

Indeed-Id OMNIKEY+PalmSecure Provider

Руководство по установке и эксплуатации



© Компания «Индид», 2009 – 2018. Все права защищены.

Этот документ входит в комплект поставки продукта. Информация, содержащаяся в этом документе, может быть изменена разработчиком без уведомления пользователя.

8 (800) 333-09-06

телефон бесплатной горячей линии

ООО Индид

ИНН/КПП 7801540219/780601001, ОГРН 1117847053103

8 (800) 333-09-06 или support@indeed-id.com

служба поддержки пользователей

<http://indeed-id.ru/>

web-сайт компании

Оглавление

Введение	4
Условные обозначения	4
О компоненте Indeed-Id OMNIKEY+PalmSecure Provider	4
Работа с Indeed-Id OMNIKEY+PalmSecure Provider	5
Регистрация аутентификатора	5
Аутентификация при помощи Indeed-Id OMNIKEY+PalmSecure Provider	10
Управление аутентификаторами	12
Установка и настройка Indeed-Id OMNIKEY+PalmSecure Provider	13
Установка компонента	13
Настройка параметров аутентификации	14

Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed. Данное руководство, предназначенное для администраторов и пользователей продуктов Indeed-Id, поможет ознакомиться с принципом работы компонента **Indeed-Id OMNIKEY+PalmSecure Provider** и параметрами его установки.

Условные обозначения

В Руководстве используются следующие условные обозначения:



Важная информация. Разделы, содержащие важную информацию, необходимую для успешной работы.



Дополнительная информация. Разделы, содержащие дополнительную информацию.

О компоненте Indeed-Id OMNIKEY+PalmSecure Provider

Indeed-Id OMNIKEY+PalmSecure Provider предназначен для совместного использования с продуктами Indeed-Id Windows Logon и Indeed-Id Enterprise SSO. Компонент объединяет в себе две технологии аутентификации пользователей: биометрическую и радиочастотную. Данный провайдер необходим для строгой аутентификации пользователей с применением бесконтактных биометрических сканеров Fujitsu (технология PalmSecure) и считывателей RFID-карт HID OMNIKEY.

На данный момент поддерживаются следующие модели сканеров HID OMNIKEY:

- OMNIKEY 5325
- OMNIKEY 6321
- OMNIKEY 5321 CLi
- OMNIKEY 6321 CLi
- OMNIKEY 5427 CK
- OMNIKEY 5421

Работа с Indeed-Id OMNIKEY+PalmSecure Provider

Регистрация аутентификатора

Аутентификатор – набор данных, создаваемый для каждого пользователя системы Indeed-Id, необходимый для прохождения процедуры аутентификации. Каждый новый пользователь системы Indeed-Id должен пройти процедуру регистрации одного или нескольких аутентификаторов.

Регистрация аутентификатора осуществляется после установки на рабочую станцию пользователя необходимых компонентов системы Indeed-Id: Indeed-Id Windows Logon/Indeed-Id ESSO Agent (в зависимости от используемой конфигурации системы) и провайдера Indeed-Id OMNIKEY+PalmSecure Provider.

Пользователь выполняет вход в систему по доменному паролю и, следуя указаниям приложения **Indeed-Id Управление аутентификаторами**, регистрирует аутентификатор.



Для успешной регистрации аутентификатора необходимо, чтобы пользователю, от имени которого осуществляется регистрация, было разрешено использовать технологию аутентификации Indeed-Id. Соответствующая настройка **выполняется администратором системы в свойствах пользователя на вкладке Настройки в консоли управления Indeed EMC.**

Подробные сведения по настройке свойств пользователя содержатся в документе *Indeed Enterprise Management Console. Руководство по установке и администрированию.pdf*.

Если аутентификатор не был зарегистрирован при первом входе пользователя в систему, регистрацию можно выполнить в любой удобный момент, запустив приложение **Indeed-Id Управление аутентификаторами** из меню Пуск – Все программы – Indeed-Id.

Для регистрации аутентификатора необходимо войти в систему по доменному паролю и выполнить следующие действия:

В окне **Управление аутентификаторами** нажмите **Продолжить** (Рисунок 1а).

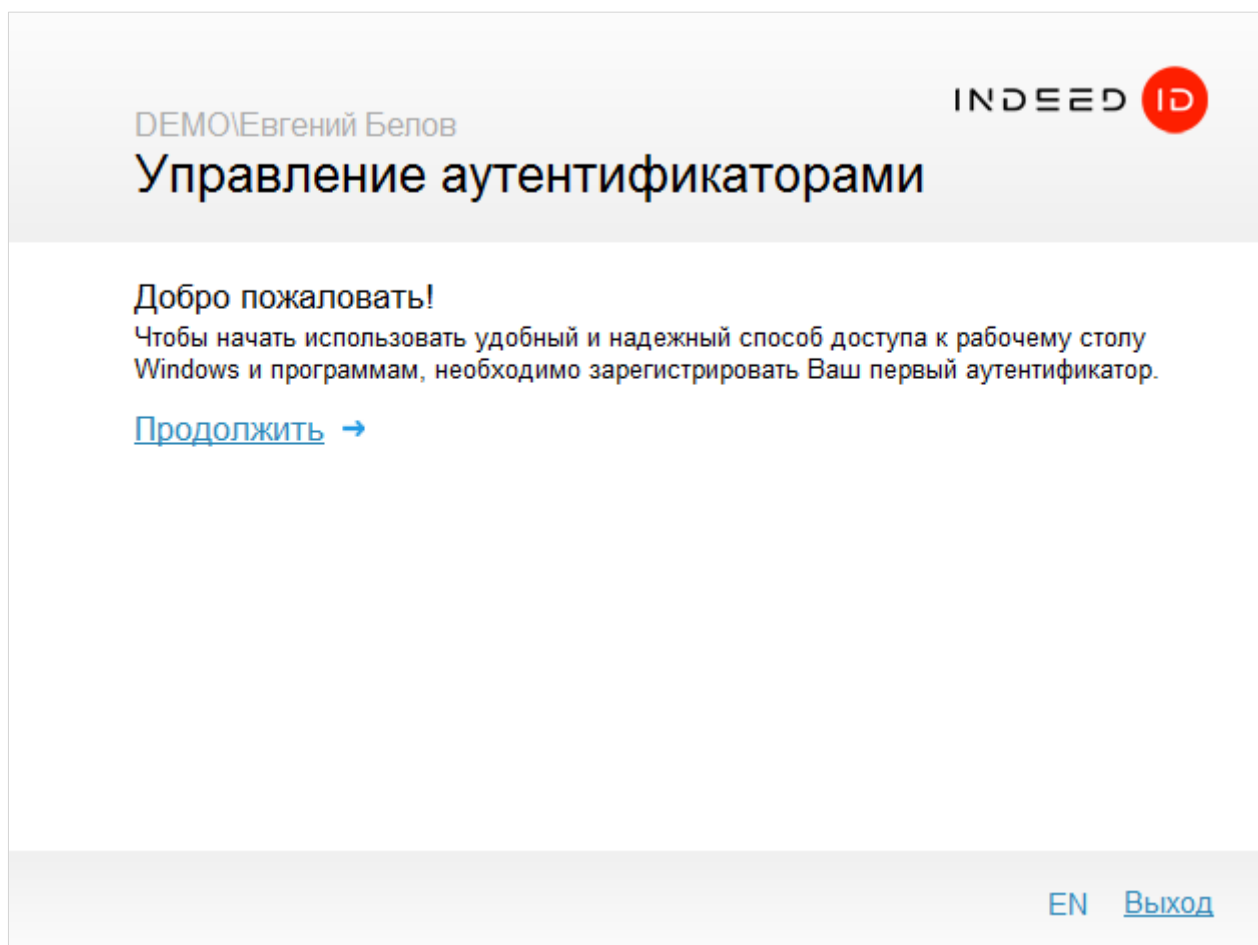


Рисунок 1а.

Если на рабочей станции пользователя установлено несколько провайдеров аутентификации, то необходимо выбрать **Карта + Ладонь (HID OMNIKEY + PalmSecure Reader)** из списка (Рисунок 1b). Если на компьютере установлен только один провайдер, окно выбора не отображается.

Управление аутентификаторами

Добро пожаловать!

Чтобы начать использовать удобный и надежный способ доступа к рабочему столу Windows и программам, необходимо зарегистрировать Ваш первый аутентификатор.

Выберите технологию аутентификации:

[Карта + Ладонь](#) →

(HID OMNIKEY + PalmSecure Reader)

[Пароль](#) →

(Passcode)

EN [Выход](#)

Рисунок 1b.

Подключите считыватель карт OMNIKEY и положите на него карту (Рисунок 1c). Во время процесса регистрации аутентификатора карта должна находиться на считывателе. Подключите сканер PalmSecure к компьютеру и поднесите к нему ладонь (Рисунок 1d).

Управление аутентификаторами

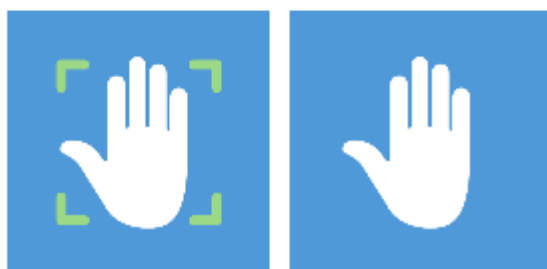


Вставьте пропуск в считыватель

[← Вернуться](#)EN [Выход](#)

Рисунок 1с.

Управление аутентификаторами



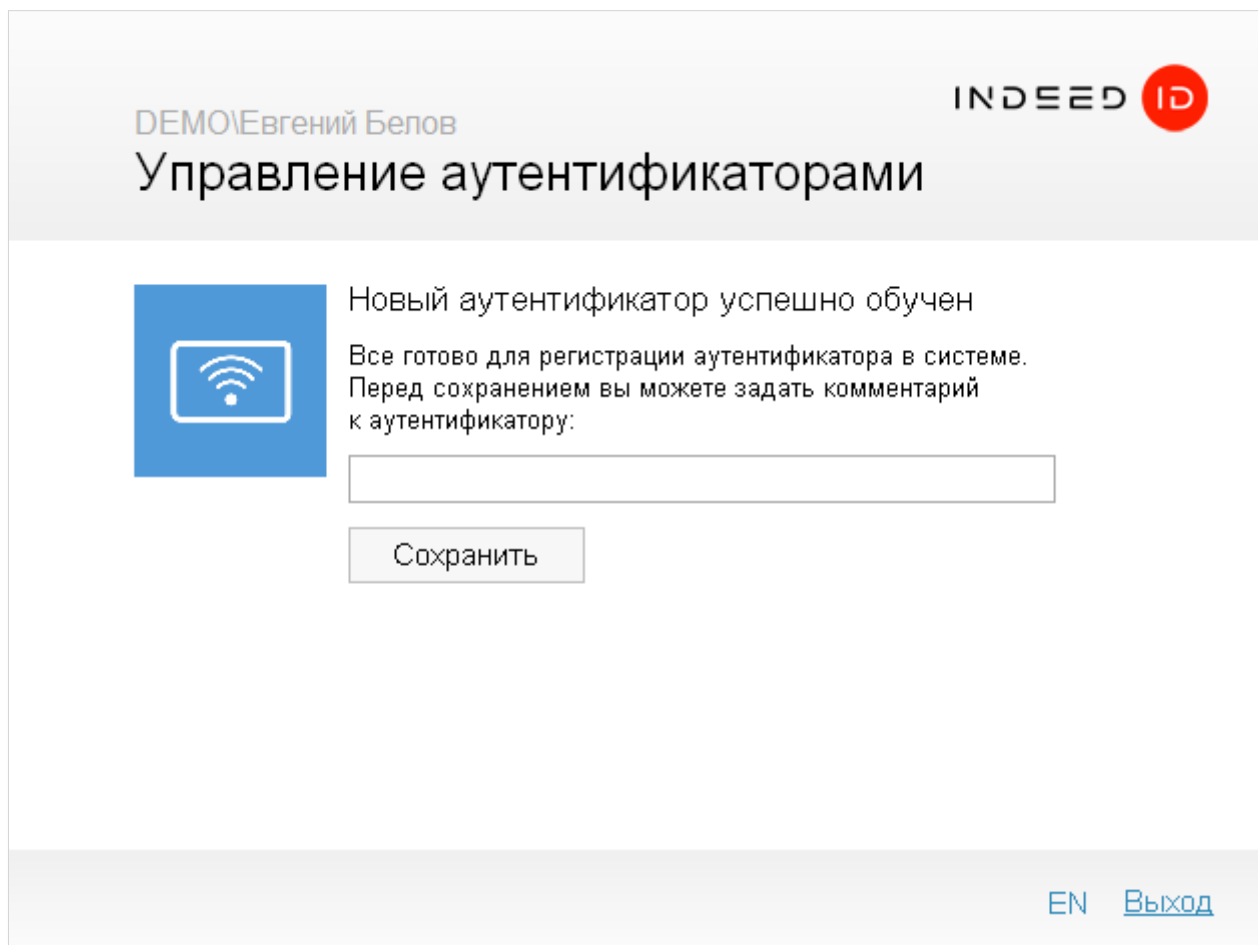
Расположите руку над сенсором

[← Вернуться](#)EN [Выход](#)

Рисунок 1d.

Следуя подсказкам мастера обучения, уберите руку со сканера и затем приложите её еще раз. Регистрация аутентификатора производится по двум снимкам ладони для более точного формирования шаблона.

При необходимости введите комментарий к заданному способу входа и нажмите кнопку **Сохранить** (Рисунок 1е).



The screenshot shows a web interface for 'Indeed ID' management. At the top, it says 'DEMO\Евгений Белов' and 'Управление аутентификаторами'. The main content area has a blue icon of a scanner with a Wi-Fi signal, followed by the text: 'Новый аутентификатор успешно обучен. Все готово для регистрации аутентификатора в системе. Перед сохранением вы можете задать комментарий к аутентификатору:'. Below this text is a text input field and a 'Сохранить' button. At the bottom right, there are links for 'EN' and 'Выход'.

Рисунок 1е.

После нажатия на кнопку **Сохранить** аутентификатор будет сохранен в системе и его можно будет использовать для аутентификации. Нажмите **Выход** для завершения работы приложения **Indeed-Id Управление аутентификаторами**.

Аутентификация при помощи Indeed-Id OMNIKEY+PalmSecure Provider

При первом входе в систему или приложение с использованием технологии аутентификации Indeed-Id необходимо выбрать способ входа. Для этого нажмите **Сменить способ входа** окне **Вход в Windows** (окно **Аутентификация** для Enterprise SSO). Выберите способ входа **Карта+Ладонь**.

Подключите считыватель карт OMNIKEY и положите на него карту (Рисунок 2а).

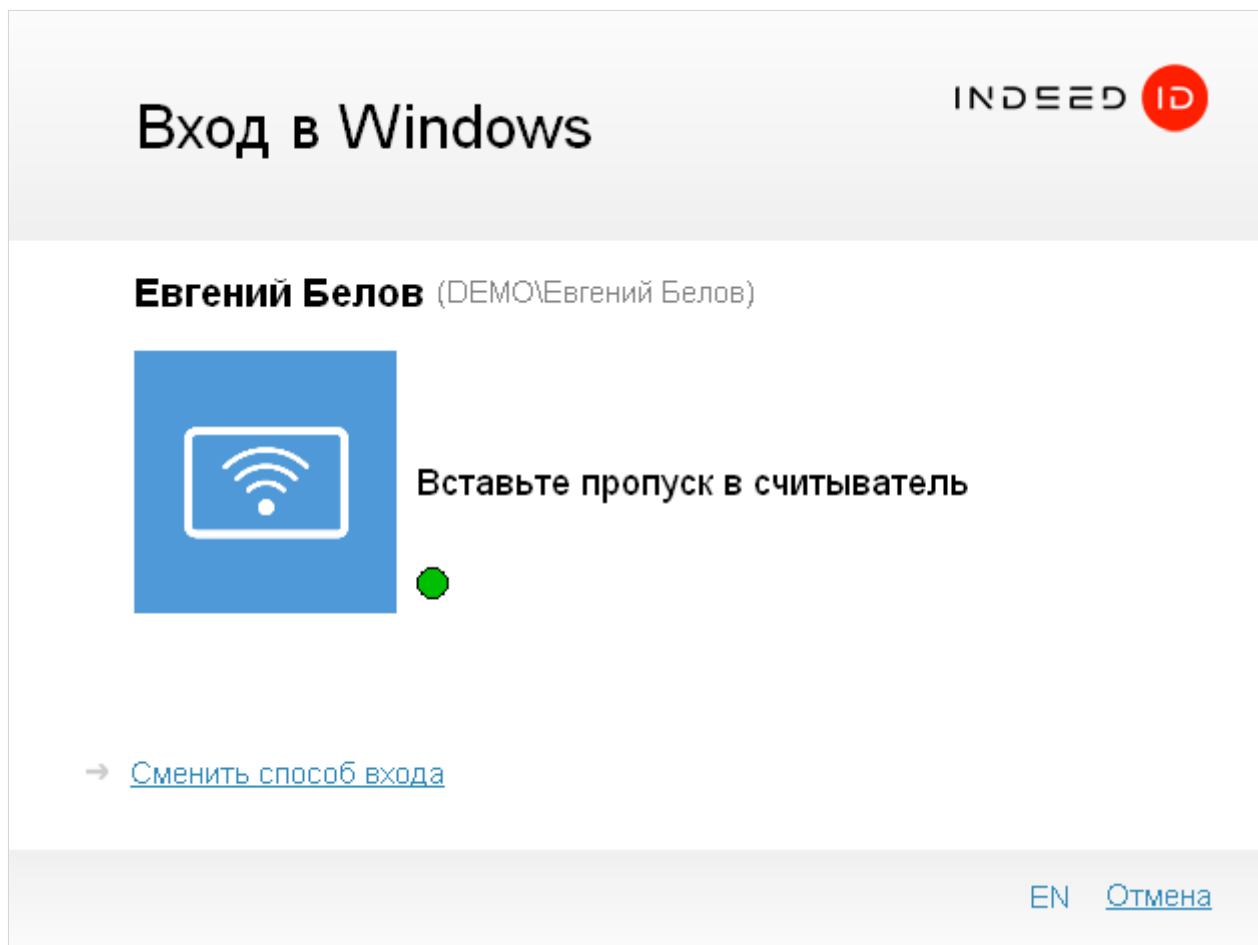


Рисунок 2а.

Подключите биометрический сканер к компьютеру и расположите ладонь над сенсором (Рисунок 2b).

Вход в Windows



Евгений Белов (DEMO\Евгений Белов)



Расположите руку над сенсором

→ [Сменить способ входа](#)

EN [Отмена](#)

Рисунок 2b.

В случае успешного входа по аутентификатору, способ входа **Карта+Ладонь** запоминается, как предпочтительный и будет автоматически предложен пользователю при следующем входе в систему или приложение.

Управление аутентификаторами

Управление аутентификаторами пользователя осуществляется при помощи приложения **Indeed-Id Управление аутентификаторами**. Приложение позволяет пользователю выполнять следующие действия с аутентификаторами:

- обучать
- переобучать
- удалять
- редактировать комментарий



Перечень действий, которые пользователь может выполнять над аутентификаторами, **задается администратором системы в свойствах пользователя на вкладке Аутентификаторы консоли управления Indeed EMC.**

Подробные сведения по настройке свойств пользователя содержатся в документе *Indeed Enterprise Management Console. Руководство по установке и администрированию.pdf*.

Запустите приложение **Indeed-Id Управление аутентификаторами** из меню Пуск – Все программы – Indeed-Id.

Для работы с приложением Indeed-Id Управление аутентификаторами необходимо выполнить вход в приложение с использованием любого из зарегистрированных аутентификаторов Indeed-Id или по доменному паролю. Если зарегистрированных аутентификаторов нет, то после аутентификации по доменному паролю пользователю будет предложено зарегистрировать аутентификатор.



В случае аутентификации по доменному паролю при наличии как минимум одного зарегистрированного аутентификатора Indeed-Id, независимо от настроек, выставленных в свойствах пользователя администратором системы, пользователю будет доступен только просмотр списка зарегистрированных аутентификаторов и проверка каждого из них.

Только пользователи, прошедшие аутентификацию по одному из обученных аутентификаторов Indeed-Id, имеют возможность управлять своими аутентификаторами (в соответствии с настройками, заданными администратором системы для пользователя).

Подробнее об управлении аутентификаторами смотрите в документах *Indeed-Id Enterprise SSO. Руководство пользователя.pdf* и *Indeed-Id Windows Logon. Руководство по установке и использованию.pdf*.

Установка и настройка Indeed-Id OMNIKEY+PalmSecure Provider

Установка компонента

В этом разделе содержатся сведения по установке и настройке Indeed-Id OMNIKEY+PalmSecure Provider. Установку Indeed-Id OMNIKEY+PalmSecure Provider необходимо выполнить на всех серверах Indeed-Id и затем на рабочих станциях пользователей.

Предварительные условия для установки

Для корректной установки компонента должны выполняться следующие условия:

- Минимум 30 Мб свободного места на жестком диске компьютера
- USB-порт для подключения сканера
- Установленные драйвера сканера PalmSecure



Для установки Indeed-Id OMNIKEY+PalmSecure Provider, пользователь, от имени которого выполняется установка, должен обладать правами администратора (быть членом локальной группы «Администраторы»).



Для развертывания Indeed-Id OMNIKEY+PalmSecure Provider на рабочих станциях пользователей в автоматическом режиме удобно использовать механизм групповых политик (Microsoft Group Policy). Или любой другой инструмент, позволяющий массово распространять и устанавливать msi-пакеты на рабочие станции пользователей (например, Microsoft System Center Configuration Manager).

Подробнее со способами распространения компонентов системы Indeed-Id в автоматическом режиме можно ознакомиться в документе *Indeed-Id. Руководство по развертыванию системы.pdf*.

Установка Indeed-Id OMNIKEY+PalmSecure Provider

1. Запустите файл IndeedID.OMNIKEY.PalmSecure.Provider.msi из дистрибутива провайдера и выполните установку, следуя указаниям мастера.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления – Программы и компоненты (Установка и удаление программ).

Настройка параметров аутентификации

В этом разделе содержится описание настраиваемых параметров работы Indeed-Id OMNIKEY+PalmSecure Provider и способах их изменения. Изменение параметров работы провайдера осуществляется через механизм групповых политик Active Directory. Настройка политик необходима для повышения уровня безопасности. Однако полноценная работа Indeed-Id OMNIKEY+PalmSecure Provider возможна и со значениями политик, определенными по умолчанию.

Политика раздела **Windows Logon® – Таймаут выполнения действия при извлечении смарт–карты** определяет продолжительность стандартного и сервисного таймаута после извлечения устройства аутентификации.

Политика задает интервал времени в секундах между извлечением смарт–карты и действием, выполняемым согласно политике Windows **Интерактивный вход: поведение при извлечении смарт–карты** (Interactive logon: Smart–card enhanced removal behavior).

Наличие **стандартного таймаута** позволяет предотвратить автоматическую блокировку компьютера при случайном извлечении устройства аутентификации.

Наличие **сервисного таймаута** позволяет предотвратить автоматическую блокировку компьютера в случаях, когда извлечение используемого устройства аутентификации необходимо (обучение дополнительного аутентификатора, получение доступа в систему от имени другой учетной записи по другому аутентификатору и т. п.). Для активации сервисного таймаута перед извлечением устройства необходимо нажать и удерживать комбинацию клавиш **[Ctrl]+[L]**.

Если политика не задана или отключена, то таймаут перед автоматической блокировкой рабочей станции не предоставляется.



Для настройки политики необходимо добавить файл политики **IndeedID.Client.adm** в список административных шаблонов политик Indeed-Id. Для получения подробной информации обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf*.

Политика **Минимально допустимое качество шаблона рисунка вен при обучении** (располагается в разделе Providers > Omnikey_PalmSecure) определяет, каково должно быть минимально приемлемое качество шаблона рисунка вен ладони при обучении аутентификатора. Качество шаблона задается целым числом от 1 до 3, где 1 соответствует максимально возможному качеству шаблона. Для достижения максимального качества шаблона при обучении необходимо располагать ладонь над сканером аккуратно и не меняя положения руки относительно сканера.



Для настройки политики необходимо добавить файл политики **IndeedID.Omnikey.PalmSecure.Provider_1049.adm** в список административных шаблонов политик Indeed-Id. Административный файл шаблона политики входит в состав дистрибутива провайдера и расположен в каталоге Misc. Для получения подробной информации об административных шаблонах политик Indeed-Id обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf*.

Политика должна быть определена на рабочие станции, где происходит обучение аутентификаторов Indeed-Id. Если политика не определена, в качестве значения по умолчанию используется 2.

После изменения настроек групповых политик необходимо выполнить обновление политик на рабочих станциях. Для немедленного обновления групповой политики используйте команду **gpupdate /force**.

Indeed-Id OMNIKEY + PalmSecure Provider

Руководство по установке и эксплуатации