# Indeed-Id Rule System

Руководство для администраторов предприятий

Установка и эксплуатация



#### © 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

Версия 1.1.3

Indeed-Id Rule System Руководство для администраторов предприятий

# Содержание

Введение	5
Условные обозначения	5
О компоненте Indeed-Id Rule System	5
Базовые термины и понятия	6
Конфигурация Indeed-Id Rule System Indeed-Id Enterprise Server — ключевой компонент решения Компоненты модуля Indeed-Id Rule System	<b>7</b> 7 7
Функционирование Indeed-Id Rule System	8
Планирование системы	9
Предварительные условия для установки системы	11
Оптимизация поиска записей в базе данных СКУД «ОРИОН»	12
Установка компонентов Indeed-Id Rule System	13
Установка компонента Indeed-Id RS Connector для СКУД «ОРИОН»	13
Установка компонента Indeed-Id RS Connector для СКУД «БАСТИОН»	15
Установка Indeed-Id RS Средства администрирования	19
Разграничение прав: Группы безопасности	21
Создание групп безопасности	21
Конфигурирование системы	22
Средства администрирования Indeed-Id Rule System	23
<b>Утилита IndeedID.acscfg.exe</b> Дополнительные вкладки свойств Indeed-Id ACS для объектов User и Computer	<b>23</b> 24
Настройка системы Настройка локальных зон Настройка общих зон Настройка турникетов Настройка компьютеров Настройка параметров компьютеров с помощью вкладки Indeed-Id ACS в консоли Active Directory Users and Computers Настройка пользователей	<b>25</b> 27 28 30 32 34 35
Пример настройки системы	38
Групповая политика «Доверять клиенту при получении от него DNS-имени»	40
Просмотр событий системы Indeed-Id Rule System	41
Список событий системы Indeed-Id Rule System	42
Список ошибок системы Indeed-Id Rule System	47
Indeed-Id Rule System	

Руководство для администраторов предприятий

Удаление и обновление Indeed-Id Rule System	50
Решение проблем	51
Запрет доступа в систему при нарушении правил	52
Отсутствует соединение с сервером базы данных	53
Пользователю не назначено ни одного токена	54
Сбор программных логов	55

# Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed. Данное Руководство поможет вам правильно установить компоненты модуля **Indeed-Id Rule System** и выполнить начальные настройки.

## 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 Rule System

Система Indeed-Id Rule System является расширением базовой конфигурации решения Indeed-Id и делает возможность с минимальными усилиями интегрировать продукты Indeed Enterprise Authentication (Indeed EA) и Indeed Enterprise SSO (Indeed ESSO) с любой системой. Примерами внешних систем могут служить система СКУД, HR, DLP, RMS и т.д.

Интеграция системы Indeed-Id с системой СКУД позволяет выполнить следующие задачи:

- Повышение уровня информационной безопасности компании за счет дополнения схемы контроля доступа новым фактором (фактор местоположения сотрудника).
- Управление правилами предоставления доступа к информационным ресурсам с учетом местоположения сотрудника.
- Унификация процедуры доступа в помещение и доступа к информационным ресурсам, например, использование одной универсальной карты сотрудника (вместо карты может быть выбрано любое другое средство аутентификации, поддерживаемое системой Indeed-Id).

Правила, согласно которым система Indeed-Id Rule System обеспечивает контроль доступа, формируются с учетом индивидуальных потребностей и могут включать следующие варианты:

- Предоставление доступа к данным:
  - только при нахождении пользователя на территории здания (выявляется по факту прохождения пользователя через определенные турникеты);
  - только при нахождении пользователя в определенном кабинете (маршрут следования до кабинета не учитывается);
  - с любого компьютера определенной зоны (например, к любому компьютеру на 3-м этаже).
- Дополнительный уровень аудита:
  - фиксирование причины отказа в доступе к данным в журнале событий Indeed-Id.

#### Базовые термины и понятия

В рамках системы Indeed-Id используются следующие базовые термины и понятия, связанные с продуктом Indeed-Id Rule System:

- Аутентификатор уникальные данные, предоставленные пользователем системе с целью подтверждения личности. В качестве аутентификатора могут служить данные, полученные с аппаратных устройств аутентификации (биометрические сканеры, смарт-карты, токены и др.) или созданные с помощью других технологий (One Time Matrix).
- Зона территория объекта, на которой контролируется право доступа (постоянного или разового). Выделяются локальные зоны, связанные с одной системой СКУД, и общие зоны, связанные с несколькими системами СКУД.
- СКУД (ACS, Access Control System) система контроля и управления доступом, обеспечивающая проверку прав доступа на объекты.
- Токен набор данных пользователя в СКУД. Состоит из ФИО пользователя и его идентификатора.
- Турникет устройство для проверки прав доступа на объекте.

## Конфигурация Indeed-Id Rule System

Базовая конфигурация системы Indeed-Id Rule System включает основной модуль решения Indeed-Id – **Indeed-Id Enterprise Server** и модуль **Indeed-Id Rule System**. При необходимости конфигурация системы может быть расширена дополнительными модулями решения Indeed-Id.

#### Indeed-Id Enterprise Server – ключевой компонент решения

**Indeed-Id Enterprise Server** (сервер Indeed-Id) является ключевым компонентом в любой конфигурации системы Indeed-Id. В рамках системы Indeed-Id Rule System сервер Indeed-Id использует специальные коннекторы, имеющие доступ к журналу событий внешних систем или иным образом отслеживающие происходящие в системе изменения. Анализируя события внешней системы и руководствуясь правилами, заданными администратором системы, сервер Indeed-Id формирует в системе Indeed-Id нужную реакцию.

#### Компоненты модуля Indeed-Id Rule System

В состав модуля **Indeed-Id Rule System** входят следующие компоненты:

- Indeed-Id RS «СКУД» Connector компонент, обеспечивающий связь сервера Indeed-Id с базой данных СКУД Орион и Бастион.
- Indeed-Id RS Средства администрирования компоненты, предназначенные для конфигурирования параметров системы. В пакет Indeed-Id RS Средства администрирования входят:
  - о **Консольная утилита Indeed-Id.acscfg.exe**, предназначенная для конфигурирования всех параметров системы.
  - Расширение консоли Active Directory Users and Computers вкладки Indeed-Id ACS для объектов User и Computer, предназначенные для управления токенами пользователей и добавления компьютеров в зоны.

## Функционирование Indeed-Id Rule System

Indeed Rules System входит в состав Indeed Enterprise Server, предоставляя интерфейс интеграции с внешними системами и одновременно выступая hosting-площадкой для коннекторов к этим системам. В данной схеме интеграция с системой СКУД достигается за счет реализации отдельного коннектора (Indeed Rules System СКУД Connector). Коннектор является переходником между Indeed Rules System и СКУД, скрывая особенности внутреннего протокола взаимодействия с системой СКУД (для разных СКУД могут требоваться разные коннекторы).

Ниже описана схема бизнес-операции получения пользователем доступа в информационную систему при помощи Indeed Enterprise SSO Агента (далее Indeed ESSO Агента), входящего в состав продукта Indeed Enterprise SSO (Рисунок 1).



#### Рисунок 1.

1. В момент получения доступа в информационную систему, Indeed ESSO Агент, установленный на рабочем месте пользователя, формирует запрос к серверу Indeed. В ходе выполнения запроса от сотрудника может потребоваться пройти процедуру аутентификации (например, с использованием универсальной карты доступа с интегрированной радиометкой).

2. Indeed Enterprise Server, получив запрос, извлекает из него информацию "от имени какой учётной записи" он пришел (например, от имени ivanov@domain.local). По имени учётной записи сервер находит соответствие между пользователем и идентификатором радиометки его карты (предположим, что пользователю ivanov@domain.local соответствует идентификатор карты 3458). Далее запрос транслируется в подсистему Indeed Rules System, которая через Коннектор обращается к журналу событий СКУД системы, определяя в какой зоне была зарегистрирована карта 3458.

3. Получив ответ, содержащий идентификатор турникета (зоны) на котором зарегистрирована карта сотрудника, Коннектор передает ответ в подсистему Rules System, где происходит его анализ на соответствие правилам системы.

4. Если местоположение сотрудника соответствует настроенным правилам (эквивалентно тому, что Rules System одобрил запрос), Indeed Enterprise Server возвращает данные, необходимые для доступа к информационной системе (как правило, логин-пароль). В противном случае, происходит отказ в доступе с указанием причины. Результат и детали обработки запроса фиксируются в журнале событий Indeed Enterprise Server.

# Планирование системы

На этапе планирования системы в пределах помещения выделяются объекты конфигурации (зоны, турникеты, компьютеры). Пример такого разделения показан на Рисунке 2:



External



- External, Office, Green, Yellow, Red, Violet, Blue физически разделённые зоны.
- GateExt1, GateExt2 внешние турникеты на входе в помещение.
- **DoorYellow**, **DoorViolet** вход в неконтролируемые зоны (доступ не контролируется системой СКУД).
- **DoorGreen**, **DoorBlueA**, **DoorBlueB** вход в контролируемые зоны (доступ контролируется системой СКУД).

С точки зрения систем СКУД и Indeed-Id Rule System, интерес представляют только контролируемые зоны. Исходя из этого, план помещения можно преобразовать, как показано на Рисунке 3.



External

Рисунок 3.

Полученный план системы реализуется на этапе ее конфигурирования.

## Предварительные условия для установки системы

Для корректной установки компонент Indeed-Id Rule System должны быть выполнены следующие требования:

#### Операционная система:

- Windows Server 2003/2003 R2 Standard/Enterprise SP2 32/64bit
- Windows Server 2008 Standard/Enterprise SP2 32/64bit
- Windows Server 2008 R2 Standard/Enterprise SP1
- Windows Server 2012/2012R2 Standard/Datacenter 32/64bit
- Windows XP SP3 32bit с установленным компонентом Пакет средств администрирования Windows Server 2003 (adminpak.msi)
- Windows Vista SP2 32/64bit с установленным компонентом «Средства удаленного администрирования сервера» (Remote Server Administration Tools) для Windows Vista
- Windows 7 SP1 32/64bit с установленным компонентом «Средства удаленного администрирования сервера» (Remote Server Administration Tools) для Windows 7.
- Windows 8.1 32/64bit с установленным компонентом «Средства удаленного администрирования сервера» (Remote Server Administration Tools) для Windows 8.1

#### Требования к инфраструктуре:

- Базовая конфигурация решения Indeed-Id (Indeed-Id Enterprise Server + Indeed-Id Windows Logon + Indeed Enterprise Management Console).
- 10 Мб свободного места на жестком диске.

#### Базы данных:

#### СКУД ОРИОН:

- База данных СКУД «ОРИОН», развернутая на сервере Microsoft SQL Server.
- Для оптимизации поиска записей в базе данных СКУД «ОРИОН» необходимо создать дополнительный индекс. Для этого в среде SQL Server Management Studio необходимо загрузить файл Orion\_pLogData\_HozOrgan\_TimeVal\_Index.sql, находящийся в каталоге /Misc дистрибутива Indeed-Id Rule System, и выполнить сценарий (см. Оптимизация поиска записей в базе данных СКУД «ОРИОН»).
- 20 Мб свободного места на жестком диске

#### СКУД БАСТИОН:

- База данных СКУД «БАСТИОН», развернутая в среде FireBird 2.5
- Установленный драйвер FireBird ODBC Driver на каждом экземпляре Indeed Enterprise Server
- Установленный FireBird Client 2.5 на каждом экземпляре Indeed Enterprise Server
- 20 Мб свободного места на жестком диске

## Оптимизация поиска записей в базе данных СКУД «ОРИОН»

Для добавления дополнительного индекса в базу данных СКУД «ОРИОН» выполните следующие действия:

- 1. В среде SQL Management Studio установите подключение к серверу SQL (от имени учетной записи с правами на добавление объектов).
- 2. Выберите базу данных СКУД «ОРИОН».
- 3. С помощью команды **Файл > Открыть** загрузите файл Orion\_pLogData\_HozOrgan\_TimeVal\_Index.sql, находящийся в каталоге /Misc дистрибутива Indeed-Id Rule System.
- 4. После открытия файла нажмите Выполнить.

🍢 Среда Microsoft SQL Server Management Studi	o Express	
Файл Правка Вид Запрос Сервис <u>О</u> кно	Сообщество Справка	
🕴 🄔 Создать запрос   📭   😂 🛃 🎒   🚱 🧾 👂	) 🎼 🖅 🖕	
ं 💷 🤮 🙀   master 🕒 🕴 🛃	полнить 🧹 = 1571 🖉 🕼 📅 🥦 🖳 🚳 🎆 🚳 🔲 🚊 🔅 連 🍃	
Object Explorer 🗸 🖓 🔀	TIDDC\\DrioeVal_Index.sql Summary	- ×
¥¥ = ⊇ T	USE [bolid]	-
E IDDC\SQLEXPRESS (SQL Server 9.0.2047 - DEMC	GO	
E 📴 Databases		
💿 🧰 System Databases	CREATE NONCLUSTERED INDEX [idx_pLogData_HozOrgan_TimeVal]	
E 📒 Orion	(	
🐑 📴 Database Diagrams	[HozOrgan] ASC,	
	[IImeval] DESC	
E Views	STATISTICS NORCONDUTE - OFF	
E Programmability	SOPT IN TEMPORE - OFF	
Security	IGNORE DUP KEY = OFF	_
E Security	DEOD EXISTING = OFF.	
Server Objects	ONLINE = OFF.	
Replication	ALLOW ROW LOCKS = ON.	
Management	ALLOW PAGE LOCKS = ON)	
	ON [PRIMARY]	
	GO	
		-
	•	_ <b>▶</b>
×	PConnected. IIDDC\SQLEXPRESS (9.0 SP1) DEM0\Administrator (52) master	0 rows
Готово	Строка 1 Столбец 1 Энак 1	BCT //.

# Установка компонентов Indeed-Id Rule System

## Установка компонента Indeed-Id RS Connector для СКУД «ОРИОН»

Indeed-Id RS Connector для СКУД - компонент, обеспечивающий связь сервера Indeed-Id с базой данных СКУД. Установка компонента Indeed-Id RS Connector для СКУД выполняется на сервере Indeed-Id. В данном разделе описан процесс установки компонента **Indeed-Id RS Connector для СКУД «ОРИОН»**.

Для установки пакета Indeed-Id RS Connector для СКУД «ОРИОН» выполните следующие действия:

- 1. Запустите программу установки IndeedID.RuleSystem.ACS.Orion.msi и дождитесь отображения Мастера установки.
- 2. Нажмите Далее чтобы начать установку
- 3. Нажмите Далее чтобы начать настройку соединения с базой данных СКУД.
- 4. В диалоге Data Link Properties на вкладке Connection выполните следующие настройки:
  - Выберите имя сервера SQL, на котором развернута база данных СКУД «ОРИОН».
  - Введите имя и пароль учетной записи для доступа на сервер SQL и выберите опцию сохранения пароля (**Allow saving password**).



Если данные учетной записи указаны неверно или не выбрана опция сохранения пароля, доступ к параметрам Rule System будет невозможен.

- Для проверки соединения используйте кнопку **Test Connection**. Если соединение с сервером SQL установлено успешно, отображается сообщение «Test connection succeeded».
- Для сохранения изменений нажмите ОК.

🖞 Data Link Properties 🔀 🔀		
Provider Connection Advanced All		
Specify the following to connect to SQL Server data:         1. Select or enter a server name:         AS101W3SRV         2. Enter information to log on to the server:         O Use Windows NT Integrated security         I use mame:         I use maseton to use mame:		
bold		
O Attach a database file as a database name:		
bold		
Using the filename:		
<u></u>		
Test Connection		
OK Cancel Help		

Если пароль не введен, при попытке сохранения настроек отображается диалог:

Програми	ма установки Indeed-ID RS Connector для СКУД 'ОРИОН' 🛛 🔀
?	Пароль пользователя, для которого будет выполняться подключение к базе данных, не указан. Если вы хотите использовать пустой пароль, ответьте "Да"("Yes"). Если вы ввели пароль в диалоге конфигурации базы данных, но видите это сообщение, ответьте "Нет"("No"), снова введите пароль и включите опцию "Разрешить сохранение пароля". Продолжить установку?
	<u>Y</u> es <u>N</u> o

Нажмите **Нет** (No), введите пароль и выберите опцию **Разрешить сохранение пароля** (Allow saving password).

- 5. Нажмите Начать и дождитесь завершения установки.
- 6. Нажмите Готово.

## Установка компонента Indeed-Id RS Connector для СКУД «БАСТИОН»

Indeed-Id RS Connector для СКУД - компонент, обеспечивающий связь сервера Indeed-Id с базой данных СКУД. Установка компонента Indeed-Id RS Connector для СКУД выполняется на сервере Indeed-Id. В данном разделе описан процесс установки компонента **Indeed-Id RS Connector для СКУД «БАСТИОН»**.

Для установки пакета Indeed-Id RS Connector для СКУД «БАСТИОН» выполните следующие действия:

- 1. Запустите программу установки IndeedID.RuleSystem.ACS.Bastion.msi и дождитесь отображения Мастера установки.
- 2. Нажмите Далее чтобы начать установку
- 3. Нажмите Далее чтобы начать настройку соединения с базой данных СКУД.
- 4. В диалоге Data Link Properties на вкладке **Connection** выберите **Use connection string** и нажмите **Build**

📑 Data Link Properties 🔀
Provider Connection Advanced All
Specify the following to connect to ODBC data: 1. Specify the source of data: C Use <u>data source name</u> <u>Refresh</u>
• Use connection string Connection string:   Build   2. Enter information to log on to the server   User name:   Password:   Blank password   Allow saving password
3. Enter the initial catalog to use:
OK Cancel Help

- 5. В появившемся окне Select Data Source перейдите на вкладку Machine Data Source и нажмите New...
- 6. Выберите System Data Source (Applies to this machine only) и нажмите Next:

Create New Data Source		>
	Select a type of data source: <u>U</u> ser Data Source (Applies to this machine only) <u>System Data Source (Applies to this machine only)</u>	
	Selecting System Data Source creates a data source which is specific to this machine, and usable by any user who logs onto this machine.	
	< <u>₿</u> ack <u>N</u> ext > Cancel	

7. Выберите драйвер FireBird и нажмите **Next**:

Name
Driver da Microsoft para arquivos texto (".bt; ".csv) e
Driver do Microsoft dPage (* dbf)
Driver do Microsoft Goal(* vis)
Driver do Microsoft Paradov (* db.)
Driver para o Microsoft Visual FoxPro
Firebird/InterBase(r) driver
Microsoft Access Driver (*.mdb)
•

8. Укажите параметры подключения в окне **Firebird ODBC Setup**:

irebird ODBC Setup			×
Data Source Name (DSN)		Driver	
BASTION_TEST		IscDbc	•
Description			
Database			
C:\BASTION\BASTION.GDB		Browse	
Client			
C:\Program Files\Firebird\Firebird	1_2_5\W0W64\fbclier	nt.dll Browse	
Database Account	Password	Role	
SYSDBA			
Character Set	1	1 [ _	-
NONE	Services	Test connection	
Options Transaction read (default write) nowait (default wait) Lock Timeout Dialect	Extend I quo I sen I auto	ed identifier properties oted identifiers isitive identifier oquoted identifier	
Safe thread	Set nu	II field SCHEMA	•
	0KCa	ncel Help	

- Введите имя соединения в поле Data Source Name (DSN)
- В поле **Database** укажите путь к подключаемой базе данных.



Если база установлена на удаленной рабочей станции, укажите DNS имя этой рабочей станции или ip-адрес.

Например: 192.168.100.6:С:\BastionDemo\Data\BASTION.GDB

- В поле **Client** укажите путь к библиотеке Firebird client 2.5 установленного на сервере Indeed.
- Ведите логин и пароль учетной записи для доступа к базе данных СКУД в поля **Database Account** и **Password** соответственно.



Если данные учетной записи указаны неверно, то доступ к параметрам Rule System будет невозможен.

- Для проверки соединения используйте кнопку **Test Connection**.
- Для сохранения изменений нажмите ОК.
- 9. В результате выполненных действий в поле Connection string появится параметры подключения к базе данных СКУД «БАСТИОН»:

🚮 Data Link Properties	×
Provider Connection Advanced All	
Specify the following to connect to ODBC data: 1. Specify the source of data: Use <u>d</u> ata source name <u>Effective</u> Use <u>connection string</u> <u>Connection string</u>	
DSN=BASTION_TEST;Driver=Firebird/InterB: Build  2. Enter information to log on to the server User name: Password: Blank password Blank password Content to use:	
I the the final catalog to ase.	
OK Cancel Help	

Нажмите **ОК** для завершения установки.

## Установка Indeed-Id RS Средства администрирования

**Indeed-Id RS Средства администрирования** – компонент, предназначенный для конфигурирования параметров системы. В пакет Indeed-Id RS Средства администрирования входят:

- Консольная утилита IndeedID.acscfg.exe, предназначенная для конфигурирования всех параметров системы.
- Расширение консоли Active Directory Users and Computers вкладки Indeed-Id ACS для объектов User и Computer, предназначенные для управления токенами пользователей и добавления компьютеров в зоны.
- Для корректного отображения вкладки Indeed-Id ACS в режиме поиска (команда Find в консоли Active Directory Users and Computers) Вы можете выполнить регистрацию вкладки с помощью специального сценария (см. Регистрация вкладки Indeed-Id ACS). Регистрация вкладки Indeed-Id ACS с помощью сценария является опциональным шагом, позволяющим решить известную проблему Microsoft не отображение дополнительных свойств объектов в режиме поиска.

Для установки пакета Indeed-Id RS Средства администрирования запустите программу установки IndeedID.RuleSystem.ACS.AdminTools.msi, дождитесь отображения Мастера установки и следуйте его указаниям.

В процессе установки будет создан журнал событий системы. В этот журнал будут заноситься все события, регистрируемые компонентами системы Indeed-Id, установленными на рабочей станции. Журнал создается однократно при установке любого продукта, входящего в состав комплекса Indeed Enterprise Authentication/Enterprise SSO за исключением Провайдеров аутентификации Indeed-Id.

# Регистрация и удаление вкладки Indeed-Id ACS в консоли Active Directory Users and Computers

Регистрация вкладки Indeed-Id ACS позволяет решить известную проблему Microsoft и обеспечить корректное отображение вкладки в режиме поиска (команда Find в консоли Active Directory Users and Computers).

Для регистрации вкладки Indeed-Id ACS необходимо выполнить сценарий RegisterACSPages.cmd, находящийся в каталоге \Misc\RegisterACSPages дистрибутива Indeed-Id Rule System. Для выполнения данной операции необходимо наличие прав **Schema Admins** и прав **Полный контроль** (Full Control) на атрибут **CN=user-Display,CN=409,CN=DisplaySpecifiers,CN=Configuration**.

Если дополнительная вкладка свойств Indeed-Id ACS не зарегистрирована с помощью сценария RegisterACSPages.cmd, она удаляется из диалога свойств пользователя/компьютера после удаления пакета Indeed-Id RS Средства администрирования. Зарегистрированная вкладка Indeed-Id ACS продолжает отображаться в режиме поиска (команда Find) даже после удаления указанного пакета. Для удаления зарегистрированной вкладки Indeed-Id ACS необходимо выполнить сценарий UnregisterACSPages.cmd, находящийся в каталоге \Misc\RegisterACSPages дистрибутива Indeed-Id Rule System. Для выполнения данной операции необходимо наличие прав

Schema Admins и прав Полный контроль (Full Control) на атрибут CN=user-Display,CN=409,CN=DisplaySpecifiers,CN=Configuration.

# Разграничение прав: Группы безопасности

С целью разграничения прав на управление системой после установки компонент Indeed-Id Rule System должны быть созданы следующие группы безопасности:

- Indeed-Id ACS System Admins участники данной группы имеют полные права на конфигурирование Rule System (создание и настройка систем, зон, турникетов, компьютеров, токенов);
- Indeed-Id ACS User Admins участники данной группы имеют права на добавление/удаление токенов пользователей;
- Indeed-Id ACS Computer Admins участники данной группы имеют права на включение компьютеров в зоны.

## Создание групп безопасности

Для создания групп безопасности используйте команду вида **IndeedID**.acscfg.exe - install:<root>.

#### Пример: IndeedID.acscfg.exe -install:"dc=demo,dc=domain"

В созданные служебные группы необходимо включить учетные записи администраторов системы. Участники группы Domain Admins по умолчанию обладают полными правами на конфигурирование системы.



Для того, чтобы изменения в правах вступили в силу, необходимо выполнить выход из системы и повторный вход.



Служебные группы Indeed-Id Rule System являются скрытыми и доступны для просмотра только при добавлении пользователя в группу.

# Конфигурирование системы

После установки компонент Indeed-Id Rule System необходимо выполнить конфигурирование системы.

Конфигурирование Indeed-Id Rule System включает:

- Настройку основных параметров:
  - Создание системы
  - Создание зон
  - Создание турникетов
- Добавление компьютеров в зоны
- Назначение токенов пользователям

Все операции конфигурирования системы могут выполняться с помощью консольной утилиты IndeedID.acscfg.exe. Операции добавления компьютеров в зоны и назначения токенов пользователям могут выполняться как с помощью указанной утилиты, так и с помощью настроек на вкладках Indeed-Id ACS для объектов User и Computer в консоли Active Directory Users and Computers.

# Средства администрирования Indeed-Id Rule System

## Утилита IndeedID.acscfg.exe

Консольная утилита IndeedID.acscfg.exe используется для конфигурирования всех параметров Indeed-Id Rule System, включая общие настройки системы (параметры системы, зон, турникетов), свойства пользователей и компьютеров. После установки пакета Indeed-Id RS Средства администрирования утилита IndeedID.acscfg.exe по умолчанию находится в каталоге C:\Program Files\Common Files\Indeed-Id (Вы можете использовать пункт меню **Программы > Indeed-Id > Rule System >Indeed-Id Rule System Командная строка**).



Имена турникетов, зон, общих зон, систем, используемые в командах, являются регистрозависимыми (acscfg.exe gateway set *gate1* и acscfg.exe gateway set *Gate1* – разные команды).

#### Синтаксис команд

При работе с утилитой IndeedID.acscfg.exe в командной строке используется следующий синтаксис:

#### Acscfg <Object Command [Parameters]> <-install:root>

Где:

- Object объект, к которому применяется команда
- *Command* команда, применяемая к объекту (зависит от типа объекта)
- Parameters дополнительные параметры (зависят от команды и типа объекта)
- -install: -команда для установки служебных групп
- root домен/подразделение, в котором создан экземпляр системы Indeed-Id

#### Список объектов

При работе со списком объектов в командной строке используется следующий синтаксис:

#### Acscfg <System Zone CommonZone Gateway Computer User> [-page] [-h] [-help]

Где:

System – управление системами

Zone – управление зонами

*CommonZone* – управление общими зонами

Gateway – управление турникетами

Computer – управление компьютерами

#### Indeed-Id Rule System

Руководство для администраторов предприятий

User – управление пользователями

-page – выводить информацию постранично

-h, -help –вывод справки по командам для выбранного объекта

#### Дополнительные вкладки свойств Indeed-Id ACS для объектов User и Computer

С помощью настроек на дополнительных вкладках Indeed-Id ACS в консоли Active Directory Users and Computers Вы можете осуществлять управление токенами пользователей и добавление компьютеров в зоны.



Для корректного отображения вкладки Indeed-Id ACS в режиме поиска (команда Find в консоли Active Directory Users and Computers) Вы можете выполнить регистрацию вкладки с помощью специального сценария (см. **Регистрация вкладки Indeed-Id ACS**). Регистрация вкладки Indeed-Id ACS с помощью сценария является опциональным шагом, позволяющим решить известную проблему Microsoft – не отображение дополнительных свойств объектов в режиме поиска.

Смотрите также:

- Настройка параметров компьютеров с помощью вкладки Indeed-Id ACS в консоли Active Directory Users and Computers
- Настройка параметров пользователей с помощью вкладки Indeed-Id ACS в консоли Active Directory Users and Computers

## Настройка системы

Настройка параметров системы выполняется с помощью утилиты IndeedID.acscfg.exe.



Для настройки параметров системы необходимы права Indeed-Id ACS System Admins.

#### Синтаксис команд и параметры

Для управления системами в командной строке используется следующий синтаксис:

### Acscfg System [Enum] [Add] [Del] [Rename] [Info] [Set] [EnumRawTokens] [EnumRawGateways]

Где:

Enum – вывести список систем с параметрами

Add – добавить новую систему <SystemName>

-progId:<ProgId> - ProgId компонента Data Provider системы <SystemName>

Значение ProgId находится в реестре в ключе HKEY\_CLASSES\_ROOT > IndeedID.ACS.Data.Provider.<Name> > CurVer.

-clsId: <clsId> - ClsId компонента Data Provider системы <SystemName>

Значение ClsId находится в реестре в ключе HKEY\_CLASSES\_ROOT > IndeedID.ACS.Data.Provider.<Name> > CLSID и указывается без скобок {}

Del-удалить систему <SystemName>

Rename - переименовать систему <SystemName>

Info-вывести параметры системы <SystemName>

Set – установить параметры системы <SystemName>

EnumRawTokens – вывести список токенов в СКУД системе <SystemName>

EnumRawGateways - вывести список турникетов в СКУД системе <SystemName>

#### Вывод списка систем с параметрами

Для вывода списка систем с параметрами используйте команду IndeedID.acscfg.exe System Enum

#### Добавление системы

Для добавления системы используйте команду вида IndeedID.acscfg.exe System Add <SystemName> -progId:<ProgId> |-clsId:<clsId>

Для успешного выполнения команды необходимо указать только один из параметров: либо – progId, либо –clsId.

Indeed-Id Rule System Руководство для администраторов предприятий

# Пример: IndeedID.srvcfg.exe System Add Orion – progId:IndeedID.Acs.DataProvider.Orion.1

#### Переименование системы

Для переименования системы используйте команду вида IndeedID.acscfg.exe System Rename <SystemName> <NewName>

#### Пример: IndeedID.acscfg.exe System Rename Orion Orion2

#### Установка параметров системы

Для установки параметров системы используйте команду **IndeedID.acscfg.exe System Set <SystemName> -progId:<ProgId> | -clsId:<clsId>** 

#### Пример для СКУД «ОРИОН»:

IndeedID.acscfg.exe System Set Orion -progId:IndeedID.Acs.DataProvider.Orion.1

#### -clsId:3CC04C59-72CD-4331-B49C-D07CE4E0A9D9

#### Пример для СКУД «БАСТИОН»:

 ${\bf IndeedID.acscfg.exe} \ {\bf System} \ {\bf Set} \ {\bf Bastion} \ {\bf -progId}: {\bf IndeedID.Acs.DataProvider}. {\bf Bastion}. 1$ 

#### -clsId:BE7EC8EE-5281-456E-A99C-F33056F7C1A7

#### Удаление системы

Для удаления системы используйте команду вида **IndeedID.acscfg.exe System Del <SystemName>** 

#### Пример: IndeedID.srvcfg.exe System Del Orion

#### Вывод параметров системы

Для вывода параметров системы используйте команду вида **IndeedID.acscfg.exe System Info <SystemName>** 

#### Пример: IndeedID.acscfg.exe System Info Orion

В результате будет выведено имя системы и значения progId и clsId.

#### Вывод списка токенов в системе

Для вывода списка токенов используйте команду вида **IndeedID.acscfg.exe System** EnumRawTokens <SystemName>

#### Пример: IndeedID.acscfg.exe System EnumRawTokens Orion

#### Вывод списка турникетов в системе

Для вывода списка турникетов с системе используйте команду вида **IndeedID.acscfg.exe System EnumRawGateways <SystemName>** 

#### Пример: IndeedID.acscfg.exe System EnumRawGateways Orion

#### Настройка локальных зон

Настройка параметров локальных зон выполняется с помощью утилиты IndeedID.acscfg.exe.

#### Синтаксис команд и параметры

Для управления зонами в командной строке используется следующий синтаксис:

### Acsfg Zone [Enum] [Add] [Del] [Rename]

Где:

Enum – вывести список зон в системе <SystemName>

Add – добавить зону <ZoneName> в системе <SystemName>

Del-удалить зону <ZoneName> в системе <SystemName>

Rename – переименовать зону <ZoneName> в системе <SystemName>

-system:<SystemName> - имя системы

#### Вывод списка зон

Для вывода списка зон в системе используйте команду вида **IndeedID.acscfg.exe Zone Enum** – system:<SystemName>

#### Пример: IndeedID.acscfg.exe Zone Enum –system:Orion

#### Добавление локальной зоны

Для добавления локальной зоны в системе используйте команду вида **IndeedID.acscfg.exe Zone** Add <ZoneName> —system:<SystemName>

#### Пример: IndeedID.acscfg.exe Zone Add Zone1 --system:Orion

#### Переименование локальной зоны

Для переименования локальной зоны в системе используйте команду вида **IndeedID.acscfg.exe Zone Rename <ZoneName> <NewName> —system:<SystemName>** 

#### Пример: IndeedID.acscfg.exe Zone Rename Zone1 Zone2 –system:Orion

#### Удаление локальной зоны

Для удаления локальной зоны в системе используйте команду вида **IndeedID.acscfg.exe Zone Del <ZoneName> —system:<SystemName>** 

#### Пример: IndeedID.acscfg.exe Zone Del Zone1 –system:Orion

### Настройка общих зон

Настройка параметров общих зон выполняется с помощью утилиты IndeedID.acscfg.exe.

#### Синтаксис команд и параметры

Для управления общими зонами в командной строке используется следующий синтаксис:

# Acscfg CommonZone [Enum] [Add] [Del] [Rename] [EnumSystems] [AddSystem] [DelSystem]

Где:

Enum – вывести список общих зон

Add – добавить общую зону <ZoneName>

Del-удалить общую зону <ZoneName>

Rename - переименовать общую зону <ZoneName>

EnumSystems – вывести список систем, в которые включена общая зона <ZoneName>

AddSystem – включить общую зону <ZoneName> в систему <SystemName>

DelSystem – исключить общую зону <ZoneName> из системы <SystemName>

-system:<SystemName> - имя системы

#### Вывод списка общих зон

Для вывода списка общих зон используйте команду IndeedID.acscfg.exe CommonZone Enum

#### Добавление общей зоны

Для добавления общей зоны используйте команду вида IndeedID.acscfg.exe CommonZone Add <ZoneName>

#### Пример: IndeedID.acscfg.exe CommonZone Add Zone3

#### Переименование общей зоны

Для переименования общей зоны используйте команду вида IndeedID.acscfg.exe CommonZone Rename <ZoneName> <NewName>

#### Пример: IndeedID.acscfg.exe CommonZone Rename Zone3 Zone4

#### Удаление общей зоны

Для удаления общей зоны используйте команду вида IndeedID.acscfg.exe CommonZone Del <ZoneName>

#### Пример: IndeedID.acscfg.exe CommonZone Del Zone3

#### Включение общей зоны в систему

Для включения общей зоны в систему используйте команду вида IndeedID.acscfg.exe CommonZone AddSystem <ZoneName> -system:<SystemName>

#### Пример: IndeedID.acscfg.exe CommonZone AddSystem Zone4 -system:Orion

#### Исключение общей зоны из системы

Для исключения общей зоны из системы используйте команду вида IndeedID.acscfg.exe CommonZone DelSystem <ZoneName> -system:<SystemName>

#### Пример: IndeedID.acscfg.exe CommonZone DelSystem Zone4 -system:Orion

#### Вывод списка систем, в которые включена общая зона

Для вывода списка систем, в которые включена общая зона, используйте команду вида IndeedID.acscfg.exe CommonZone EnumSystems <ZoneName>

#### Пример: IndeedID.acscfg.exe CommonZone EnumSystems Zone4

### Настройка турникетов

Настройка параметров турникетов выполняется с помощью утилиты IndeedID.acscfg.exe.

#### Синтаксис команд и параметры

Для управления турникетами в командной строке используется следующий синтаксис:

### Acscfg Gateway [Enum] [Add] [Del] [Rename] [Info] [Set]

Где:

Enum – вывести список турникетов в системе

Add – добавить турникет <GatewayName>в системе <SystemName>

Del-удалить турникет <GatewayName>в системе <SystemName>

Rename – переименовать турникет <GatewayName>в системе <SystemName>

Info – вывести параметры турникета <GatewayName>в системе <SystemName>

Set –установить параметры турникета <GatewayName>в системе <SystemName>

-system:<SystemName> - имя системы

-zone1:<ZoneName> -имя зоны на входе

-zone2:<ZoneName> -имя зоны на выходе

-rawId:<Id>- идентификатор турникета в системе СКУД

#### Вывод списка турникетов

Для вывода списка турникетов используйте команду **IndeedID.acscfg.exe Gateway Enum -** system:<SystemName>

#### Пример: IndeedID.acscfg.exe Gateway Enum -system:Orion

#### Добавление турникета в систему

Для добавления турникета в систему используйте команду вида IndeedID.acscfg.exe Gateway Add <GatewayName> -system:<SystemName> -zone1:<ZoneName> -zone2:<ZoneName> -rawId:<Id>

Пример: IndeedID.acscfg.exe Gateway Add Gateway1 -system:Orion -zone1:Zone3 - zone2:Zone4 -rawId:12345

#### Переименование турникета в системе

Для переименования турникета в системе используйте команду вида **IndeedID.acscfg.exe** Gateway Rename <GatewayName> <NewName> -system:<SystemName>

Пример: IndeedID.acscfg.exe Gateway Rename Gateway1 Gateway2 -system:Orion

#### Удаление турникета из системы

Для удаления турникета из системы используйте команду вида IndeedID.acscfg.exe Gateway Del <GatewayName> -system:<SystemName>

#### Пример: IndeedID.acscfg.exe Gateway Del Gateway1 -system:Orion

#### Вывод параметров турникета в системе

Для вывода параметров турникета в системе используйте команду вида **IndeedID.acscfg.exe** Gateway Info <GatewayName> -system:<SystemName>

#### Пример: IndeedID.acscfg.exe Gateway Info Gateway1 -system:Orion

#### Установка параметров турникета в системе

Для установки параметров турникета в системе используйте команду вида IndeedID.acscfg.exe Gateway Set <GatewayName> [-zone1:<ZoneName> -zone2:<ZoneName>][-id:<Id>]system:<SystemName>

#### Пример: IndeedID.acscfg.exe Gateway Set Gateway1 -zone1:Zone2 -zone2:Zone3 id:12345 —system:Orion

#### Настройка компьютеров

Настройка параметров компьютеров может выполняться как с помощью утилиты IndeedID.acscfg.exe, так и с помощью дополнительной вкладки Indeed-Id ACS в консоли Active Directory Users and Computers.



Для настройки параметров компьютеров необходимы права Indeed-Id ACS Computer Admins.

#### Настройка параметров компьютеров с помощью утилиты IndeedID.acscfg.exe

#### Синтаксис команд и параметры

Для управления компьютерами в командной строке используется следующий синтаксис:

#### Acscfg Computer [EnumZones] [AddZone] [DelZone] [AddCommonZone] [DelCommonZone]

Где:

EnumZones – вывести список зон, в которые включен компьютер <ComputerName>

AddZone – включить компьютер <ComputerName> в зону <ZoneName> в системе <SystemName>

*DelZone* – исключить компьютер <ComputerName> из зоны <ZoneName> в системе <SystemName>

AddCommonZone – включить компьютер <ComputerName> в общую зону <ZoneName>

DelCommonZone – исключить компьютер <ComputerName> из общей зоны <ZoneName>

-system:<SystemName> - имя системы

-zone:<ZoneName> - имя зоны

#### Вывод списка зон, в которые включен компьютер

Для вывода списка зон, в которые включен компьютер, используйте команду IndeedID.acscfg.exe Computer EnumZones <ComputerName>

#### Пример: IndeedID.acscfg.exe Computer EnumZones iddc

#### Включение компьютера в локальную зону

Для включения компьютера в локальную зону используйте команду вида **IndeedID.acscfg.exe Computer AddZone <ComputerName> -system:<SystemName> -zone:<ZoneName>** 

#### Пример: IndeedID.acscfg.exe Computer AddZone iddc –system:Orion –zone:Zone3

#### Исключение компьютера из локальной зоны

Для исключения компьютера из локальной зоны используйте команду вида IndeedID.acscfg.exe Computer DelZone <ComputerName> -system:<SystemName> -zone:<ZoneName>

#### Пример: IndeedID.acscfg.exe Computer DelZone iddc –system:Orion –zone:Zone3

#### Включение компьютера в общую зону

Для включения компьютера в общую зону используйте команду вида IndeedID.acscfg.exe Computer AddCommonZone <ComputerName> -zone:<ZoneName>

#### Пример: IndeedID.acscfg.exe Computer AddCommonZone iddc -zone:Zone5

#### Исключение компьютера из общей зоны

Для исключения компьютера из общей зоны используйте команду вида IndeedID.acscfg.exe Computer -DelCommonZone <ComputerName> -zone:<ZoneName>

#### Пример: IndeedID.acscfg.exe Computer DelCommonZone iddc -zone:Zone5

# Настройка параметров компьютеров с помощью вкладки Indeed-Id ACS в консоли Active Directory Users and Computers

Для включения компьютера в локальную зону откройте раздел **Свойства** (Properties) компьютера, перейдите на вкладку Indeed-ID ACS, выберите в списке систему СКУД, нужную зону в системе и нажмите **Применить** (Apply).

7X86CLIENT Properties	? ×
General Operating System Member Of Delegation Password R Location Managed By Object Security Dial-in Attribute Editor Inde	eplication ( ed-ID ACS
Локальные зоны СКУД система: Orion	
Общая зона	
Зона: <Компьютер не включен в зону>	
OK Cancel Apply	Help

Для включения компьютера в общую зону выберите в списке нужную зону и нажмите **Применить** (Apply).

#### Настройка пользователей

Настройка параметров пользователей может выполняться как с помощью утилиты IndeedID.acscfg.exe, так и с помощью вкладки Indeed-Id ACS в консоли Active Directory Users and Computers.

Для настройки параметров пользователей необходимы права Indeed-Id ACS User Admins.

#### Настройка параметров пользователей с помощью утилиты IndeedID.acscfg.exe

Синтаксис команд и параметры

Для управления пользователями в командной строке используется следующий синтаксис:

#### Acscfg User [EnumTokens] [AddToken] [DelToken]

Где:

EnumTokens – вывести список токенов пользователя <UserName> в системе <SystemName>

AddToken – добавить токен для пользователя <UserName> в системе <SystemName>

DelToken - удалить токен пользователя <UserName> в системе <SystemName>

-system:<SystemName> - имя системы

-rawid: <Id> - идентификатор токена в системе СКУД

#### Вывод списка токенов

Для вывода списка токенов пользователя в системе используйте команду **IndeedID.acscfg.exe** User EnumTokens <UserName> -system:<SystemName>

Пример: IndeedID.acscfg.exe User EnumTokens Anna.Nikolayeva –system:Orion

#### Добавление токена

Для добавления токена используйте команду вида **IndeedID.acscfg.exe User AddToken** <**UserName> -system:<SystemName> -rawid:<Id>** 

Пример: IndeedID.acscfg.exe User AddToken Anna.Nikolayeva -system:Orion -rawid:234

#### Удаление токена

Для удаления токена используйте команду вида IndeedID.acscfg.exe User DelToken </br><UserName> -system:<SystemName> -rawid:<Id>

#### Пример: IndeedID.acscfg.exe User DelToken Anna.Nikolayeva -system:Orion -rawid:234

# Настройка параметров пользователей с помощью вкладки Indeed-Id ACS в консоли Active Directory Users and Computers



Свойства пользователя на вкладке Indeed-Id ACS доступны, только если для данного пользователя разрешено использование технологии аутентификации Indeed-Id.

#### Добавление и удаление токена

Для добавления токена выберите в списке нужный токен и нажмите кнопку 🗌

Добавленный токен отображается в списке токенов, назначенных пользователю.

Для удаления токена выберите в списке нужный токен и нажмите кнопку 🔼

Свойства: Оператор Дежурный	<u>? ×</u>
Member Of Dial-in Sessions Remote control Rem	Environment
Personal Virtual Desktop COM+ Inc	deed-ID Indeed-ID ACS
Отключить проверку нахождения пользов	ателя в зоне компьютера
СКУД система: Orion	1
Список токенов, назначенных пользователю: Имя	Идентификатор
Список токенов в СКУД:	
Имя	Идентификатор
Служебный 104 О Служебный 105 О Служебный 106 О Оперативный дежурный 1 0 1	836 837 838 833
Оператор Дежурный	1087 🗾
OK Cancel	Apply Help

#### Параметры зонирования

Опция Отключить проверку нахождения пользователя в зоне компьютера позволяет отключить проверку местоположения пользователя при его аутентификации на рабочей станции или в приложении. По умолчанию система проверяет, прошел ли пользователь через турникеты зоны, в которой находится его компьютер или нет.

В случае необходимости (например, для удаленного подключения к рабочей станции пользователя) проверка зонирования может быть отключена. В этом случае пользователь получит доступ к компьютеру или приложению, вне зависимости от того находится ли он физически в той же зоне, что и его рабочая станция или нет. Для отключения проверки нахождения пользователя в зоне компьютера отметьте опцию **Отключить проверку нахождения пользователя в зоне** компьютера на вкладке Indeed ACS в свойствах профиля пользователя и нажмите кнопку **Применить** (Apply).

# Пример настройки системы

Ниже приведен список команд, используемых для настройки параметров системы в соответствии с планом:



External

#### Определение зон:

IndeedID.acscfg.exe zone add External -system:<название системы> IndeedID.acscfg.exe zone add Office -system:<название системы> IndeedID.acscfg.exe zone add Green -system:<название системы> IndeedID.acscfg.exe zone add Red -system:<название системы> IndeedID.acscfg.exe zonr add Blue -system:<название системы>

#### Определение турникетов:

IndeedID.acscfg.exe gateway add GateExt1 -system:<название системы> -zone1:External zone2:Office -rawid:<ID турникета GateExt1 в БД SQL> IndeedID.acscfg.exe gateway add GateExt2 -system:<название системы> -zone1:External zone2:Office -rawid:<ID турникета GateExt2 в БД SQL> IndeedID.acscfg.exe gateway add DoorGreen -system:<название системы> -zone1:Office zone2:Green -rawid:<ID двери DoorGreen в БД SQL> IndeedID.acscfg.exe gateway add DoorRed -system:<название системы> -zone1:Green -zone2:Red -rawid:<ID двери DoorRed в БД SQL> IndeedID.acscfg.exe gateway add DoorBlueA -system:<название системы> -zone1:Office zone2:Blue -rawid:<ID двери DoorBlueA в БД SQL> IndeedID.acscfg.exe gateway add DoorBlueA -system:<название системы> -zone1:Office zone2:Blue -rawid:<ID двери DoorBlueA в БД SQL> IndeedID.acscfg.exe gateway add DoorBlueA в БД SQL> IndeedID.acscfg.exe gateway add DoorBlueA в БД SQL> IndeedID.acscfg.exe gateway add DoorBlueB в БД SQL> IndeedID.acscfg.exe gateway add DoorBlueB -system:<название системы> -zone1:Office zone2:Blue -rawid:<ID двери DoorBlueA в БД SQL> IndeedID.acscfg.exe gateway add DoorBlueB -system:<название системы> -zone1:Office zone2:Blue -rawid:<ID двери DoorBlueB в БД SQL> Настройка параметров пользователей, добавление токенов:

IndeedID.acscfg.exe User AddToken <имя пользователя> -system: <название системы> -rawid:<идентификатор токена>

Настройка параметров компьютеров:

IndeedID.acscfg.exe Computer AddZone PCoA -system:<имя системы> -zone:Office
IndeedID.acscfg.exe Computer AddZone PCvA -system:<имя системы> -zone:Office
IndeedID.acscfg.exe Computer AddZone PCvB -system:<имя системы> -zone:Office
IndeedID.acscfg.exe Computer AddZone PCvC -system:<имя системы> -zone:Office
IndeedID.acscfg.exe Computer AddZone PCgA -system:<имя системы> -zone:Green
IndeedID.acscfg.exe Computer AddZone PCgB -system:<имя системы> -zone:Green
IndeedID.acscfg.exe Computer AddZone PCgC -system:<имя системы> -zone:Green
IndeedID.acscfg.exe Computer AddZone PCyA -system:<имя системы> -zone:Green
IndeedID.acscfg.exe Computer AddZone PCyB -system:<имя системы> -zone:Green
IndeedID.acscfg.exe Computer AddZone PCyC -system:<имя системы> -zone:Green
IndeedID.acscfg.exe Computer AddZone PCyD -system:<имя системы> -zone:Green
IndeedID.acscfg.exe Computer AddZone PCyE -system:<имя системы> -zone:Green
IndeedID.acscfg.exe Computer AddZone PCrA -system:<имя системы> -zone:Red
IndeedID.acscfg.exe Computer AddZone PCbA -system:<имя системы> -zone:Blue
IndeedID.acscfg.exe Computer AddZone PCbB -system:<имя системы> -zone:Blue
IndeedID.acscfg.exe Computer AddZone PCbC -system:<имя системы> -zone:Blu

# Групповая политика «Доверять клиенту при получении от него DNS-имени»

Политика раздела Server - **Доверять клиенту при получении от него DNS-имени** - определяет, может ли Сервер Indeed-Id доверять клиенту при получении его DNS-имени. Включение данной политики позволяет избежать запрета на вход в систему в случае, если Серверу Indeed-Id не удалось разрешить ip-адрес клиента.

Для использования данной политики необходимо добавить шаблон IndeedID.Server.adm, включенный в состав дистрибутива Indeed-Id, в список административных шаблонов. Для получения подробной информации обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf*.

Если политика включена, при подключении к Серверу Indeed-Id клиент сообщает серверу Indeed-Id клиент сообщает серверу Indeed-Id свое DNS-имя.

- Если Серверу Indeed-Id не удалось самостоятельно разрешить имя клиента, будет использоваться имя, сообщенное Серверу клиентом; при этом в журнале событий фиксируется предупреждение.
- Если Серверу Indeed-Id удалось самостоятельно разрешить имя клиента, Сервер Indeed-Id сверяет это имя с именем, которое сообщил клиент. Если имена совпадают, Сервер Indeed-Id разрешает вход в систему. Если имена не совпадают, вход в систему запрещается; при этом в журнале событий фиксируется сообщение об ошибке.

# Просмотр событий системы Indeed-Id Rule System

Детали и результаты запросов, обрабатываемых системой Indeed-Id Rule System фиксируются в созданном в момент установки журнале Indeed-ID<sup>1</sup>. Для просмотра журнала событий перейдите в раздел **Администрирование – Просмотр событий – Журналы приложений и служб – Indeed-ID** (Administration Tools – Event Viewer – Application and Services Logs – Indeed-ID) панели управления Windows. Размер журнала составляет до 10Мб, если компонент установлен на серверных ОС. Если компонент, который создает журнал, устанавливается на клиентскую ОС, то размер журнала будет определен в соответствии с настройками операционной системы.

Локальный и удаленный просмотр событий осуществляется с помощью стандартной MMC-оснастки "Просмотр событий" (Event Viewer).

Eile Action View Help ← → È III 🚰 ⓒ 🗟	😫 💵					
	🔮 💵					
Event Viewer (Lecal)						
	Indeed-ID 57	event(s)				
	Туре	Date	Time	Source	Category	Event 🔺
System	Information	28.08.2010	20:23:49	Indeed-ID	ACS configuration	6018
	Information	28.08.2010	20:22:38	Indeed-ID	ACS configuration	6012
DNS Server	Information	28.08.2010	20:12:29	Indeed-ID	ACS configuration	6000
File Replication Service	Information	28.08.2010	20:11:35	Indeed-ID	ACS configuration	6009
Indeed-ID	Information	28.08.2010	20:10:43	Indeed-ID	ACS configuration	6009
	Information	28.08.2010	20:04:57	Indeed-ID	ACS configuration	6021
	💰 Success Audit	28.08.2010	20:00:41	Indeed-ID	User management	1010
	💰 Success Audit	28.08.2010	20:00:39	Indeed-ID	User management	1008
	Information	28.08.2010	19:55:52	Indeed-ID	SSO internal events	10000
	Information	28.08.2010	19:55:52	Indeed-ID	SSO internal events	10000
4	\rm Warning	28.08.2010	19:55:49	Indeed-ID	SSO internal events	10009
4	\rm Warning	28.08.2010	19:55:49	Indeed-ID	SSO internal events	10009
	💰 Success Audit	28.08.2010	19:55:11	Indeed-ID	ESSO agent events	10004
	💰 Success Audit	28.08.2010	19:55:11	Indeed-ID	ESSO agent events	10004
	Information	28.08.2010	19:51:04	Indeed-ID	SSO internal events	10001 🖕
	<u>.</u>					i i i i i i i i i i i i i i i i i i i
	<u> </u>					

#### Смотрите также: Список событий системы Indeed-Id Rule System

<sup>&</sup>lt;sup>1</sup> В версиях Indee-Id RS Administration Tools до 1.0.34 включительно события также могут быть записаны в стандартный журнал Application, если он был выбран на этапе установки компонента. При обновлении на новые версии Indeed-Id Administration Tools журнал событий не изменится.

# Список событий системы Indeed-Id Rule System

В данном разделе представлен список сообщений о событиях системы, генерируемых компонентом AcsStorage, с кратким описанием ситуаций возникновения событий.

Код	Категория	Текст сообщения	Причины возникновения
6000	Информационное	Добавлена новая общая зона.	Успешное создание общей зоны.
		Имя зоны:	
6001	Информационное	Общая зона удалена.	Успешное удаление общей
		Имя зоны:	зоны.
6002	Информационное	Общая зона	Успешное переименование
		переименована.	оощеи зопы.
		Старое имя зоны:	
		Новое имя зоны:	
6003	Информационное	Общая зона	Успешное добавление
		добавлена в систему.	общей зоны в систему.
		Имя зоны:	
		Имя системы:	
6004	Информационное	Общая зона удалена	Успешное удаление общей
		из системы.	зоны из системы.
		Имя зоны:	
		Имя системы:	
6005	Информационное	Добавлена новая	Успешное добавление
		система.	новои системы.
		Имя системы:	
		Data Provider CLSID:	
6006	Информационное	Система удалена.	Успешное удаление
		Имя системы:	системы.
6007	Информационное	Система	Успешное переименование
		переименована.	системы.
		Старое имя системы:	

		Новое имя системы:	
6008	Информационное	Параметры системы изменены. Имя системы: Data Provider CLSID: Старое значение: Новое значение:	Успешное изменение параметров системы.
6009	Информационное	Добавлена новая зона. Имя системы: Имя зоны:	Успешное добавление зоны.
6010	Информационное	Зона удалена. Имя системы: Имя зоны:	Успешное удаление зоны.
6011	Информационное	Зона переименована. Имя системы: Старое имя зоны: Новое имя зоны:	Успешное переименование зоны.
6012	Информационное	Добавлен новый турникет. Имя системы: Имя турникета: Имя зоны на входе: Имя зоны на входе: Идентификатор турникета в СКУД:	Успешное добавление нового турникета.
6013	Информационное	Турникет удален. Имя системы: Имя турникета:	Успешное удаление турникета.

6014	Информационное	Турникет	Успешное переименование
		переименован.	турникета.
		Имя системы:	
		Старое имя	
		турникета:	
		Новое имя турникета:	
6015	Информационное	Параметры турникета	Успешное изменение
		изменены.	параметров турникета
		Имя системы:	(входная/выходная зона).
		Имя турникета:	
		Зона на входе:	
		Старое значение:	
		Новое значение:	
		Зона на выходе:	
		Старое значение:	
		Новое значение:	
6016	Информационное	Параметры турникета	Успешное изменение
			(идентификатор).
		Имя системы:	
		Имя турникета:	
		Идентификатор	
		турникета в СКУД:	
		Старое значение	
		Новое значение:	
6017	Информационное	Компьютер добавлен	Успешное добавление
		в общую зону.	компьютера в общую зону.
		Имя компьютера:	
		Имя зоны:	
6018	Информационное	Компьютер добавлен	Успешное добавление
		в зону.	компьютера в зону.

	Имя компьютера:	
	Имя системы:	
	Имя зоны:	
Информационное	Компьютер удален из общей зоны.	Успешное удаление компьютера из общей зоны.
	Имя компьютера:	
	Имя зоны:	
Информационное	Компьютер удален из зоны.	Успешное удаление компьютера из зоны.
	Имя компьютера:	
	Имя системы:	
	Имя зоны:	
Информационное	Пользователю добавлен токен.	Успешное назначение токена пользователю.
	Имя пользователя:	
	Имя системы:	
	Идентификатор	
	токена в СКУД:	
Информационное	У пользователя	Успешный отзыв токена у
	Имя системы.	
	токена в СКУД:	
Информационное	Проверка нахождения	Администратор системы
	пользователя в зоне	отключил проверку
	выключена.	зоне компьютера.
	Имя пользователя:	
Информационное	Проверка нахождения	Администратор системы
	пользователя в зоне компьютера	включил проверку нахождения пользователя в
	Информационное Информационное Информационное Информационное	Имя компьютера:Имя системы:Имя зоны:ИнформационноеКомпьютер удален из общей зоны.ИнформационноеКомпьютер удален из зоны:ИнформационноеКомпьютер удален из зоны.ИнформационноеКомпьютер удален из зоны.ИнформационноеКомпьютер удален из зоны.ИнформационноеПользователю добавлен токен.ИнформационноеПользователю добавлен токен.ИнформационноеПользователя: имя системы:ИнформационноеУ пользователя удален токен.ИнформационноеУ пользователя удален токен.ИнформационноеУ пользователя удален токен.ИнформационноеУ пользователя зокена в СКУД:ИнформационноеПроверка нахождения пользователя в зоне компьютера выключена.ИнформационноеПроверка нахождения пользователя в зоне компьютера выключена.ИнформационноеПроверка нахождения пользователя в зоне компьютера выключена.

		включена.	зоне компьютера.
		Имя пользователя:	
6300	Предупреждение	Система пропустила проверку нахождение пользователя в зоне компьютера, поскольку данная проверка выключена для данного пользователя. Имя пользователя: Имя компьютера:	Пользователь вошел в систему без проверни на нахождение в зоне компьютера.
6126	Ошибка	Пользователю не назначено ни одного токена.	Неуспешная попытка аутентификации. У пользователя отсутствует зарегистрированный в системе аутентификатор (токен).
6127	Ошибка	Пользователь не прошел через турникет. Имя турникета: Доп. данные:	Неуспешная попытка аутентификации. Вход в систему запрещен сервером правил. Нарушены установленные условия доступа (не зарегистрировано прохождение турникета, соответствующего зоне, к которой привязана данная рабочая станция; нужный турникет пройден с предоставлением системе чужого аутентификатора).

# Список ошибок системы Indeed-Id Rule System

Код	Категория	Текст сообщения	Причины возникновения
0xC40017D4 (6100)	Ошибка	Общая зона не найдена.	Системе не удалось обнаружить общую зону, указанную в запросе.
0xC40017D5 (6101)	Ошибка	Система не найдена.	Не удалось обнаружить систему, указанную в запросе.
0xC40017D6 (6102)	Ошибка	Зона не найдена.	Системе не удалось обнаружить зону, указанную в запросе.
0xC40017D7 (6103)	Ошибка	Турникет не найден.	Системе не удалось обнаружить турникет, указанный в запросе.
0xC40017D8 (6104)	Ошибка	Общая зона с таким именем существует.	Попытка добавления общей зоны с именем, которое уже существует в системе.
0xC40017D9 (6105)	Ошибка	На данный объект ссылаются другие объекты.	Попытка удаления общей зоны без предварительного удаления существующих связей с другими объектами системы.
0xC40017DA (6106)	Ошибка	Общая зона уже включена в указанную систему.	Попытка добавления общей зоны в систему, где уже существует зона с таким именем.
0xC40017DB (6107)	Ошибка	Общая зона не включена в указанную систему.	Системе не удалось обнаружить общую зону в указанной системе.
0xC40017DC (6108)	Ошибка	Система с таким именем существует.	Попытка добавления системы с именем, которое уже существует.
0xC40017DD (6109)	Ошибка	Зона с таким именем существует.	Попытка добавления зоны с именем, которое уже существует.
0xC40017DE (6110)	Ошибка	На данный объект ссылаются другие объекты.	Попытка удаления зоны без предварительного удаления связей с другими объектами системы.
0xC40017E0 (6112)	Ошибка	Турникет с таким именем существует.	Попытка добавления турникета с именем, которое уже существует.
0xC40017E1 (6113)	Ошибка	Турникет с таким RawId существует.	Попытка добавления турникета с идентификатором, который уже существует.

0xC40017E2 (6114)	Ошибка	Компьютер не	Системе не удалось обнаружить
		включен ни в одну из	компьютер ни в одной из зон
		зон в указанной	указанной системы.
		системе.	
	Quintera		
UXC40017E3 (0115)	Ошиока	компьютер уже	
		в указанной системе.	компьютер с таким именем.
0xC40017E4 (6116)	Ошибка	Система с таким	Попытка добавления системы с
		идентификатором	идентификатором, который уже
		существует.	существует.
0xC40017E5 (6117)	Ошибка	Токен не найлен.	Системе не удадось обнаружить
	ошлока	токен не наидени	токен, указанный в запросе.
0xC40017E6 (6118)	Ошибка	Пользователю уже	Попытка назначения токена с
		назначен токен с	идентификатором, который уже
		таким	существует у данного
		идентификатором.	пользователя.
0xC40017E7 (6119)	Ошибка	Компьютер уже	Попытка добавления компьютера
		включен в одну из	в общую зону, где уже существует
		общих зон.	компьютер с таким именем.
0xC40017E8 (6120)	Ошибка	Компьютер не	Системе не удалось обнаружить
		включен ни в одну из	компьютер ни в одной из общих
		общих зон.	зон.
0,(240117E0,(6121))	Outrefield		
UXC40117E9 (0121)	Ошиока	Турникет не наиден в	системе не удалось оонаружить
		скуд системе.	Турникет, указанный в запросе.
0xC40117EA (6122)	Ошибка	Токен не найден в	Системе не удалось обнаружить
		СКУД системе.	токен, указанный в запросе.
0xC40117EB (6123)	Ошибка	Невозможно	Отсутствует связь с сервером
	ошлока	установить	базы данных или Сервером
		соединение с	Indeed-Id.
		сервером базы	
		данных.	
$0_{V}$ C40217EC (6124) <sup>2</sup>	Oumers		
UXC4UZI/EC (0124) <sup>-</sup>	Ошиока		пеуспешная попытка
			аутентификации. Э пользователя
			системе аутентификатор (токец)

<sup>&</sup>lt;sup>2</sup> Код ошибки отображается в журнале событий в качестве описания для события сервера 1001 (Неуспешный вход в систему).

0xC40217ED (6125) <sup>3</sup>	Ошибка	Пользователь не	Неуспешная попытка
		прошел через	аутентификации. Вход в систему
		турникет.	запрещен сервером правил.
			Нарушены установленные условия
			доступа (не зарегистрировано
			прохождение турникета,
			соответствующего зоне, к которой
			привязана данная рабочая
			станция; нужный турникет
			пройден с предоставлением
			системе чужого
			аутентификатора).

<sup>&</sup>lt;sup>3</sup> Код ошибки отображается в журнале событий в качестве описания для события сервера 1001 (Неуспешный вход в систему).

# Удаление и обновление Indeed-Id Rule System

Для удаления компонент Indeed-Id Rule System выполните следующие действия:

- 1. На Панели управления выберите Установка и удаление программ.
- 2. В списке установленных программ выберите нужный компонент (Indeed-Id RS Connector для СКУД/Indeed-Id RS Средства администрирования) и нажмите **Удалить**.
- 3. Подтвердите действие и дождитесь завершения удаления.



Дополнительная вкладка свойств Indeed-Id ACS, зарегистрированная с помощью сценария RegisterACSPages.cmd, продолжает отображаться в режиме поиска даже после удаления пакета Indeed-Id RS Средства администрирования. В этом случае необходимо выполнить сценарий для отмены регистрации вкладки (см. **Регистрация и** удаление зарегистрированной вкладки Indeed-Id ACS).

Для обновления компонент Indeed-Id Rule System не требуется удалять текущую версию (при отсутствии специальных указаний). При установке новой версии ранее установленные компоненты заменяются новыми.

# Решение проблем

Данный раздел содержит информацию о решении известных проблем.

Если Вашей проблемы нет в списке, обратитесь к администратору системы или в службу технической поддержки (см. **Контактная информация**). При письменном обращении в службу поддержки необходимо прилагать к заявке программные логии (см. **Сбор программных логов**).

# 

#### Вход в систему

- Запрет доступа в систему при нарушении правил
- Отсутствует соединение с сервером базы данных
- Пользователю не назначено ни одного токена

## Запрет доступа в систему при нарушении правил

#### Проблема:

При попытке входа в операционную систему или приложение отображается сообщение «Ошибка входа в систему. Пользователь не прошел через турникет»:

Вход в Windows	
Евгений Белов (DEMO\Евгений Белов)	
→ <u>Карта</u> (Z2 USB Card Reader)	
→ <u>Карта + Ладонь</u> (HID OMNIKEY + PalmSecure Rea	ader)
→ Одноразовая матрица	
→ Одноразовый пароль	
→ <u>Пароль</u>	
Ошибка при входе в систему. Пользователь не прошел че	ерез турникет.
	EN <u>Отмена</u>

#### Возможные причины:

Вход в систему запрещен сервером правил. Нарушены установленные условия доступа (не пройден нужный турникет; нужный турникет пройден с предоставлением системе чужой карты).

#### Действия по устранению:

Совместно с сотрудниками службы безопасности выполните проверку обстоятельств доступа в здание/помещение и принадлежности (действительности) средства аутентификации. Список назначенных пользователю токенов отображается на дополнительной вкладке свойств пользователя Active Directory).

## Отсутствует соединение с сервером базы данных

#### Проблема:

При попытке входа в операционную систему или приложение отображается сообщение «Ошибка входа в систему. Невозможно установить соединение с сервером базы данных».

Bход в Windows	
<b>Евгений Белов</b> (DEMO\Евгений Белов)	
→ <u>Карта</u> (Z2 USB Card Reader)	
→ <u>Карта + Ладонь</u> (HID OMNIKEY + PalmSecure Read	er)
→ <u>Одноразовая матрица</u>	
→ <u>Одноразовый пароль</u>	
Ошибка при входе в систему. Невозможно установить соед данных.	цинение с сервером базы
	EN <u>Отмена</u>

#### Возможные причины:

Сервер базы данных недоступен по сети, отключен или находится в состоянии перезагрузки.

#### Действия по устранению:

Выполните проверку соединения и состояния сервера.

### Пользователю не назначено ни одного токена

#### Проблема:

При попытке входа в систему отображается сообщение «Ошибка при входе в систему. Пользователю не назначено ни одного токена».

Вход в Windows	
<b>Евгений Белов</b> (DEMO\Евгений Белов)	
→ <u>Карта</u> (Z2 USB Card Reader)	
→ Карта + Ладонь (HID OMNIKEY + PalmSecure Rea	ader)
→ <u>Одноразовая матрица</u>	
→ Одноразовый пароль	
Ошибка при входе в систему. Пользователю не назначен	о ни одного токена.
	EN <u>Отмена</u>

#### Возможные причины:

Токен пользователя отсутствует или не найден. Используемое средство аутентификации не зарегистрировано в системе для данного пользователя.

#### Действия по устранению:

Выполните проверку параметров учетной записи пользователя.

## Сбор программных логов

Наличие программных логов Indeed-Id позволяет специалистам службы поддержки оперативно локализовать причины возможных проблемных ситуаций и принять меры к их устранению. Сбор программных логов осуществляется с помощью утилиты Indeed-Id GetLog, поставляемой в составе Indeed-Id Access Management. Для получения подробной информации обратитесь к Руководству пользователя Indeed-Id GetLog.