей Exchange Server, Outlook Web App и панели управления Exchange устанавливаются глобально для всего домена. Параметры для остальных подключаемых модулей Web Application устанавливаются на каждом сервере отдельно.

2FA можно включать и выключать для каждого Web Application отдельно. После установки 2FA включена по умолчанию. Чтобы применить изменения в параметрах конфигурации, службу World Wide Web Publishing нужно перезапустить на всех серверах, на которых размещено Web Application.

9.1.1 Допуск пользователей без двухфакторной аутентификации

Для пользователей, которые не используют 2FA, в модуле можно настроить разрешение или запрет на вход в Web Application. Для этих целей используется параметр конфигурации Allow non 2FA.

Это можно делать в тех случаях, когда для пользователей не настроено ни использование одноразовых паролей (OTP — One-Time Password) из SMS, ни использование Mobile Application, при этом включен параметр конфигурации Web Application, который позволяет входить пользователям non-2FA. Параметр конфигурации, который позволяет входить пользователям non-2FA, после установки включен по умолчанию.

В таком случае пользователь может войти в Web Application с помощью своего пароля Active Directory.

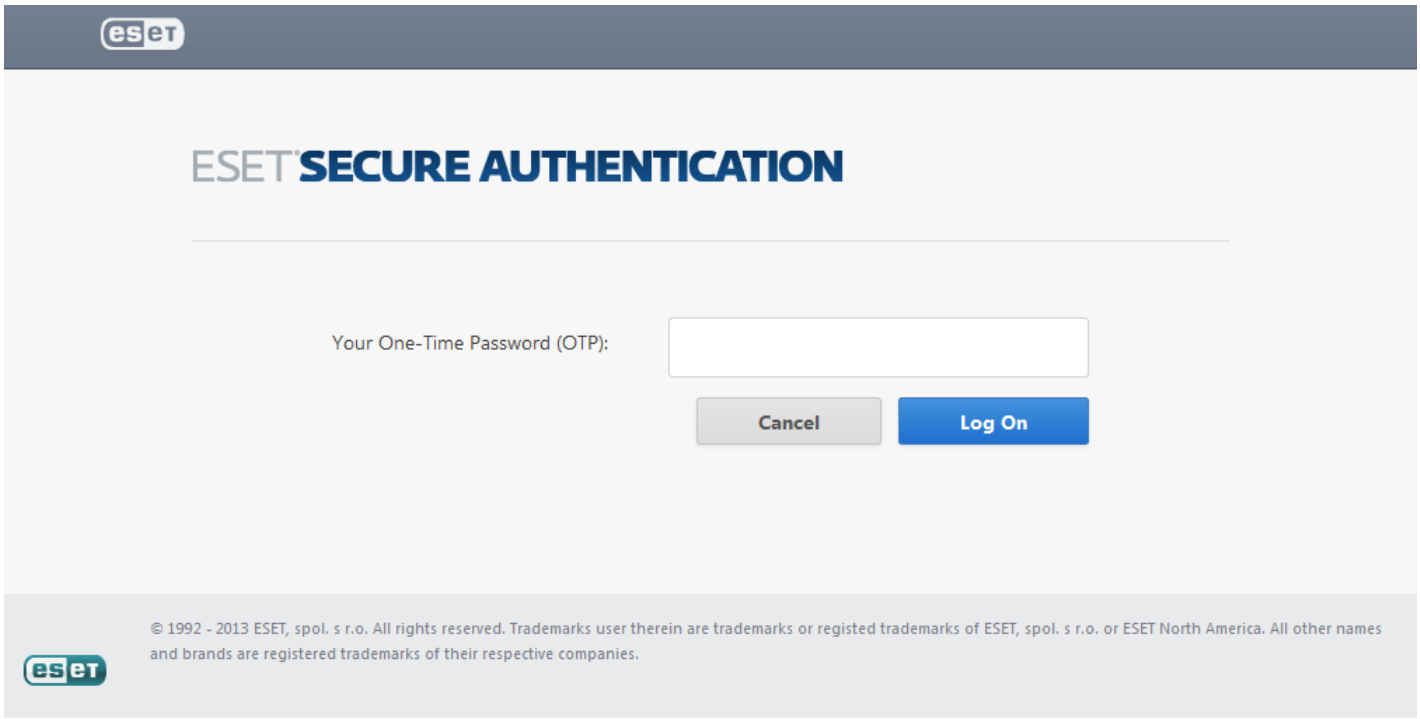
Если параметр конфигурации, который позволяет входить пользователям non-2FA, отключен, пользователь не сможет войти в Web Application.

9.2 Использование

Для всех поддерживаемых Web Apps используется одна и та же процедура 2FA.

Работу модуля Web Application Protection можно проверить следующим образом.

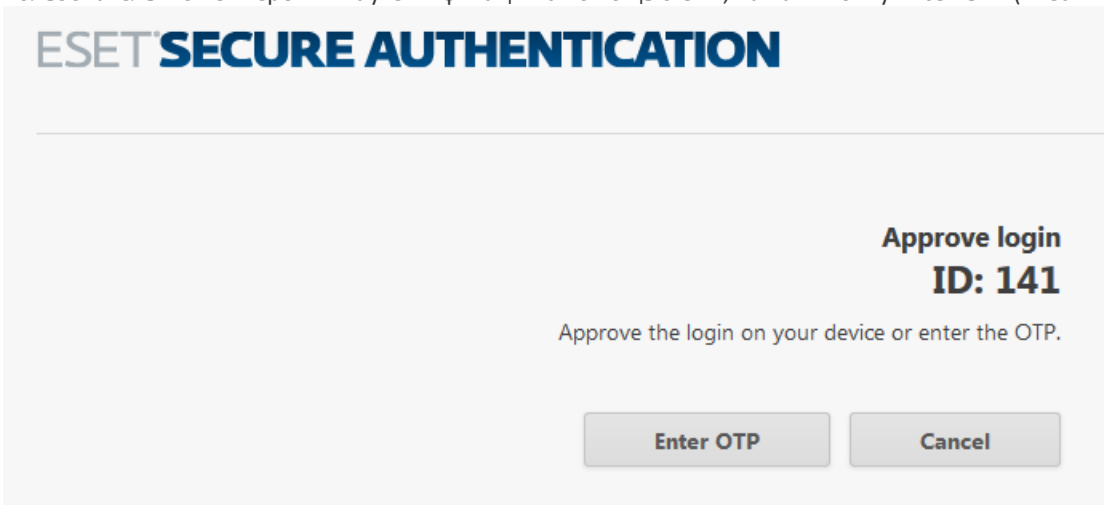
1. Для тестирования требуется пользователь, для которого в средстве управления ADUC включена ESA 2FA. У пользователя должен быть также доступ к Web App.
2. На ПК откройте в браузере Web App и проведите обычную аутентификацию тестового пользователя с помощью учетных данных Active Directory.
3. Должна отобразиться страница аутентификации ESA, как показано на рисунке ниже. В ОС Windows Server 2008 и Microsoft Dynamics CRM 2011 в подключаемом модуле Remote Desktop Web Access не будет отображаться кнопка «Cancel».
4. Должна отобразиться страница аутентификации ESA, как показано на рисунке ниже. В подключаемых модулях Remote Desktop Web Access (Веб-доступ к удаленным рабочим столам) в Windows Server 2008 и подключаемых модулях Microsoft Dynamics CRM не отображается кнопка Cancel (Отмена).



a. Если для пользователя настроена отправка SMS OTP, ему будет отправлено SMS с OTP, который нужно ввести для аутентификации.

b. Если у пользователя на телефоне установлено мобильное приложение ESA, OTP для аутентификации можно создать с помощью этого приложения. Из соображений удобочитаемости OTP в мобильном приложении отображаются с пробелом между третьей и четвертой цифрами. Модуль Web Application Protection удаляет пробелы, поэтому при вводе OTP пользователь может либо оставить эти пробелы, либо удалить их. Это не повлияет на процесс аутентификации.

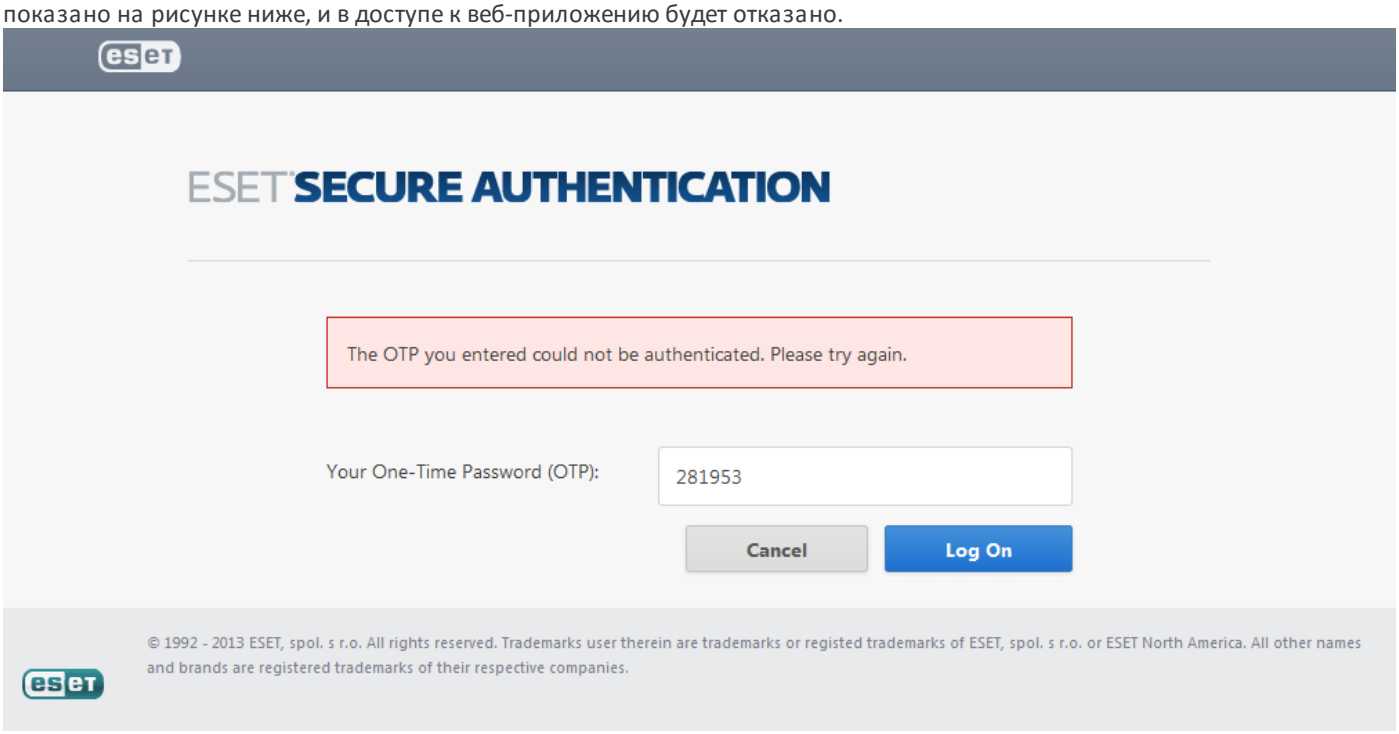
c. Если пользователь установил мобильное приложение ESA на свой телефон и имеет право использовать оба метода аутентификации (OTP и Push), на экране появится утверждение push-уведомления или запрос на ввод OTP. Кроме того, пользователь может перейти к аутентификации с помощью OTP, нажав кнопку **Enter OTP** (Ввести OTP).



5. Если push-уведомление утверждено или введен действительный OTP, пользователь будет перенаправлен на страницу, которую он изначально запросил. После этого пользователь сможет работать с Web App.

6. Если push-уведомление не утверждено в течение 2 минут, пользователь будет перенаправлен на страницу, которая запрашивает ввод OTP. Если введен неправильный одноразовый пароль (OTP), отобразится сообщение об ошибке, как

показано на рисунке ниже, и в доступе к веб-приложению будет отказано.



Если необходимо отображать настраиваемый логотип в окне ввода одноразового пароля (OTP ,) или утвердить уведомление вместо используемого по умолчанию логотипа ESET Secure Authentication, выполните следующие действия. Все действия выполняются на компьютере, на котором установлено ядро ESA core.

1. Сохраните необходимый логотип как файл изображения с расширением *.png*. Рекомендуемые максимальные размеры — 350 x 100 пикселей (ширина x высота).
2. Разместите логотип в папке *C:\ProgramData\ESET Secure Authentication\Customization* и дайте ему имя «*logo.png*».

10. Защита удаленного рабочего стола

Модуль ESA Remote Desktop Protection добавляет 2FA в процесс аутентификации пользователей Remote Desktop. Модуль загрузится в следующий раз, когда пользователь с включенной двухфакторной аутентификацией (2FA) попытается использовать удаленный рабочий стол (Remote Desktop), чтобы войти на удаленный компьютер, на котором установлен ESA Credential Provider.

Пользователи будут входить, используя обычный процесс аутентификации для Remote Desktop. После аутентификации на Remote Desktop пользователю будет предложено ввести OTP. Доступ к компьютеру будет разрешен только в том случае, если введен правильный OTP.

Сеанс с 2FA будет оставаться активным, пока пользователь не завершит его или не отключится от Remote Desktop.

ПРИМЕЧАНИЕ. ESA не может защитить клиенты RDP, которые не указали имя пользователя и пароль. То есть RDP на клиенте, на котором имя пользователя и пароль не настроены и не запрашиваются, не будет запрашиваться и пароль OTP .

10.1 Настройка

Чтобы настроить Remote Desktop 2FA для пользователей ADUC, необходимо включить 2FA для соответствующих пользователей. У этих пользователей также должен быть доступ к Remote Desktop.

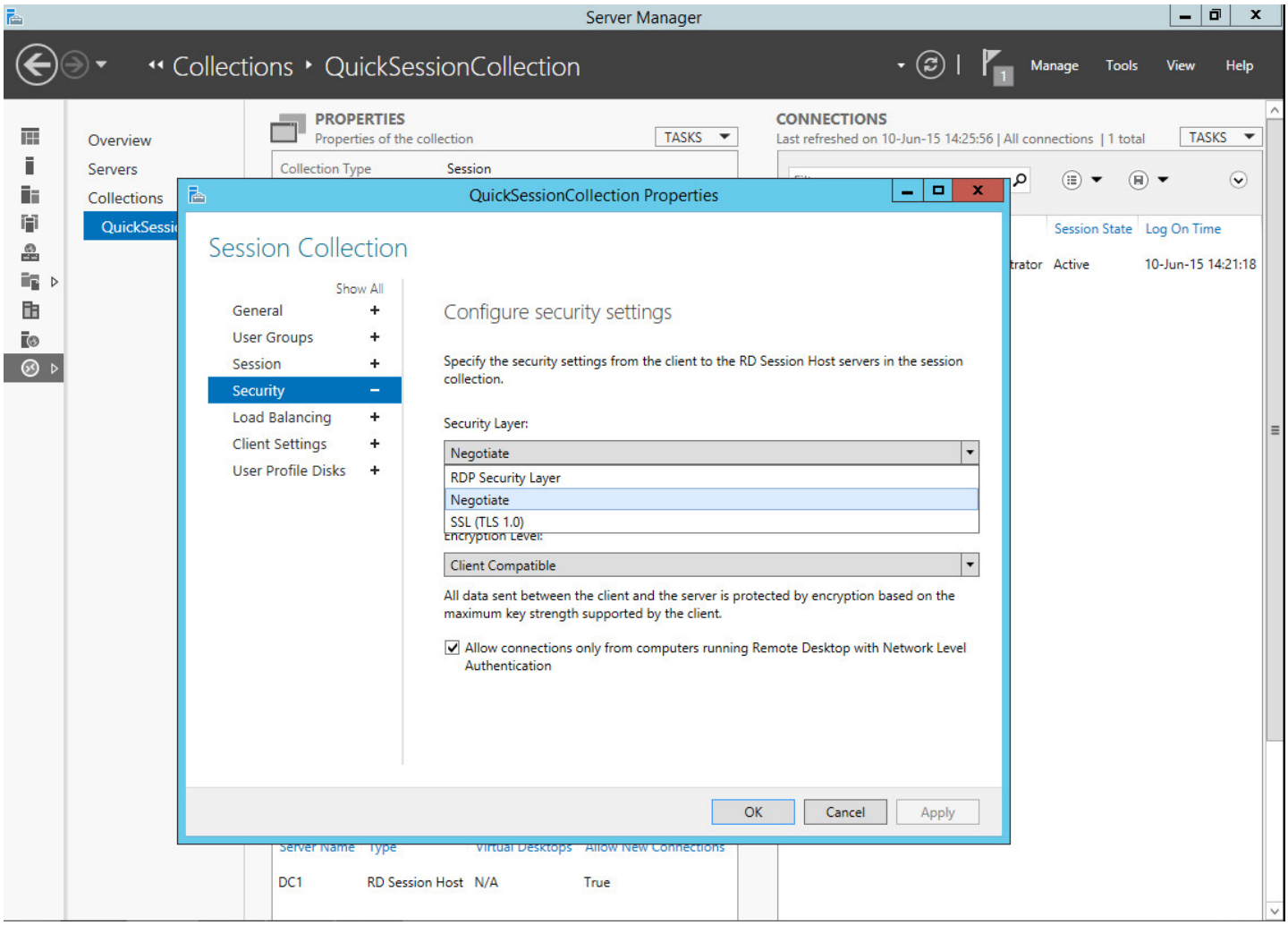
Чтобы использовать защиту удаленного рабочего стола, в узле сеанса удаленного рабочего стола нужно настроить использование *SSL (TLS 1.0)* или *Negotiate*.

Чтобы изменить настройки в ОС Windows Server 2008 или более ранней версии, выполните следующие действия:

1. Откройте меню «Пуск» (**Start**) и последовательно щелкните **Administrative Tools** (Администрирование) > **Remote Desktop Services** (Службы удаленного рабочего стола) > **Remote Desktop Session Host Configuration** (Конфигурация узла сеанса удаленного рабочего стола).
2. В разделе **Connections** (Подключения) откройте элемент **RDP-Tcp**.
3. Откройте вкладку **General** (Общие).
4. В разделе **Security** (Безопасность) для параметра **Security Layer** (Уровень безопасности) нужно задать значение *SSL (TLS 1.0)* или *Negotiate*

Чтобы изменить настройки в ОС Windows Server 2012, выполните следующие действия:

1. Откройте диспетчер серверов (**Server Manager** (Диспетчер серверов)).
2. На левой панели щелкните **Remote Desktop Services** (Службы удаленного рабочего стола).
3. Откройте свойства **Collections** (Коллекции).
4. В разделе **Security** (Безопасность) для параметра **Security Layer** (Уровень безопасности) нужно задать значение *SSL (TLS 1.0)* или *Negotiate*



10.1.1 Допуск пользователей без двухфакторной аутентификации

Для пользователей, которые не используют 2FA, в модуле можно настроить разрешение или запрет на вход на удаленные компьютеры с помощью протокола удаленного рабочего стола (Remote Desktop Protocol).

Это можно делать в тех случаях, когда для пользователей не настроено ни использование одноразовых паролей (OTP — One-Time Password) из SMS, ни использование Mobile Application, при этом включен параметр конфигурации Remote Desktop, который позволяет входить пользователям non-2FA. Параметр конфигурации, который позволяет входить пользователям non-2FA, после установки включен по умолчанию.

В такой конфигурации пользователь может войти на удаленный компьютер с помощью своего пароля Active Directory.

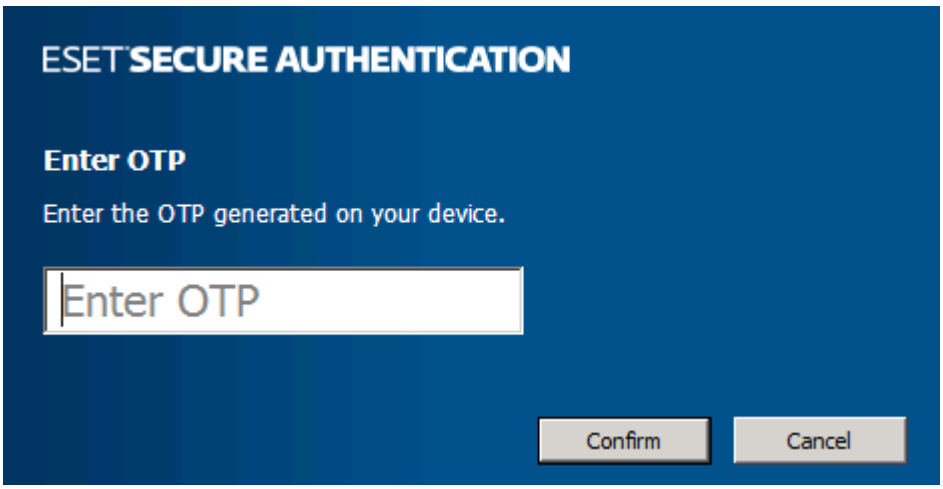
Если параметр конфигурации, который позволяет входить пользователям non-2FA, отключен, пользователь не сможет войти на удаленный компьютер с помощью Remote Desktop Protocol.

Чтобы изменить конфигурацию модуля, перейдите в ESA Management Console к узлу домена (например, acswin2012.com), затем выберите **Remote Desktop Settings** (Параметры удаленного рабочего стола), щелкните **Show Settings...** (Показать параметры), после чего появится окно **Computer list** (Список компьютеров) со списком всех компьютеров, на которых установлен компонент Remote Desktop Protection решения ESA.

10.2 Использование

Работу модуля Remote Desktop Protection можно проверить следующим образом.

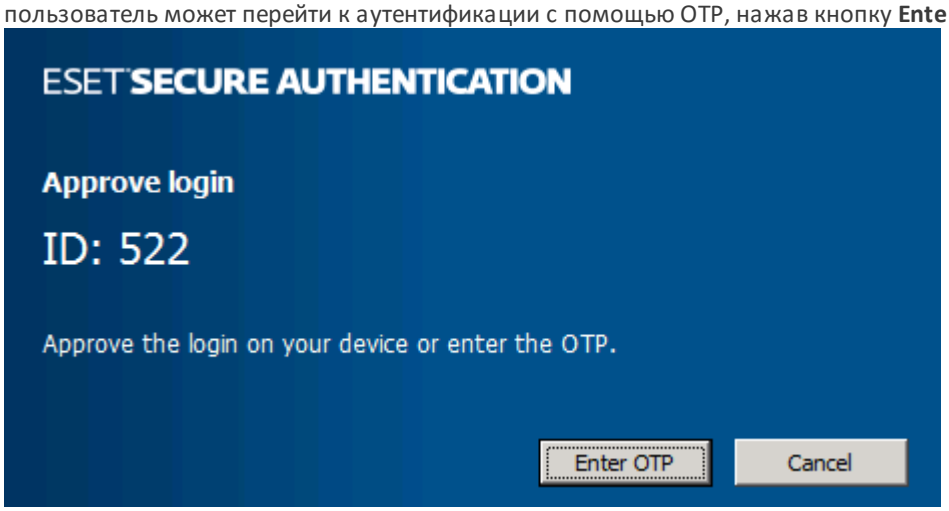
1. Для тестирования требуется пользователь домена, для которого в средстве управления ADUC включена ESA 2FA. Этот пользователь должен быть добавлен на удаленном компьютере в качестве допустимого пользователя Remote Desktop.
2. Кроме того, требуется компьютер, на котором настроен Remote Desktop Access.
3. Подключитесь к удаленному компьютеру с помощью клиента Remote Desktop и пройдите обычную аутентификацию тестового пользователя с помощью учетных данных Active Directory.
4. Должно отобразиться окно для ввода OTP, как показано на рисунке ниже.



   a. Если для пользователя настроена отправка OTP посредством SMS, будет отправлено SMS с OTP, который нужно ввести для аутентификации.

   b. Если у пользователя на телефоне установлено мобильное приложение ESA, OTP для аутентификации можно создать с помощью этого приложения. Из соображений удобочитаемости OTP в мобильном приложении отображаются с пробелом между третьей и четвертой цифрами. Модуль Remote Desktop Protection удаляет пробелы, поэтому при вводе OTP пользователь может либо оставить эти пробелы, либо удалить их. Это не повлияет на процесс аутентификации.

   c. Если пользователь установил мобильное приложение ESA на свой телефон и имеет право использовать оба метода аутентификации (OTP и Push), на экране появится утверждение push-уведомления. Кроме того, пользователь может перейти к аутентификации с помощью OTP, нажав кнопку **Enter OTP** (Ввести OTP).



5. Если введен действительный OTP, пользователю будет предоставлен доступ к компьютеру, к которому он пытается подключиться.
6. Если введен неправильный OTP, отобразится сообщение об ошибке и пользователю будет отказано в доступе.

10.3 Веб-доступ к удаленному рабочему столу

Если вы используете двухфакторную аутентификацию (2FA) для протокола RDP на сервере, на котором размещен сайт веб-доступа к удаленным рабочим столам (RDWA), параметры по умолчанию предусматривают необходимость аутентификации 2FA для запуска приложений, доступных на этом сайте.

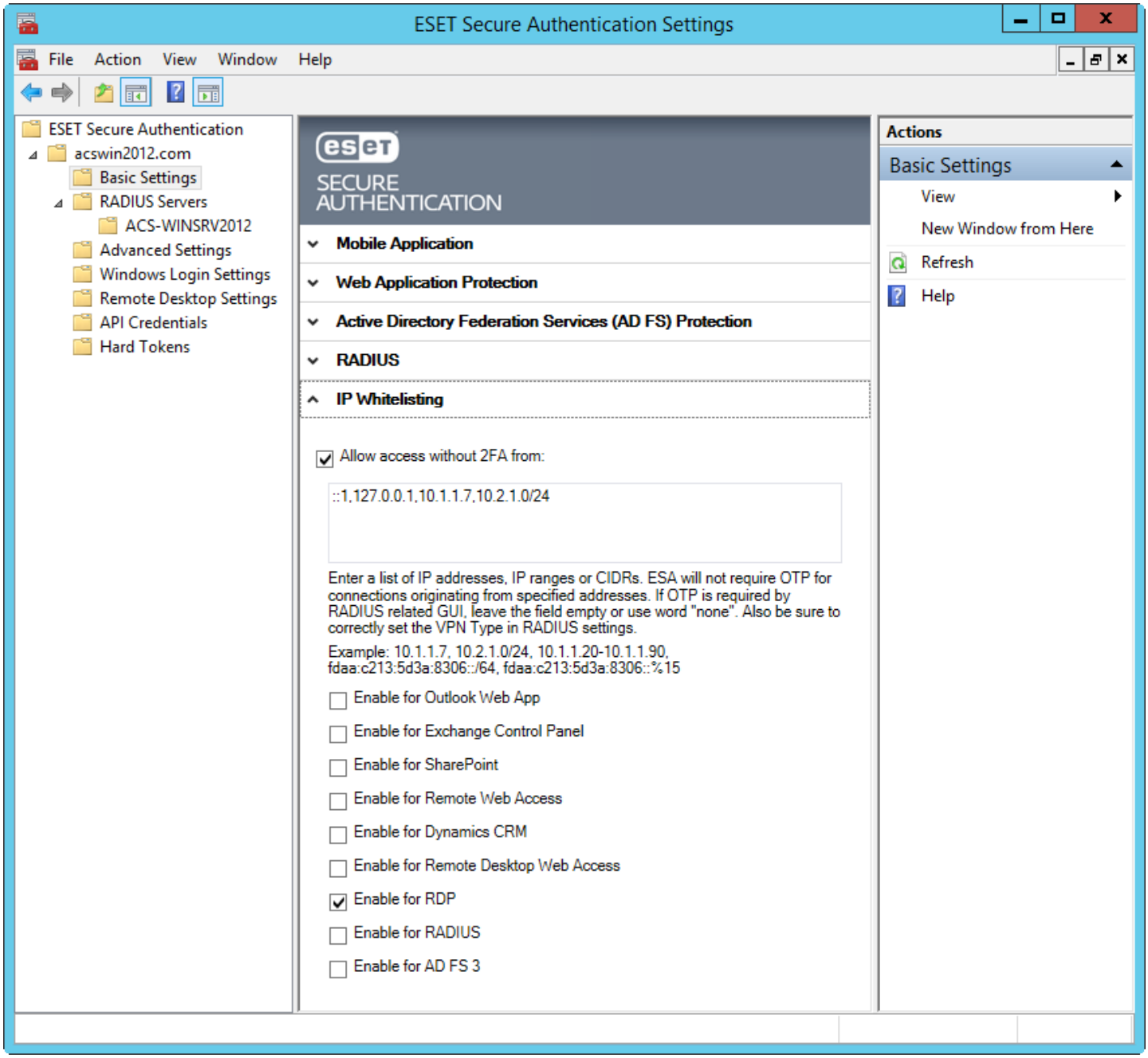
Это означает, что если пользователь пытается получить доступ к сайту RDWA, то ему будет предложено ввести пароль OTP. После того как пользователь введет верный пароль OTP, войдет в систему и попытается запустить приложение, доступное на веб-сайте, ему снова будет предложено ввести пароль OTP.

Чтобы аутентифицированный пользователь (который указал допустимый пароль OTP для входа на веб-сайт RDWA) не вводил повторно пароль OTP при запуске приложения на веб-сайте, выполните следующие действия.

1. В консоли управления ESA (ESA Management Console) последовательно откройте элементы **ESET Secure Authentication** > <домен> > **Basic Settings** (Основные параметры) > **Trusted Networks** (Доверенные сети).
2. Щелкните строку **Помещение IP-адреса в белый список**.
3. Укажите IP-адрес localhost 127.0.0.1,::1
4. Установите флажок **RDP**.
5. Нажмите кнопку **Save** (Сохранить).

11. Помещение IP-адреса в белый список

Если вы хотите предоставить отдельным пользователям доступ к удаленному рабочего столу (Remote Desktop) или поддерживаемым веб-приложениям, защищенным при помощи двухфакторной аутентификации (2FA), без необходимости ввода одноразового пароля OTP, IP-адреса таких пользователей можно поместить в белый список. Для этого откройте консоль управления ESA (ESA Management Console) в приложении **ESET Secure Authentication Settings** (Параметры ESET Secure Authentication) и последовательно выберите **ESET Secure Authentication** > <домен > > **Basic Settings** (Основные параметры) > **Trusted Networks** (Доверенные сети).



Установите флажок рядом с параметром **Allow access without 2FA from** (Разрешить доступ без 2FA с адреса), укажите необходимый IP-адрес, выберите службы, которые нужно поместить в белый список, и щелкните **Save** (Сохранить).

Если соединение с VPN защищено с помощью двухфакторной аутентификации (2FA) и пользователям, IP-адреса которых помещены в белый список, необходимо предоставить доступ к VPN без ввода пароля OTP, должны выполняться следующие условия:

- в разделе конфигурации клиента RADIUS для параметра **VPN Type** (Тип VPN) выберите **VPN validates AD username and password** (VPN проверяет имя пользователя и пароль AD), а также установите флажок **Active Directory passwords without OTPs** (Пароли Active Directory без одноразовых паролей);
- убедитесь, что у пользователя, которому принадлежит помещенный в белый список IP-адрес, не включены какие-либо из параметров двухфакторной аутентификации (2FA) — см. раздел Управление пользователями.

Если эти условия соблюдены, пользователь получит доступ к VPN и ему не нужно будет вводить пароль или использовать в качестве пароля слово **none**.

Не путайте удаленный веб-доступ и веб-доступ к удаленному рабочему столу.

12. Маркеры оборудования

Маркер оборудования — это устройство, которое создает одноразовые пароли (OTP) и может параллельно использоваться для доступа к чему-либо. Маркерами оборудования могут быть различные типы устройств: это может быть брелок, который можно закрепить на связке ключей, или пластина в форме кредитной карты, которую можно хранить в портмоне.

ESA поддерживает все совместимые с OATH маркеры оборудования HOTP, но ESET не предоставляет их. Пароли HOTP маркеров оборудования можно использовать так же, как и пароли OTPs, созданные мобильным приложением или отправленные пользователю через SMS. Эти пароли можно использовать для переноса устаревших маркеров, для обеспечения соответствия требованиям или корпоративным политикам. Обратите внимание, что пароли TOTP маркеров OATH (временные одноразовые пароли OTP) не поддерживаются.

12.1 Управление маркерами оборудования

В этом разделе описывается, как активировать маркеры оборудования и управлять ими через ESA Management Console.

Процесс управления состоит из трех функций:

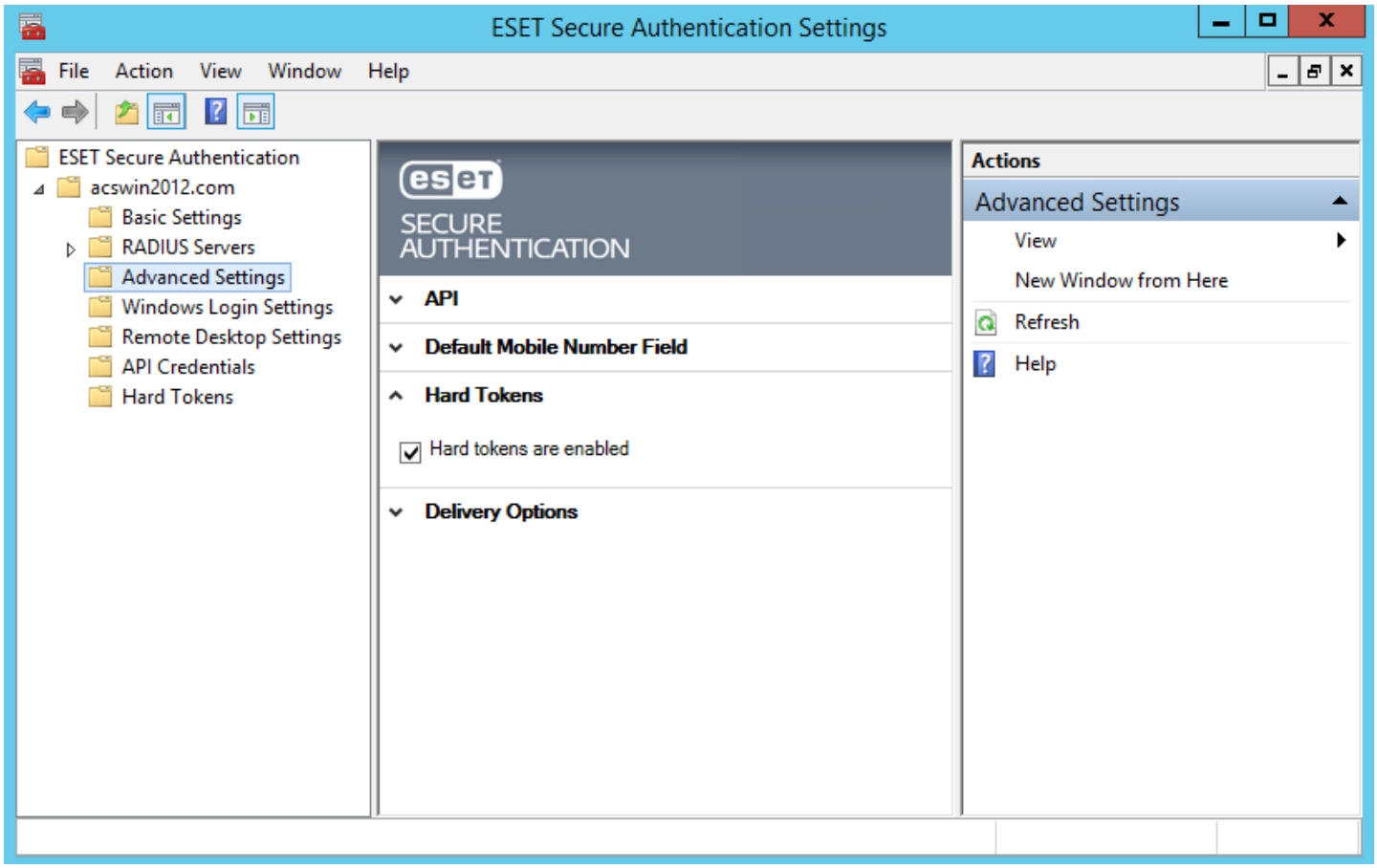
1. импорт маркеров оборудования в систему;
2. удаление маркеров оборудования;
3. повторная синхронизация маркеров оборудования.

12.1.1 Активация

По умолчанию маркеры оборудования отключены, и их необходимо включить перед использованием. После активации маркеры оборудования нужно импортировать, после чего станут доступны все возможности по работе с ними.

Чтобы активировать маркеры оборудования, выполните следующие действия.

1. Запустите ESET Secure Authentication Management Console и перейдите к узлу **Advanced Settings** (Дополнительные настройки) вашего домена.
2. Разверните раздел **Hard Tokens** (Маркеры оборудования) и установите флажок **Hard tokens are enabled** (Маркеры оборудования включены). Сохраните изменения.
3. Если все пройдет успешно, появится узел **Hard Tokens** (Маркеры оборудования). Здесь осуществляется управление маркерами оборудования.

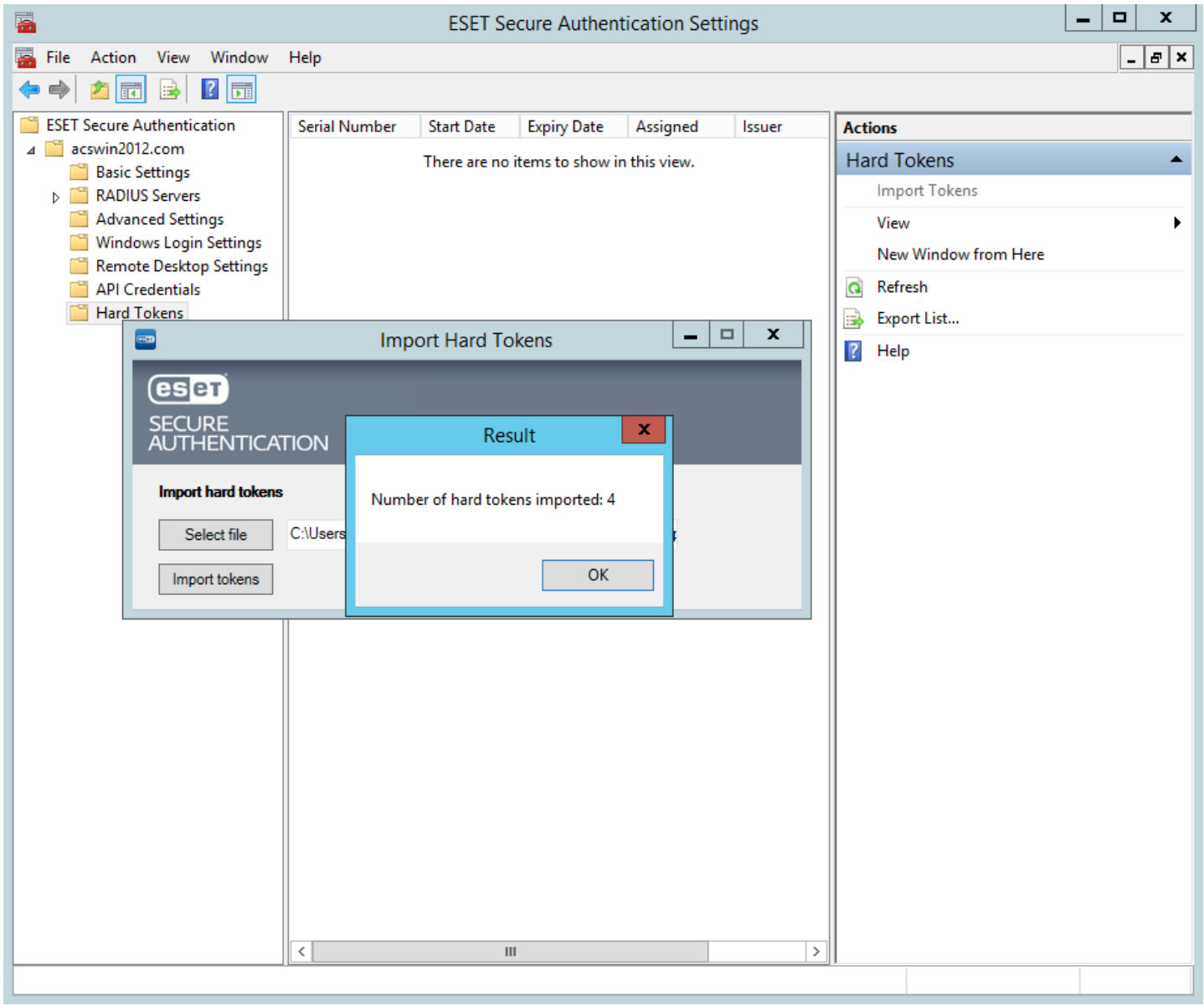


12.1.2 Импорт

Для реализации всех возможностей маркеров оборудования маркеры необходимо импортировать. После импорта маркеры можно назначать пользователям.

Импорт маркеров выполняется следующим образом.

1. Запустите ESET Secure Authentication Management Console и перейдите к узлу **Hard Tokens** (Маркеры оборудования) вашего домена.
2. Щелкните действие **Import Tokens** (Импорт маркеров).
3. Выберите импортируемый файл. Это должен быть файл в формате XML или PSKC. ПРИМЕЧАНИЕ. Если вы не получили этот файл от поставщика маркеров оборудования, обратитесь в службу поддержки ESA.
4. Нажмите кнопку **Import tokens** (Импорт маркеров).
5. Откроется окно с результатами импорта, в котором будет указано, сколько маркеров было импортировано.
6. После нажатия кнопки **OK** окно закроется и отобразятся импортированные маркеры.

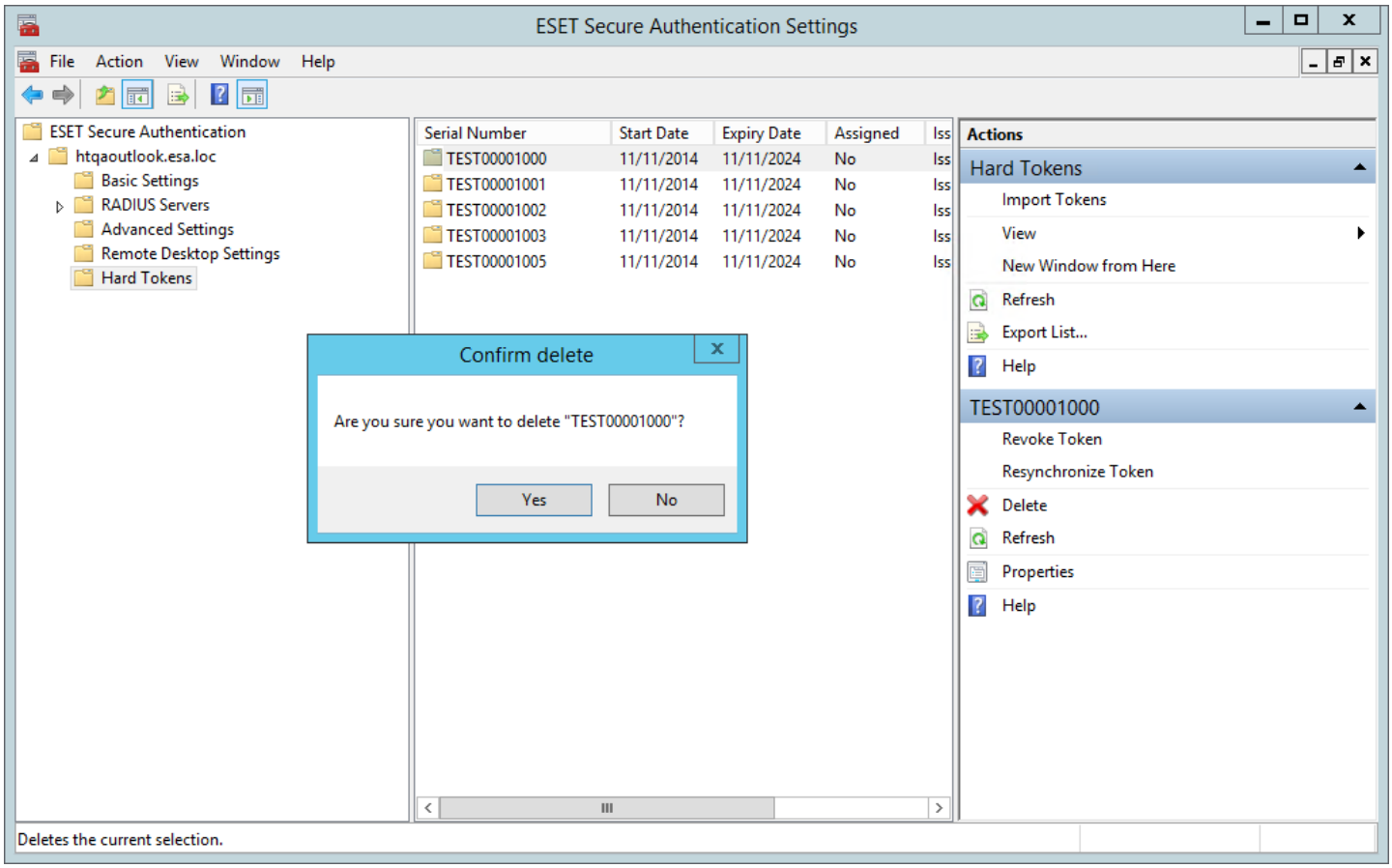

ESET Secure Authentication Settings
File
Action
View
Window
Help
ESET Secure Authentication
acswin2012.com
Basic Settings
RADIUS Servers
Advanced Settings
Windows Login Settings
Remote Desktop Settings
API Credentials
Hard Tokens
Serial Number
Start Date
Expiry Date
Assigned
Issuer
There are no items to show in this view.
Actions
Hard Tokens
Import Tokens
View
New Window from Here
Refresh
Export List...
Help
Import Hard Tokens
SECURE AUTHENTICATION
Import hard tokens
Select file
C:\Users
Import tokens
Result
Number of hard tokens imported: 4
OK

12.1.3 Удаление

Иногда может возникнуть необходимость удалить маркер оборудования из системы.

Удаление маркеров выполняется следующим образом.

1. Запустите ESET Secure Authentication Management Console и перейдите к узлу **Hard Tokens** (Импорт маркеров) вашего домена.
2. Выберите маркер оборудования, который нужно удалить.
3. Выберите для него действие **Delete** (Удалить).
4. В окне с подтверждением нажмите кнопку **Yes** (Да).

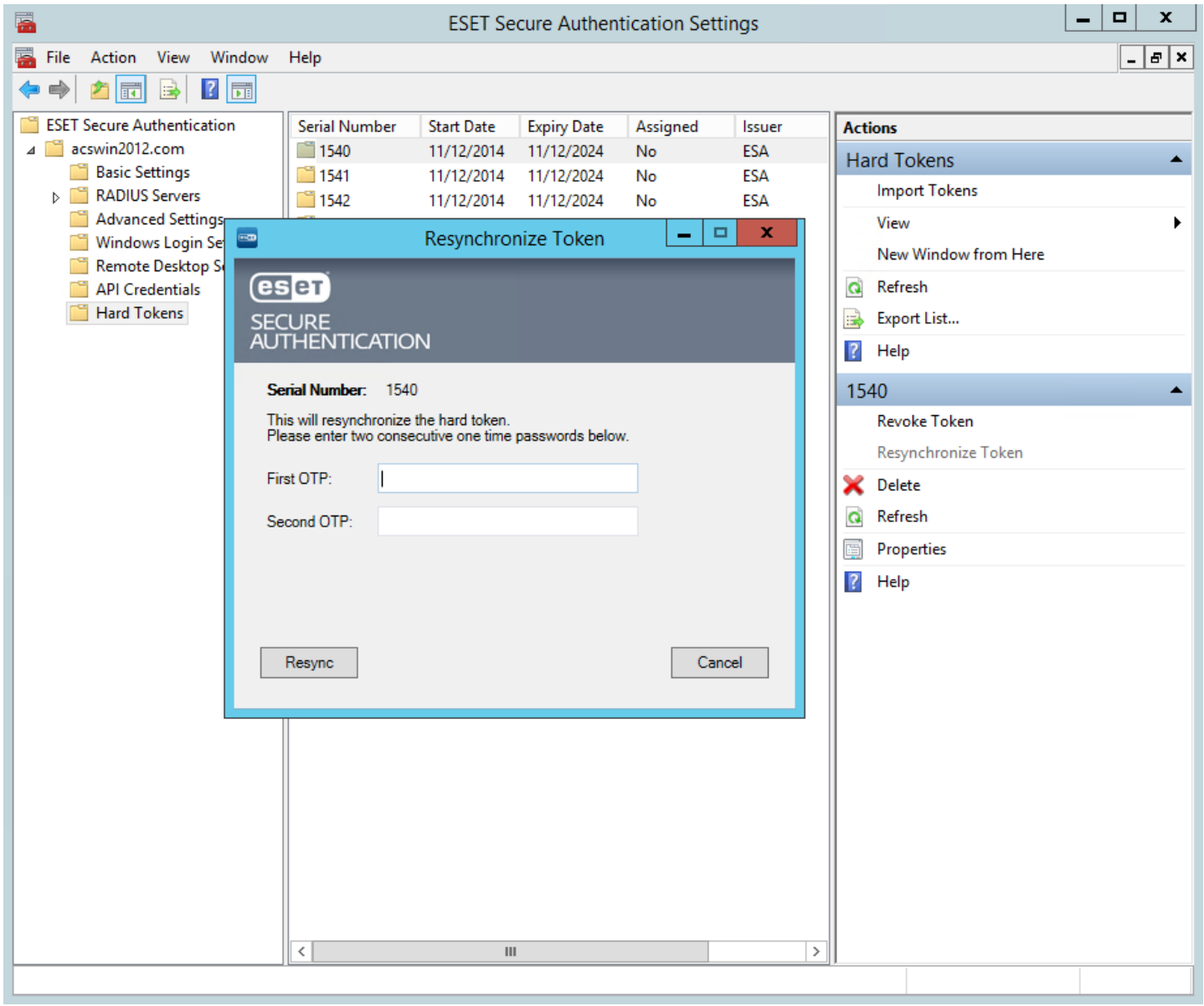


12.1.4 Повторная синхронизация

Если за короткий промежуток времени пользователь создает множество одноразовых паролей, маркер оборудования может рассинхронизироваться с системой. В этом случае понадобится повторная синхронизация.

Чтобы повторно синхронизировать маркер, выполните следующие действия:

1. Запустите ESET Secure Authentication Management Console и перейдите к узлу **Hard Tokens** (Маркеры оборудования) вашего домена.
2. Выберите маркер оборудования, который нужно повторно синхронизировать.
3. Выберите для него действие **Resynchronize Token** (Повторно синхронизировать маркер).
4. Откроется окно **Hard Token Resync** (Повторная синхронизация маркера оборудования).
5. С помощью выбранного маркера последовательно создайте и введите два одноразовых пароля.
6. Нажмите кнопку **Resync** (Повторная синхронизация).
7. Должно появиться сообщение о том, что операция выполнена успешно.



12.2 Управление пользователями маркеров оборудования

В этом разделе рассматривается управление пользователями маркеров оборудования. Для управления пользователями маркеры оборудования должны быть активированы в системе и импортированы.

Управление осуществляется в средстве ADUC на вкладке ESET Secure Authentication.

Доступны две функции:

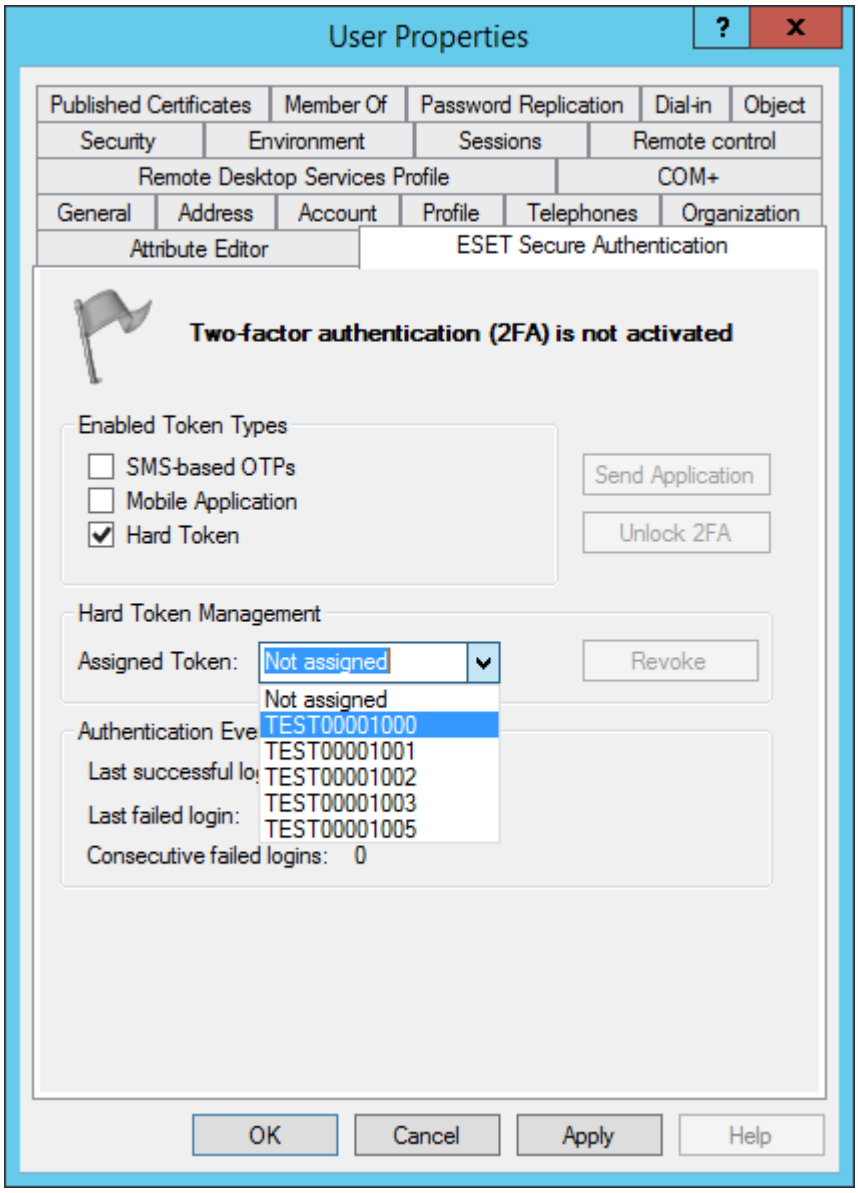
1. Активация аутентификации с использованием маркера оборудования и назначение маркера.
2. Отзыв маркера, связанного с пользователем.

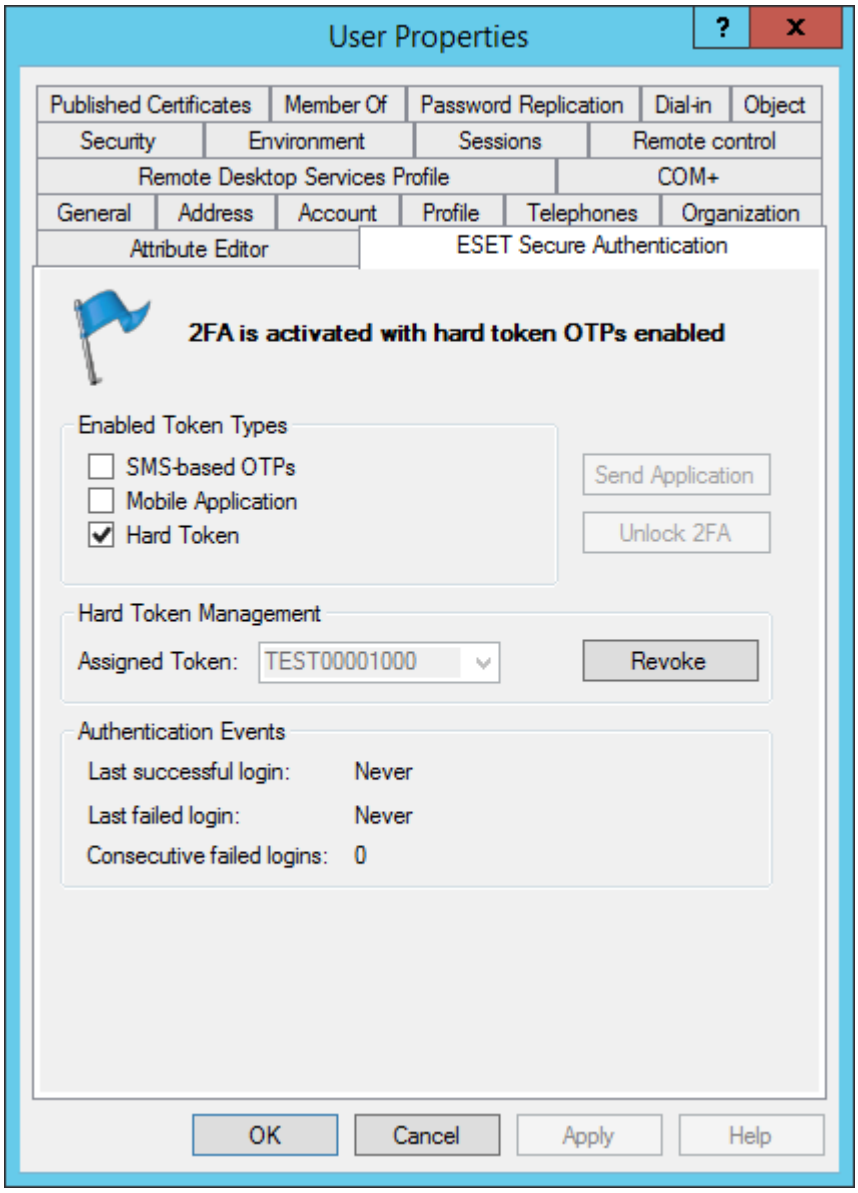
12.2.1 Активация и назначение

Активировав для пользователя аутентификацию с использованием маркеров оборудования, назначьте ему один маркер.

Активация и назначение выполняются следующим образом.

1. Откройте профиль пользователя с помощью ADUC.
2. Откройте вкладку ESET Secure Authentication.
3. Активируйте тип маркера **Hard Token** (Маркер оборудования).
4. В группе **Hard Token Management** (Управление маркерами оборудования) выберите назначаемый маркер.
5. Нажмите кнопку **Apply** (Применить). Теперь маркер оборудования назначен пользователю.


User Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Attribute Editor
ESET Secure Authentication
Two-factor authentication (2FA) is not activated
Enabled Token Types
SMS-based OTPs
Mobile Application
Hard Token
Send Application
Unlock 2FA
Hard Token Management
Assigned Token:
Not assigned
Revoke
Not assigned
TEST00001000
TEST00001001
TEST00001002
TEST00001003
TEST00001005
Authentication Eve
Last successful lo
Last failed login:
Consecutive failed logins: 0
OK
Cancel
Apply
Help



12.2.2 Отзыв

Отзыв маркера оборудования приведет к тому, что пользователь не сможет использовать этот маркер для аутентификации.

Чтобы отозвать маркер, выполните следующие действия:

1. Откройте профиль пользователя с помощью средства ADUC.
2. Откройте вкладку ESET Secure Authentication.
3. Нажмите кнопку **Revoke** (Отозвать).

13. API

ESA API — это веб-служба, в основе которой лежит концепция REST и которая позволяет быстро добавлять двухфакторную аутентификацию (2FA) в существующие приложения.

В большинстве веб-приложений для получения доступа к защищенным ресурсам пользователи проходят аутентификацию. Запрос дополнительного этапа аутентификации при входе в систему делает такие приложения более устойчивыми к атаке.

Полная документация по API для разработчиков находится в руководстве пользователя API.

13.1 Обзор интеграции

Интерфейс API состоит из двух конечных точек, которые текст формата POSTing JSON вызывает к соответствующим URL-адресам API. Все ответы также кодируются в текст формата JSON, который содержит результат метода и все применимые сообщения об ошибках. Первая конечная точка (Authentication API) используется для аутентификации пользователей, а вторая (User Management API) — для управления пользователями.

API доступен на всех серверах, на которых установлен компонент Authentication Core, работающий через защищенный протокол HTTPS и порт 8001.

API аутентификации доступен в URL-адресах типа https://127.0.0.1:8001/auth/v1/, а User Management API — в URL-адресах типа https://127.0.0.1:8001/manage/users/v1/.. Стандартная HTTP Basic Authentication защищает обе конечные точки от несанкционированного доступа, требуя предоставить действительные API Credentials. Обработка запроса начнется только после получения таких данных.

Установщик ESET Secure Authentication автоматически выбирает соответствующий сертификат безопасности SSL, установленный на компьютере. Если сертификат не найден, установщик создает новый самозаверяющий сертификат.

13.2 Настройка

По умолчанию интерфейс API отключен, и его необходимо включить перед использованием. После включения необходимо создать учетные данные API для авторизации запросов.

1. Запустите ESET Secure Authentication Management Console и перейдите к узлу **Advanced Settings** вашего домена.
2. Разверните раздел **API** и установите флажок **API is enabled** (Интерфейс API включен). Сохраните изменения.
3. Откройте стандартную консоль служб Windows и перезагрузите службу ESET Secure Authentication Core, чтобы изменения вступили в силу.
4. Перейдите к новому узлу **API Credentials** (Учетные данные API) своего домена.
5. Щелкните **Add Credentials** (Добавить учетные данные), чтобы создать новый набор учетных данных.
6. Дважды щелкните созданные учетные данные, чтобы получить имя пользователя и пароль, которые будут использоваться для аутентификации API.
7. Установите флажок **Enabled for Auth API** (Включено для API аутентификации), **Enabled for User Management API** (Включено для API управления пользователями) или оба сразу.

Можно создать много наборов учетных данных API. Рекомендуем создать различные наборы для каждого защищаемого приложения, а также набор для тестирования.

Если интерфейс API включен, все серверы с установленным компонентом Authentication Core после перезапуска будут отвечать на авторизованные запросы API. После создания или удаления учетных данных перезапускать службу Authentication Core не нужно.

13.3 Замена сертификата SSL

Для защиты подключений API от прослушивания интерфейс API использует сертификат SSL. Установщик автоматически выбирает соответствующий сертификат, установленный на компьютере. Если сертификат не найден, установщик создает новый самозаверяющий сертификат.

В этом разделе объясняется, как заменить один сертификат на любой другой. Здесь вы найдете информацию о том, как импортировать новый сертификат в ОС Windows, а затем использовать его для ESA.

13.3.1 Необходимые условия

Чтобы соблюсти требования этого руководства, потребуются следующие компоненты.

- Все операционные системы:
  - установленный компонент ESET Secure Authentication Core;
  - администраторский доступ к компьютеру, на котором установлен продукт ESET Secure Authentication;
  - сертификат SSL, который будет использоваться, в формате PKCS12 (pfx или p12);
    - файл сертификата с копиями закрытого и открытого ключей.
- Только Windows 2003:
  - средство httpcfg.exe из пакета «Windows Support Tools» (находится на установочном CD или доступен для загрузки по адресу http://www.microsoft.com/ru-ru/download/details.aspx?id=18546).

ПРИМЕЧАНИЕ. ESA Authentication API не нужно отключать для замены сертификата.

13.3.2 Импорт нового сертификата

Чтобы использовать новый сертификат, его следует поместить в хранилище персональных сертификатов на локальном компьютере.

1. Запустите консоль управления Microsoft (MMC).
   - Windows Server 2003: откройте меню «Пуск», выберите пункт «Выполнить», введите «mmc.exe» и нажмите клавишу **Enter**.
   - Windows Server 2008 и более новые выпуски: откройте меню «Пуск», введите «mmc.exe» и нажмите клавишу **Enter**.
2. Добавьте оснастку сертификатов.
   - Windows Server 2003:
     - Последовательно щелкните **Файл** -> **Добавить или удалить оснастку** -> **Добавить** (кнопка).
     - В списке выберите **Сертификаты**.
     - Нажмите кнопку **Добавить**.
     - Выберите **Учетная запись компьютера**.
     - Нажмите кнопку **Далее**.
     - Выберите **Локальный компьютер**.
     - Нажмите кнопку **Готово**.
     - Нажмите кнопку **Закрыть**.
     - Нажмите кнопку **ОК**.
   - Windows Server 2008+:
     - Последовательно щелкните **Файл** -> **Добавить или удалить оснастку**.
     - В столбце слева выберите **Сертификаты**.
     - Нажмите кнопку **Добавить**.
     - Выберите **Учетная запись компьютера**.
     - Нажмите кнопку **Далее**.

- Выберите **Локальный компьютер**.
- Нажмите кнопку **Готово**.
- Нажмите кнопку **ОК**.

3. Сохраните оснастку (необязательно) для использования в будущем (**Файл** -> **Сохранить**).
4. В дереве щелкните **Сертификаты (локальный компьютер)** и выберите узел **Персональные**.
5. Щелкните правой кнопкой мыши и выберите **Все задачи** -> **Импорт**.
6. Следуйте инструкциям мастера импорта и поместите сертификат в хранилище **персональных** сертификатов.
7. Дважды щелкните сертификат и убедитесь, что отображается строка **У вас есть закрытый ключ, соответствующий этому сертификату**.

13.3.3 Замена сертификата ESA

ПРИМЕЧАНИЕ. Служба ESA Core Authentication не будет запускаться, если отсутствует настроенный сертификат. Если вы удалите сертификат, вам необходимо будет добавить другой, чтобы служба Core работала корректно.

Чтобы определить правильный сертификат для использования, выполните следующие действия.

1. Откройте диспетчер сертификатов MMC, используя вышеуказанную процедуру.
2. Найдите сертификат, который нужно использовать, в папке **Персональные** и дважды щелкните его.
3. Убедитесь, что на вкладке **Общие** отображается сообщение **У вас есть закрытый ключ, соответствующий этому сертификату**.
4. На вкладке **Сведения** выберите поле **Отпечаток**.
5. Отпечаток сертификата появится на нижней панели (наборы двух шестнадцатеричных цифр, разделенные пробелами).

Windows Server 2003:

1. Последовательно щелкните **Пуск** -> **Все программы** -> **Средства поддержки Windows** -> **Командная строка**.
2. Введите «httpcfg query ssl -i 0.0.0.0:8001» и нажмите клавишу **Enter**.
3. Скопируйте и вставьте содержимое поля **Hash** в надежное место на случай, если вам потребуется еще раз добавить существующий сертификат.
4. Введите «httpcfg delete ssl –i 0.0.0.0:8001» и нажмите клавишу **ВВОД**.
5. Должно появиться сообщение **HttpDeleteServiceConfiguration completed with 0**.
6. Введите «httpcfg set ssl –i 0.0.0.0:8001 –g {BA5393F7-AEB1-4AC6-B759-1D824E61E442} –h <THUMBPRINT>», указав вместо «**<THUMBPRINT>**» значения из отпечатка сертификата без пробелов, и нажмите клавишу **Enter**.
7. Должно появиться сообщение **HttpSetServiceConfiguration completed with 0**.
8. Перезапустите службу ESET Secure Authentication Core, чтобы новый сертификат вступил в силу.

Windows Server 2008 и более новые версии:

Щелкните **Пуск** и введите «cmd.exe».

В списке программ щелкните пункт **cmd.exe** правой кнопкой мыши и выберите команду **Запуск от имени администратора**.

Введите «netsh http show sslcert ipport=0.0.0.0:8001» и нажмите клавишу **Enter**.

Скопируйте и вставьте содержимое поля **Certificate Hash** (Хэш сертификата) в надежное место на случай, если вам потребуется еще раз добавить существующий сертификат.

Введите «netsh http delete sslcert ipport=0.0.0.0:8001» и нажмите клавишу **Enter**.

Должно появиться сообщение **SSL Certificate successfully deleted** (Сертификат SSL удален).

Введите «netsh http add sslcert ipport=0.0.0.0:8001 appid={BA5393F7-AEB1-4AC6-B759-1D824E61E442} certhash=<THUMBPRINT>», указав вместо «**<THUMBPRINT>**» значения из отпечатка сертификата без пробелов, и нажмите клавишу **Enter**.

Должно появиться сообщение **SSL Certificate successfully added** (Сертификат SSL добавлен).

Перезапустите службу ESET Secure Authentication Core, чтобы новый сертификат вступил в силу.

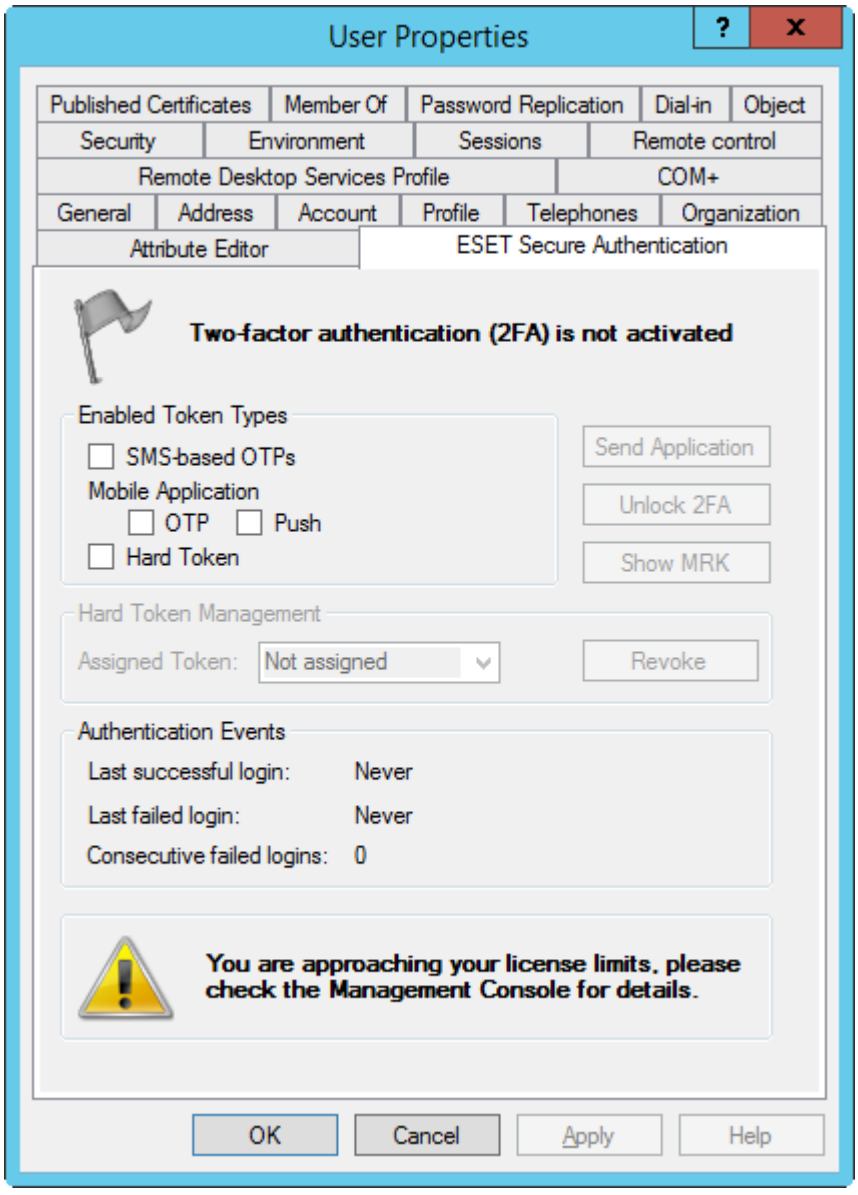
14. Расширенное управление пользователями

Вкладка ESET Secure Authentication в ADUC разделена для пользователя на четыре раздела.

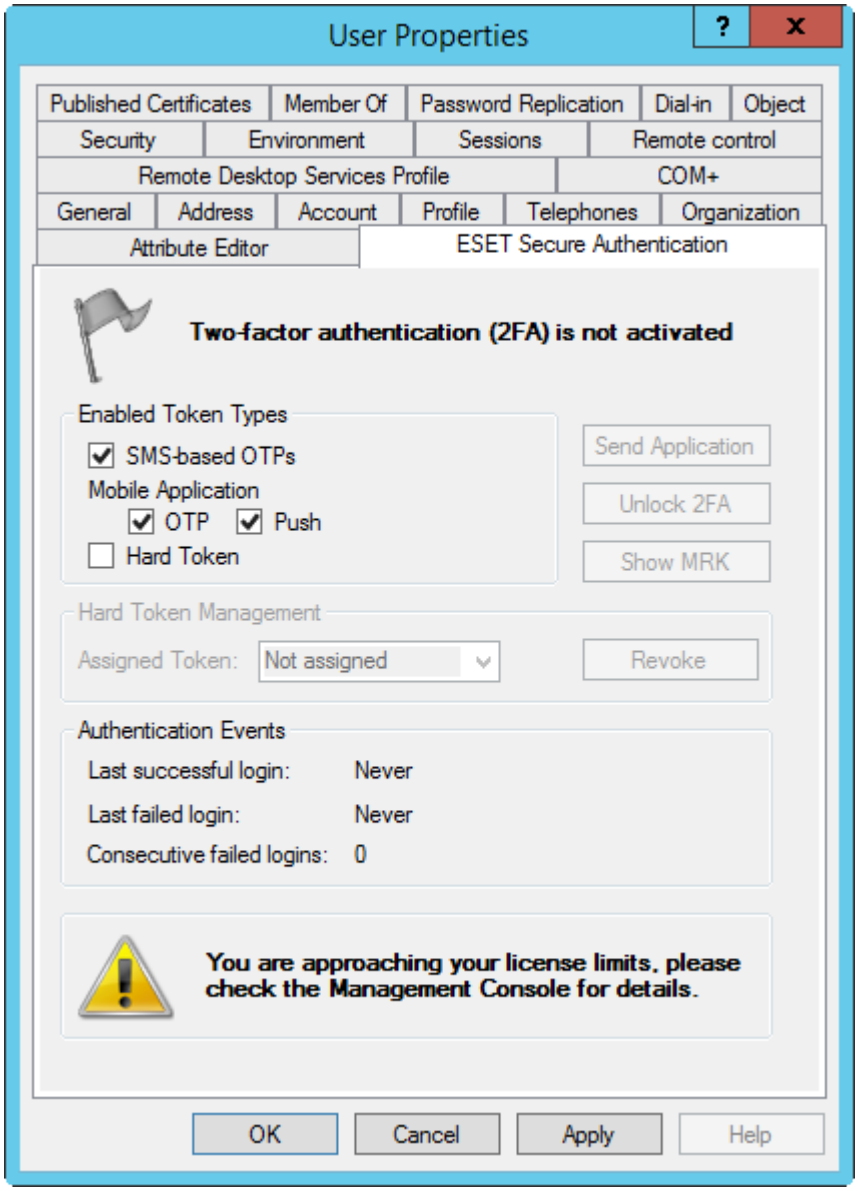
- User State (обозначается для удобства цветным флагом);
- Enabled Token Types (флажки);
- Administrator Actions (кнопки);
- Auditing Data (текстовые данные, обозначающие события аутентификации).

14.1 Состояния пользователя

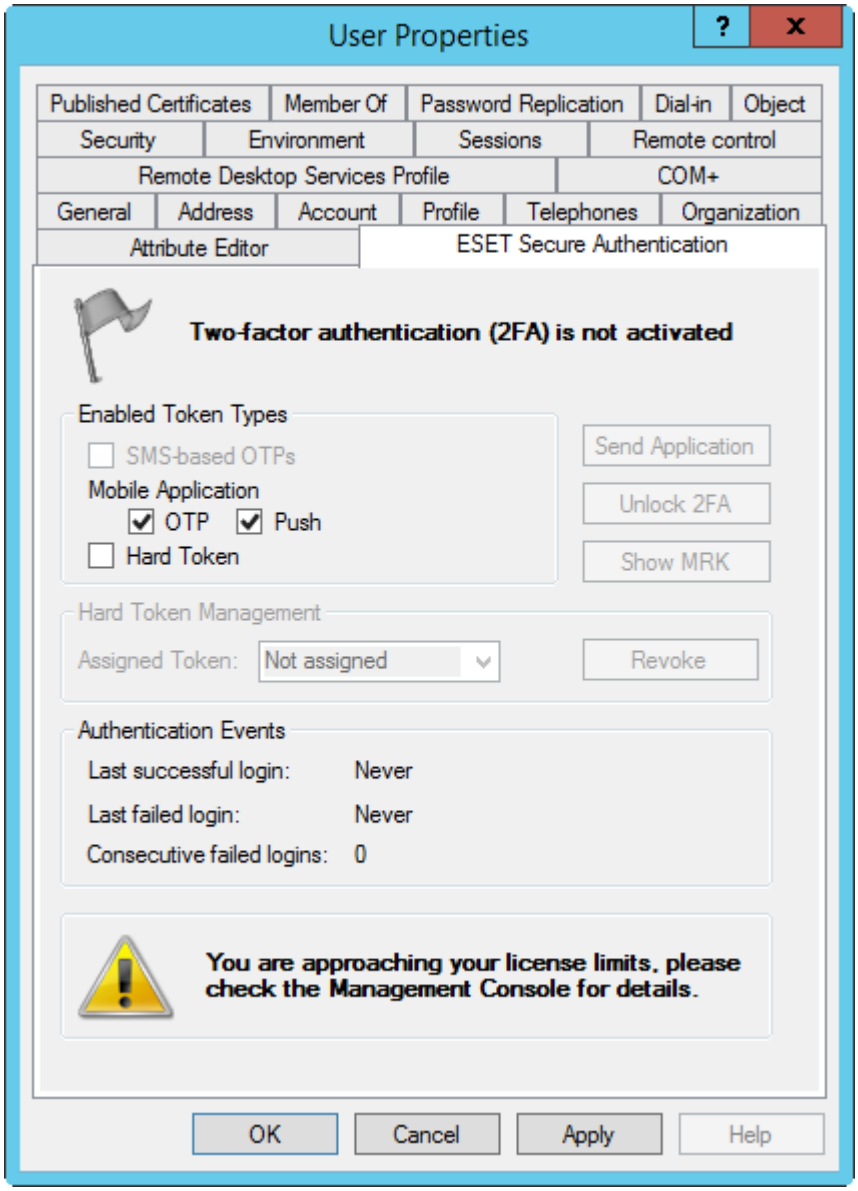
Во время работы пользователя его состояние может меняться. Если для пользователя не включена 2FA, то он считается неинициализированным.



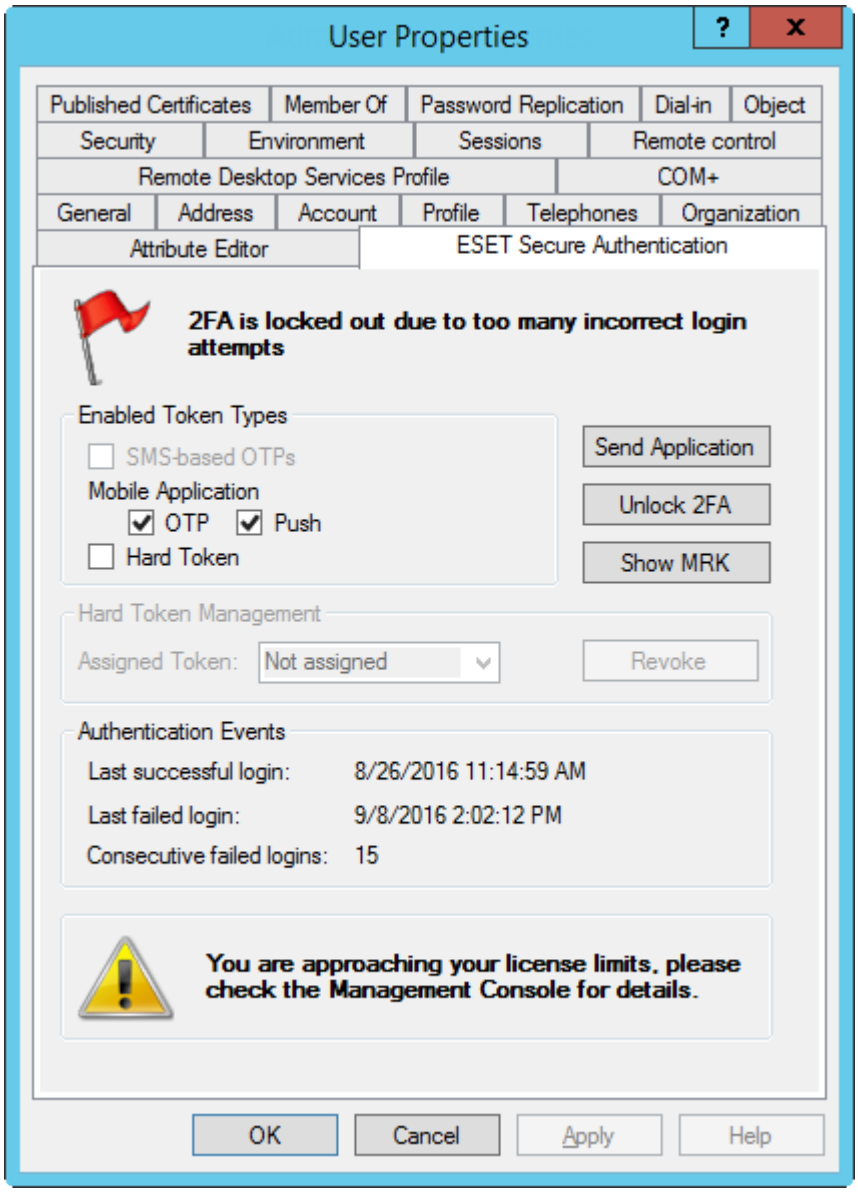
Для пользователя могут быть настроены OTP из SMS, OTP из Mobile Application или одновременно оба типа. Если включены оба типа аутентификации, пользователь находится в переходном состоянии.



В этом состоянии пользователь получает SMS с OTP, когда инициируются попытки аутентификации. Но если для аутентификации используется действительный OTP мобильного приложения или утверждено push-уведомление (запрос на аутентификацию), SMS OTP-сообщения будут отключены и пользователь сможет использовать для аутентификации только OTP мобильного приложения или push-уведомления. Если пользователь успешно прошел аутентификацию с помощью OTP мобильного приложения, отображается зеленый флаг:



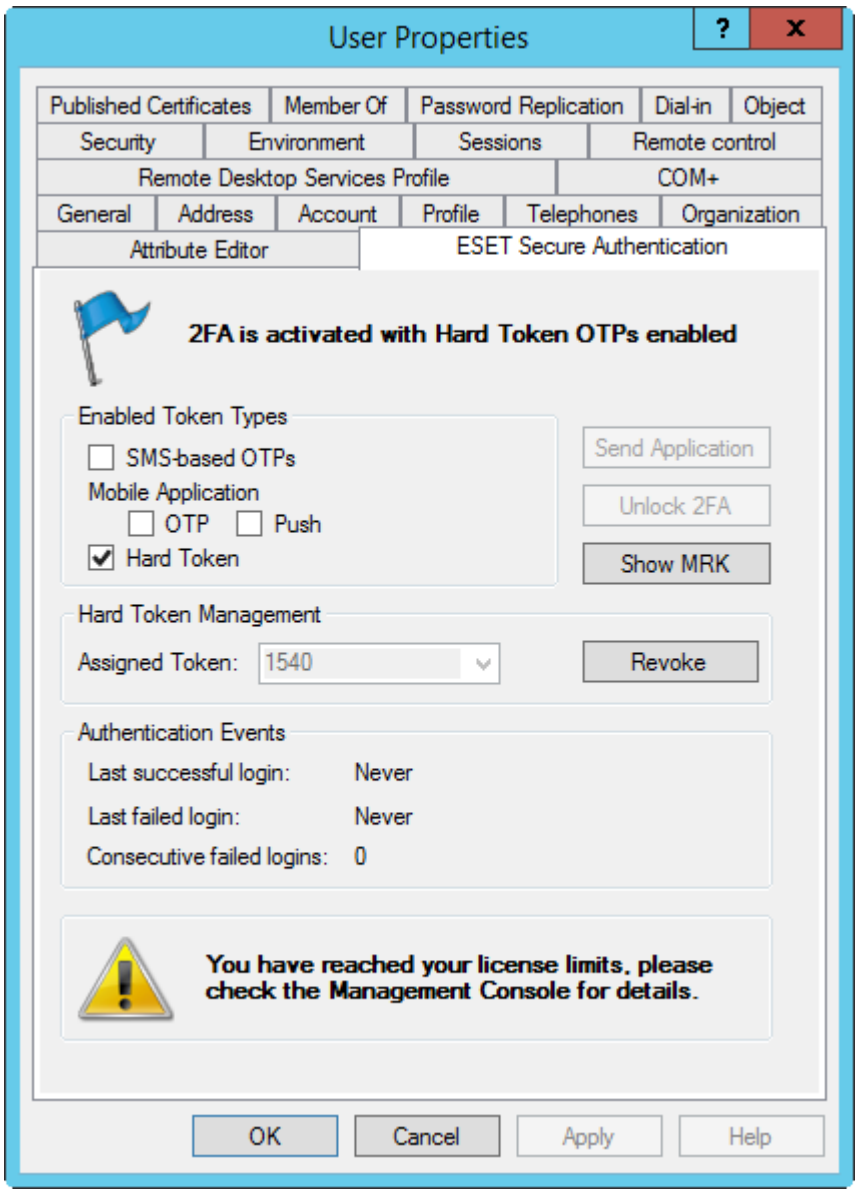
Во время аутентификации с помощью OTP пользователь может ввести неправильный OTP максимум 10 раз. После одиннадцати неправильных вводов OTP 2FA пользователя блокируется. Это позволяет предотвратить угадывание OTP злоумышленниками. Когда 2FA заблокирована для пользователя, отображается красный флажок.



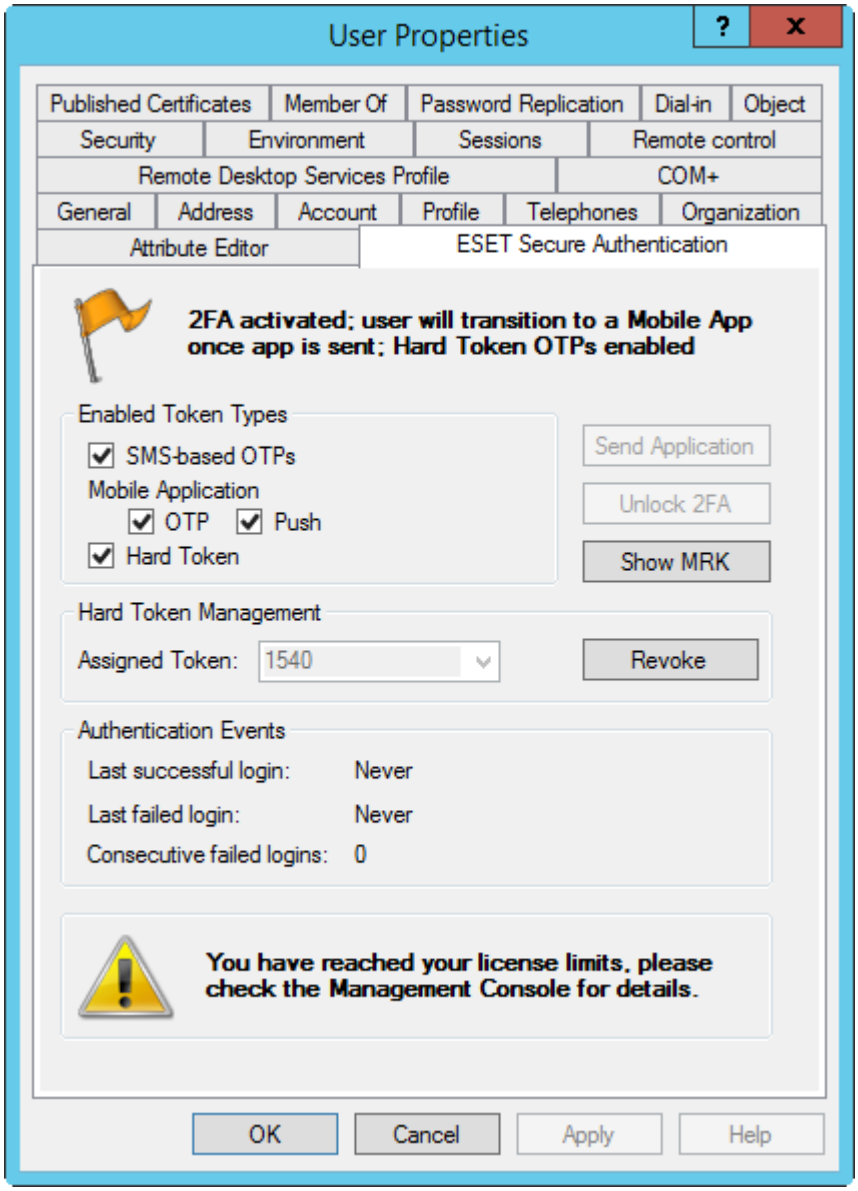
Если будет подтверждено, что учетная запись пользователя не взломана, 2FA для пользователя можно будет разблокировать. Для этого нужно нажать кнопку «Unlock 2FA».

Если в консоли MMC включены Hard Token OTPs, активируется флажок «Маркер оборудования». Это значит, что потенциальных состояний пользователя стало больше. Для пользователя можно включить любое сочетание из трех типов OTP, в том числе переходное состояние. Разные возможности описаны ниже.

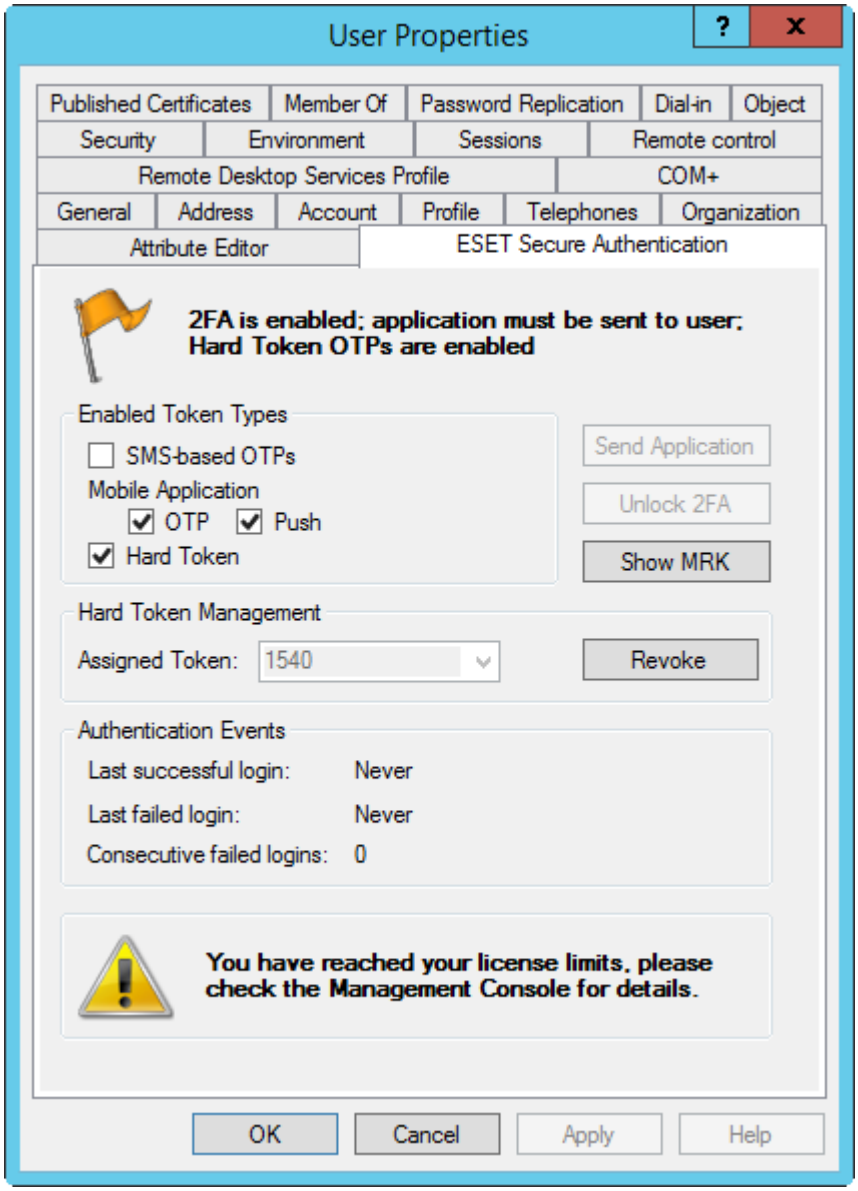
Пользователь может быть в состоянии, в котором включены только Hard Token OTP.



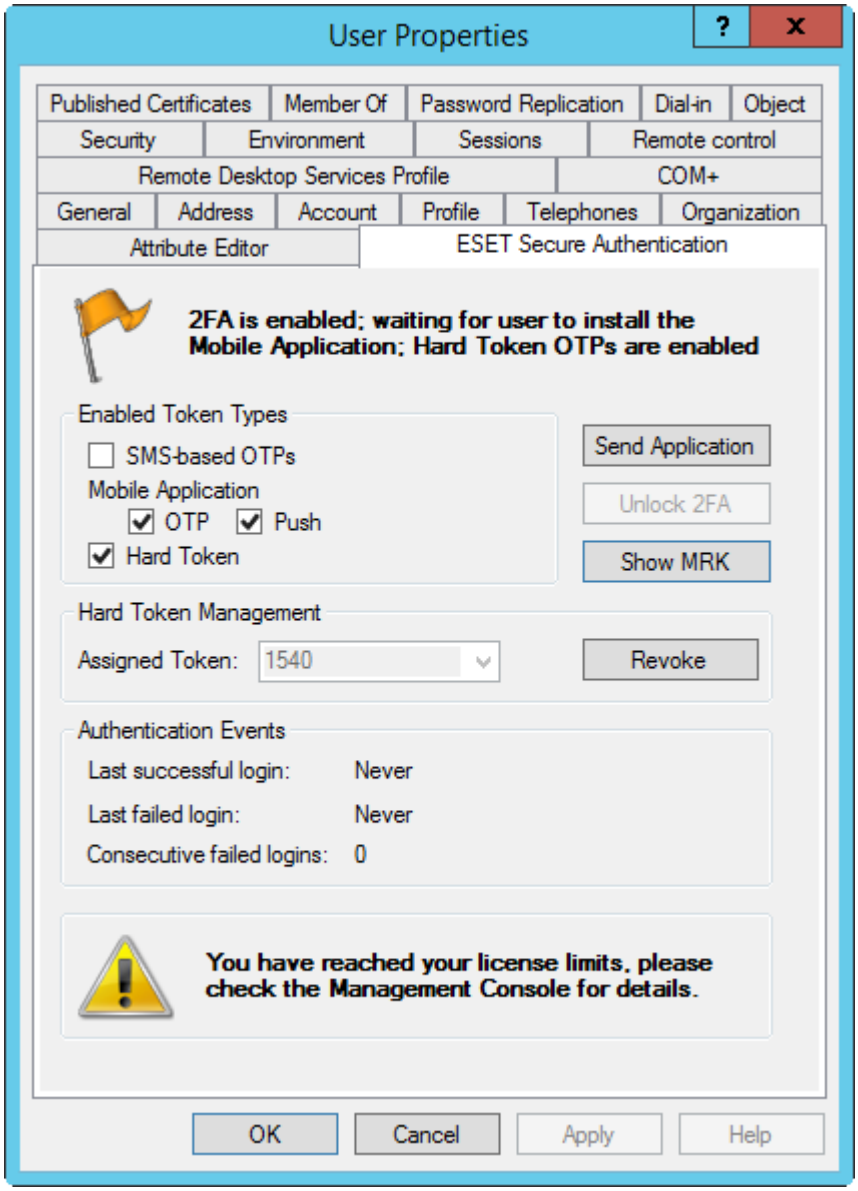
Пользователь может быть также в переходном состоянии, в котором включены все три типа OTP. В этом состоянии пользователь получает SMS с OTP, когда инициируются попытки аутентификации. Но если для аутентификации используется действительный OTP из мобильного приложения, SMS OTP будут отключены и пользователь сможет проходить аутентификацию, используя только пароли из мобильного приложения или Hard Token OTP:



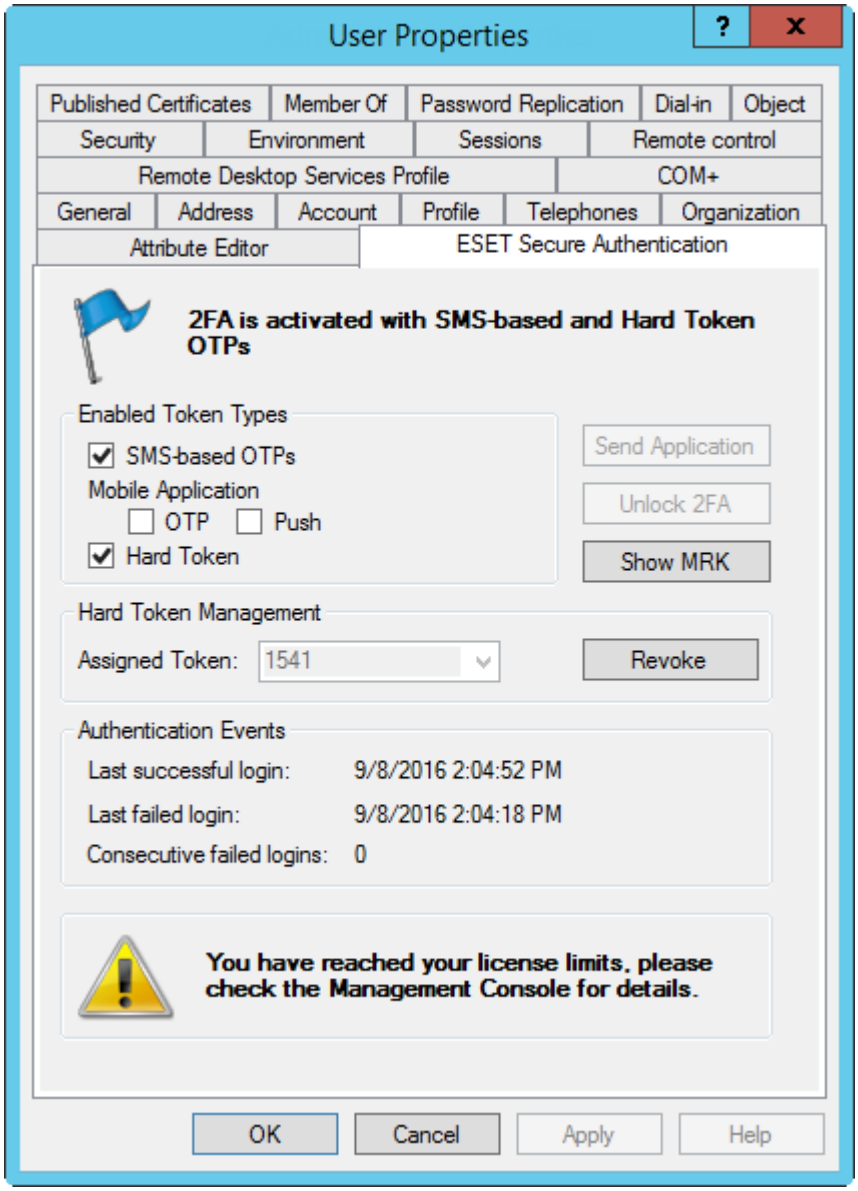
В состоянии, показанном на рисунке ниже, для пользователя включены Hard Token и OTPs:



Если мобильное приложение отправлено, но еще не установлено, состояние пользователя будет следующим.



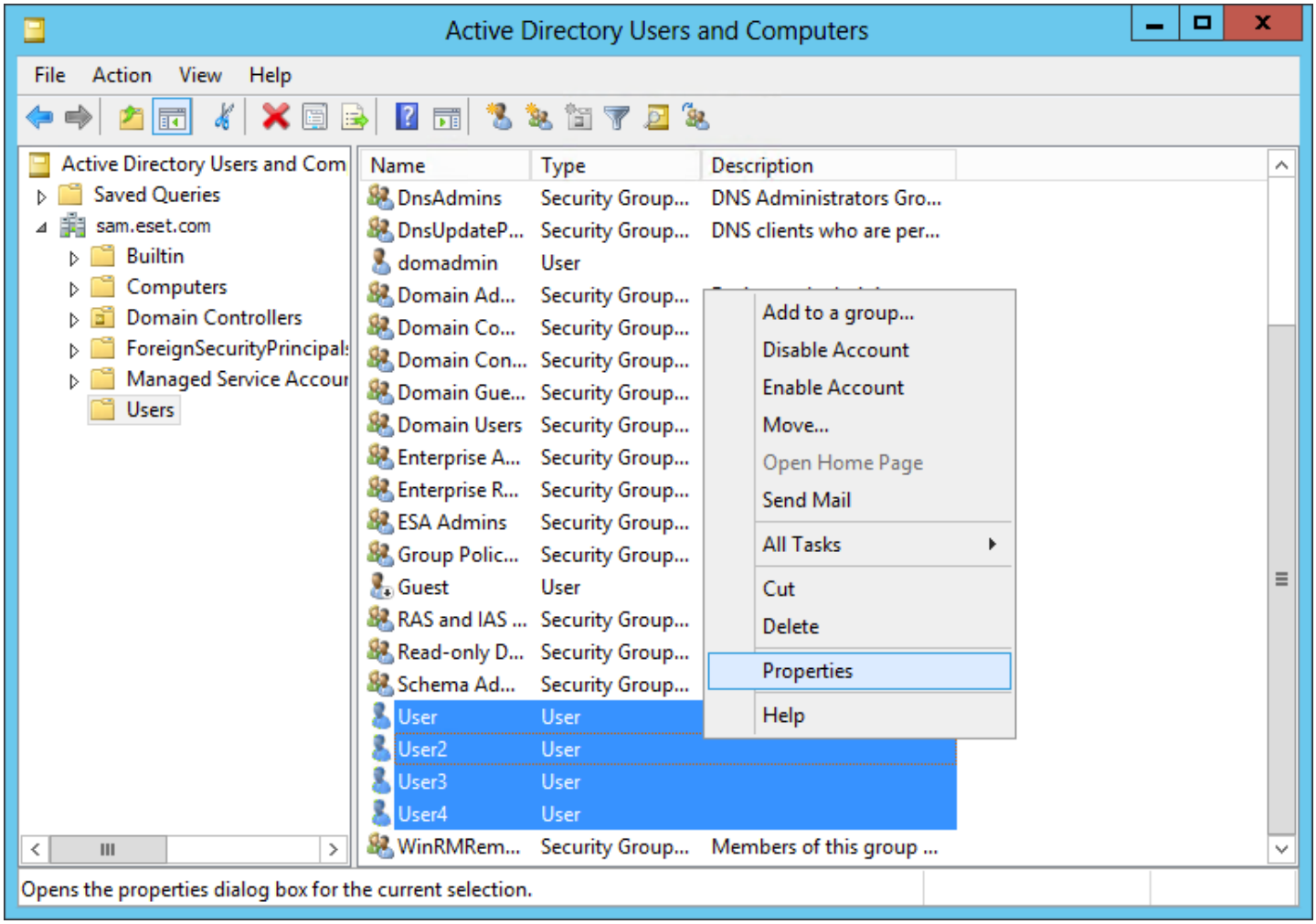
Могут быть включены пароли на основе SMS и Hard Token OTPs, и это тоже отдельное состояние.



14.2 Подготовка нескольких телефонов

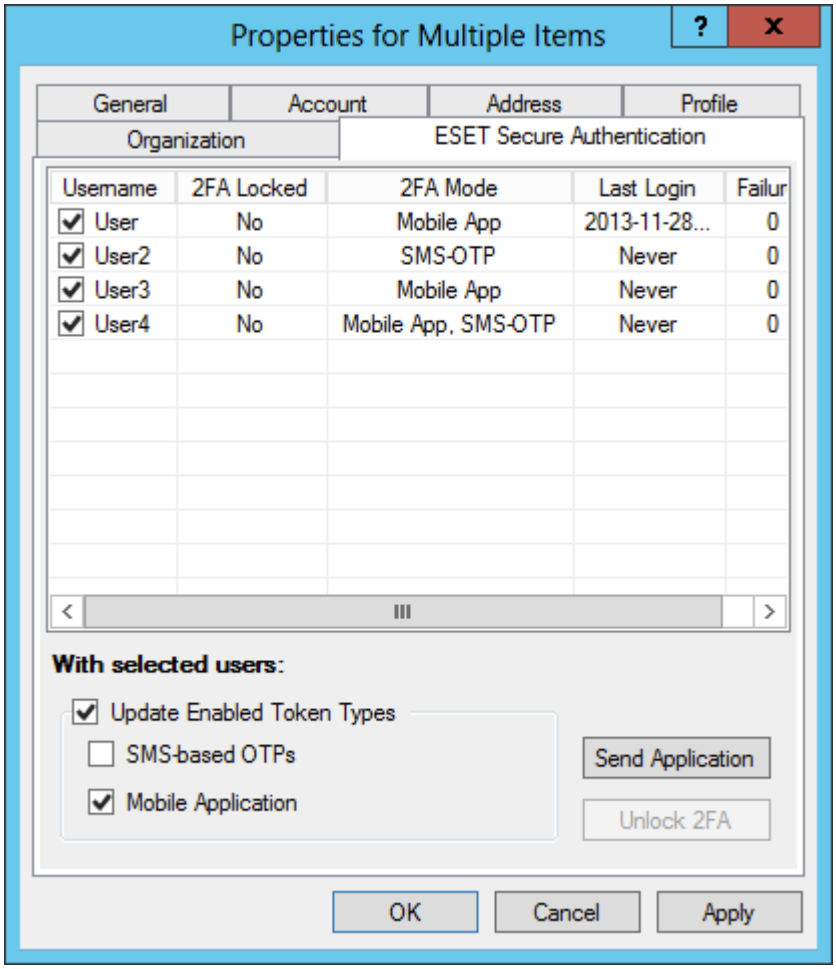
С помощью ADUC мобильное приложение ESET Secure Authentication или службу текстовых сообщений (SMS) можно отправить на несколько мобильных телефонов. Чтобы подготовка нескольких телефонов прошла успешно, в окне «User Properties» в поле 'Mobile' для каждого пользователя нужно указать действительный номер мобильного телефона. Инструкции по вводу номера мобильного телефона в окне «User Properties» см. в разделе Управление пользователями.

1. Откройте обычное представление пользователей ADUC.
2. Удерживая нажатой клавишу **CTRL**, выберите пользователей, которых нужно подготовить.
3. Щелкните правой кнопкой мыши группу подготавливаемых пользователей и выберите в контекстном меню пункт **Properties** (Свойства).



4. В окне **Properties for Multiple Items** (Свойства нескольких элементов) откройте вкладку ESET Secure Authentication.
5. Установите флажки **Update Enabled Token Types** (Обновить типы включенных маркеров) и **Mobile Application** (Мобильное приложение). Флажок **OTP** из **SMS** устанавливать не нужно.

6. Нажмите кнопку **Send Application** (Отправить приложение). Клиентские телефоны получат текстовое сообщение, содержащее ссылку на страницу загрузки мобильного приложения ESA.



Инструкции по установке и использованию мобильных приложений (выберите мобильную ОС, чтобы перейти к соответствующей статье):

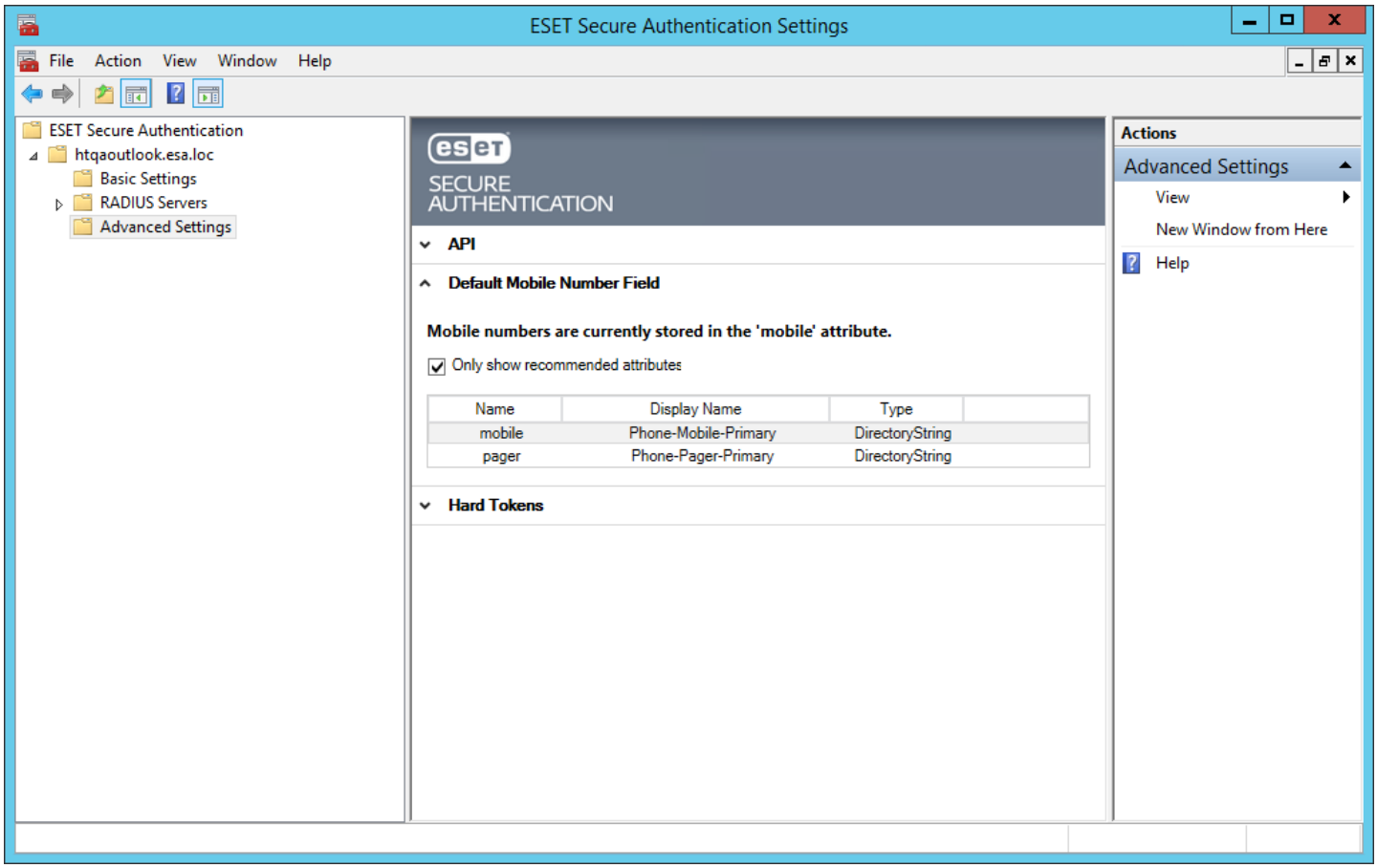
- Android
- BlackBerry
- iPhone
- Windows Phone

14.3 Переопределение поля с номером мобильного телефона

Вы можете указать поле Active Directory, из которого будет загружаться номер мобильного телефона пользователя. По умолчанию используется поле «Mobile».

Чтобы изменить поле номера мобильного телефона, выполните следующие действия:

1. Откройте ESA Management Console.
2. Разверните узел вашего домена.
3. Перейдите к узлу **Advanced Settings** (Дополнительные настройки).
4. Разверните панель **Default Mobile Number Field** (Поле номера мобильного телефона по умолчанию).



5. Для загрузки номера мобильного телефона можно указать другое поле.
6. После выбора другого поля нажмите кнопку **Save** (Сохранить).
7. Перезапустите службу ESET Secure Authentication Core Authentication Service.
    a. Найдите службу ESET Secure Authentication **Core Service** в Windows Services (для этого последовательно щелкните элементы **Control Panel** (Панель управления) - **Administrative Tools** (Администрирование) - **View Local Services** (Просмотр локальных служб)).
    b. Щелкните ESET Secure Authentication **Radius Service** правой кнопкой мыши и выберите пункт **Restart** (Перезапустить).

14.4 Управление пользователями с помощью групп

В больших доменах становится все сложнее отслеживать, для каких пользователей в домене активирована двухфакторная аутентификация. Для решения этой задачи в приложении ESET Secure Authentication предусмотрены средства ведения учета таких пользователей с помощью групп Active Directory.

В частности, во время установки создаются три группы Active Directory:

- Пользователи ESA.

В этой группе нет собственно пользователей. Вместо них здесь содержатся группы пользователей SMS-уведомлений ESA и мобильных приложений ESA. Таким образом, с помощью этой группы можно найти всех пользователей с двухфакторной аутентификацией в домене.

- Пользователи SMS-уведомлений ESA.

В эту группу входят все пользователи в домене, для которых настроена отправка SMS-уведомлений с одноразовыми паролями.

- Пользователи мобильных приложений ESA.

В эту группу входят все пользователи, для которых настроена функция одноразовых паролей для мобильных приложений.

Участие в той или иной группе изменяется сразу же, когда в ADUC настраиваются параметры пользователей. Найти всех пользователей, для которых, например, настроена отправка SMS-уведомлений с одноразовыми паролями, очень просто.

1. Откройте ADUC.
2. Щелкните узел домена правой кнопкой мыши и выберите пункт **Find** (Найти).
3. Введите поисковый запрос «ESA SMS» и нажмите клавишу ВВОД. Нужная группа появится в разделе **Search Result** (Результат поиска).
4. Дважды щелкните имя группы и перейдите на вкладку **Members** (Участники). Здесь будут показаны все пользователи в домене, для которых настроена отправка SMS-уведомлений с одноразовыми паролями.

15. Дополнительные разделы по VPN

Эта глава содержит сведения обо всех параметрах, доступных во время настройки двухфакторной аутентификации для VPN.

15.1 Параметры аутентификации VPN

Этот раздел содержит сведения о параметрах, доступных во время настройки клиента RADIUS с помощью консоли управления ESA Management Console.

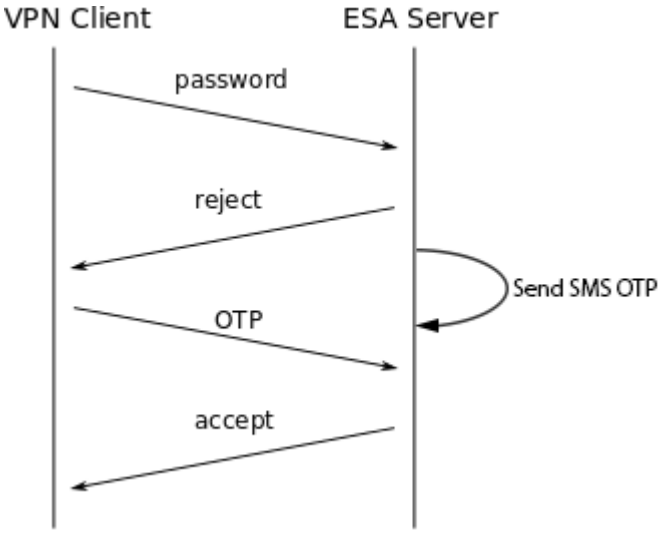
15.1.1 Одноразовые пароли из SMS

Этот сценарий используется, когда для пользователя настроена отправка OTP через SMS, а клиент RADIUS настроен на выполнение аутентификации с использованием OTP из SMS.

В этой ситуации пользователь входит в систему с помощью пароля Active Directory. Первая попытка аутентификации, выполненная клиентом VPN, завершится сбоем, и пользователю будет предложено ввести свой пароль еще раз. В это же время пользователь получит SMS с OTP. Получив в SMS свой OTP, пользователю нужно войти в систему с помощью этого пароля. Если введен правильный OTP, доступ будет предоставлен.

Эта последовательность показана на рисунке 1: RADIUS SMS OTP Authentication.

Поддерживаемые протоколы аутентификации: PAP, MSCHAPv2.



15.1.2 Одноразовые пароли из SMS по запросу

Решение ESET Secure Authentication поддерживает «On-demand SMS OTP» для некоторых систем, которые поддерживают выполнение первичной аутентификации в службе Active Directory, а вторичной — на сервере RADIUS. В этом случае пользователи, уже прошедшие аутентификацию в службе Active Directory, должны ввести текст 'sms' (без апострофов) в поле **ESA OTP** (Одноразовый пароль ESA), чтобы получить одноразовый пароль (One Time Password) в SMS-сообщении.

ПРИМЕЧАНИЕ. Эту функцию можно использовать, только если официальное Integration Guide ESET Secure Authentication содержит соответствующее указание. При неправильном использовании эта функция может позволить пользователям проходить аутентификацию только с OTP.

15.1.3 Мобильное приложение

Этот сценарий используется, когда для пользователя настроена только отправка пароля OTP и/или push-уведомления (Push), а для клиента RADIUS настроена аутентификация с помощью паролей OTP в мобильном приложении (Mobile Application OTPs) и/или push-уведомлений в мобильном приложении (Mobile Application Push).

Пользователь выполняет вход с помощью пароля OTP, созданного мобильным приложением (Mobile Application), или с помощью подтверждения push-уведомления на мобильном устройстве Android или часах Android. Обратите внимание, что, чтобы обеспечить второй этап аутентификации, в этом случае настоятельно рекомендуется использовать PIN.

Поддерживаемые протоколы PPTP: PAP, MSCHAPv2.

ПРИМЕЧАНИЕ. Если в мобильном приложении Mobile Application включена защита с помощью PIN-кода, пользователю будет разрешен доступ с помощью неправильного PIN-кода для защиты правильного PIN-кода от атаки методом подбора. Например, если злоумышленник пытается войти в приложение Mobile Application с помощью неправильного PIN-кода,

доступ может быть предоставлен, но пароль OTP не будет работать. После ввода нескольких неправильных паролей OTPпроизойдет автоматическая блокировка 2FA в учетной записи пользователя (к которой относится приложение Mobile Application). Это связано с небольшими проблемами для пользователя. Если пользователь случайно войдет в приложение Mobile Application с помощью неправильного PIN-кода, а затем сменит PIN-код на новый, все маркеры в приложении Mobile Application станут недействительными. Эти маркеры нельзя восстановить. Единственный выход из ситуации — повторно подготовить маркеры для мобильного приложения (Mobile Application). Поэтому мы рекомендуем пользователям попробовать использовать одноразовый пароль, прежде чем менять PIN-код. Если пароль OTP работает, то PIN-код смело можно менять.

Обратите внимание, что если мобильное приложение Mobile Application защищено PIN-кодом, сообщение **Утвердить по телефону** отображается на Android-часах при создании push-уведомления.

Compound Authentication Enforced

Этот сценарий используется, если в клиенте RADIUS настроена **Compound Authentication** (Сложная аутентификация). Этот метод аутентификации предназначен только для пользователей, которые могут использовать Mobile Application OTPs.

В этом случае пользователь входит в VPN, используя свой пароль для Active Directory (AD), в который добавлен OTP, созданный Mobile Application. Например, если паролем AD является слово «password», а одноразовый пароль — 123456, на клиенте VPN пользователь должен ввести в поле пароля текст «password123456».

Поддерживаемые протоколы аутентификации: PAP.

15.1.4 Маркеры оборудования

Этот сценарий применяется, когда для пользователя и клиента RADIUS настроено использование паролей маркеров оборудования,Hard Token OTPs.

В зависимости от конфигурации клиента VPN можно применять либо одиночную аутентификацию с использованием маркеров оборудования (Hard Token), либо сложную аутентификацию с использованием маркеров оборудования (Hard Token).

В случае применения сложной аутентификации с использованием маркера оборудования (Hard Token) пользователь входит в VPN после ввода пароля Active Directory (AD), соединенного с одноразовым паролем OTP, созданным маркером оборудования (Hard Token). Например, если паролем AD является слово password и задан пароль OTP 123456, пользователь должен ввести password123456 в поле пароля на клиенте VPN.

Поддерживаемые протоколы аутентификации: PAP.

15.1.5 Переход с одноразовых паролей из SMS на пароли из мобильного приложения

Этот сценарий имеет место, если для пользователя настроено использование OTP из SMS и Mobile Application, а в клиенте RADIUS настроена аутентификация с использованием OTP.

В этом случае пользователь может использовать для входа либо OTP из SMS, либо Mobile Application OTP (как описано выше).

Если пользователь входит с помощью OTP из Mobile Application, аутентификация с использованием SMS OTP автоматически выключается. При последующих попытках входа OTP из SMS не будет приниматься в качестве учетных данных для входа.

Поддерживаемые протоколы аутентификации: PAP, MSCHAPv2.

15.1.6 Транзитная передача без двухфакторной аутентификации

Такая передача имеет место, если для пользователя не включено использование одноразовых паролей на основе SMS-, Mobile Application- или Hard Token-based OTPs,, а выбран параметр конфигурации клиента RADIUS, который предусматривает использование **Active Directory passwords without OTPs** (Пароли Active Directory без одноразовых паролей).

В этом случае пользователь входит в систему с помощью пароля Active Directory.

Поддерживаемые протоколы аутентификации: PAP, MSCHAPv2.

ПРИМЕЧАНИЕ.: Для сетей VPN сервера маршрутизации и удаленного доступа Майкрософт, которые используют протокол PPTP (Microsoft Routing & Remote Access Server (RRAS) PPTP VPN), подключение к VPN не шифруется, если используется протокол аутентификации PAP. Поэтому применять шифрование не рекомендуется. Большинство других поставщиков VPN шифруют соединение независимо от протокола аутентификации.

15.1.7 Управление доступом с помощью групп

ESA позволяет предоставлять доступ к VPN с помощью двухфакторной аутентификации (2FA) только участникам конкретной группы безопасности AD. Этот параметр можно настроить для каждого клиента RADIUS в отдельности в меню **Access Control** (Контроль доступа).

15.2 Одноразовые пароли и пробелы

Для удобочитаемости OTP в мобильном приложении отображается с пробелом между третьей и четвертой цифрами. Все методы аутентификации, кроме MS-CHAPv2, удаляют пробелы из введенных учетных данных. Поэтому при вводе одноразового пароля пользователь может либо оставить эти пробелы, либо удалить их. Это не повлияет на процесс аутентификации.

15.3 Методы аутентификации ESA и совместимость с PPP

В этом разделе объясняется, какие методы аутентификации PPP совместимы с конкретными методами аутентификации ESA. На сервере VPN должны быть разрешены все протоколы, которыми могут пользоваться клиенты. Для конечных клиентов VPN нужно настроить только один протокол.

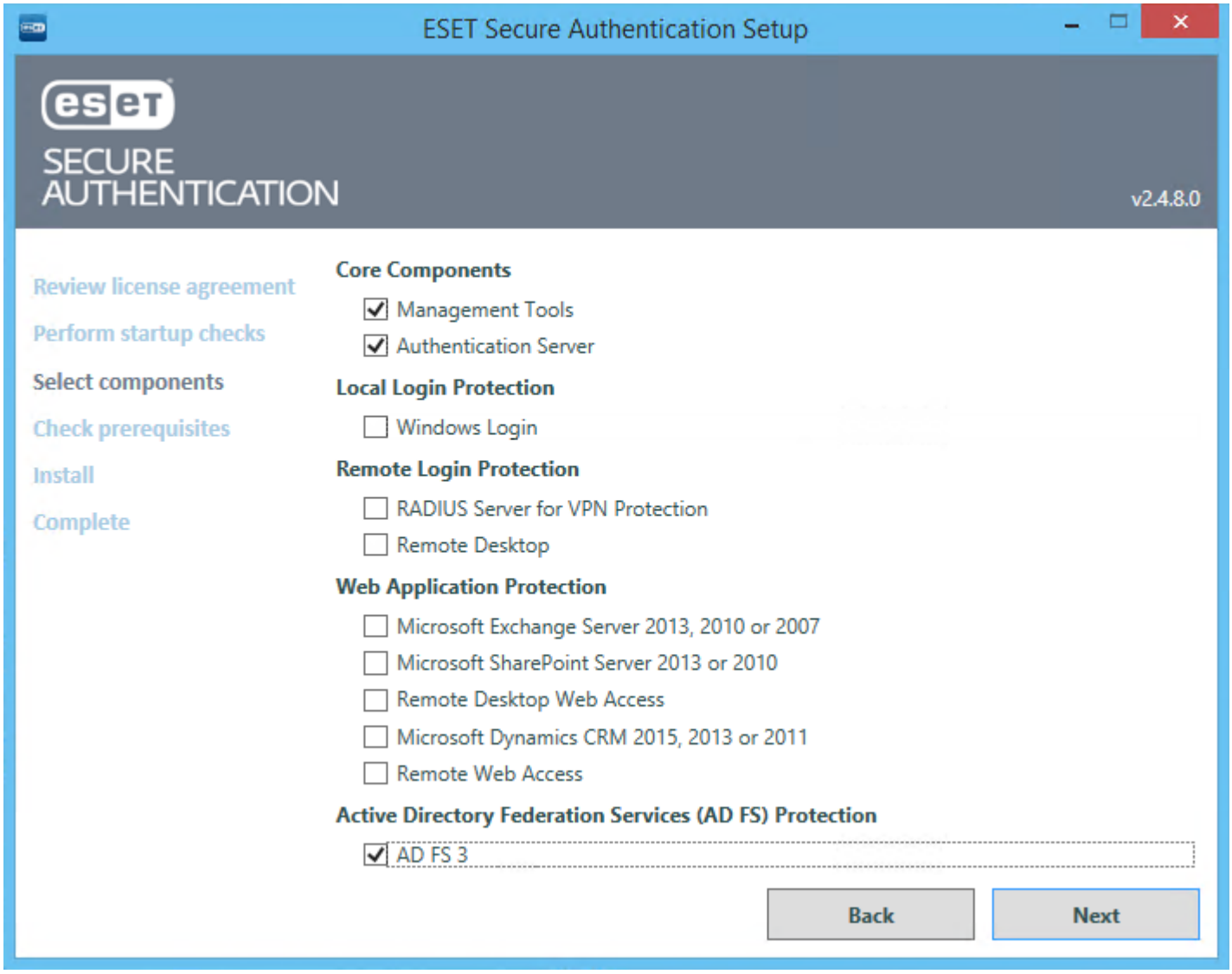
Если поддерживается несколько протоколов, в клиентах VPN нужно настроить использование протокола MS-CHAPv2 с 128-bit MPPE. Это означает, что PAP рекомендуется использовать только для Compound Authentication.

Метод аутентификации	**PAP**	**MS-CHAPv2**
SMS-Based OTPs	Поддерживается	Поддерживается
On-demand SMS-Based OTPs	Поддерживается	Поддерживается
Mobile-Application (OTP или Push)	Поддерживается	Поддерживается
Mobile Application (Compound Authentication)	Поддерживается	Не поддерживается
Hard Token OTPs	Поддерживается	Поддерживается
Hard Token (Compound Authentication)	Поддерживается	Не поддерживается
Пароли Active Directory без OTPs	Поддерживается	Поддерживается

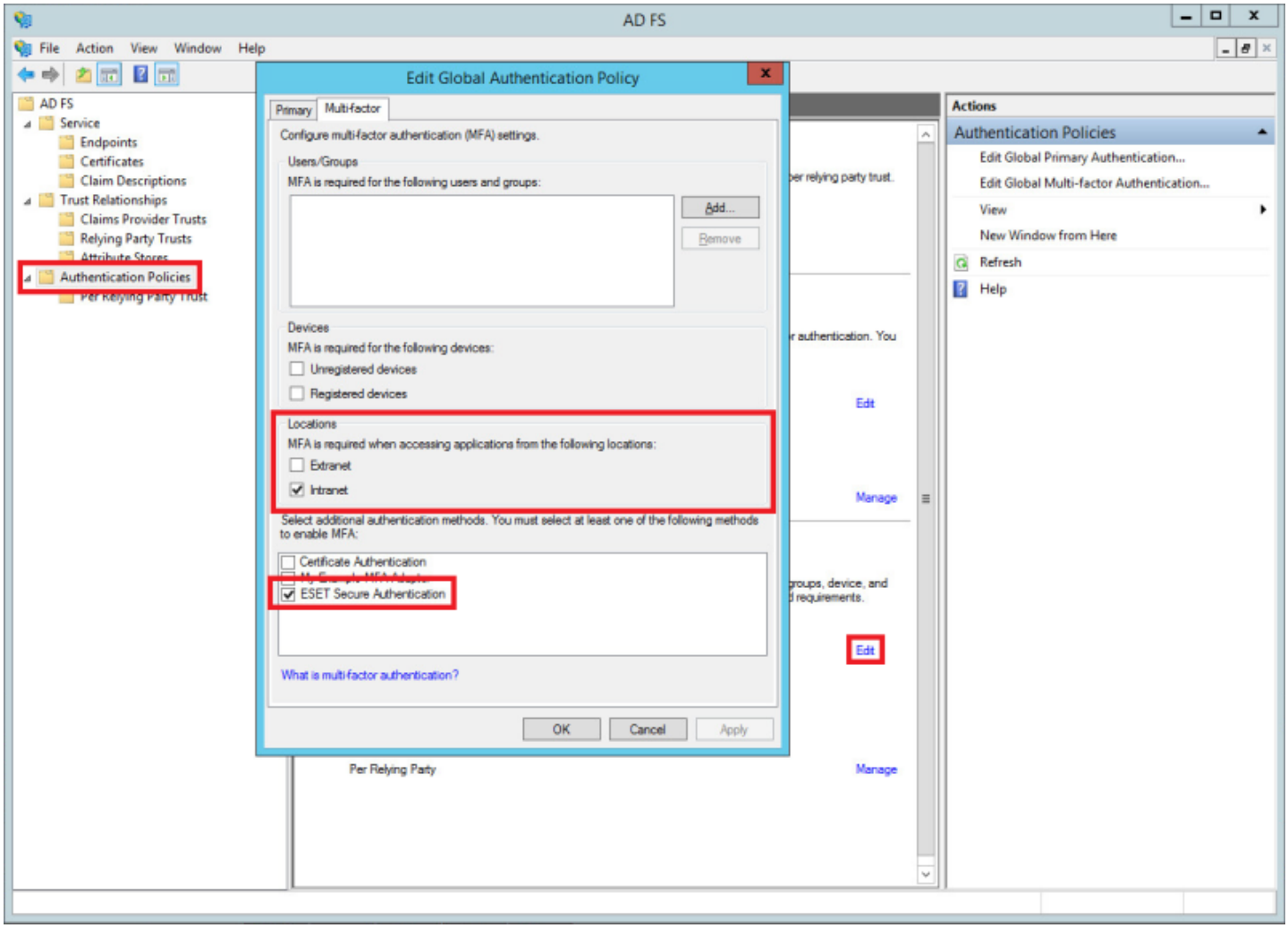
16. AD FS

Решение ESA — это отличный выбор для безопасности, если вы используете службы Active Directory Federation Services (AD FS) 3 or 4 и нужно обеспечить их безопасность с помощью метода аутентификации2FA (двухфакторная аутентификация).

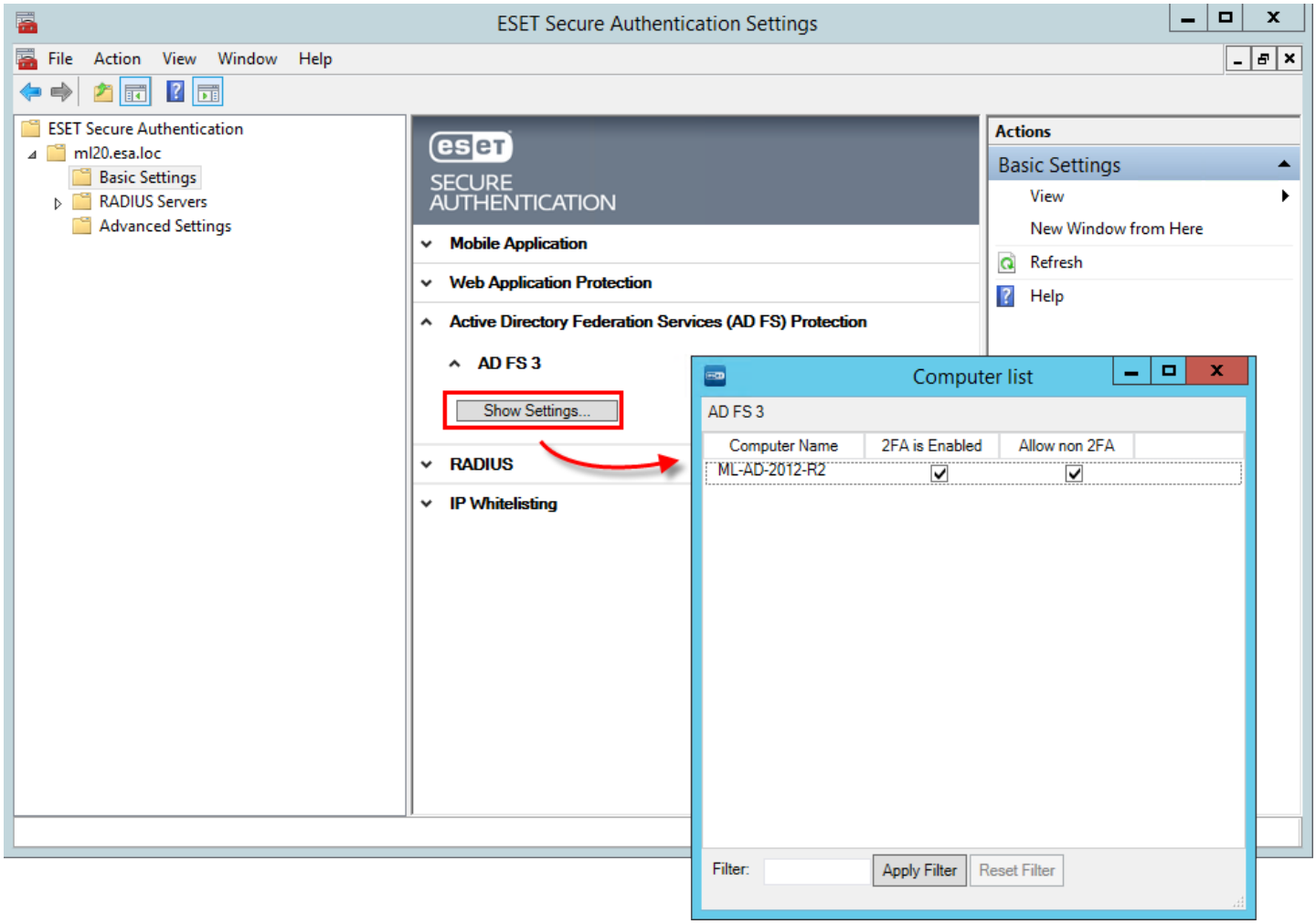
При установке решения ESA на компьютере, на котором запущена служба AD FS 3 or 4, выберите компонент **AD FS 3 or 4** (AD FS 3 или 4) и завершите установку.



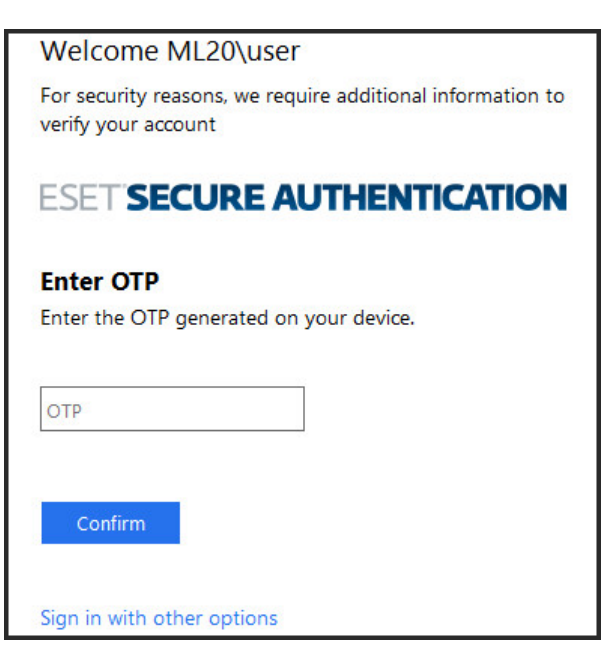
Во время установки служб AD FS изменяется конфигурация: добавляется метод аутентификации ESET Secure Authentication и, если расположение не указано, используются расположения обоих следующих типов: из частной (Intranet) и внешней (Extranet) сетей. На рисунке ниже отображены изменения конфигурации. Расположение интрасети (**Intranet**) выбрано до установки компонента AD FS 3 or 4 решения ESA.



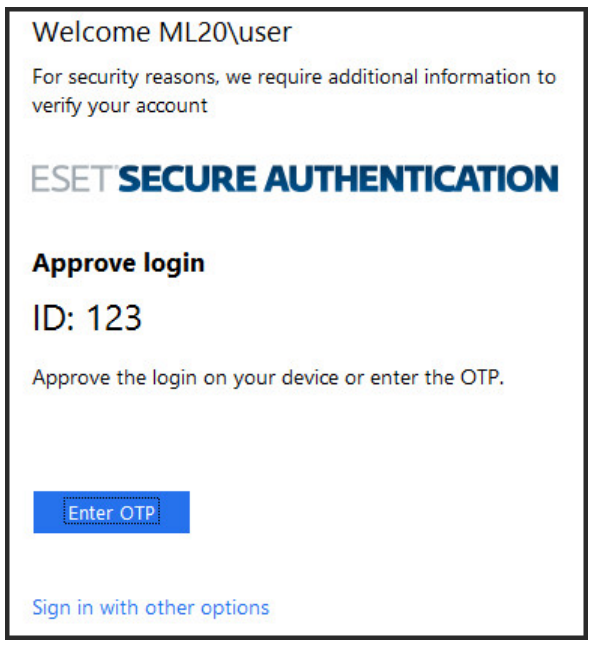
По окончании установки откройте консоль управления ESA (ESA Management Console), перейдите к элементу **Basic Settings** (Основные параметры), разверните элемент **Active Directory Federation Services (AD FS) Protection** (Защита Active Directory Federation Services (AD FS)), и отобразятся параметры **Protect AD FS 3 on this machine with 2FA** (Защита AD FS 3 на этом компьютере с помощью метода двухфакторной аутентификации) и **Users without 2FA enabled may still log in** (Пользователи, у которых не включен метод двухфакторной аутентификации, могут входить).



Если веб-сайт, требующий аутентификации, проверяет удостоверение в службе AD FS 3 or 4, а двухфакторная аутентификация (2FA) с помощью решения ESA применяется к определенной службе AD FS 3, то после успешной проверки удостоверения отображается запрос на ввод одноразового пароля OTP или на подтверждение push-уведомления:



Требуется одноразовый пароль



Требуется подтверждение push-уведомления

Если необходимо отображать настраиваемый логотип в окне ввода одноразового пароля (OTP ,) или утвердить уведомление вместо используемого по умолчанию логотипа ESET Secure Authentication, выполните следующие действия. Все действия выполняются на компьютере, на котором установлено ядро ESA core.

1. Сохраните необходимый логотип как файл изображения с расширением *.png*. Рекомендуемые максимальные размеры — 350 x 100 пикселей (ширина x высота).
2. Разместите логотип в папке *C:\ProgramData\ESET Secure Authentication\Customization* и дайте ему имя «*logo.png*».

17. Аудит и лицензирование

17.1 Аудит

ESA записывает записи аудита в журналы событий Windows, в частности в журнал Application в разделе «Windows Logs». Для просмотра записей аудита можно использовать средство «Windows Event Viewer».

Записи аудита делятся на следующие категории.

- Аудит пользователей.
  - Успешные и неудачные попытки аутентификации.
  - Изменение состояния 2FA, когда блокируется учетная запись пользователя.
- Аудит системы.
  - Изменения параметров ESA.
  - Запуск или остановка службы ESA.

Использование стандартной архитектуры ведения журнала событий Windows облегчает использование средств агрегации и отчетности от сторонних разработчиков (например, LogAnalyzer).

17.2 Лицензирование

17.2.1 Обзор

Лицензия ESA имеет три параметра:

- User Total
- Expiry Date
- SMS Credits

Подробная информация о лицензии извлекается из системы ESET Licensing, и система ESA автоматически проверяет действительность лицензии.

Сервер ESA Provisioning может обеспечить использование лицензий, ограничивая количество SMS OTP и подготовку пользователей. Кроме того, сервер аутентификации ESA обеспечивает использование лицензий, ограничивая действия по управлению пользователями и (в крайних случаях) отключая их аутентификацию.

17.2.2 Предупреждения

Предупреждения передаются ESA Administrator в подключаемом модуле User Management консоли ADUC и в ESA Management Console.

Во время управления пользователями

Если состояние лицензии не соответствует норме, в интерфейсе ADUC (управление пользователями) будет отображаться предупреждение. Это предупреждение указывает на серьезность проблемы, но из-за ограниченного места не содержит подробности.

Во время администрирования системы

В интерфейсе управления системой отображается полное состояние лицензии. Оно включает в себя общее состояние лицензии, а также сведения об использовании (количество пользователей, оставшиеся кредиты SMS, оставшийся срок действия лицензии).

17.2.3 Состояния лицензий

Лицензия сервера ESA может находиться в одном из шести состояний.

1. **OK**: все параметры лицензии находятся в заданных пределах.
2. **Warning**: как минимум один параметр приближается к граничному значению.
3. **SMS Credits Expired**: закончились кредиты на SMS, SMS-уведомления с OTP и данными для подготовки отправляться не будут.
4. **Violation (full functionality)**: один из параметров лицензии превысил граничное значение, но никаких принудительных мер не предпринято.
5. **Violation (limited functionality)**: параметр лицензии превышает граничное значение более 7 дней, некоторые функции управления пользователями отключены.
6. **ESA Disabled**: срок действия лицензии ESA истек более 30 дней назад, аутентификация отключена. В этом случае вызовы аутентификации не будут выполняться: аутентификация будет заблокирована, пока система ESA не будет удалена, отключена администратором или повторно лицензирована.

Подробные сведения о License States

В следующей таблице описано, как каждый из параметров лицензии может стать причиной появления одного из состояний ошибки или предупреждения, перечисленных выше.

	Warning	SMS Credits depleted	Violation (full functionality)	Violation (limited functionality)	ESA Disabled
License Expiry	Менее 30 дней до окончания срока действия	Н/д	Не более 7 дней после истечения срока действия	Более 7 дней после истечения срока действия	Более 30 дней после истечения срока действия
Количество пользователей	Доступно менее 10 % или 10 мест в зависимости от того, какое количество меньше	Н/д	Количество активных пользователей превышает количество лицензированных пользователей	Количество активных пользователей превышает количество лицензированных более 7 дней	Никогда
SMS Credits	Осталось менее 10 кредитов SMS (введение + пополнение)	0 кредитов SMS осталось	Никогда	Никогда	Никогда

17.2.4 Обеспечение использования лицензии

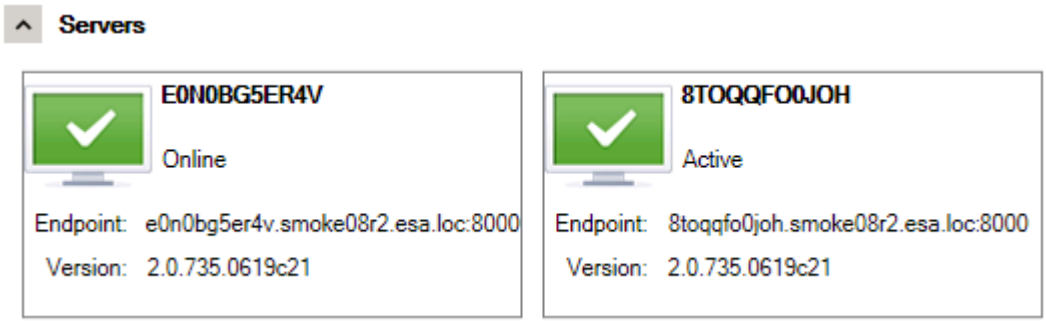
В следующей таблице показано, как обеспечивается использование лицензии на сервере аутентификации ESA. Администратор всегда имеет возможность отключить аутентификацию ESA для определенного количества пользователей (путем отключения 2FA для этих пользователей) или для всех пользователей (через настройки системы или удаление продукта).

	OK	Warning	SMS Credits depleted	Violation (full functionality)	Violation (limited functionality)	ESA Disabled
Enable Users for 2FA	Разрешено	Разрешено	Разрешено	Разрешено	Отключено	Отключено
Provision Users	Разрешено	Разрешено	Отключено	Разрешено	Отключено	Отключено
Authenticate with SMS OTP	Разрешено	Разрешено	Отключено	Разрешено	Разрешено	Отключено
Authenticate with mobile app (OTP, Push)	Разрешено	Разрешено	Разрешено	Разрешено	Разрешено	Отключено
Authenticate with hard token	Разрешено	Разрешено	Разрешено	Разрешено	Разрешено	Отключено

Manage system configuration	Разрешено	Разрешено	Разрешено	Разрешено	Разрешено	Разрешено
Disable Users for 2FA	Разрешено	Разрешено	Разрешено	Разрешено	Разрешено	Разрешено

18. Просмотр высокой доступности

Все установленные серверы отображаются в консоли управления ESA на панели **Servers** (Серверы). Если в сети обнаружено несколько основных служб, отображаются все серверы. Подключенные к сети и активные серверы отображаются зеленым цветом, а серверы в автономном режиме — красным.



Каждая ESA Authentication Service, которая устанавливается в домене, регистрирует себя в AD DNS, используя запись SRV (как _esetsecauth._tcp). Когда конечная точка (например, веб-приложение или устройство VPN) начинает аутентификацию, она сначала сверяется со своим внутренним списком известных серверов. Если список пуст, она выполняет поиск по записям SRV. Поиск по записям SRV возвращает все Authentication Servers в домене. После этого конечная точка выбирает Authentication Server для подключения. Если подключение невозможно, точка выбирает другой сервер из списка и пытается подключиться снова.

Если для защиты VPN с помощью ESA избыточность сети является проблемой, на устройстве VPN рекомендуется настроить первичный и вторичный аутентификаторы RADIUS. Затем необходимо установить в сети два сервера ESA RADIUS и настроить их соответствующим образом.

19. Глоссарий

AD — Active Directory.

ADUC — интерфейс управления пользователями и компьютерами Active Directory (Active Directory Users and Computers).

COS — операционная система клиента.

ESA — ESET Secure Authentication.

ESA core — сервер аутентификации, который проверяет действительность введенного пароля OTP.

GPO — объект групповой политики.

MRK — главный ключ восстановления.

Online (оперативный режим) — компьютер, на котором установлены основные компоненты решения ESA (по крайней мере сервер аутентификации) и запущена служба аутентификации ESET Secure Authentication Service. Этот компьютер доступен через подключение по протоколу TCP/IP.

Offline (автономный режим) — компьютер, на котором установлены основные компоненты решения ESA, при этом на нем не запущена служба аутентификации ESET Secure Authentication Service или он недоступен через подключение по протоколу TCP/IP.

OS — операционная система.

OTP — одноразовый пароль с ограниченным временем действия.

Mobile Application Push — push-уведомление с ограниченным сроком действия.

RDP — протокол удаленного рабочего стола. Защищенный законодательством об интеллектуальной собственности протокол, разработанный корпорацией Майкрософт. Он дает возможность подключаться к другому компьютеру по сети с помощью графического пользовательского интерфейса.

SOS — операционная система сервера.