ESMART®

ESMART Token

Авторизация в домене Windows

Содержание

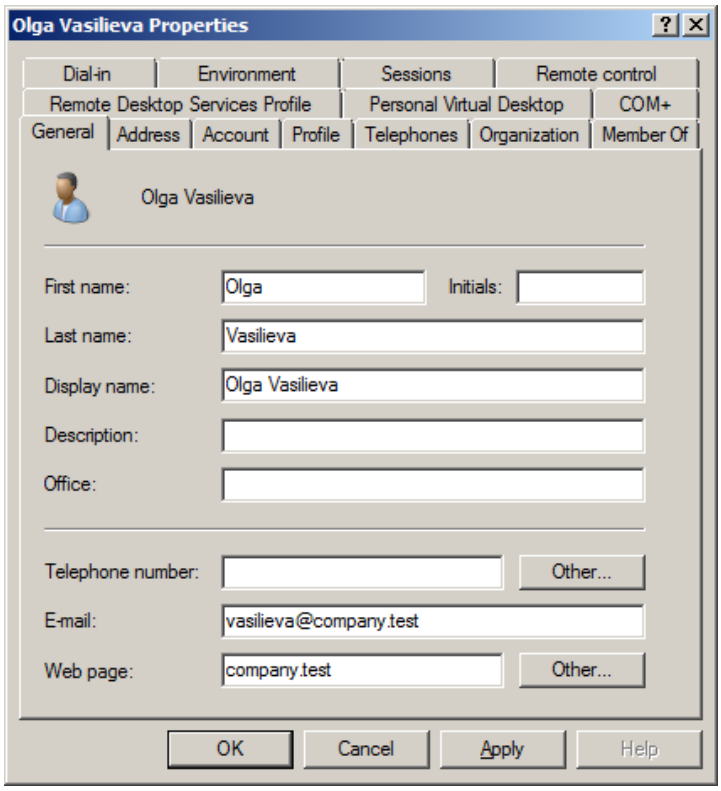
1. Преимущества использования ESMART Token

ESMART Token позволяет пользователям не запоминать длинные пароли, а использовать двухфакторную идентификацию, т.е. пользователь должен предъявить системе свою карту или USB-ключ ESMART Token и ввести ПИН-код карты. Администратор сети в соответствии с корпоративными правилами может разрешить вход в систему только по карте или разрешить вход и по карте, и по логину и паролю.

2. Выдача сертификата пользователя

Удостоверяющие центры (в текущей локализации Windows Server – «Центры сертификации») на базе Windows Server 2003 и Windows Server 2008 и выше используют разные методы выписки пользовательских сертификатов. Для выдачи сертификатов одному или нескольким администраторам должны быть выписаны сертфикаты по шаблону Enrollment Agent или производному шаблону. Подробно процедура выдачи сертификатов администратора с правом запрашивать сертфикаты пользователей описана в руководствах по развертыванию центра сертификации для Windows Server 2003 и Windows Server 2008 соответственно.

Создайте или откройте учетную карточку пользователя. Если выданный сертификат планируется использовать для электронной подписи, а не только для входа в систему, добавьте адрес корпоративной электронной почты пользователя.



Windows 2003 Server – выпишите сертификат пользователя на карту, используя Internet Explorer. Можно использовать подключение через удаленный рабочий стол или выписать сертификаты непосредственно на сервере. См. ***Руководство по развертыванию центра сертификации Windows Server 2003****.*

Windows 2008 Server и выше – выпишите сертификат пользователя на карту, используя консоль с оснасткой сертификатов certmgr.msc. Можно использовать подключение через удаленный рабочий

стол или выписать сертификаты непосредственно на сервере. См. ***Руководство по развертыванию центра сертификации Windows Server 2008****.*

Наличие собственного центра сертификации позволяет гибко настраивать параметры выдаваемых сертификатов. Помимо стандартных шаблонов могут быть созданы шаблоны с требуемыми параметрами, например в руководстве по развертыванию центра сертификации показан пример создания нового шаблона сертификата на основе стандартного шаблона ***Пользователь со смарт-картой*** *(Smartcard User), в который добавлена поддержка EFS-шифрования. Таким образом, вход в систему и использование возможностей EFS совмещено в одном сертификате. Данный пример не является рекомендацией, т.к. необходимо обратить внимание на процедуру отзыва такого сертификата, чтобы не потерять ключевую пару, которой зашифрованы файлы.*

3. Подготовка к работе

3.1 Инициализация токена

Инициализируйте токен при помощи ESMART PKI Client (см. ***руководство администратора ESMART Token PKI Client****) или бесплатной утилитой pkcs11-tool (см.* ***руководство ESMART Token PKCS11****).*

3.2 Подготовка ПК пользователя

Подключите считыватель смарт-карт к USB-порту. Если драйвера устройств не могут быть установлены автоматически через Windows Update, установите их вручную. Установите на компьютер, на котором необходимо реализовать вход в домен, пакет ESMART PKI Client. См. ***руководство администратора ESMART Token PKI Client****.*

Убедитесь, что корневой сертификат УЦ имеется в списке корневых доверенных, если нет, установите его вручную или распространите посредством групповой политики, как показано в руководстве по развертыванию центра сертификации.

4. Повышение безопасности системы

Использование смарт-карт или USB-ключей ESMART Token для входа в ПК позволяет повысить безопасность системы.

Для этого используются два механизма:

- *Обязательное предъявление смарт-карты или USB-ключа для входа;*
- *Поведение при извлечении смарт-карты или USB-ключа.*

Особенно эффективны оба этих механизма, когда карта или USB-ключ пользователя используются одновременно в системе контроля и управления доступом (СКУД[1]). Тогда пользователь не сможет уйти, оставив карту в считывателе.

Если разрешен вход в систему только с использованием смарт-карт, необходимо позаботится о процедуре быстрой выдачи временных сертификатов для входа, если пользователь забыл карту. При этом постоянный сертификат может быть временно отозван (причина отзыва ***Certificate Hold****), а через один или несколько дней такому сертификату можно будет вернуть статус действующего.*

Как правило, при извлечении карты компьютер пользователя блокируется, и возобновить работу с системой можно только после предъявления карты/ключа и ввода ПИН-кода. Также при извлечении карты сеанс пользователя может автоматически завершаться. Тем не менее, использовать такой вариант нежелательно, если есть возможность потери несохраненных данных.

---

[1] *Стоимость и условия поставки смарт-карт и USB-ключей с возможностью использования в СКУД оговаривается отдельно при заказе.*

5. Методы настройки

Методы повышения безопасности могут настраиваться как на локальной машине, так и через групповую политику домена. Настройки через групповую политику подробно описаны в руководстве по развертыванию центра сертификации на Windows Server 2008. В данном руководстве показаны только настройки локального ПК.

***Внимание!** Если настройки не заданы через групповую политику в домене, опытные пользователи могут изменить их самостоятельно, если у них остаётся доступ к редактору локальной групповой политики и к редактору реестра.*

5.1 Запуск службы удаления смарт-карт

Если служба политики удаления смарт-карт (SCPolicySVC – Smartcard Removal Policy) не запущена, при извлечении смарт-карты или USB-ключа ESMART Token не будет происходить никаких изменений при любых настройках. По умолчанию служба запущена только в ОС Windows XP. В Windows Vista и выше службу SCPolicySVC необходимо запустить вручную или через доменные групповые политики. Далее описан запуск службы для локальной машины. Автоматический запуск службы через доменные групповые политики описан в руководстве по развертыванию центра сертификации.

*Для запуска службы SCPolicySVC на локальной машине откройте диспетчер задач и перейдите во вкладку Службы. Найдите службу **SCPolicySVC – Политика удаления смарт-карт** и запустите ее. Рекомендуется поставить автоматический режим запуска.*

5.2 Изменение реестра

Изменение записи в реестре позволяет настроить поведение сеанса при извлечении пользователем смарт-карты. Групповые политики имеют больший приоритет и позволяют осуществить больше настроек. Если правило задано через групповую политику, изменение реестра невозможно.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\scremoveoption

Опция scremoveoption может принимать следующие значения:

0 – ничего не делать;

1 – блокировать рабочую станцию;

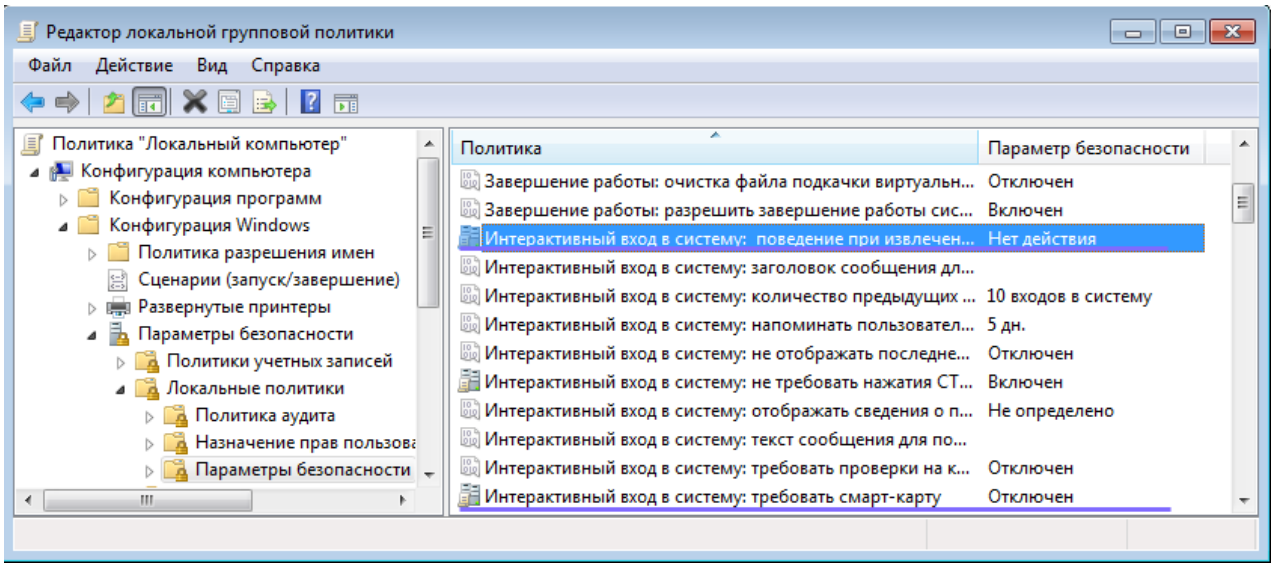
2 – принудительный выход из системы;

3 – отключение в случае удаленного сеанса служб терминалов.

5.3 Настройка групповых политик

*Групповая политика может быть настроена как для локальной машины, так и в домене. В примере в руководстве по настройке центра сертификации рассмотрена настройка групповой политики в домене. Изменение параметров для локального ПК производится через консоль **gpedit.msc**:*

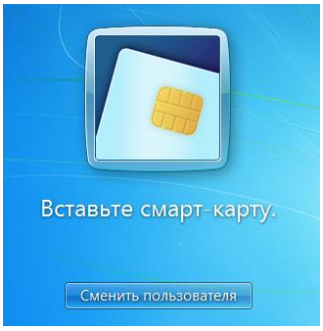
> *Конфигурация компьютера › Конфигурация Windows › Параметры безопасности › Локальные политики › Параметры безопасности*



6. Окно ввода ПИН-кода в разных ОС

Windows XP

Windows 7



Windows 8