Identity Console

Руководство по администрированию

Май 2021 г.

Уведомление

Дополнительную юридическую информацию, сведения о товарных знаках, заявлениях об отказах, гарантиях, экспортных ограничениях и ограничениях на использование, правах правительства США, политиках в отношении патентов и соответствии требованиям FIPS (Федеральный стандарт обработки информации) см. на веб-странице https://www.netiq.com/company/legal/.

Об этой книге и библиотеке 9
О NetIQ Corporation 11

1 Что такое Identity Console? 15

Возможности Identity Console . . . 15

2 Как получить доступ к Identity Console? 17

Доступ к Identity Console . . . 17

3 Навигация в интерфейсе Identity Console 19

I Управление eDirectory с использованием Identity Console 23

4 Выполнение поиска 25

5 Управление пользователями 29

Создание пользователя . . . 29
Удаление пользователя . . . 30
Изменение пользователей . . . 31
Поиск пользователей . . . 32
Настройка ограничений паролей . . . 33
Запрет и разрешение учетной записи пользователя . . . 33
Установка даты окончания срока действия учетной записи . . . 34
Проверка и сброс блокировки нарушителя . . . 35

6 Управление группами 37

Создание группы . . . 37
Удаление групп . . . 38
Изменение групп . . . 39
Добавление или изменение участников группы . . . 40
Поиск групп . . . 41

7 Управление объектами 43

Создание объекта . . . 43
Удаление объектов . . . 44
Изменение объектов . . . 45
Поиск объекта . . . 46
Перемещение объекта . . . 47
Переименование объекта . . . 48

8 Управление правами 51

Изменение фильтра наследуемых прав . . . 51
Изменение прав опекуна . . . 52
Просмотр действующих прав . . . 53

9 Представление дерева 55

Фрейм навигации в разделе "Дерево" . . . 55
Область содержимого в разделе "Дерево" . . . 55

10 Управление схемой 59

Создание атрибута . . . 59
Создание класса . . . 60
Назначение атрибутов классу . . . 61
Просмотр информации об атрибуте . . . 62
Удаление атрибута . . . 62
Удаление класса . . . 63
Расширение объекта . . . 64

11 Управление событиями аудита 67

Настройка событий аудита CEF . . . 67
Типы событий CEF . . . 69
Настройка фильтрации аудита CEF . . . 70
Фильтрация событий eDirectory с помощью фильтра исключений . . . 71
Фильтрация событий объектов CEF . . . 71
Фильтрация событий атрибута CEF . . . 72

12 Управление зашифрованными атрибутами 73

Создание политики для зашифрованных атрибутов . . . 73
Удаление политики для зашифрованных атрибутов . . . 74
Изменение политики зашифрованных атрибутов . . . 75

13 Управление репликацией с шифрованием 77

Включение репликации с шифрованием для разделов . . . 77

14 Управление разделами и репликами 79

Создание раздела . . . 79
Слияние разделов . . . 80
Изменение разделов . . . 81
Перемещение раздела . . . 81

15 Управление индексами 83

Создание индекса . . . 83
Удаление индекса . . . 84
Копирование индекса . . . 85
Изменение состояния индекса . . . 85

16 Настройка объектов LDAP 87

Создание объектов LDAP . . . 87
Удаление объектов LDAP . . . 88
Изменение объектов LDAP . . . 89

17 Управление сертификатами 91

Управление сертифицирующей организацией (CA) . . . 91
Создание объекта "Корпоративная сертифицирующая организация (CA)" . . . 92
Резервное копирование сертификатов корпоративной сертифицирующей организации (CA) . 92
Восстановление корпоративной сертифицирующей организации (CA) . . . 93
Проверка сертификатов сертифицирующей организации (CA) . . . 94
Замена сертификатов корпоративной сертифицирующей организации (CA) . . . 94
Отзыв сертификатов корпоративной сертифицирующей организации (CA) . . . 94
Управление сертификатами сервера . . . 95
Создание объектов "Сертификат" сервера . . . 95
Экспорт объектов "Сертификат" сервера . . . 95
Проверка объектов "Сертификат" сервера . . . 96
Замена объекта "Сертификат" сервера . . . 96
Отзыв объектов "Сертификат" сервера . . . 96
Удаление объектов "Сертификат" сервера . . . 97
Управление сертификатами пользователя . . . 97
Создание объектов "Сертификат" пользователя . . . 97
Экспорт объектов "Сертификат" пользователя . . . 97
Проверка объектов "Сертификат" пользователя . . . 98
Отзыв объектов "Сертификат" пользователя . . . 98
Удаление объектов "Сертификат" пользователя . . . 98
Управление доверенным корнем и контейнерами . . . 99
Создание контейнера доверенного корня . . . 99
Создание объекта "Сертификат доверенного корня" . . . 99
Экспорт объектов "Сертификат доверенного корня" . . . 100
Проверка объектов "Сертификат доверенного корня" . . . 100
Удаление объектов "Сертификат доверенного корня" . . . 100
Удаление контейнеров доверенного корня . . . 101
Создание объектов "Сертификат сервера по умолчанию" . . . 101
Выпуск сертификата открытого ключа . . . 102
Управление объектом "SAS Service" . . . 105
Создание или удаление объекта "SAS Service" . . . 105

18 Управление Authentication Framework 107

Управление методами входа и послевходовыми методами, а также последовательностями команд при входе в систему и после входа в нее . . . 107
Установка метода входа или метода после входа . . . 107
Обновление существующего метода входа или послевходового метода . . . 108
Удаление методов входа и послевходовых методов . . . 109
Создание новой последовательности команд при входе в систему для данного метода . . . 110
Изменение последовательности команд при входе в систему для данного метода . . . 111
Авторизация и отмена авторизации для последовательности команд при использовании этого метода входа в систему . . . 111
Настройка последовательности команд при входе в систему для данного метода . . . 112
Удаление последовательностей команд при входе в систему для данного метода . . . 113
Управление политиками паролей . . . 114
Создание политики паролей с настройками по умолчанию . . . 114
Создание политики паролей с пользовательскими настройками . . . 115
Изменение политики паролей . . . 118
Удаление политики паролей . . . 119
Управление набором удостоверяющих вопросов . . . 119
Создание нового набора удостоверяющих вопросов . . . 120
Изменение набора удостоверяющих вопросов . . . 120
Удаление наборов удостоверяющих вопросов . . . 121

19 Управление объектами "Группа SNMP" 123

Создание объектов "Группа SNMP" . . . 123
Изменение объектов "Группа SNMP" . . . 123
Удаление объектов "Группа SNMP" . . . 123

20 Управление расширенной фоновой аутентификацией Enhanced Background Authentication (EBA) 125

II Управление Identity Manager с использованием Identity Console 127

21 Управление драйверами и наборами драйверов 129

Добавление и удаление серверов . . . 129
Активация набора драйверов с использованием ключа активации продукта . . . 130
Просмотр информации об активации наборов драйверов . . . 131
Запуск и останов драйверов . . . 132
Поиск драйверов . . . 132
Фильтрация драйверов и наборов драйверов . . . 133
Удаление набора драйверов . . . 134
Действия с драйверами . . . 134

22 Управление свойствами набора драйверов 135

Настройка наборов драйверов . . . 135
Поименованный пароль . . . 135
Значения глобальной конфигурации . . . 136
Настройка параметров среды Java . . . 136
Управление списком атрибутов со значениями . . . 137
Настройка заданий и наборов драйверов . . . 137
Управление библиотеками для определенного набора драйверов . . . 138
Просмотр и удаление существующей библиотеки . . . 138
Просмотр и удаление объектов в библиотеке . . . 138
Настройка уровней протоколирования и трассировки для наборов драйверов . . . 139
Настройка уровня протоколирования . . . 139
Настройка уровня трассировки . . . 140
Отслеживание сценария DirXML . . . 141
Управление инспектором набора драйверов и статистикой . . . 142
Просмотр статистики набора драйверов . . . 142
Просмотр информации о версии . . . 143
Просмотр статистики по ассоциациям . . . 143

23 Управление свойствами драйвера 145

Параметры подключения . . . 145
Конфигурация драйвера . . . 146
Параметры драйвера . . . 146
Значения глобальной конфигурации . . . 147
Значения, присвоенные элементу управления ядром . . . 147
Параметры запуска . . . 151
Поименованный пароль . . . 152
Эквиваленты по правам . . . 152
Исключенные объекты . . . 152
Управление списком атрибутов со значениями . . . 153
Преобразование и синхронизация данных . . . 153
Представление синхронизации данных . . . 153

Фильтры атрибута класса . . . 155
ECMA Script . . . 156
Назначение обратного атрибута . . . 156
Дополнительные параметры . . . 158
Управление наделения правами . . . 158
Управление таблицей назначений объектов . . . 159
Управление заданиями для драйверов . . . 159
Настройка уровней протоколирования и трассировки для драйверов . . . 160
Настройка уровня протоколирования . . . 160
Настройка уровня трассировки . . . 161
Просмотр подробной информации о драйверах . . . 162
Инспектор драйвера . . . 162
Инспектор кэша драйвера . . . 163
Инспектор кэша синхронизации по внешнему каналу . . . 164
Манифест драйвера . . . 165
Мониторинг работоспособности драйвера . . . 165

24 Управление статистикой набора драйверов 171

25 Проверка объектов Identity Manager 173

26 Управление потоком данных 175

27 Управление получателями наделения правами 177

Ссылки наделения правами . . . 177
Результаты наделения правами . . . 177

28 Управление порядками работ 179

Создание нового порядка работ . . . 179
Удаление существующего порядка работ . . . 180
Фильтрация списка порядка работ . . . 180

29 Управление состоянием и синхронизацией пароля 183

Проверка состояния синхронизации пароля . . . 183
Проверка настроек синхронизации пароля . . . 184

30 Управление библиотеками 187

Просмотр и удаление существующей библиотеки . . . 187
Просмотр и удаление объектов в библиотеке . . . 187

Об этой книге и библиотеке

В документе *Руководство по администрированию* предоставлена концептуальная информация о продукте NetIQ Identity Console (Identity Console). В этом руководстве определена терминология и рассмотрены сценарии внедрения.

Самая актуальная версия документа *NetIQ Identity Console Administration Guide (Руководство по администрированию NetIQ Identity Console)* доступна на английском языке на веб-сайте электронной документации по NetIQ Identity Console.

Целевая аудитория

Это руководство ориентировано на сетевых администраторов.

Другая информация в библиотеке

В данной библиотеке представлены перечисленные ниже информационные ресурсы.

Руководство по установке

В этом документе описана процедура установки Identity Console. Руководство предназначено для администраторов сети.

О NetIQ Corporation

Мы глобальная компания, которая разрабатывает корпоративное программное обеспечение, уделяя основное внимание трем постоянным проблемам в вашей среде: изменениям, сложности и риску. Мы работаем над тем, чтобы помочь вам контролировать их.

Наша точка зрения

Адаптация к изменениям и управление сложностью и риском — ничего нового

Из всех проблем, с которыми вы сталкиваетесь, указанные три проблемы, вероятно, являются самыми существенными препятствиями к тому, чтобы получить необходимый вам контроль для безопасного измерения, наблюдения и управления в отношении физических сред, виртуальных сред и сред облачных вычислений.

Обеспечение работы критически важных бизнес-сервисов: лучше и быстрее

Мы считаем, что единственный способ обеспечить своевременное и экономичное предоставление сервисов — предоставить ИТ-организациям максимально возможный контроль. По мере того как организации меняются и технологии, необходимые для управления этими изменениями, становятся все более сложными, постоянные проблемы будут только углубляться.

Наша философия

Продавать интеллектуальные решения, а не просто программное обеспечение

Чтобы обеспечить надежный контроль, сначала мы должны понять реальные сценарии, в которых изо дня в день работают ИТ-организации, наподобие вашей. Для нас это единственная возможность разрабатывать практичные, интеллектуальные ИТ-решения, которые обеспечат доказанные и измеримые результаты. И это гораздо более оправдано с точки зрения удовлетворенности результатами работы, чем просто продавать программное обеспечение.

Мы стремимся помочь вам быть более успешными

В своей работе мы ставим ваш успех на первое место. На всех этапах создания продукта — от начала разработки до развертывания — мы понимаем, что вам нужны хорошо работающие ИТ-решения, которые могут беспрепятственно интегрироваться с имеющимися ресурсами, постоянная поддержка и обучение после развертывания, а также люди, с которыми по-настоящему легко работать. Все это ради изменений. И наконец, ваш успех означает наш общий успех.

Наши решения

- Определение подлинности и управление доступом
- Управление доступом
- Управление безопасностью

- Управление системами и приложениями
- Управление рабочей нагрузкой
- Управление сервисами

Контактная информация службы поддержки продаж

С вопросами о продуктах, ценах и возможностях обращайтесь к местному партнеру. Если вам не удается связаться с партнером, обратитесь в службу поддержки продаж.

Интернациональный (Worldwide):	www.netiq.com/about_netiq/officelocations.asp
США и Канада:	1-888-323-6768
Электронная почта:	info@netiq.com
Веб-сайт:	www.netiq.com

Контактная информация службы технической поддержки

С особыми вопросами о продукте обращайтесь в нашу службу технической поддержки.

Интернациональный (Worldwide):	www.netiq.com/support/contactinfo.asp
Северная и Южная Америка:	1-713-418-5555
Европа, Ближний Восток, Африка:	+353 (0) 91-782 677
Электронная почта:	support@netiq.com
Веб-сайт:	www.netiq.com/support

Контактная информация службы документации

Наша цель — предоставить документацию, которая соответствует вашим потребностям. Если вы хотите поделиться своими предложениями по улучшению, перейдите по ссылке **Добавить комментарий** в нижней части любой HTML-страницы документации www.netiq.com/documentation. Также можно связаться с нами по электронной почте Documentation-Feedback@netiq.com. Мы высоко ценим ваше мнение. Ваши отзывы всегда желанны для нас.

Информация для доступа к интернет-сообществу пользователей

Qmunity — интерактивное сообщество NetIQ — сеть совместной работы, которая позволяет связаться с вашими коллегами и экспертами по NetIQ. В сообществе Qmunity вы можете получить информацию из первых рук, найти полезные ссылки и ресурсы, пообщаться с

экспертами по NetIQ. Таким образом, у вас есть возможность овладеть знаниями, необходимыми для реализации полного потенциала инвестиций в ИТ, на которые вы полагаетесь. Дополнительную информацию см. на веб-сайте http://community.netiq.com.

1 Что такое Identity Console?

Identity Console — это мощная веб-консоль администрирования, предоставляющая виртуальный, защищенный настраиваемый доступ к средствами сетевого администрирования из любого места: требуется лишь подключение к Интернету и веб-навигатор. Identity Console позволяет значительно упростить децентрализацию административных задач.

Возможности Identity Console

В Identity Console доступны следующие возможности:

- Администрирование объектов eDirectory, пользователей, схемы, разделов, реплик, прав и т. д.
- Управление драйверами и наборами драйверов Identity Manager
- Просмотр и управление статистикой производительности драйверов
- Проверка объектов, просмотр потока данных драйвера, управление наделением правами, порядком работ и т. д.
- Управление состоянием синхронизации паролей и настройками для драйверов
- Управление политиками паролей и методами входа
- Управление сертификатами
- Администрирование сетевых ресурсов
- Усиленная безопасность для защиты данных
- Улучшенная масштабируемость для управления более крупными объектами eDirectory
- Безопасный вход на портал Identity Console с помощью One SSO Provider (OSP)
- Самые современные в отрасли технологии пользовательского интерфейса
- Удобная установка и настройка с помощью контейнеров Docker

2 Как получить доступ к Identity Console?

Для доступа к Identity Console и полному набору функций этого решения можно использовать любой поддерживаемый веб-навигатор. Доступ к Identity Console возможен и из веб-навигаторов, не указанных в списке, но мы не гарантируем полную функциональность и не предоставляем поддержку для навигаторов, которые не поддерживаются официально.

ЗАМЕЧАНИЕ. Список поддерживаемых веб-браузеров см. в документе *Identity Console Installation Guide (Руководство по установке Identity Console)*.

Доступ к Identity Console

Для доступа к серверному интерфейсу Identity Console выполните следующие действия:

1. Введите следующий URL-адрес в адресной строке поддерживаемого веб-навигатора.

   Безопасный вход: `https://<ip-адрес-сервера/имя_узла>:<порт>/identityconsole/`

   В примерах в поле < *IP-адрес сервера*> должен быть IPv4-адрес. По умолчанию используется порт 9000.

2. Войдите в систему, используя ваше имя пользователя и пароль.

ПРИМЕЧАНИЕ

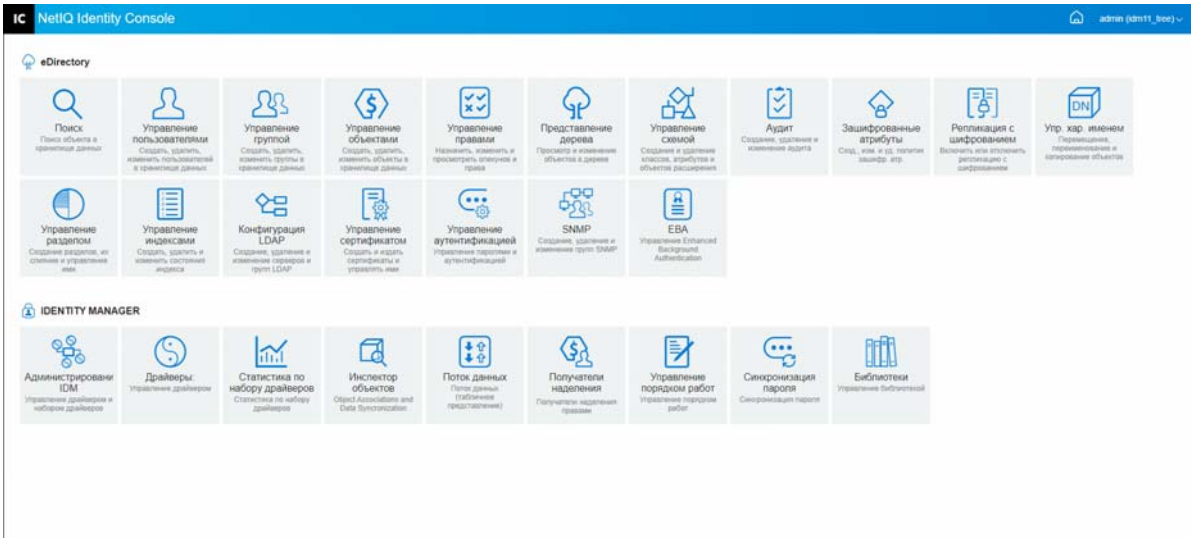
- При обновлении любой вкладки в Identity Console выполняется принудительный выход пользователя из системы по соображениям безопасности.
- Открытие дубликатов вкладок Identity Console в навигаторе приводит к выходу пользователя из системы по соображениям безопасности.
- Имя пользователя должно быть указано в формате `cn=admin,ou=sa,o=system`.

---

3 Навигация в интерфейсе Identity Console

В этом разделе описывается навигация в веб-интерфейсе Identity Console.

Рисунок 3-1 *Интерфейс Identity Console*



ЗАМЕЧАНИЕ. В этом руководстве используются анимационные изображения в формате GIF. Они действуют только в документации в Интернете. При переключении на документацию в формате PDF будут отображаться только снимки экрана.

Таблица 3-1 *Описание модулей веб-портала Identity Console*

Название модуля	Описание
Поиск	Поиск объекта в хранилище данных. Дополнительную информацию см. в разделе Глава 4 на стр. 25: "Выполнение поиска".
Управление пользователями	Создание, удаление и изменение пользователей в хранилище данных. Дополнительную информацию см. в разделе Глава 5 на стр. 29: "Управление пользователями".
Управление группами	Создание, удаление и изменение групп в хранилище данных. Дополнительную информацию см. в разделе Глава 6 на стр. 37: "Управление группами".

Название модуля	Описание
Управление объектами	Создание, удаление и изменение объектов в хранилище данных. Дополнительную информацию см. в разделе Глава 7 на стр. 43: "Управление объектами".
Управление правами	Назначение, изменение и просмотр опекунов и прав. Дополнительную информацию см. в разделе Глава 8 на стр. 51: "Управление правами".
Представление дерева	Просмотр и изменение объектов в дереве. Дополнительную информацию см. в разделе Глава 9 на стр. 55: "Представление дерева".
Schema Management (управление Схемой)	Создание и удаление классов, вспомогательных классов и атрибутов, расширение объектов. Дополнительную информацию см. в разделе Глава 10 на стр. 59: "Управление схемой".
Аудит	Включение и отключение аудита CEF, управление им. Дополнительную информацию см. в разделе Глава 11 на стр. 67: "Управление событиями аудита".
Зашифрованные атрибуты	Создание, изменение, удаление и просмотр политики зашифрованных атрибутов. Дополнительную информацию см. в разделе Глава 12 на стр. 73: "Управление зашифрованными атрибутами".
Зашифрованная репликация	Включение, отключение и просмотр репликации с шифрованием. Дополнительную информацию см. в разделе Глава 13 на стр. 77: "Управление репликацией с шифрованием".
Упр. хар. именем	Перемещение, переименование и копирование объектов. Дополнительную информацию см. в разделе Глава 7 на стр. 43: "Управление объектами".
Управление разделом	Создание, слияние и перемещение разделов и реплик. Дополнительную информацию см. в разделе Глава 14 на стр. 79: "Управление разделами и репликами".
Управление индексами	Создание, модификация и изменение состояния индексов. Дополнительную информацию см. в разделе Глава 15 на стр. 83: "Управление индексами".
Конфигурация LDAP	Создание, удаление и изменение объектов LDAP. Дополнительную информацию см. в разделе Глава 16 на стр. 87: "Настройка объектов LDAP".
Управление сертификатами	Создание сертификатов сервера и CA и управление ими. Дополнительную сведения см. в разделе Глава 17 на стр. 91: "Управление сертификатами".

Название модуля	Описание
Управление аутентификацией	Создание последовательностей команд при входе в систему и методов входа и управление ими. Этот модуль позволяет управлять политиками паролей и наборами удостоверяющих вопросов. Дополнительную информацию см. в разделе Глава 18 на стр. 107: "Управление Authentication Framework".
SNMP	Создание, удаление и изменение групп SNMP. Дополнительные сведения см. в разделе Глава 19 на стр. 123: "Управление объектами "Группа SNMP"".
EBA	Управление улучшенной фоновой аутентификацией. Дополнительную информацию см. в разделе Глава 20 на стр. 125: "Управление расширенной фоновой аутентификацией Enhanced Background Authentication (EBA)".
Администрирование IDM	Управление драйверами и наборами драйверов Identity Manager. Дополнительные сведения см. в Глава 21 на стр. 129: "Управление драйверами и наборами драйверов". С помощью этого модуля можно также управлять свойствами набора драйверов. Дополнительную информацию см. в разделе Глава 22 на стр. 135: "Управление свойствами набора драйверов".
Свойства драйвера	Управление свойствами различных драйверов. Дополнительную информацию см. в разделе Глава 23 на стр. 145: "Управление свойствами драйвера".
Статистика набора драйверов	Просмотр и управление статистикой наборов драйверов Дополнительную информацию см. в разделе Глава 24 на стр. 171: "Управление статистикой набора драйверов".
"Объект" Инспектор	Управление ассоциированием объектов и синхронизацией данных. Дополнительную информацию см. в разделе Глава 25 на стр. 173: "Проверка объектов Identity Manager".
Поток данных	Просмотр т потока данных драйверов и управление им. Дополнительную информацию см. в разделе Глава 26 на стр. 175: "Управление потоком данных".
Получатели наделения правами	Управление получателями наделения правами. Дополнительную информацию см. в разделе Глава 27 на стр. 177: "Управление получателями наделения правами".
Управление порядком работ	Управление порядком работ. Дополнительную информацию см. в разделе Глава 28 на стр. 179: "Управление порядками работ".
Синхронизация паролей	Управление синхронизацией паролей и ее состоянием. Дополнительную информацию см. в разделе Глава 29 на стр. 183: "Управление состоянием и синхронизацией пароля".

Название модуля	Описание
Управление библиотекой	Управление библиотеками. Дополнительную информацию см. в разделе Глава 30 на стр. 187: "Управление библиотеками".

Управление eDirectory с использованием Identity Console

В этом разделе описаны различные задачи по управлению серверами eDirectory с использованием портала Identity Console.

- Глава 4 на стр. 25: "Выполнение поиска"
- Глава 5 на стр. 29: "Управление пользователями"
- Глава 6 на стр. 37: "Управление группами"
- Глава 7 на стр. 43: "Управление объектами"
- Глава 8 на стр. 51: "Управление правами"
- Глава 9 на стр. 55: "Представление дерева"
- Глава 10 на стр. 59: "Управление схемой"
- Глава 11 на стр. 67: "Управление событиями аудита"
- Глава 12 на стр. 73: "Управление зашифрованными атрибутами"
- Глава 13 на стр. 77: "Управление репликацией с шифрованием"
- Глава 14 на стр. 79: "Управление разделами и репликами"
- Глава 15 на стр. 83: "Управление индексами"
- Глава 16 на стр. 87: "Настройка объектов LDAP"
- Глава 17 на стр. 91: "Управление сертификатами"
- Глава 18 на стр. 107: "Управление Authentication Framework"
- Глава 19 на стр. 123: "Управление объектами "Группа SNMP""
- Глава 20 на стр. 125: "Управление расширенной фоновой аутентификацией Enhanced Background Authentication (EBA)"

4 Выполнение поиска

С помощью плитки "Поиск" можно настроить операцию поиска в дереве каталогов и отобразить результаты. Можно искать различные объекты, пользователей, группы и другие элементы. Для поиска различных объектов в хранилище данных выполните следующие действия:

1. Укажите имя объекта для поиска. Для ввода частичного имени используйте звездочку (*). Пример: `ldap*`, `*cert`, `*server*` и т. п. Если указать в этом поле только звездочку, то Identity Console возвратит все результаты поиска, соответствующие указанному **типу** и **контексту**.

   ПРИМЕЧАНИЕ. Используя браузер контекста, можно просматривать все дерево eDirectory, указав звездочку (*) в поле поиска. Кроме того, с помощью звездочки можно фильтровать объекты в контекстном браузере. Пример: `admin*`. Эти функции контекстного браузера поддерживаются в различных модулях Identity Console.

   ---

2. Выберите тип объекта для поиска в поле **Тип**. В Identity Console будут показаны объекты только указанного типа. По умолчанию в этом поле выбран тип **Пользователь**.

   Щелкните значок  , чтобы определить дополнительные настройки поиска на уровне атрибутов. Дополнительную информацию см. в разделе "Настройка расширенного поиска" на стр. 26.

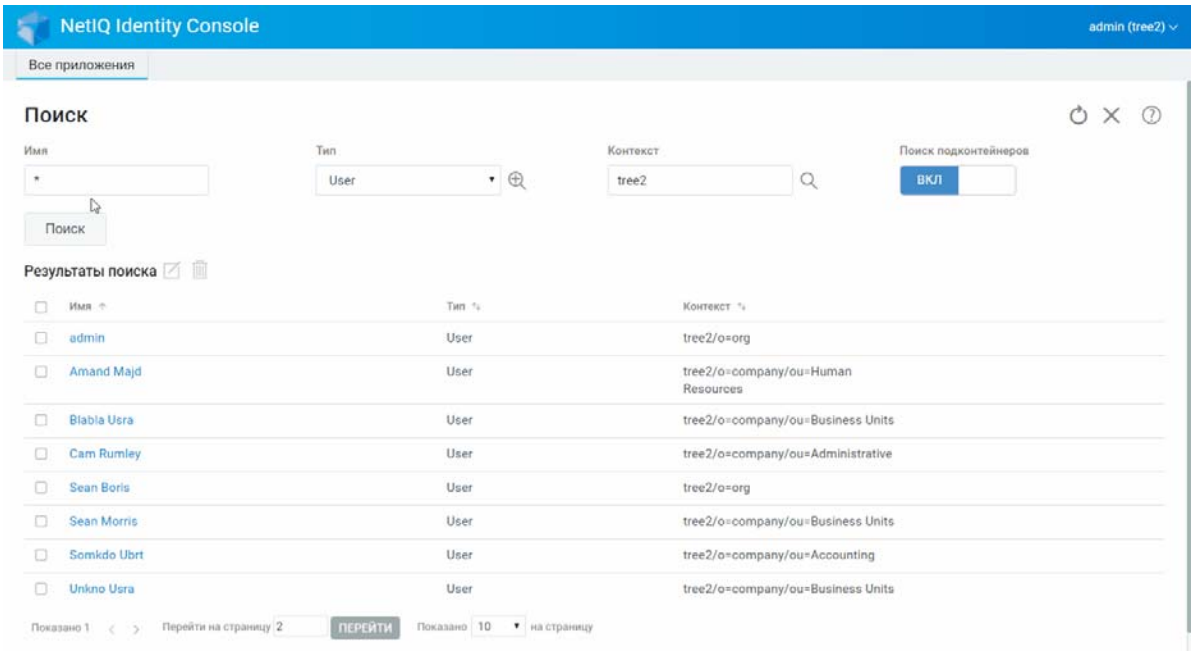
3. Укажите начальный контейнер для операции поиска в поле **Контекст**.

4. Если нужно, чтобы поиск распространялся и на подчиненные контейнеры, выберите **Вкл.** для параметра "Поиск в подчиненных контейнерах".

5. Щелкните кнопку 

.

Рисунок 4-1 *Выполнение операции поиска*



Настройка расширенного поиска

Этот способ выбора объектов предоставляет доступ к среде поиска объектов в каталоге, поддерживающей более широкие возможности настройки.

"Тип объекта". Это поле определяет базовый класс искомых объектов. например "Пользователь".

"Вспомогательные классы". Щелкните значок +, чтобы указать вспомогательный класс для включения в поиск.

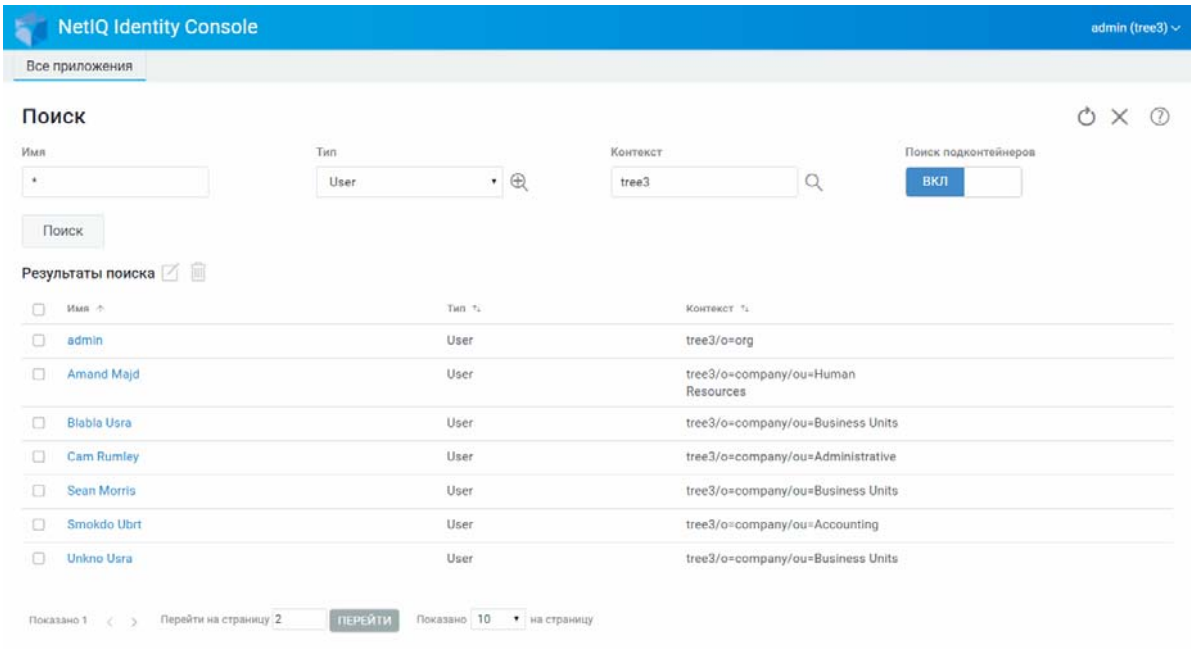
"Атрибут". Это поле позволяет указать атрибут (свойство), который нужно использовать в фильтре.

"Оператор". Это поле позволяет указать логический оператор, который нужно применить к фильтру. Имеются следующие опции.

Значение. Определяет значение атрибута, используемое в качестве фильтра. Для указания части значения можно использовать звездочку (*). Примеры: smi*, *th, *mit*.

Кроме того, можно объединить несколько фильтров атрибутов в группу фильтров: щелкните значок + Rule, чтобы добавить второй атрибут в список. При использовании нескольких фильтров атрибутов их можно связывать с помощью операций "логическое И" и "логическое ИЛИ".

Рисунок 4-2 *Настройка расширенного поиска*



5 Управление пользователями

Управление пользователями и их доступом к сети — основное назначение хранилища данных. С помощью веб-портала Identity Console можно выполнять следующие задачи, связанные с пользователями:

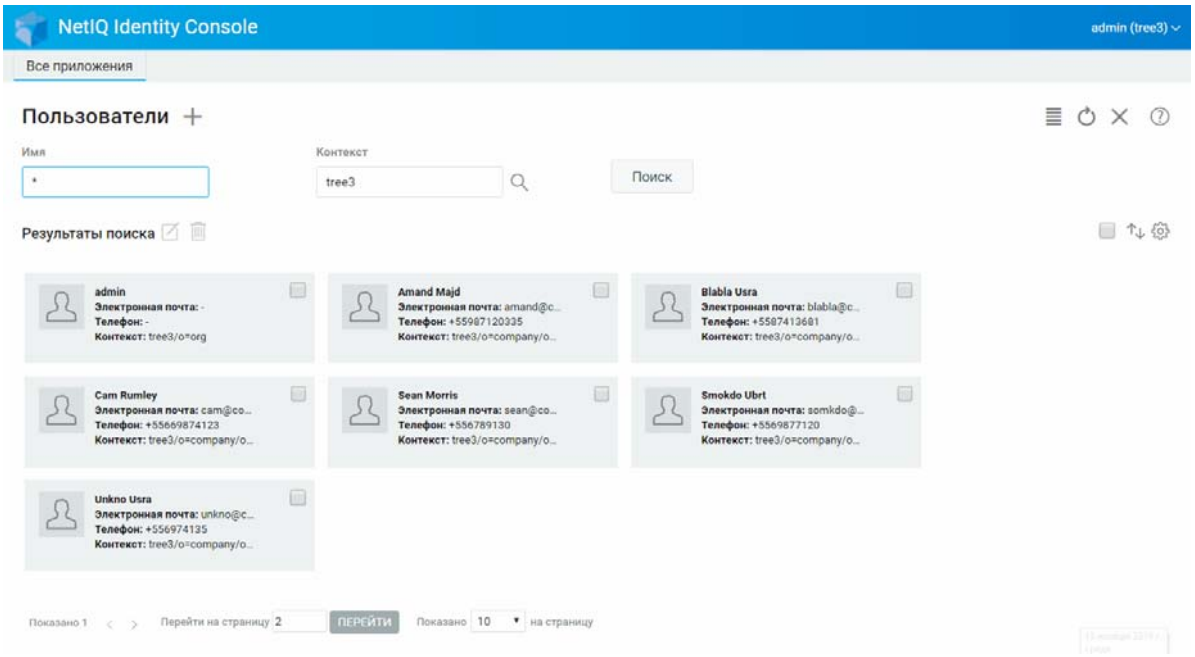
- "Создание пользователя" на стр. 29
- "Удаление пользователя" на стр. 30
- "Изменение пользователей" на стр. 31
- "Поиск пользователей" на стр. 32
- "Настройка ограничений паролей" на стр. 33
- "Запрет и разрешение учетной записи пользователя" на стр. 33
- "Установка даты окончания срока действия учетной записи" на стр. 34
- "Проверка и сброс блокировки нарушителя" на стр. 35

Создание пользователя

Чтобы создать объект "Пользователь", выполните указанные ниже действия.

1. Щелкните **Управление пользователями** на целевой странице Identity Console.
2. Щелкните значок +.
3. На странице "Создать пользователя" введите необходимую информацию о пользователе, затем щелкните кнопку Создать.
   - **Имя пользователя**
   - **Контекст**
   - **Фамилия**
   - **Пароль**
4. Появится сообщение, подтверждающее создание объекта «Пользователь».

Рисунок 5-1 *Создание пользователей*

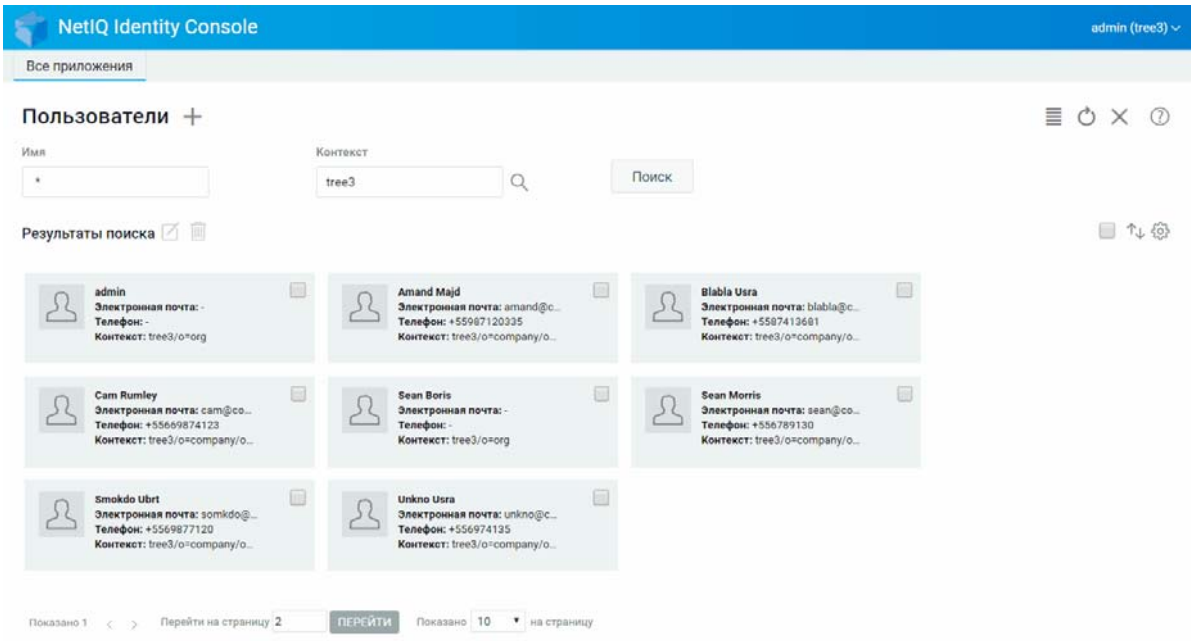


Удаление пользователя

Чтобы удалить объект "Пользователь", выполните указанные ниже действия.

1. Щелкните **Управление пользователями** на целевой странице Identity Console.
2. Введите имя и контекст объекта или найдите его с помощью функции поиска, затем щелкните кнопку Поиск.
3. Выберите объект пользователя в списке поиска и щелкните значок 🗑.
4. Появится сообщение, подтверждающее удаление объекта «Пользователь».

Рисунок 5-2 *Удаление пользователя*

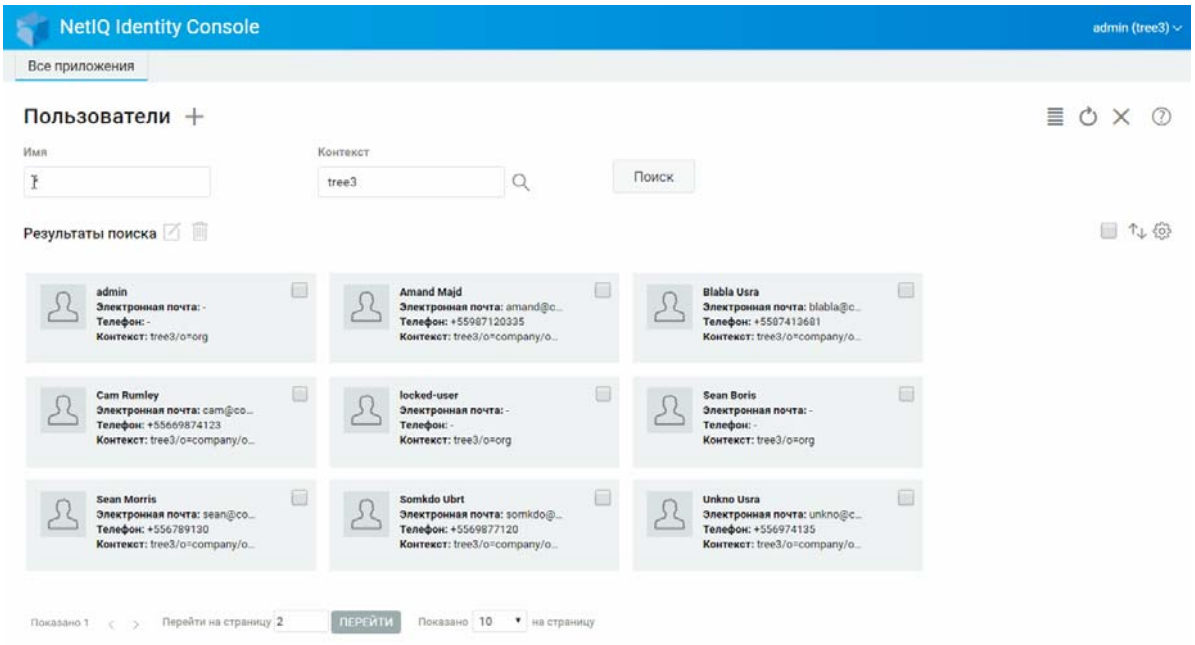


Изменение пользователей

Изменение объекта пользователя:

1. Щелкните **Управление пользователями** на целевой странице Identity Console.
2. Введите имя и контекст объекта или найдите его с помощью функции поиска, затем щелкните кнопку Поиск.
3. Выберите объект пользователя в списке поиска и щелкните значок .
4. Внесите изменения, затем щелкните кнопку Сохранить.
5. Появится сообщение, подтверждающее изменение объекта «Пользователь».

Рисунок 5-3 *Изменение пользователя*



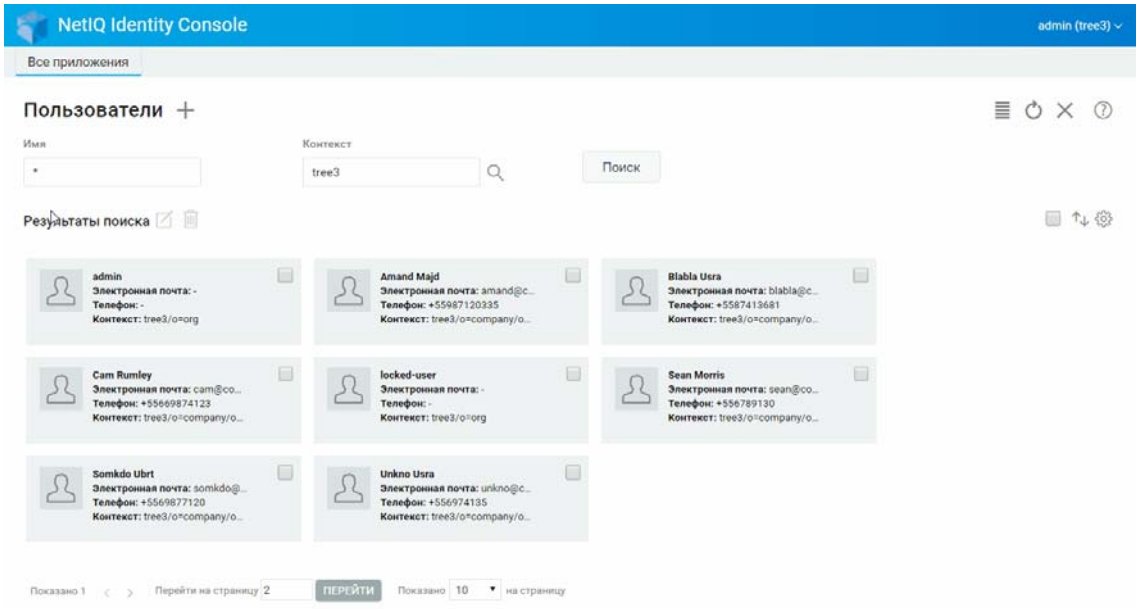
Поиск пользователей

Поиск объекта пользователя:

1 Щелкните **Управление пользователями** на целевой странице Identity Console.

2 Можно искать пользователей только по имени или по имени и контексту. Укажите необходимые данные и щелкните значок Поиск.

Рисунок 5-4 *Поиск пользователя*

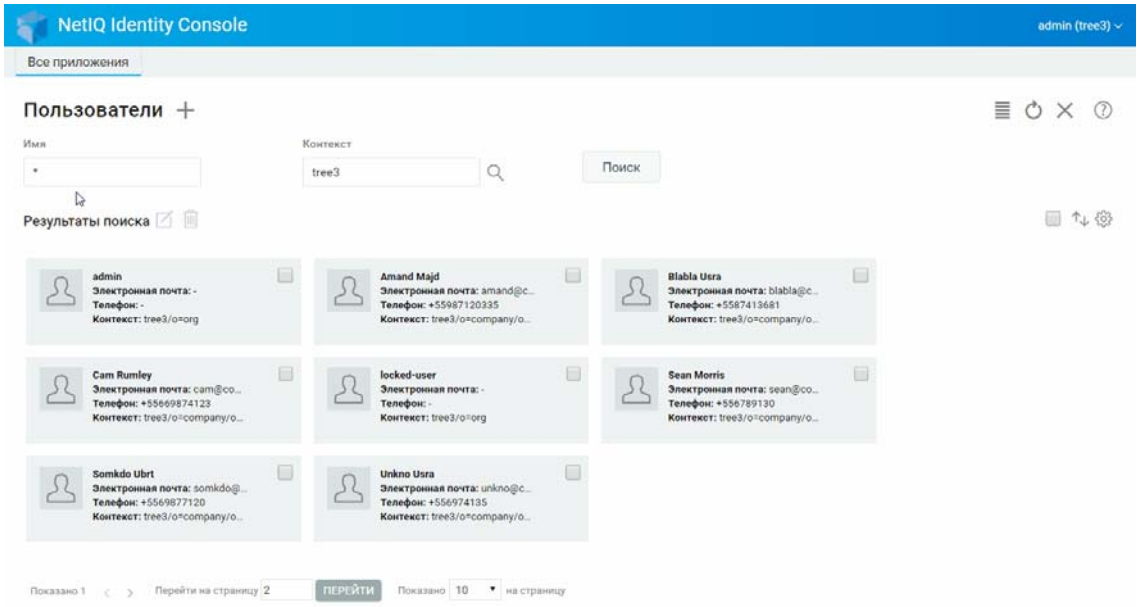


Настройка ограничений паролей

С помощью ограничений паролей можно выполнять следующие действия:

- Разрешить пользователям изменять свои пароли
- Требовать пароль для входа в систему
- Указать стойкость пароля
- Требовать периодически сменять пароль
- Указать дату окончания срока действия пароля
- Требовать создавать уникальный пароль
- Указать период входа в систему с просроченным паролем.

Рисунок 5-5 *Ограничения пароля*

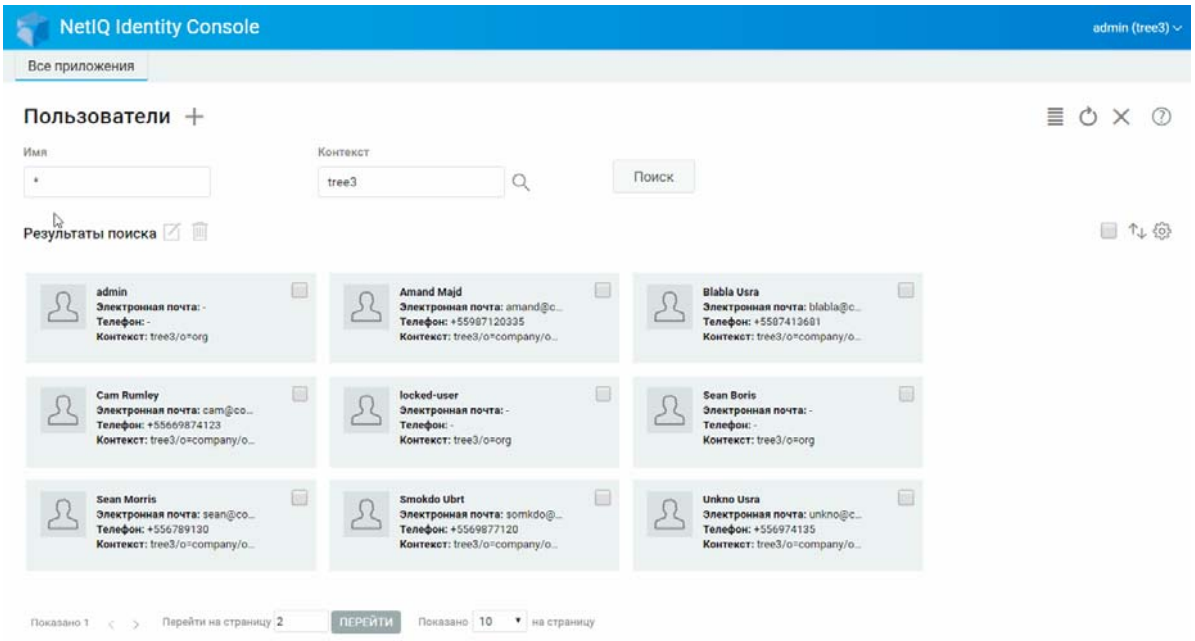


Запрет и разрешение учетной записи пользователя

Чтобы запретить учетную запись пользователя, выполните следующие действия:

1. Выберите пользователя, учетную запись которого нужно запретить, и щелкните значок .
2. Перейдите на вкладку **Ограничения** на странице **Изменить пользователя**.
3. Разверните вкладку **Ограничения входа** и установите флажок **Учетная запись запрещена**.
4. Щелкните значок Сохранить.
5. Теперь учетная запись пользователя запрещена. Чтобы разрешить запрещенную учетную запись пользователя, снимите флажок **Учетная запись запрещена**.

Рисунок 5-6 *Запрет и разрешение учетной записи пользователя*

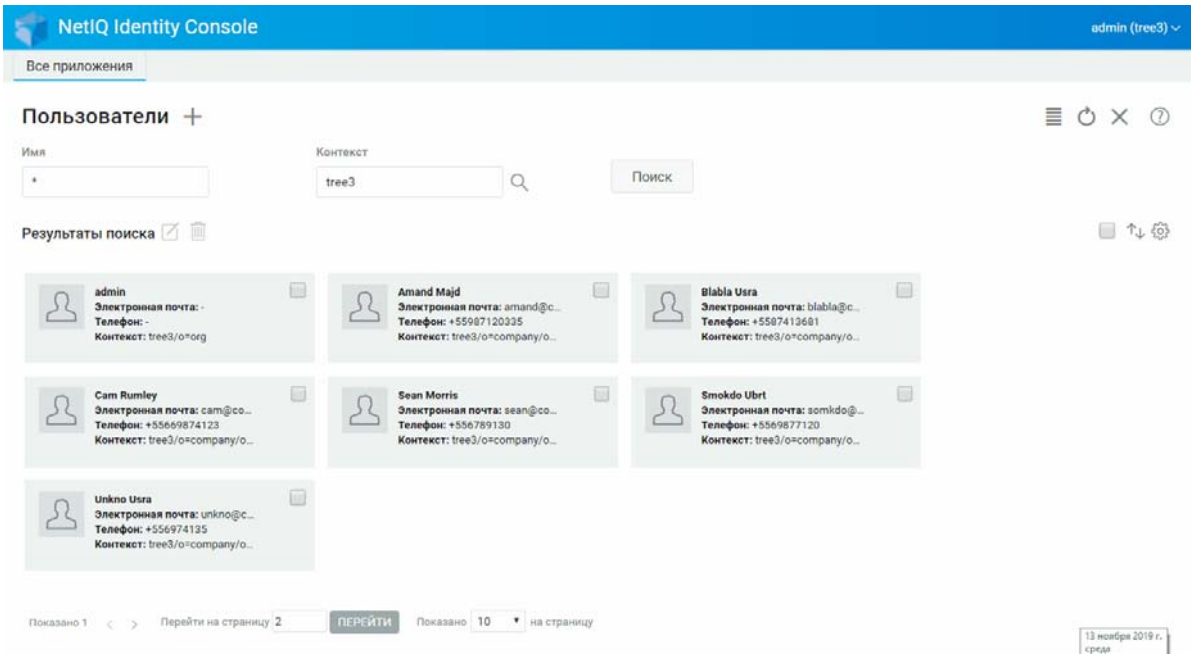


Установка даты окончания срока действия учетной записи

Чтобы установить для пользователей дату окончания срока действия учетной записи, выполните следующие действия:

1. Выберите пользователя, для учетной записи которого нужно установить дату окончания срока действия, и щелкните значок .
2. Перейдите на вкладку **Ограничения** на странице **Изменить пользователя**.
3. Разверните вкладку **Ограничения входа**, установите флажок **Срок действия учетной записи ограничен** и укажите **дату окончания срока действия**.
4. Щелкните значок Сохранить.

Рисунок 5-7 *Установка даты окончания срока действия учетной записи*

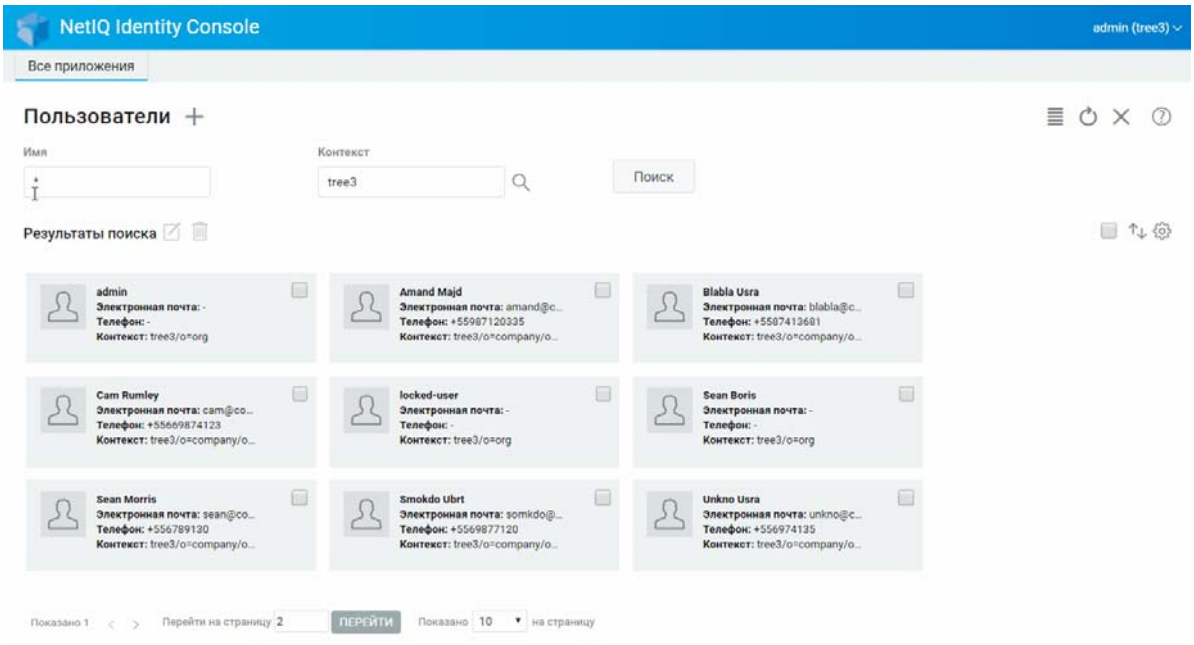


Проверка и сброс блокировки нарушителя

С помощью веб-портала Identity Console можно просмотреть сведения о блокировке нарушителей для любых учетных записей пользователей. Просмотр сведений о блокировке нарушителя:

1. Выберите пользователя, для которого нужно просмотреть сведения о блокировке нарушителя, и щелкните значок .
2. Перейдите на вкладку **Ограничения** на странице **Изменить пользователя**.
3. Разверните вкладку **Блокировка нарушителя** и просмотрите сведения о блокировке.
4. Перейдите на вкладку **Сбросить блокировку** и щелкните кнопку Сбросить блокировку.
5. Щелкните кнопку Сохранить.

Рисунок 5-8 *Проверка и сброс блокировки нарушителя*



6 Управление группами

Группы обычно содержат несколько участников. Любой пользователь, создающий группу, автоматически становится владельцем этой группы. С помощью функции управления группами можно выполнять следующие операции:

- "Создание группы" на стр. 37
- "Удаление групп" на стр. 38
- "Изменение групп" на стр. 39
- "Добавление или изменение участников группы" на стр. 40
- "Поиск групп" на стр. 41

Дополнительную информацию об использовании и настройке объектов "Группа" см. в документе *NetIQ eDirectory 9.2 Administration Guide (Руководство по администрированию NetIQ eDirectory 9.2)* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

Создание группы

Чтобы создать группу:

1. Щелкните **Управление группами** на целевой странице Identity Console.
2. Щелкните значок +.
3. На странице "Создать группу" введите следующие данные:
   - Укажите имя группы
   - Укажите контекст

   Выберите **Динамическая группа**, чтобы созданная группа была динамической и относилась к классу `dynamicGroup`. В противном случае созданная группа будет статической.

   Чтобы сделать новую группу вложенной (класс `nestedGroupAux`), выберите параметр **Вложенная группа**.

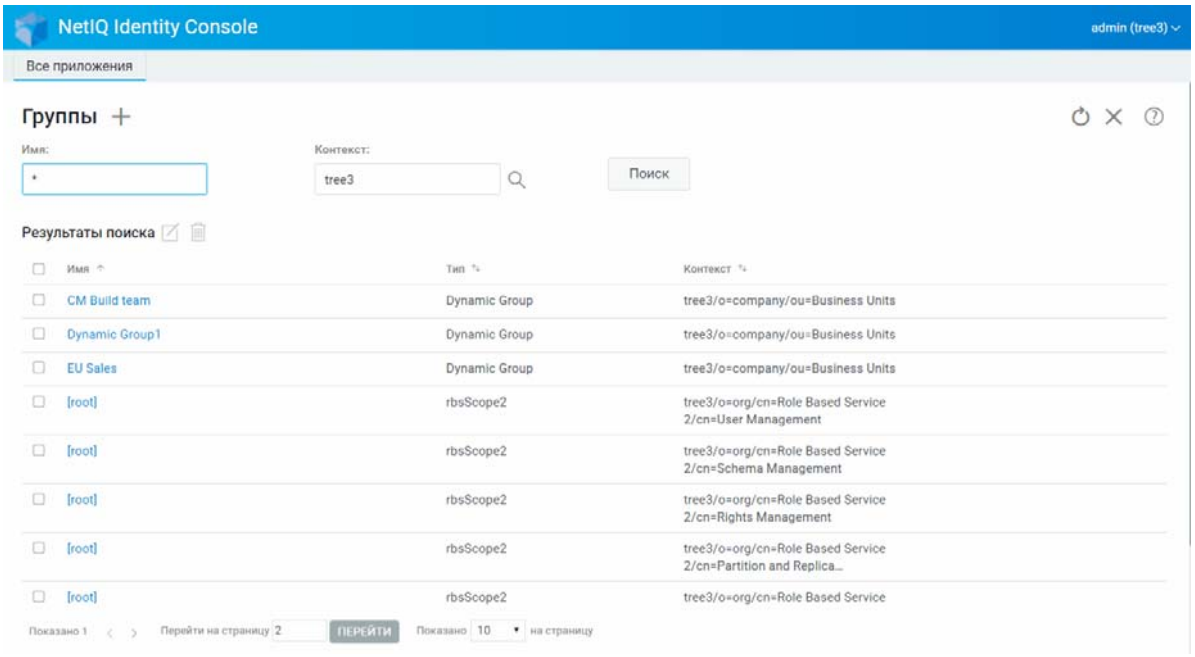
   ПРИМЕЧАНИЕ. Можно преобразовать статическую группу в динамическую или вложенную группу с помощью процедуры, описанной в разделе Изменение объектов. При этом выбранный объект группы будет относиться соответственно к классу `dynamicGroupAux` или к классу `nestedGroupAux`.

   Группа может быть вложенной или динамической. Нельзя создать группу, которая является одновременно вложенной и динамической.

   ---

4. Укажите необходимые данные и щелкните кнопку Создать.
5. Появится сообщение, подтверждающее создание группы.

Рисунок 6-1 *Создание группы*

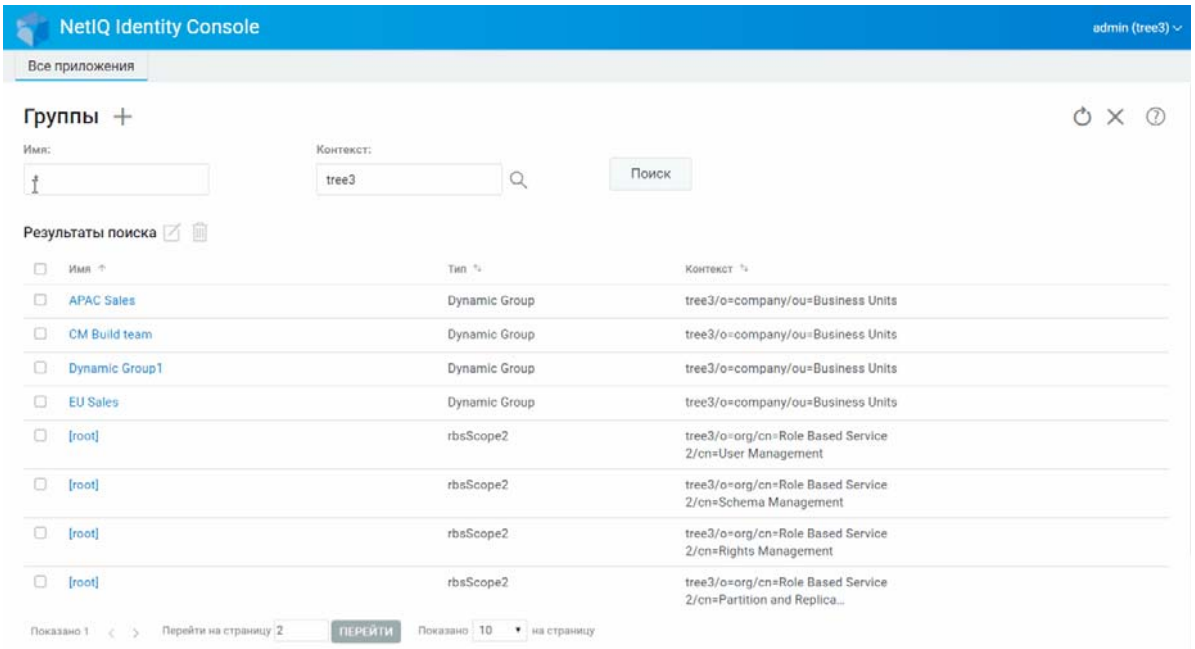


Удаление групп

Удаление групп:

1. Щелкните **Управление группами** на целевой странице Identity Console.
2. Укажите имя и контекст группы или найдите ее с помощью функции поиска, затем щелкните кнопку Поиск.
3. Выберите группу, которую нужно удалить, и щелкните значок 🗑.
4. Появится сообщение, подтверждающее удаление группы.

Рисунок 6-2 *Удаление групп*

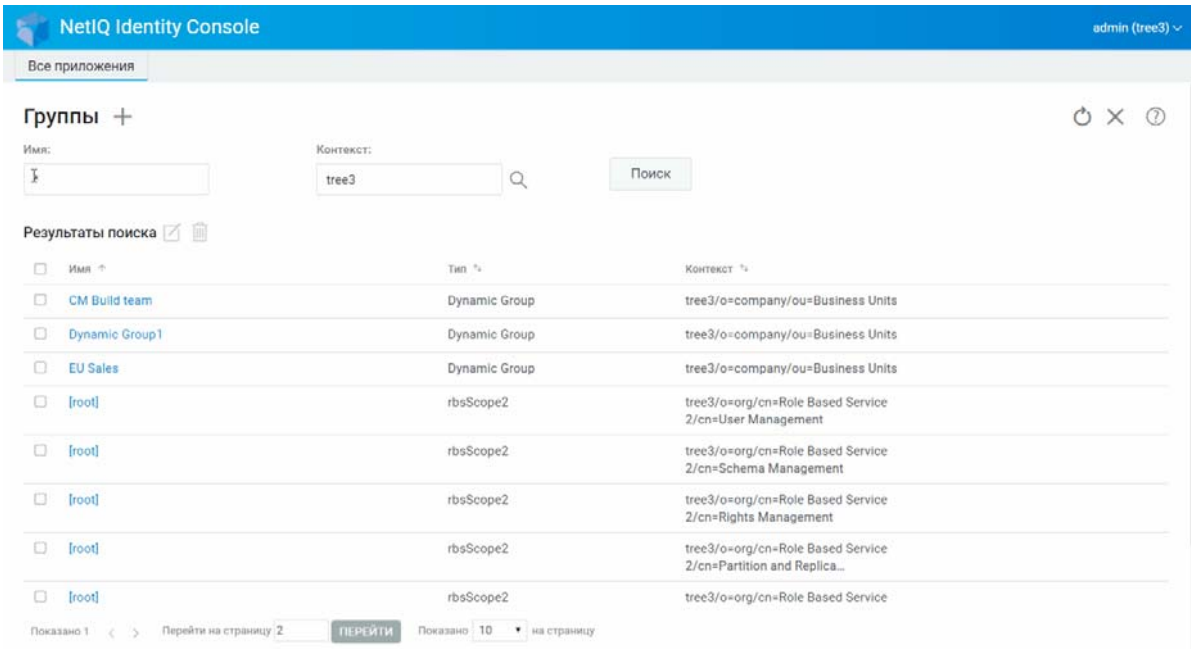


Изменение групп

Изменение групп:

1. Щелкните **Управление группами** на целевой странице Identity Console.
2. Введите имя и контекст группы, затем щелкните кнопку Поиск.
3. Выберите группу, которую нужно изменить, и щелкните значок .
4. Внесите изменения, затем щелкните кнопку Сохранить.
5. Появится сообщение, подтверждающее изменение группы.

Рисунок 6-3 *Изменение групп*

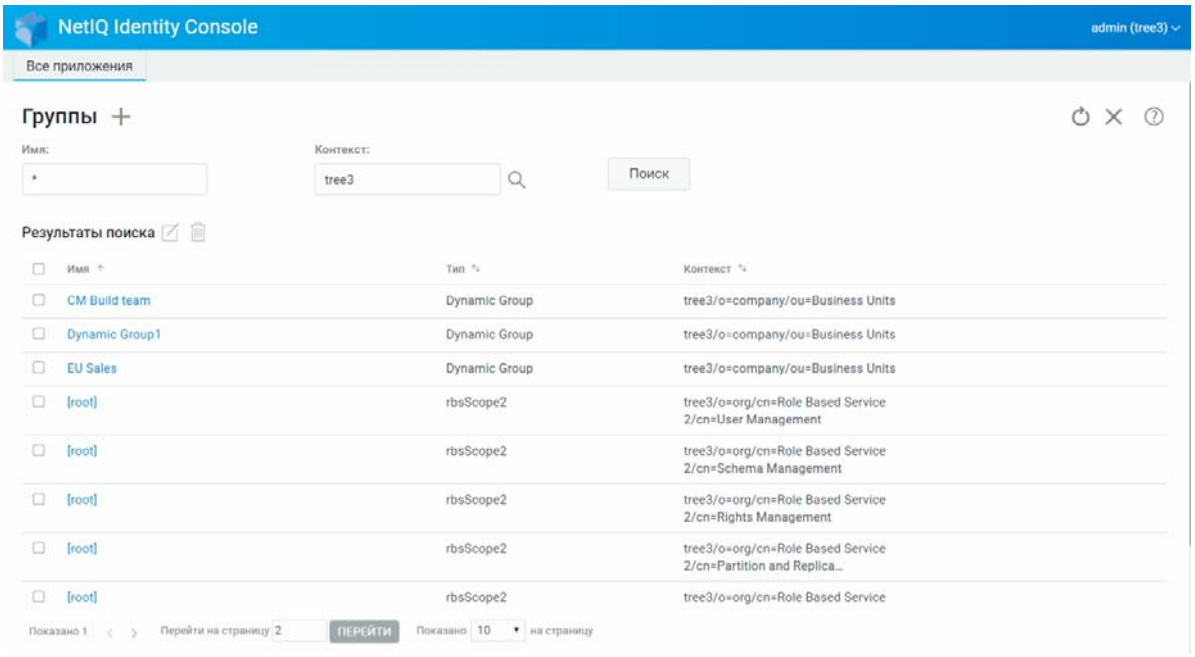


Добавление или изменение участников группы

Добавление или изменение участников группы:

1. Щелкните **Управление группами** на целевой странице Identity Console.
2. Введите имя и контекст группы, затем щелкните кнопку Поиск.
3. Выберите группу и щелкните значок .
4. Перейдите на вкладку **Участники** на странице **Изменить группу**.
5. Щелкните значок , чтобы добавить нового участника в группу. Чтобы удалить участников из группы, щелкните значок .
6. Внесите изменения, затем щелкните кнопку Сохранить.
7. Появится сообщение, подтверждающее изменение группы.

Рисунок 6-4 *Добавление или изменение участников группы*

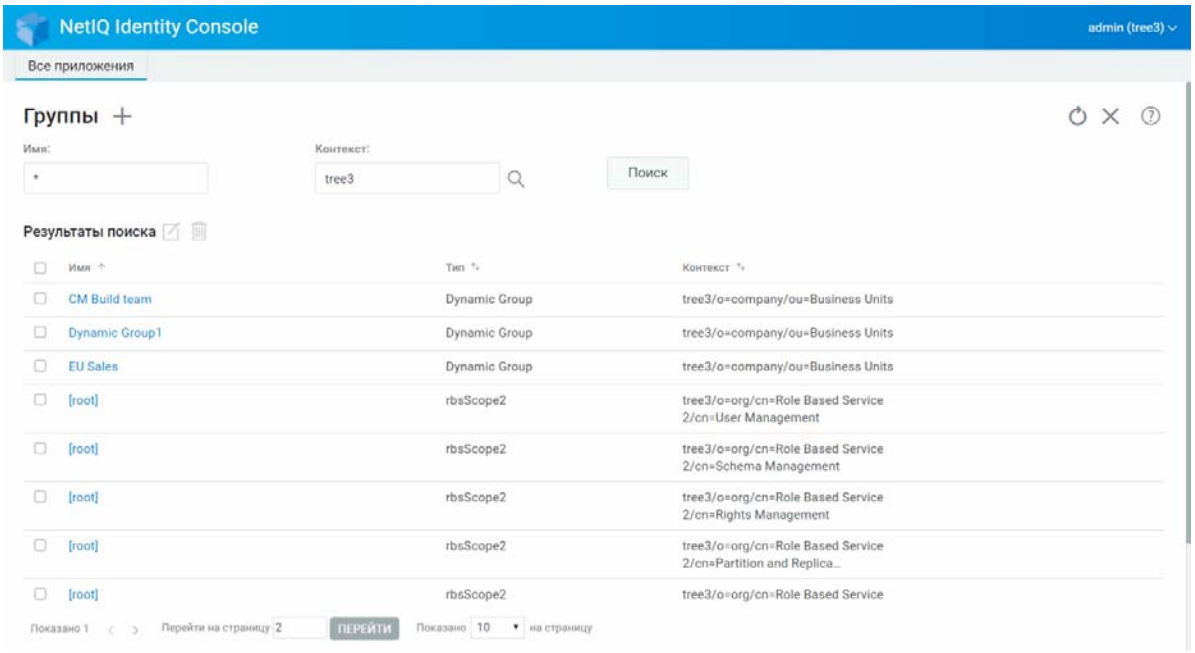


Поиск групп

Поиск групп:

1. Щелкните **Управление группами** на целевой странице Identity Console.
2. Можно искать группы только по имени или по имени и контексту.
3. Укажите необходимые данные и щелкните значок Поиск.

Рисунок 6-5 *Поиск групп*



7 Управление объектами

В Identity Console можно управлять различными объектами в хранилище данных. С помощью этого модуля можно создавать, изменять, удалять и искать объекты.

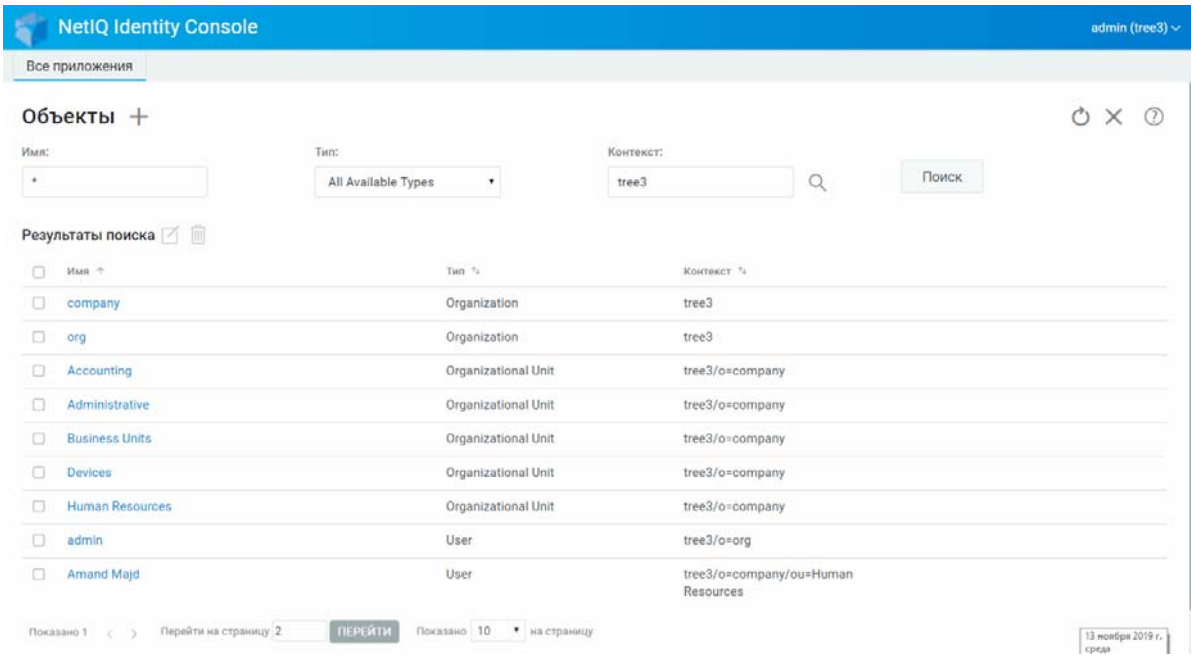
- "Создание объекта" на стр. 43
- "Удаление объектов" на стр. 44
- "Изменение объектов" на стр. 45
- "Поиск объекта" на стр. 46
- "Перемещение объекта" на стр. 47
- "Переименование объекта" на стр. 48

Создание объекта

Создание нового объекта:

1. Щелкните **Управление объектами** на целевой странице Identity Console.
2. Щелкните значок +.
3. На странице "Создать объект" введите следующие данные:
   - Укажите имя объекта
   - Укажите тип
   - Укажите контекст
4. Укажите необходимые данные и щелкните кнопку **Далее** > **Создать**.
5. Появится сообщение, подтверждающее создание объекта.

Рисунок 7-1 *Создание объекта*

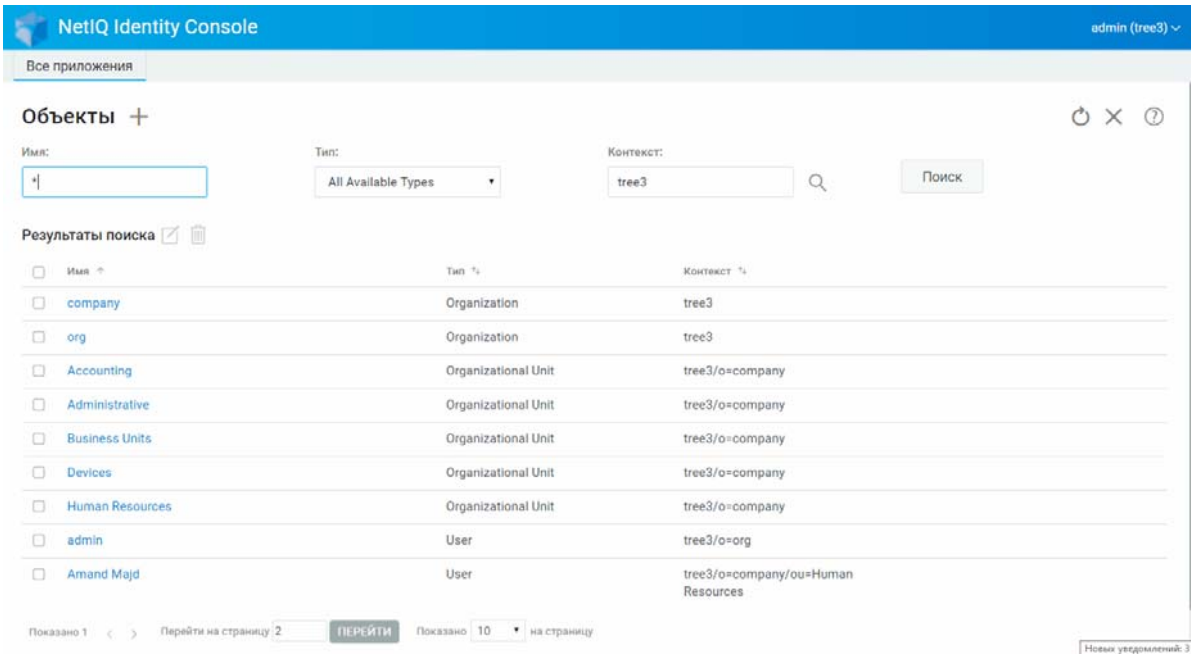


Удаление объектов

Удаление объектов:

1. Щелкните **Управление объектами** на целевой странице Identity Console.
2. Укажите имя, тип и контекст объекта или найдите его с помощью функции поиска, затем щелкните кнопку Поиск.
3. Выберите объект в списке поиска и щелкните значок .
4. Появится сообщение, подтверждающее удаление объекта.

Рисунок 7-2 *Удаление объектов*

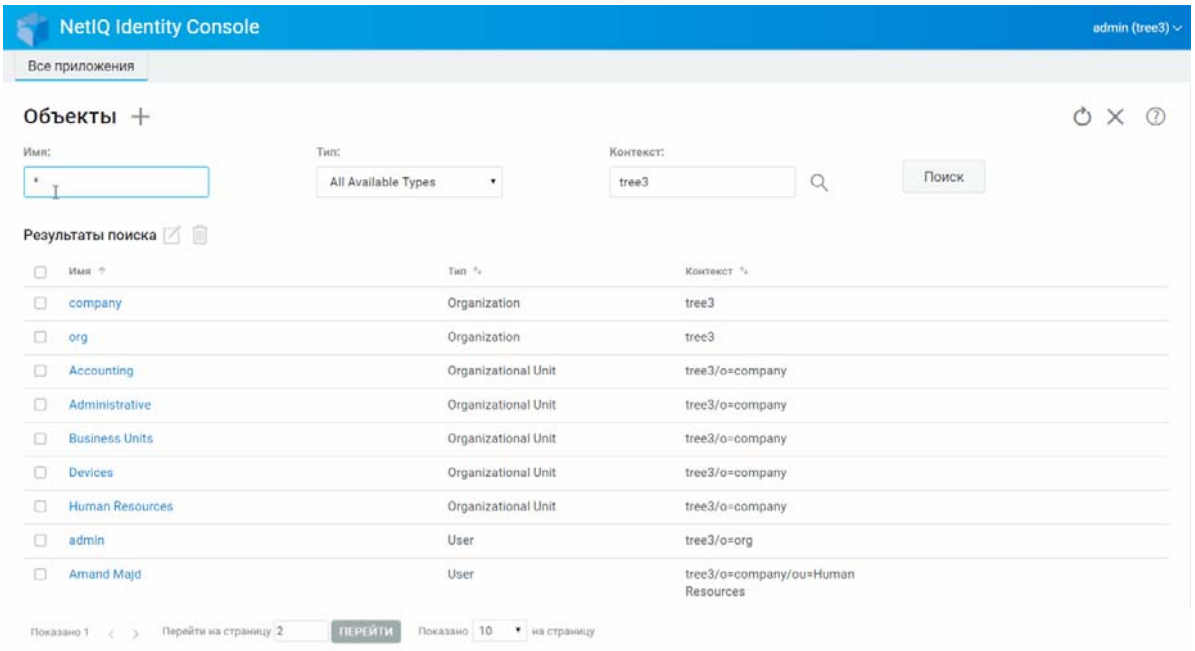


Изменение объектов

Изменение объектов:

1. Щелкните **Управление объектами** на целевой странице Identity Console.
2. Введите имя, тип и контекст объекта, затем щелкните кнопку Поиск.
3. Выберите объект в списке поиска и щелкните значок .
4. Внесите изменения, затем щелкните кнопку Сохранить.
5. Появится сообщение, подтверждающее изменение объекта.

Рисунок 7-3 *Изменение объектов*

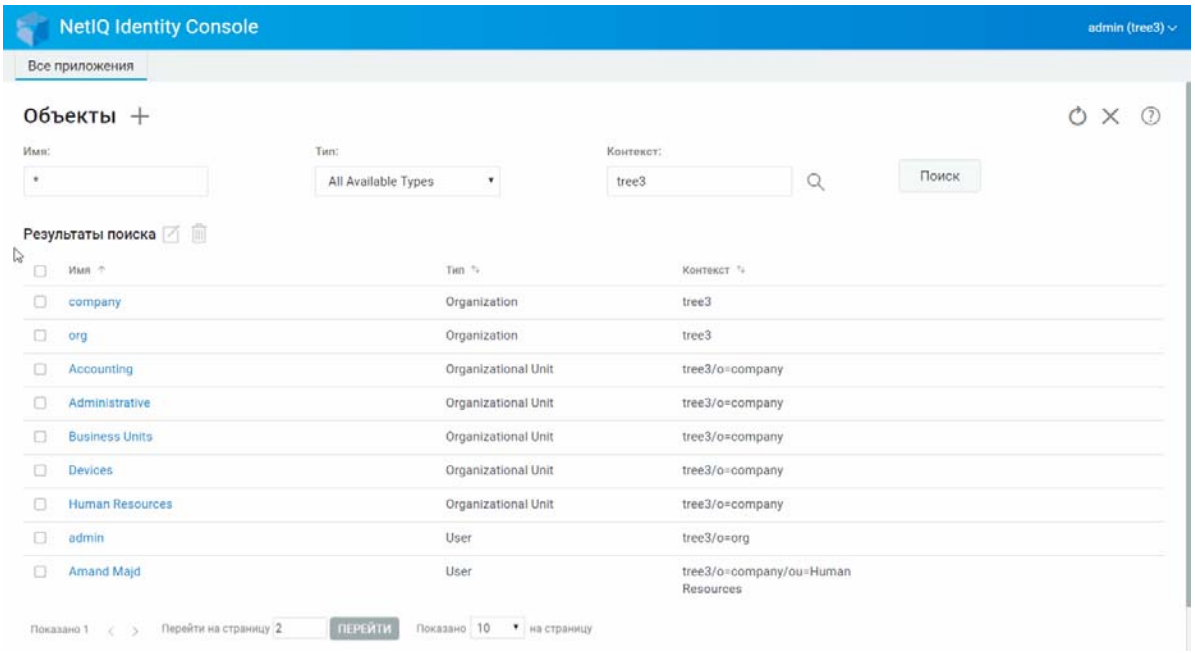


Поиск объекта

Поиск объектов:

1. Щелкните **Управление объектами** на целевой странице Identity Console.
2. Можно искать объекты только по имени или по имени, типу и контексту.
3. Укажите необходимые данные и щелкните кнопку Поиск.

Рисунок 7-4 *Поиск объекта*



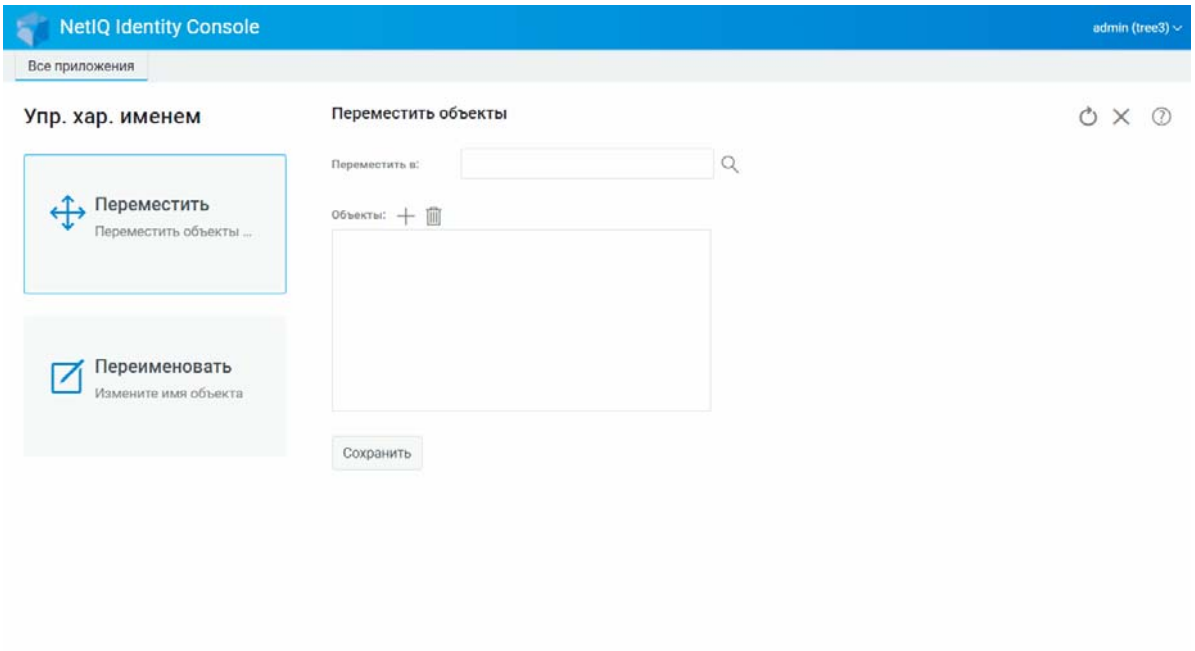
Перемещение объекта

Перемещение объектов:

1. Щелкните **Управление характерным именем** на целевой странице Identity Console.
2. По умолчанию будет выбрана команда **Переместить объект**.
3. В поле **Переместить в** выберите контейнер, в который нужно переместить объект.
4. Щелкните значок +, чтобы добавить объект, который нужно переместить в другой контейнер.

   Чтобы удалить выбранный объект, щелкните значок .
5. Щелкните кнопку Сохранить.
6. Появится сообщение, подтверждающее перемещение объекта.

Рисунок 7-5 *Перемещение объекта*

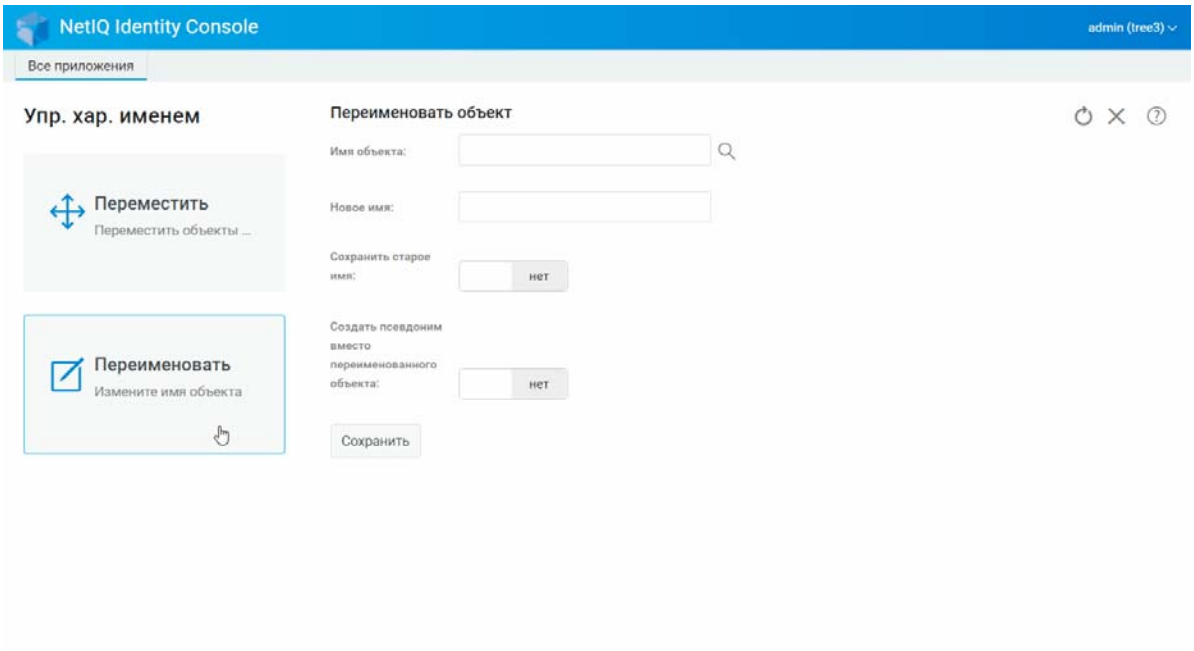


Переименование объекта

Чтобы переименовать объект:

1. Щелкните **Управление характерным именем** на целевой странице Identity Console.
2. Выберите **Переименовать объект**.
3. С помощью функции поиска найдите объект, который нужно переименовать, в поле **Имя объекта**.
4. Укажите новое имя объекта в поле **Новое имя**. Не указывайте контекст.
5. Если необходимо сохранить старое имя объекта, установите соответствующий флажок.
6. Щелкните кнопку Сохранить.
7. Появится сообщение, подтверждающее переименование объекта.

Рисунок 7-6 *Переименование объекта*



8 Управление правами

Здесь понятие "права" относится к правам опекунов и опекунам eDirectory. При создании дерева назначаются права по умолчанию, предоставляющие общий доступ и общий уровень безопасности для вашей сети. В Identity Console можно выполнять следующие задачи, связанные с правами:

- "Изменение фильтра наследуемых прав" на стр. 51
- "Изменение прав опекуна" на стр. 52
- "Просмотр действующих прав" на стр. 53

Дополнительную информацию о правах в eDirectory см. в документе *NetIQ eDirectory 9.2 Administration Guide (Руководство по администрированию NetIQ eDirectory 9.2)* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

Изменение фильтра наследуемых прав

В eDirectory предусмотрен фильтр унаследованных прав (IRF) для блокирования наследования прав для отдельных подчиненных элементов.

Дополнительную информацию о фильтрах наследуемых прав см. в документе *NetIQ eDirectory 9.2 Administration Guide (Руководство по администрированию NetIQ eDirectory 9.2)* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

1. Щелкните **Управление правами** на целевой странице Identity Console
2. Выберите **Фильтр унаследованных прав**.

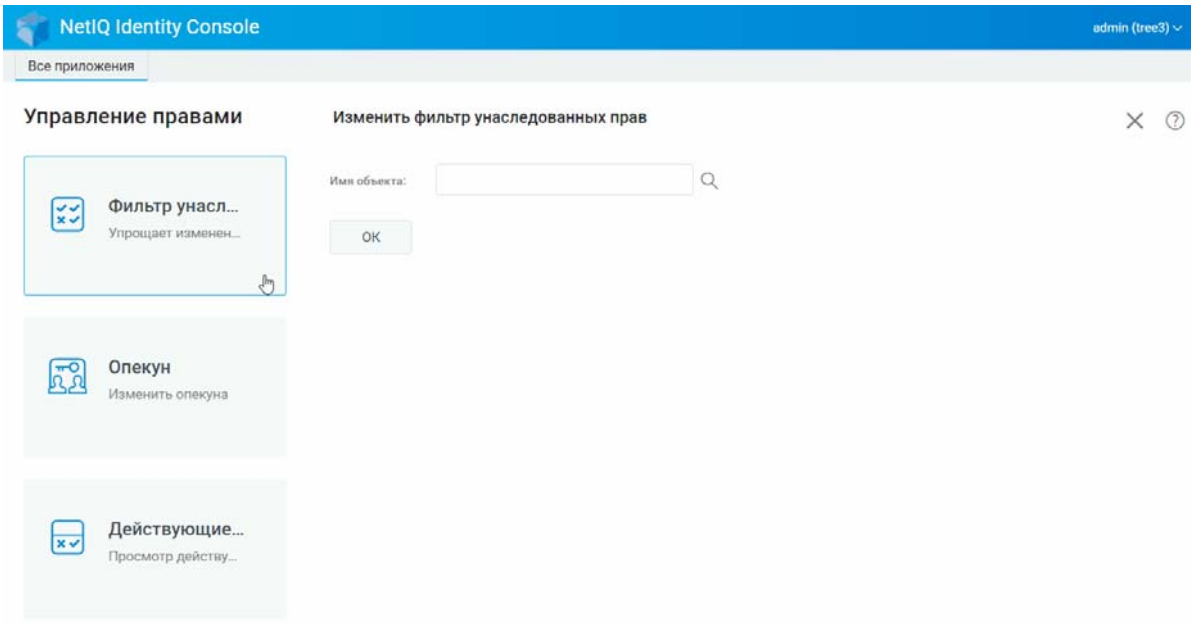
   ПРИМЕЧАНИЕ. Фильтр унаследованных прав выбран по умолчанию.

3. Укажите полное имя объекта, для которого нужно изменить фильтр унаследованных прав, или найдите его с помощью значка выбора объектов, затем щелкните кнопку **OK**.

   Будет показан список фильтров наследуемых прав, которые уже определены для данного объекта.
4. В окне **Свойства** отредактируйте список фильтров унаследованных прав, затем щелкните кнопку **Применить**.

   Для редактирования этого списка необходимо иметь право "Супервизор" или "Управление доступом" на свойство ACL данного объекта. Вы можете определить фильтры, которые будут блокировать наследуемые права в целом, права на все свойства объекта, а также на отдельные свойства.

Рисунок 8-1 *Изменение фильтра наследуемых прав*



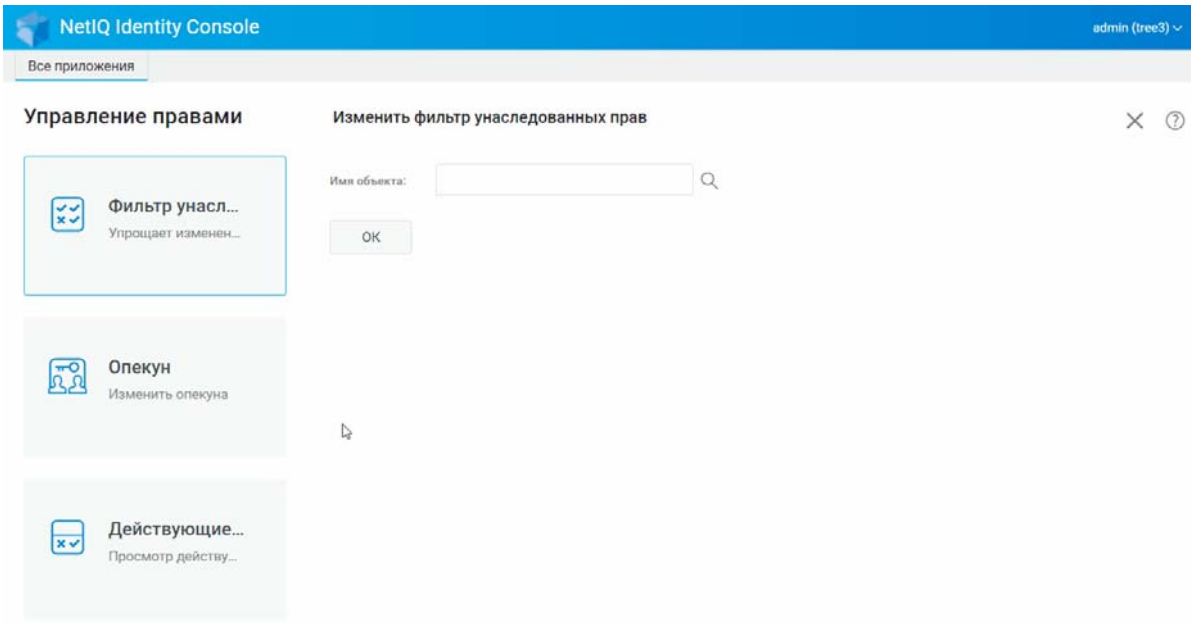
Изменение прав опекуна

Опекун — это объект, которому явно предоставлены права на выполнение операций над другим объектом в дереве каталога. Чтобы изменить список опекунов для конкретного объекта, выполните указанные ниже действия.

1. Щелкните **Управление правами** на целевой странице Identity Console
2. Выберите **Опекун**.
3. Укажите имя объекта, для которого нужно просмотреть список опекунов, или найдите его с помощью значка выбора объектов, затем щелкните кнопку **ОК**.

   Будет показан список опекунов, назначенных объекту в настоящее время.
4. Измените список опекунов в соответствии с требованиями и щелкните кнопку **ОК**.
   - Чтобы добавить опекуна, щелкните значок +.
   - Чтобы удалить опекуна, установите флажок этого опекуна и щелкните значок.
   - Чтобы изменить для опекуна назначения прав, щелкните ссылку **Назначенные права**.

Рисунок 8-2 *Изменение прав опекуна*



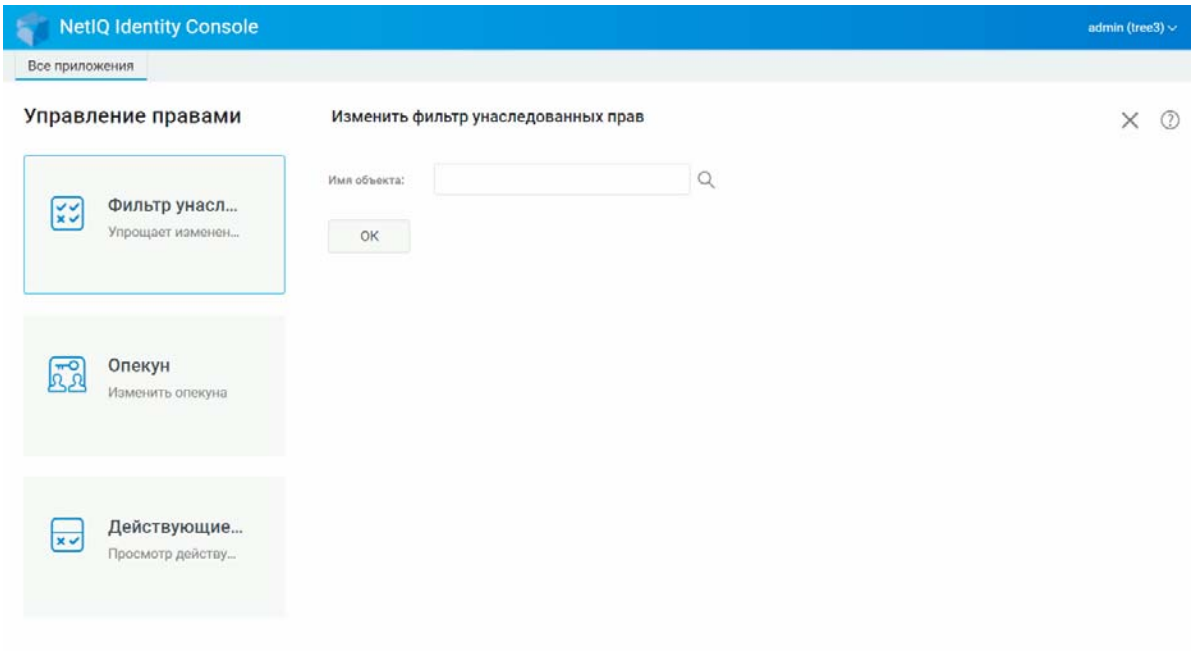
Просмотр действующих прав

Действующие права объединяют явные и наследуемые права, которыми объект обладает в той или иной точке дерева каталогов. Чтобы просмотреть действующие права объекта на другой объект, выполните указанные ниже действия.

1. Щелкните **Управление правами** на целевой странице Identity Console
2. Выберите **Действующие права**.
3. Укажите имя опекуна, для которого нужно просмотреть права, или найдите его опекуна с помощью значка выбора объектов , затем щелкните кнопку **OK**.
4. В поле "Имя объекта" укажите имя объекта, для которого нужно просмотреть действующие права опекуна.

   Действующие права будут рассчитаны и отображены в поле **Действующие права**.

Рисунок 8-3 *Просмотр действующих прав*



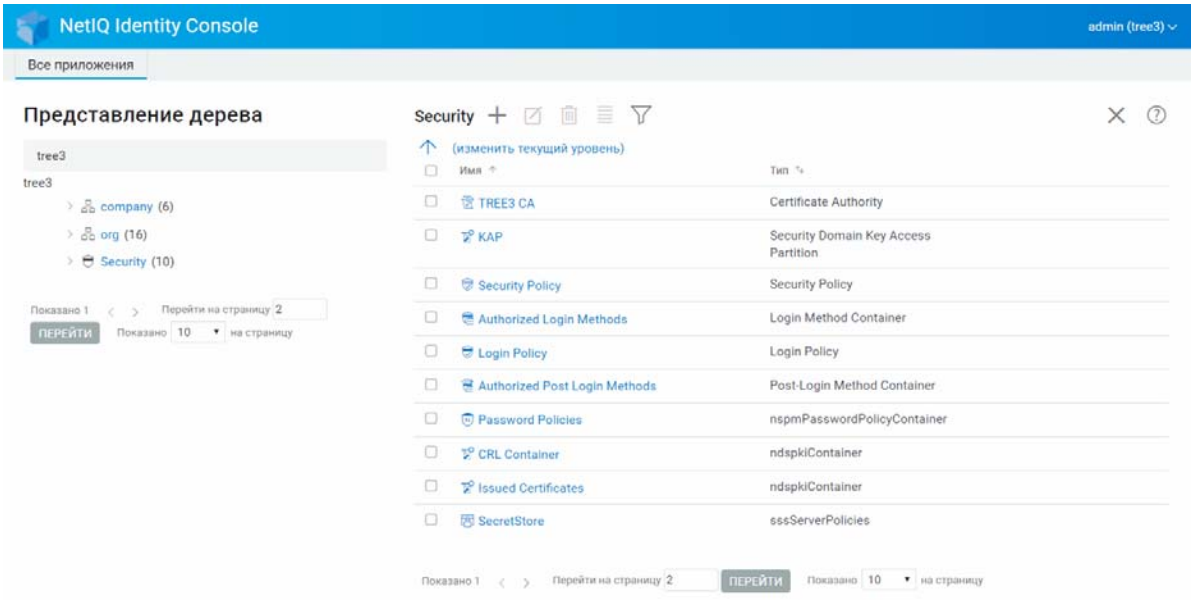
9 Представление дерева

В представлении дерева можно просматривать структуру каталогов, а также создавать, редактировать и изменять различные объекты в этом дереве. В представлении дерева отображается область навигации и область содержимого.

Фрейм навигации в разделе "Дерево"

В представлении дерева область навигации содержит структуру каталогов. В области навигации отображаются контейнеры, включая том (файловая система), объекты и т. п. Все элементы управления под областью навигации можно использовать для более удобного просмотра структуры каталогов. По умолчанию в области навигации отображается до 10 подчиненных объектов в каждом контейнере, но можно изменить эту настройку под панелью навигации в представлении дерева.

Рисунок 9-1 *Окно навигации в представлении дерева*



Область содержимого в разделе "Дерево"

Если выбрать один из объектов-контейнеров в области навигации, в области содержимого будут отображены все объекты в этом контейнере. В области содержимого можно просматривать и изменять объекты каталога. Область содержимого включает заголовок, с помощью которого можно выполнять ряд действий:

Строка заголовка. В строке заголовка области содержимого отображается имя объекта-контейнера, выбранного в текущий момент.

Заголовок списка объектов. Заголовок списка объектов предоставляет доступ к указанным ниже элементам.

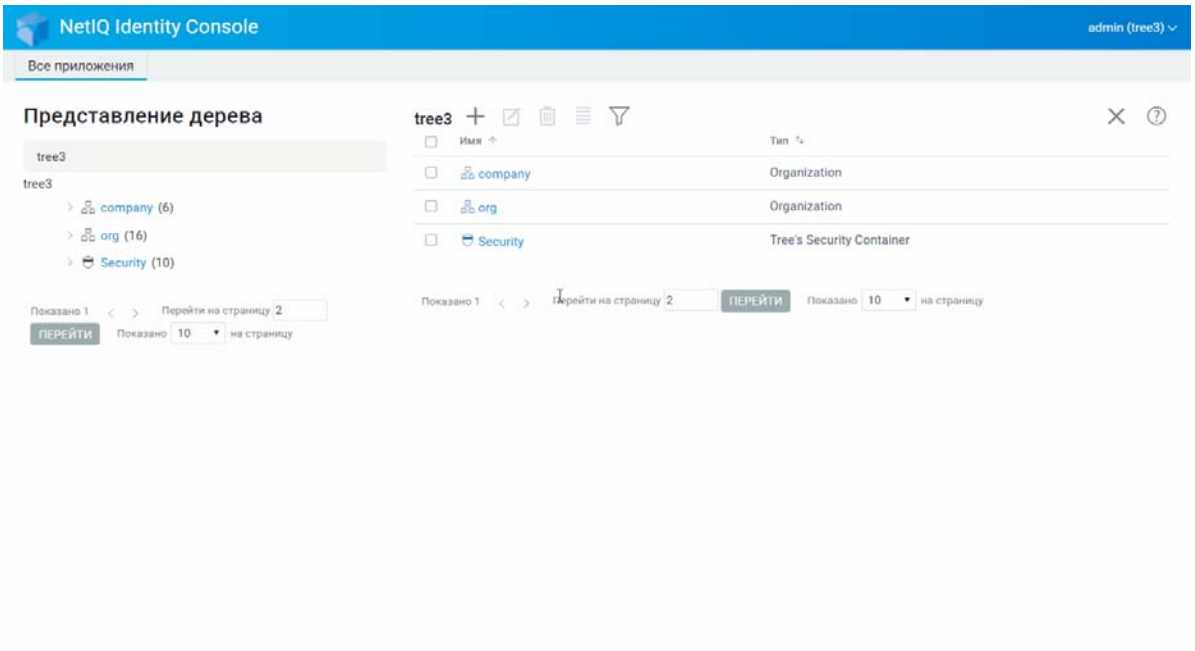
- **Добавить**: щелкните значок  , чтобы добавить новый объект.
- **Изменить**: выберите объект и щелкните значок  , чтобы изменить этот объект. Откроется окно свойств выбранного объекта, где можно будет изменить атрибуты этих свойств. Невозможно изменить одновременно несколько объектов.
- **Удалить**: выберите объект и щелкните значок  , чтобы удалить выбранные объекты. Можно удалить одновременно несколько объектов. Невозможно удалить неконечные объекты.
- **Действия**: выберите объект и щелкните значок  , чтобы открыть раскрывающееся меню поддерживаемых задач для выбранного объекта. Чтобы выполнить задачу, выберите ее в раскрывающемся меню и укажите необходимые данные.
- **Количество объектов**: в представлении дерева в нижней части страницы отображается количество объектов на текущей странице. По умолчанию в области содержимого отображается до 20 подчиненных объектов в каждом контейнере, но можно изменить эту настройку.
- **Выбрать все**: этот флажок в заголовке аналогичен такому же флажку на текущей странице объектов.
- **Сортировать**: поддерживается сортировка в столбцах **Имя** и **Тип**. Если щелкнуть заголовок или значок, порядок сортировки имен объектов по алфавиту изменится на противоположный.
- **Фильтр поиска**: щелкните значок  , чтобы открыть всплывающее окно фильтра. С помощью этого параметра можно создать фильтр, ограничивающий количество объектов, которые отображаются в списке объектов. Можно создавать фильтры по типу и имени объекта.

  Выберите  , чтобы открыть диалоговое окно "Расширенный фильтр", где можно создать фильтр с использованием практически любых атрибутов объектов. Дополнительную информацию см. в разделе "Настройка расширенного поиска" на стр. 26.

Чтобы выполнить какое-либо действие с объектов, установите флажок этого объекта, затем щелкните значок действия  в заголовке списка объектов. Чтобы выполнить действие над текущим контейнером, выберите объект текущего уровня. С помощью этой функции можно выполнять следующие действия:

- "Изменение фильтра наследуемых прав" на стр. 51
- "Изменение прав опекуна" на стр. 52
- "Расширение объекта" на стр. 64
- "Переименование объекта" на стр. 48
- Установить пароль
- "Просмотр действующих прав" на стр. 53

Рисунок 9-2 *Окно содержимого в представлении дерева*



10 Управление схемой

Схема каталогов определяет типы объектов, которые можно создавать в дереве (пользователи, принтеры, группы и т. п.), и информацию, обязательную или необязательную для создания объектов. В Identity Console доступны следующие возможности, связанные со схемой:

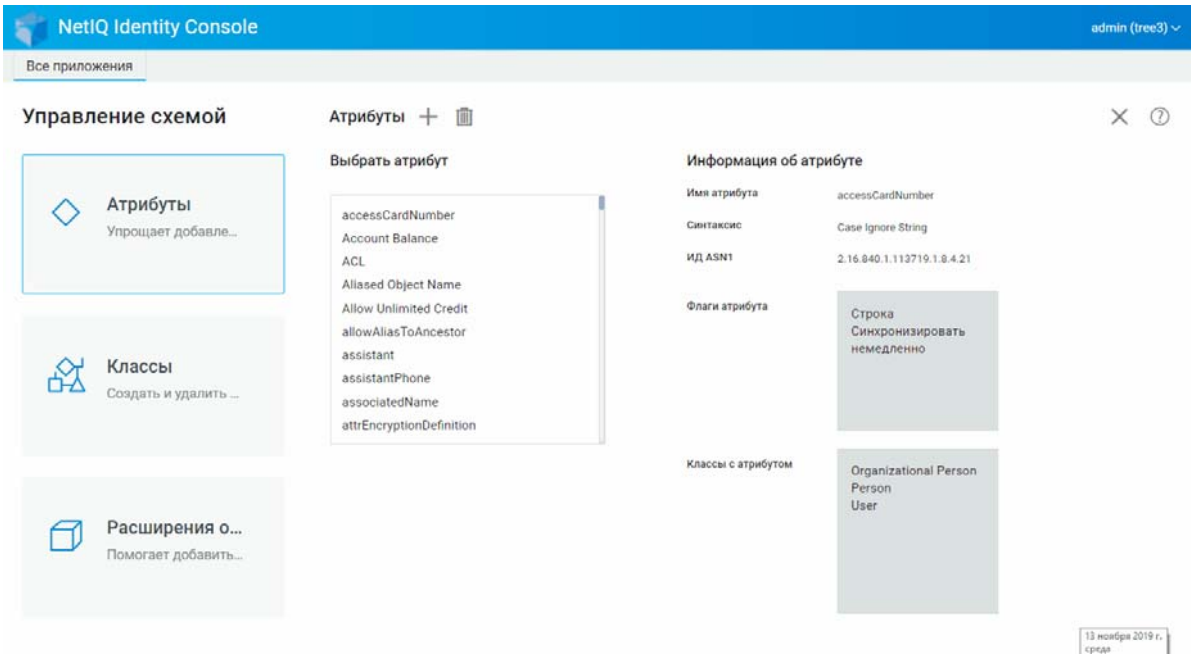
- "Создание атрибута" на стр. 59
- "Создание класса" на стр. 60
- "Назначение атрибутов классу" на стр. 61
- "Просмотр информации об атрибуте" на стр. 62
- "Удаление атрибута" на стр. 62
- "Удаление класса" на стр. 63
- "Расширение объекта" на стр. 64

Создание атрибута

Вы можете определить собственные настраиваемые типы атрибутов и добавить их в качестве дополнительных атрибутов к существующим классам объектов. Однако к существующим классам нельзя добавлять обязательные атрибуты. Чтобы создать атрибут, выполните указанные ниже действия.

1. Щелкните **Управление схемой** на целевой странице Identity Console.
2. Щелкните значок +.
3. На странице "Создать атрибут" введите следующие данные:
   - Имя атрибута
   - ИД ASN1 (необязательно)
   - Синтаксис
   - Флаги атрибута
4. Укажите необходимые данные и щелкните кнопку Создать.
5. Появится сообщение, подтверждающее создание атрибута.

Рисунок 10-1 *Создание атрибута*



Создание класса

С помощью параметра **Управление схемой** можно определять собственные классы. Можно расширять отдельные объекты с помощью свойств, определенных в классах. Создавать классы:

1. Щелкните **Управление схемой** на целевой странице Identity Console и выберите **Классы**.
2. Щелкните значок +.
3. На странице "Создать атрибут" введите следующие данные:
   - Имя класса
   - ИД ASN1 (необязательно)
   - Флаги класса: выберите один из следующих флагов классов:
     - **Действующий класс.** Установите этот флаг, если требуется создать действующий класс, который можно использовать для создания объектов.
     - **Недействующий класс.** Используется как резервное пространство для группы атрибутов. Недействующий класс не может использоваться для создания объектов, но может быть определен как класс, от которого другие классы могут наследовать атрибуты. Например, класс "Персона" является недействующим классом, содержащим атрибуты, наследуемые классом "Пользователь".
     - **Вспомогательный класс.** Набор атрибутов, которые могут быть связаны только с отдельными объектами, но не с целыми классами.
     - **Контейнерный класс.** Установите этот флаг, если требуется сделать класс контейнерным. Когда он используется для создания объектов, эти объекты становятся контейнерами (например объект "Подразделение"). Не устанавливайте этот флаг для конечного класса объектов.

ПРИМЕЧАНИЕ. Если выбрать действующий и недействующий классы, необходимо также указать значения для родительского класса. Если выбран вспомогательный класс, то указывать родительский класс не обязательно.

4 Укажите необходимые данные и щелкните кнопку **Далее**.

5 На следующем экране выберите необязательные и обязательные атрибуты, а также атрибуты именования и щелкните кнопку **ОК**.

6 Появится сообщение, подтверждающее создание класса.

Назначение атрибутов классу

К существующим классам можно добавить дополнительные атрибуты, если необходимо изменить информацию об организации или подготовиться к объединению деревьев. Чтобы добавить атрибут к существующему классу, выполните указанные ниже действия.

ПРИМЕЧАНИЕ. Обязательные атрибуты можно определить только при создании класса. Обязательным атрибутом является атрибут, который должен быть задан при создании объекта.

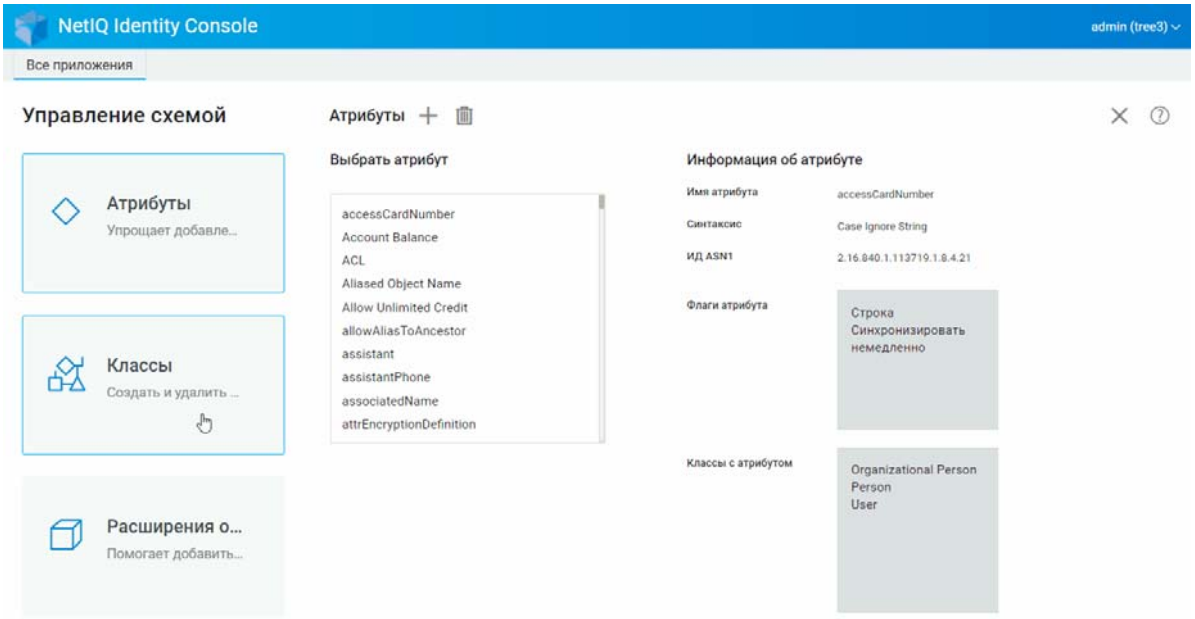
1 Щелкните **Управление схемой** на целевой странице Identity Console и выберите **Классы**.

2 Щелкните любой класс в списке **Выбрать класс**.

3 В правой части экрана появится информация о соответствующем классе.

4 Щелкните кнопку + рядом с параметром **Атрибуты**, выберите атрибуты, которые нужно добавить, затем щелкните кнопку **Добавить** > **Сохранить**.

Рисунок 10-2 *Назначение атрибутов классу*

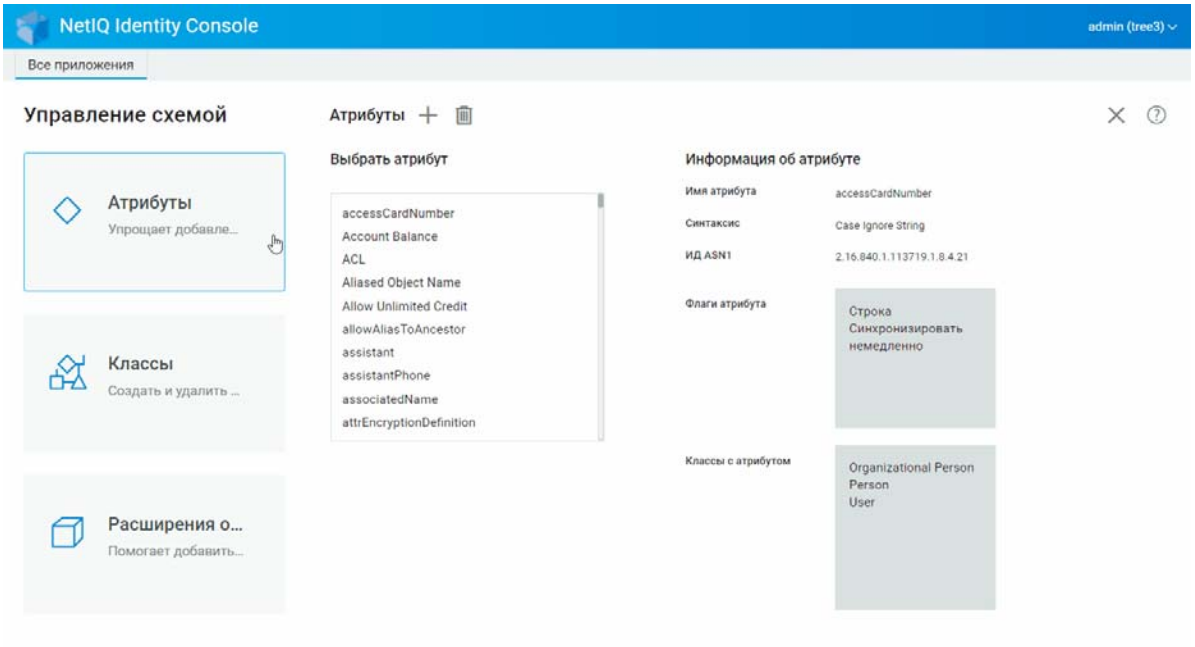


Просмотр информации об атрибуте

В iManager можно просматривать структурные характеристики атрибута, такие как синтаксис, флаги и классы, использующие атрибут. Чтобы просмотреть информацию об атрибуте, выполните указанные ниже действия.

1. Щелкните **Управление схемой** на целевой странице Identity Console и выберите **Атрибуты**.
2. Щелкните любой класс в списке **Выбрать атрибут**.
3. В правой части экрана появится информация о соответствующем атрибуте.

Рисунок 10-3 *Просмотр информации об атрибуте*



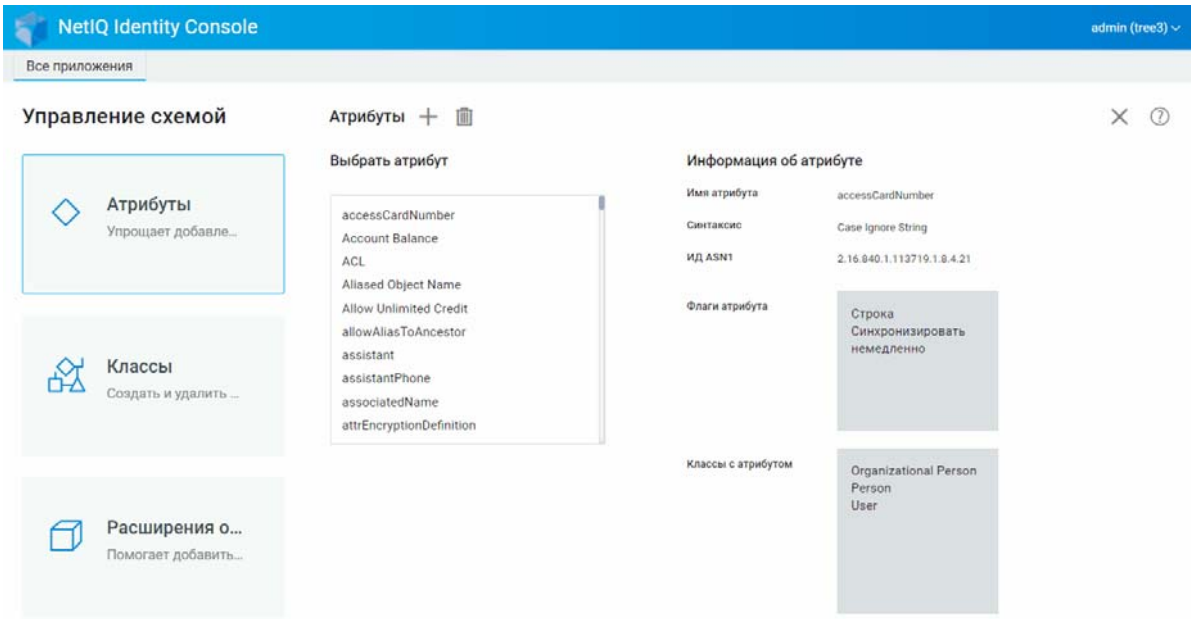
Удаление атрибута

Неиспользуемые атрибуты, которые не являются частью основной схемы дерева eDirectory, можно удалить. Это может оказаться полезным после объединения двух деревьев каталога или после устаревания атрибута. Чтобы удалить атрибут, выполните указанные ниже действия.

1. Щелкните **Управление схемой** на целевой странице Identity Console и выберите **Атрибуты**.
2. Выберите атрибут, который нужно удалить, в списке **Выбрать атрибут**, и щелкните значок .

   ПРИМЕЧАНИЕ. Значок будет включен только при выборе атрибута, который можно удалить.
3. Щелкните кнопку **ОК**, чтобы подтвердить удаление.

Рисунок 10-4 *Удаление атрибута*



Удаление класса

Неиспользуемые классы, которые не являются частью основной схемы дерева eDirectory, можно удалить. Identity Console не позволит удалить классы, которые в настоящее время используются в разделах с локальными репликами. Чтобы удалить класс, выполните указанные ниже действия.

1 Щелкните **Управление схемой** на целевой странице Identity Console и выберите **Классы**.

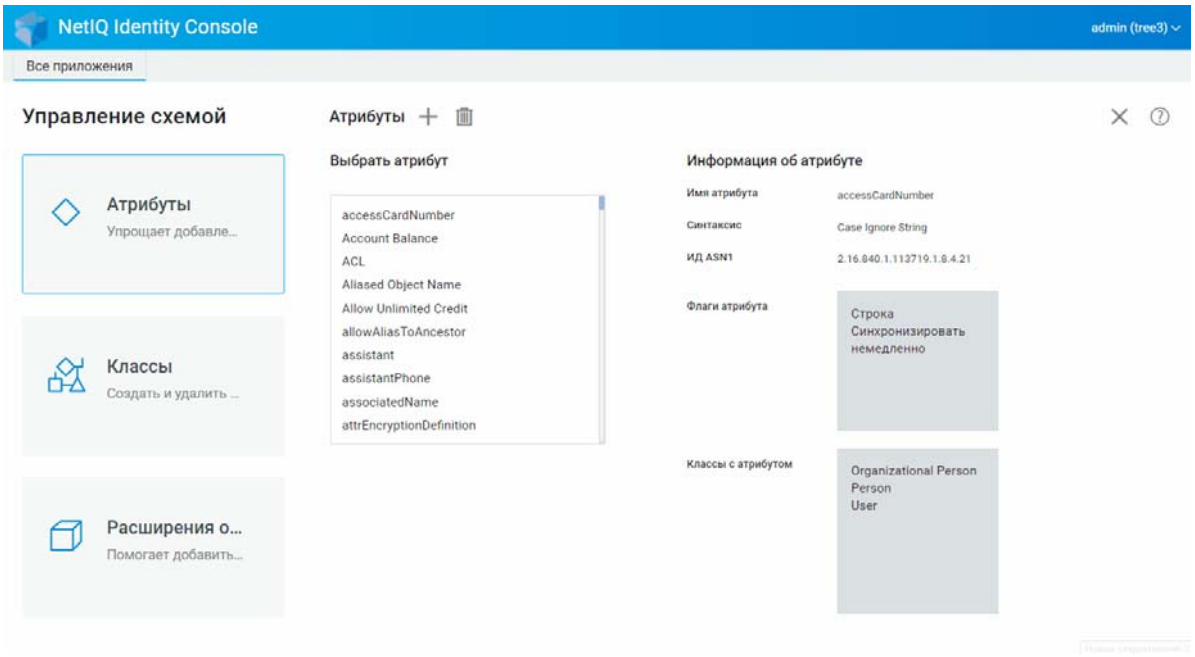
2 Выберите класс, который нужно удалить, в списке **Выбрать класс**, и щелкните значок .

ПРИМЕЧАНИЕ. Значок будет включен только при выборе класса, который можно удалить.

---

3 Щелкните кнопку **ОК**, чтобы подтвердить удаление.

Рисунок 10-5 *Удаление класса*



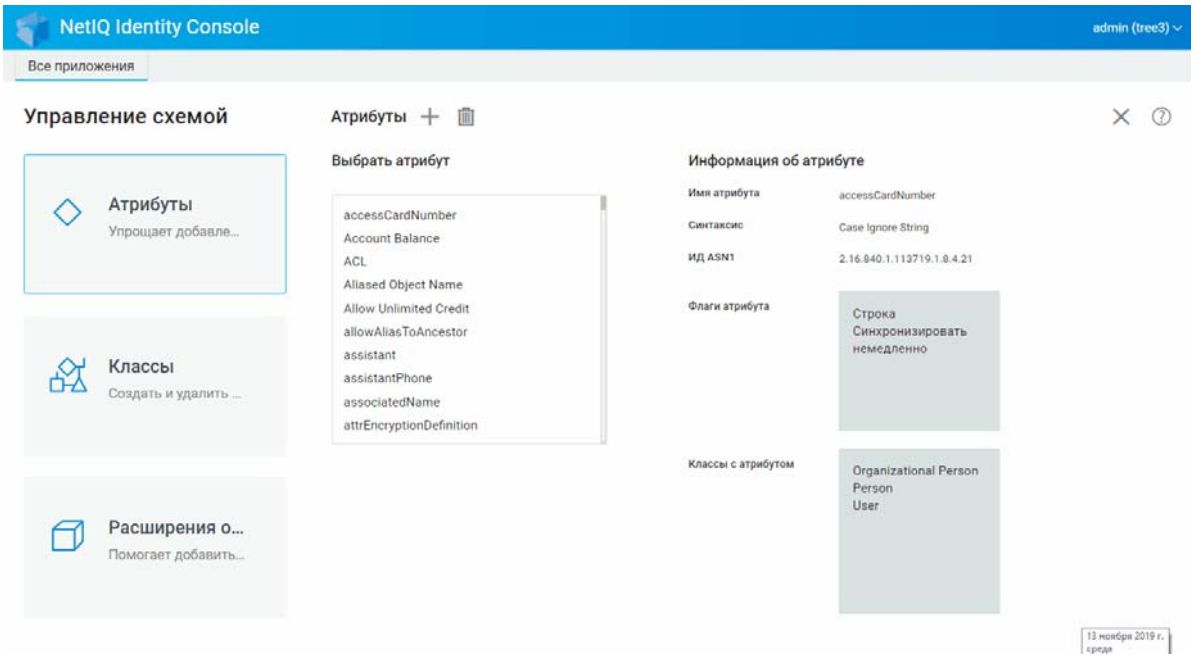
Расширение объекта

Выполните следующие действия, чтобы расширить объект:

1. Щелкните **Управление схемой** на целевой странице Identity Console и выберите **Расширение объекта**.
2. Укажите имя объекта, который нужно расширить, или найдите его с помощью значка выбора объектов, затем щелкните значок .
3. Щелкните значок и выберите вспомогательный класс, затем щелкните кнопку **ОК**.

   ПРИМЕЧАНИЕ. Если любой обязательный атрибут присоединен к выбранному вспомогательному классу, то будет предложено ввести необходимые значения во всплывающем окне **Обязательные атрибуты**.
4. Появится подтверждение добавления вспомогательного класса к объекту.
5. Чтобы удалить существующий вспомогательный класс из объекта, выберите класс и щелкните значок .

Рисунок 10-6 *Расширение объекта*



11 Управление событиями аудита

В этой главе поясняется управление различными событиями аудита с помощью Identity Console. Эта функция позволяет включать и отключать события аудита для сервера NCP.

- "Настройка событий аудита CEF" на стр. 67
- "Типы событий CEF" на стр. 69
- "Настройка фильтрации аудита CEF" на стр. 70

Настройка событий аудита CEF

1. Войдите в Identity Console, указав имя пользователя и пароль.
2. Выберите **Аудит**.
3. Выберите NCP Server, за которым следует наблюдать, и щелкните кнопку **ОК**.

   ПРИМЕЧАНИЕ. После первого включения событий CEF для любого сервера NCP по умолчанию будет выбрано несколько событий.

4. Настройка событий аудита CEF
   - **Конфигурация событий.** Включение или отключение следующих событий в зависимости от требований аудита для вашей среды

ПРИМЕЧАНИЕ. Отдельные категории событий в разделе конфигурации событий по умолчанию будут свернуты. Можно развернуть любую категорию, чтобы выбрать отдельные события.

Параметры	Описание
События безопасности	Выберите события безопасности, которые необходимо записывать в журнал. Можно записывать события для добавления и удаления участников, обнаружения нарушителей, изменения паролей, проверки подлинности пользователей и т. п.
События объекта	Выберите события объекта, которые необходимо записывать в журнал. Можно записывать события для удаления, переименования, перемещения и поиска объектов.
События атрибута	Выберите события атрибута, которые необходимо записывать в журнал. Запись событий в журнал можно использовать для чтения и удаления атрибутов, а также для добавления, удаления и сравнения значений атрибутов.
События LDAP	Выберите события LDAP, которые необходимо записывать в журнал.

- **Дополнительные настройки.** С помощью дополнительных настроек можно выполнять следующие действия.
  - **Глобальный.** Можно выбрать или очистить глобальные настройки для дублирующихся записей.
    - **Не отправлять события репликации.** Выберите этот параметр, чтобы прекратить получать дублированные события из-за репликации с других серверов.
  - **Записывать значения события в журнал.** События записываются в текстовый файл. Значения событий размером более 768 байт считаются крупными. Записывать в журнал можно события любого размера.
    - **Записывать большие значения в журнал.** Выберите этот параметр, чтобы записывать в журнал события, размер которых превышает 768 байт.
    - **Записывать значения атрибутов в журнал.** Выберите этот параметр, чтобы показать значения атрибутов. Этот параметр применим только для событий **Добавить значение** и **Удалить значение**.
    - **Записывать значения зашифрованного атрибута в журнал.** Выберите этот параметр, чтобы показать значения зашифрованных атрибутов. Этот параметр применим только для событий **Добавить значение** и **Удалить значение**.

    ПРИМЕЧАНИЕ. Если размер события превышает 768 байт, значение события усекается и сохраняется в файле журнала.

Типы событий CEF

Можно настроить CEF для записи событий в следующих категориях:

- Безопасность
- Объекты
- Атрибуты
- LDAP

Можно проводить аудит для следующего набора типов событий по умолчанию:

Категория	Тип события
Безопасность	◆ ACL изменен ◆ Добавление участника ◆ Удаление участника ◆ Обнаружен нарушитель ◆ Вход отключен ◆ Вход включен ◆ Регистрация ◆ Изменение эквивалентов по правам ◆ Настройка аудита ◆ Смена пароля ◆ Разблокирование учетной записи ◆ Выход ◆ Соединение ◆ Олицетворение ◆ Аутентификация ◆ Повторный ввод пароля ◆ Изменение конфигурации входа ◆ Запрос учетных данных
Объекты	◆ Создание объекта ◆ Удаление объекта ◆ Переименование объекта ◆ Перемещение объекта ◆ Чтение DSA ◆ Поиск
Атрибуты	◆ Чтение атрибутов ◆ Удаление атрибута ◆ Добавление значения ◆ Удаление значения ◆ Сравнение значения атрибута

Категория	Тип события
LDAP	◆ LDAP-операция подключения ◆ Ответ на LDAP-операцию подключения ◆ LDAP-операция отключения ◆ Подключение к серверу LDAP ◆ LDAP-операция поиска ◆ Ответ на LDAP-операцию поиска ◆ Ответ на LDAP-операцию поиска записи ◆ LDAP-операция добавления ◆ Ответ на LDAP-операцию добавления ◆ LDAP-операция сравнения ◆ Ответ на LDAP-операцию сравнения ◆ LDAP-операция изменения ◆ Ответ на LDAP-операцию изменения ◆ LDAP-операция удаления ◆ Ответ на LDAP-операцию удаления ◆ LDAP-операция модификации различающегося имени ◆ Ответ на LDAP-операцию модификации различающегося имени ◆ Прерывание LDAP ◆ Сообщения от расширенных операций LDAP ◆ Расширенная системная операция LDAP ◆ Ответ на расширенную операцию LDAP ◆ Изменение конфигурации сервера LDAP ◆ Неизвестная операция LDAP ◆ Модификация пароля LDAP

Настройка фильтрации аудита CEF

С помощью фильтров и уведомлений о событиях CEF может информировать о возникновении событий определенного типа или об отсутствии таких событий. Можно фильтровать события по одному или нескольким классам объектов или атрибутов, в зависимости от типа события. CEF сравнивает все сформированные события с фильтрами, настроенными на сервере eDirectory, и записывает в журнал лишь те события, которые соответствуют этим фильтрам.

В этом разделе содержится информация о настройке системных фильтров и уведомлений.

- "Фильтрация событий eDirectory с помощью фильтра исключений" на стр. 71
- "Фильтрация событий объектов CEF" на стр. 71
- "Фильтрация событий атрибута CEF" на стр. 72

Фильтрация событий eDirectory с помощью фильтра исключений

Перейдите по ссылке **Фильтр исключений**, чтобы настроить фильтрацию классов объектов и атрибутов, для которых не нужно формировать события. Можно выбрать классы и атрибуты объектов.

Настройка фильтрации для нежелательных событий eDirectory:

1. В Identity Console выберите **Аудит** на главной странице.
2. Выберите NCP Server, за которым следует наблюдать, и щелкните кнопку **ОК**.
3. Перейдите в раздел **Дополнительные настройки** и щелкните **Фильтр исключений** в разделе **Фильтры**.

   Появится окно "Фильтрация исключений CEF".
4. В списке **Доступные классы объектов** выберите классы объектов, для которых не нужно собирать события, затем щелкните стрелку вправо, чтобы переместить эти классы в список **Выбранные классы объектов**.
5. В списке **Доступные атрибуты** выберите любое количество атрибутов. Выберите атрибут и щелкните стрелку вправо, чтобы добавить этот атрибут в выбранный список атрибутов.
6. Щелкните **ОК**.

Модуль аудита CEF использует настроенный фильтр и прекратит формировать события для всех выбранных классов и атрибутов объектов.

Фильтрация событий объектов CEF

Можно настроить фильтрацию объектов так, чтобы использовать только определенные события. Например, если нужно получать уведомления, когда кто-либо создает учетную запись пользователя в eDirectory, можно создать фильтр, выбрав класс объекта "Пользователь", чтобы записывать события для создания новых объектов этого класса.

Чтобы настроить фильтрацию учетных записей, перейдите со ссылке "События объекта", выберите класс, затем щелкните кнопку **ОК**, чтобы выйти из приложения.

Настройка фильтров для событий управления учетными записями:

1. В Identity Console выберите **Аудит** на главной странице.
2. Выберите NCP Server, за которым следует наблюдать, и щелкните кнопку **ОК**.
3. Перейдите в раздел **Дополнительные настройки** и щелкните **События объекта** в разделе **Фильтры**.

   Появится окно "Фильтрация объектов CEF".
4. В списке **Доступные классы объектов** выберите любой класс объектов, затем щелкните стрелку вправо, чтобы переместить этот класс объектов в список **Выбранные классы объектов**, и щелкните кнопку **ОК**.

Модуль аудита CEF использует настроенный фильтр, проверит все формируемые события для выбранных классов объектов и запишет в журнал эти события.

Фильтрация событий атрибута CEF

Перейдите по ссылке **События атрибута**, чтобы настроить фильтрацию для событий атрибутов. Например, если нужно получать уведомления, когда кто-либо добавляет новое значение атрибута в eDirectory, можно создать фильтр, чтобы записывать события для добавления новых значений.

Настройка фильтрации для событий атрибута:

1. В Identity Console выберите **Аудит** на главной странице.
2. Выберите NCP Server, за которым следует наблюдать, и щелкните кнопку **ОК**.
3. Перейдите в раздел **Дополнительные настройки** и щелкните **События атрибута** в разделе **Фильтры**.

   Появится окно **Фильтрация конфигурации атрибутов**.
4. В списке **Доступные классы объектов** выберите классы объектов, для которых нужно собирать события, затем щелкните стрелку вправо, чтобы переместить эти классы в список **Выбранные классы объектов**.
5. В списке **Доступные атрибуты** выберите любое количество атрибутов для выбранных классов объектов. Выберите атрибут и щелкните стрелку вправо, чтобы добавить этот атрибут в выбранный список атрибутов.

   ПРИМЕЧАНИЕ. Если выбрать класс объектов, то будут выбраны все события атрибута для всех атрибутов этого класса объектов. В этом случае вы получите события для всех атрибутов выбранных классов объектов.

   ---
6. Щелкните **ОК**.

Модуль аудита CEF использует настроенный фильтр, проверит все формируемые события для выбранных классов объектов и атрибутов и запишет в журнал эти события.

12 Управление зашифрованными атрибутами

Identity Console может безопасно прочитывать зашифрованные атрибуты с сервера eDirectory. С помощью Identity Console можно создавать, изменять и удалять политики для таких зашифрованных атрибутов.

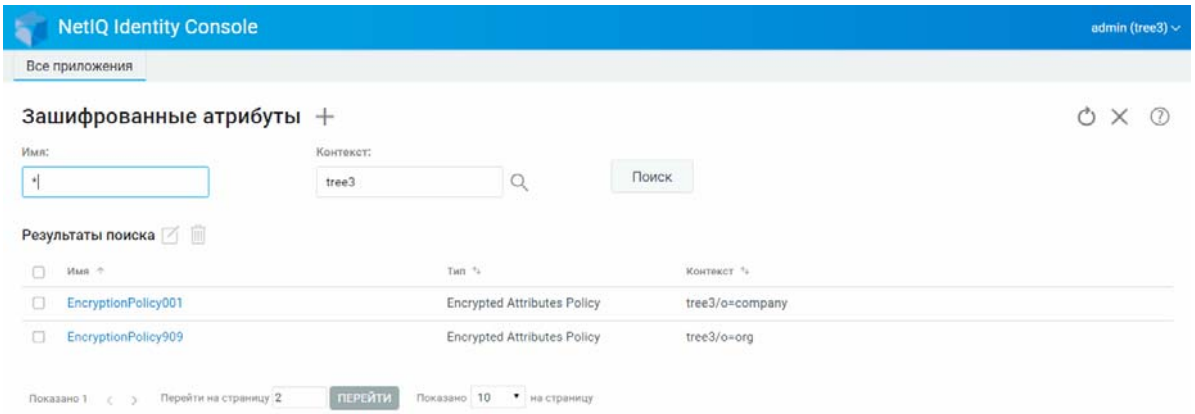
- "Создание политики для зашифрованных атрибутов" на стр. 73
- "Удаление политики для зашифрованных атрибутов" на стр. 74
- "Изменение политики зашифрованных атрибутов" на стр. 75

Создание политики для зашифрованных атрибутов

Создание новой политики атрибутов:

1. Щелкните **Зашифрованные атрибуты** на целевой странице Identity Console.
2. Щелкните значок +.
3. На странице "Создать политику для зашифрованных атрибутов" введите следующие данные:
   - Укажите имя политики
   - Введите или выберите контекст
   - Выберите NCP Server
   - Выберите атрибуты
4. Укажите необходимые данные и щелкните кнопку **Готово**.
5. Появится сообщение, подтверждающее создание политики.

Рисунок 12-1 *Создание политики зашифрованных атрибутов*

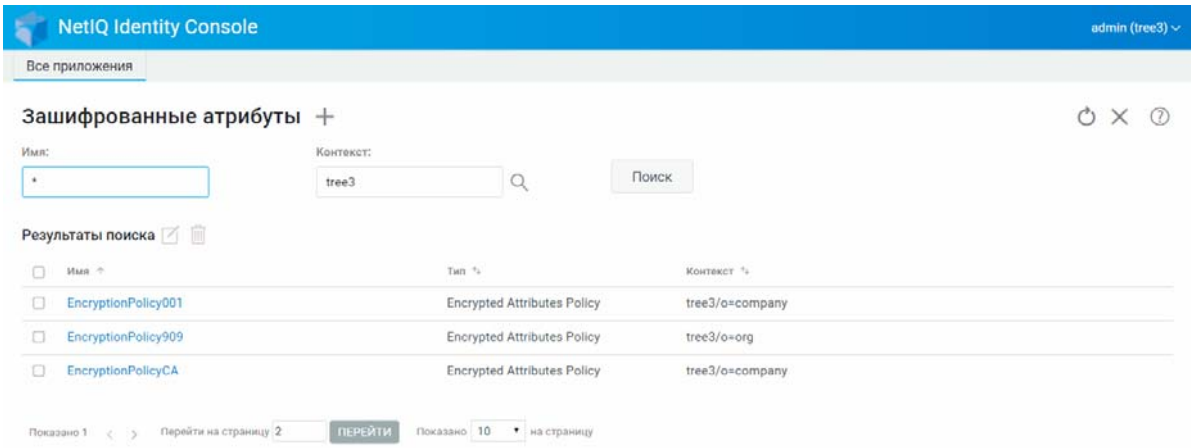


Удаление политики для зашифрованных атрибутов

Удаление политики для зашифрованных атрибутов:

1. Щелкните **Зашифрованные атрибуты** на целевой странице Identity Console.
2. Укажите имя и контекст атрибута или найдите его с помощью функции поиска, затем щелкните кнопку Поиск.
3. Выберите атрибуты в списке и щелкните значок 🗑.
4. Появится сообщение, подтверждающее удаление политики.

Рисунок 12-2 *Удаление политики зашифрованных атрибутов*

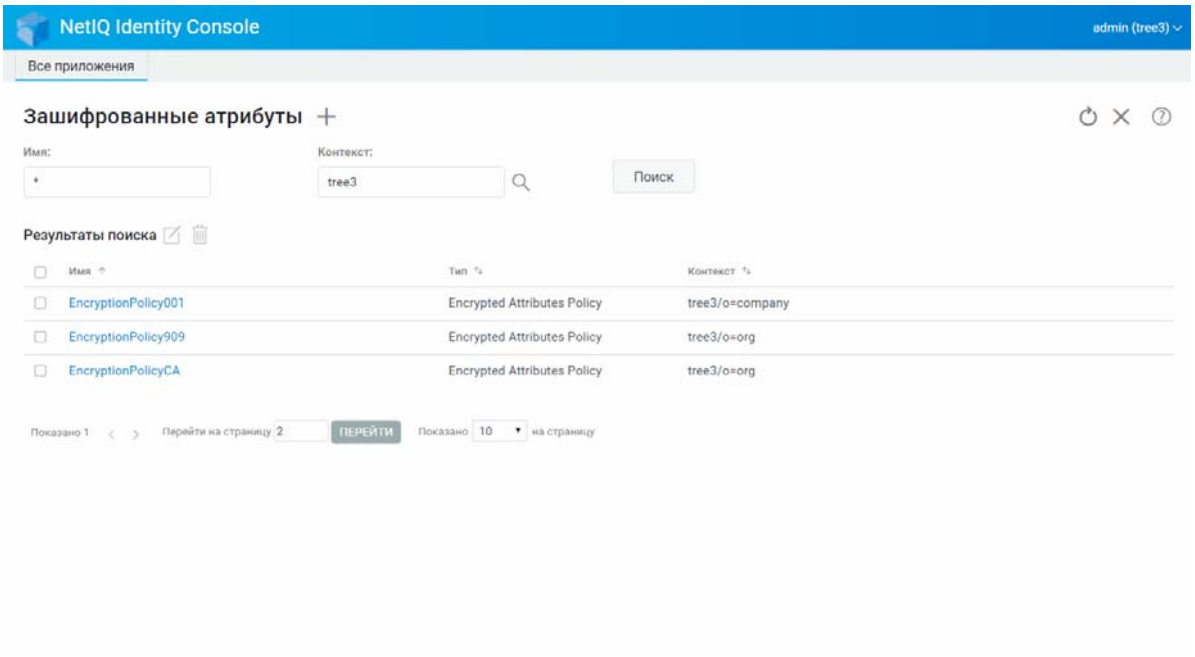


Изменение политики зашифрованных атрибутов

Изменение политики зашифрованных атрибутов:

1. Щелкните **Зашифрованные атрибуты** на целевой странице Identity Console.
2. Введите имя и контекст объекта, затем щелкните кнопку Поиск.
3. Выберите атрибут в списке объектов и щелкните значок .
4. Внесите изменения, затем щелкните кнопку Сохранить.
5. Появится сообщение, подтверждающее изменение политики.

Рисунок 12-3 *Изменение политики зашифрованных атрибутов*



13 Управление репликацией с шифрованием

Чтобы включить репликацию с шифрованием, нужно настроить раздел для репликации с шифрованием. Настройки конфигурации сохраняются в корневом объекте раздела. Включить репликацию с шифрованием можно только на уровне разделов. При включении репликации с шифрованием на уровне раздела шифрование будет применено к репликации между всеми репликами, в которых размещен этот раздел. Например, предположим, что у раздела P1 есть реплики R1, R2, R3 и R4. Можно зашифровать репликацию между всеми репликами.

- "Включение репликации с шифрованием для разделов" на стр. 77

Включение репликации с шифрованием для разделов

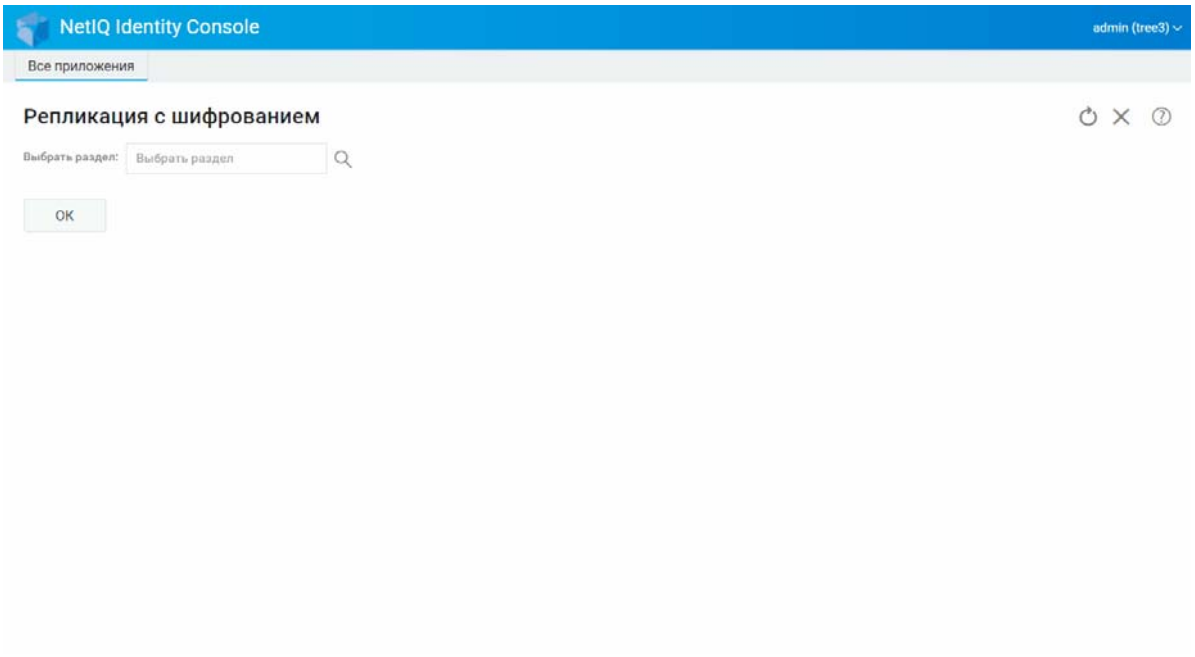
Включение репликации с шифрованием для разделов:

ПРИМЕЧАНИЕ. Чтобы включить раздел для репликации с шифрованием, на всех серверах, на которых размещен этот раздел, требуется eDirectory 9.2 или более поздней версии.

---

1. Щелкните **Репликация с шифрованием** на целевой странице Identity Console.
2. Укажите или выберите раздел, для которого нужно включить репликацию с шифрованием.
3. Установите флажок **Включить репликацию с шифрованием**. Снимите этот флажок, чтобы отключить репликацию с шифрованием для раздела.
4. Щелкните кнопку **Готово**.
5. Появится сообщение, подтверждающее включение репликации с шифрованием.

Рисунок 13-1 *Включение репликации с шифрованием для разделов*



14 Управление разделами и репликами

Операции с разделами и репликами позволяют управлять физической структурой eDirectory и распространением eDirectory на серверах каталогов.

Разделы определяют логическое деление дерева eDirectory. Например, если выбран объект "Подразделение" и необходимо создать на его основе новый раздел, нужно отделить этот объект и все подчиненные ему объекты от его родительского раздела. Выбранный объект "Подразделение" становится корнем нового раздела. Реплики нового раздела находятся на тех же серверах, что и реплики родительского раздела, а объекты нового раздела принадлежат корневому объекту нового раздела.

Модуль "Раздел" позволяет выполнить следующие задачи:

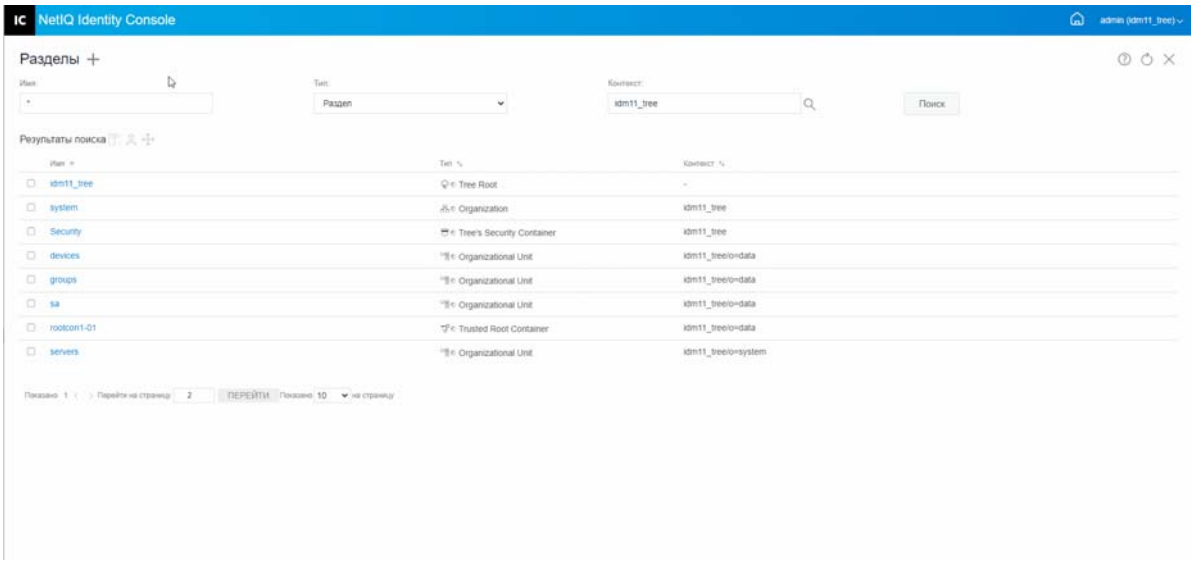
- "Создание раздела" на стр. 79
- "Слияние разделов" на стр. 80
- "Изменение разделов" на стр. 81
- "Перемещение раздела" на стр. 81

Создание раздела

Порядок создания нового раздела

1. На целевой странице Identity Console щелкните параметр **Управление разделом**.
2. Щелкните значок +.
3. На странице создания раздела укажите контейнер, который будет использоваться в качестве корня нового раздела, или найдите нужный контейнер с помощью инструмента выбора объектов и щелкните **Создать**.
4. Появится сообщение, подтверждающее создание раздела.

Рисунок 14-1 *Создание нового раздела*

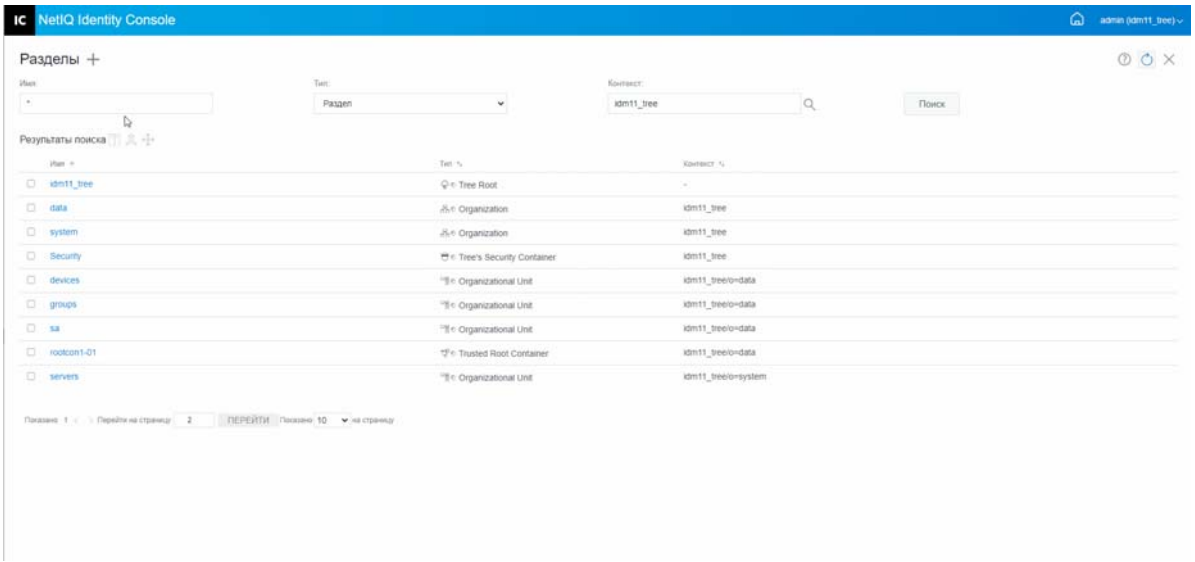


Слияние разделов

Порядок слияния радела с его родительским разделом

1. На целевой странице Identity Console щелкните параметр **Управление разделом**.
2. Укажите имя, тип и контекст раздела или найдите его с помощью функции поиска, затем щелкните кнопку Поиск.
3. Выберите раздел в списке поиска и щелкните значок , затем щелкните **ОК**.
4. Появится сообщение, подтверждающее слияние раздела.

Рисунок 14-2 *Слияние разделов*



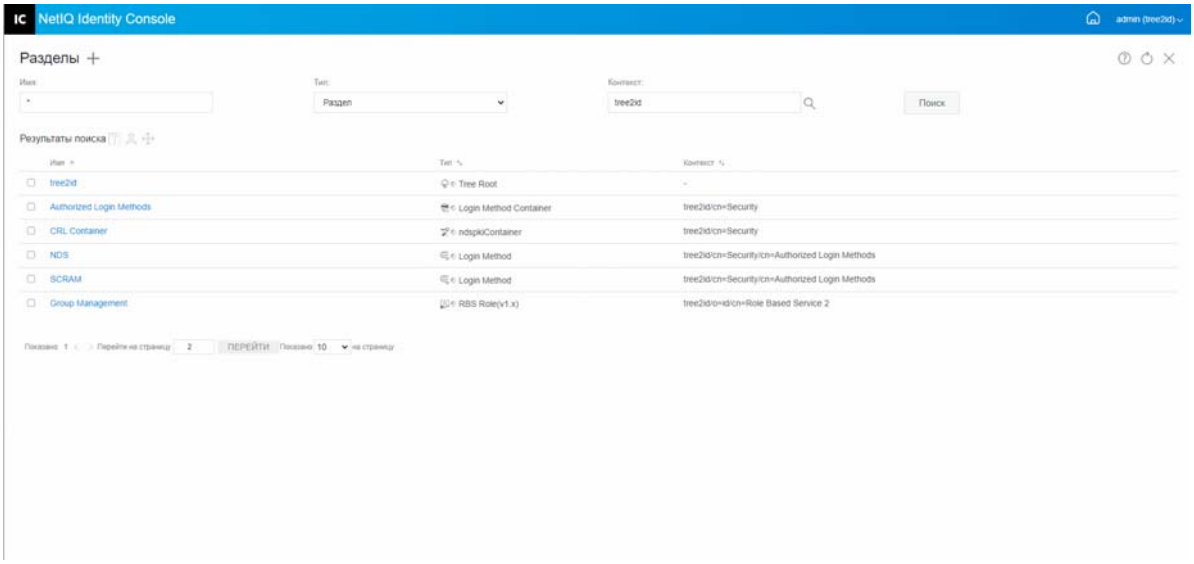
Изменение разделов

Порядок изменения разделов

1. На целевой странице Identity Console щелкните параметр **Управление разделом**.
2. Введите имя, тип и контекст раздела, затем щелкните кнопку Поиск.
3. Выберите раздел в списке поиска и щелкните значок .
4. Щелкните параметр **Изменить** в области **Фильтр** для изменения фильтров реплики и соответствующих ей классов и атрибутов, затем щелкните **ОК**.

   Если для поля **Тип** выбрано значение **Сервер**, отобразится список всех серверов. При щелчке конкретного сервера отображается список всех его разделов.
5. Появится сообщение, подтверждающее изменение раздела.

Рисунок 14-3 *Изменение разделов*



Перемещение раздела

Задача перемещения раздела позволяет переносить поддерево в дереве каталога. Эту задачу еще называют операцией удаления и пересадки. Перемещать можно только те разделы, которые не имеют подчиненных разделов. Если подчиненные разделы есть, перед перемещением раздела их необходимо объединить.

При перемещении раздела eDirectory изменяет все ссылки на корневой объект раздела. Хотя общее имя объекта остается неизменным, полное имя контейнера (и всех содержащихся в нем подчиненных объектов) изменяется.

ПРИМЕЧАНИЕ. При перемещении раздела необходимо соблюдать правила контейнирования eDirectory. Например, переместить объект "Подразделение" непосредственно в корень текущего дерева нельзя, поскольку правила контейнирования корня допускают перемещение туда только объектов "Местонахождение", "Страна" или "Организация", но не "Подразделение".

Порядок перемещения раздела

1 На целевой странице Identity Console щелкните параметр **Управление разделом**.

2 Введите имя, тип и контекст раздела, затем щелкните кнопку Поиск.

3 Выберите раздел в списке поиска и щелкните значок ✣.

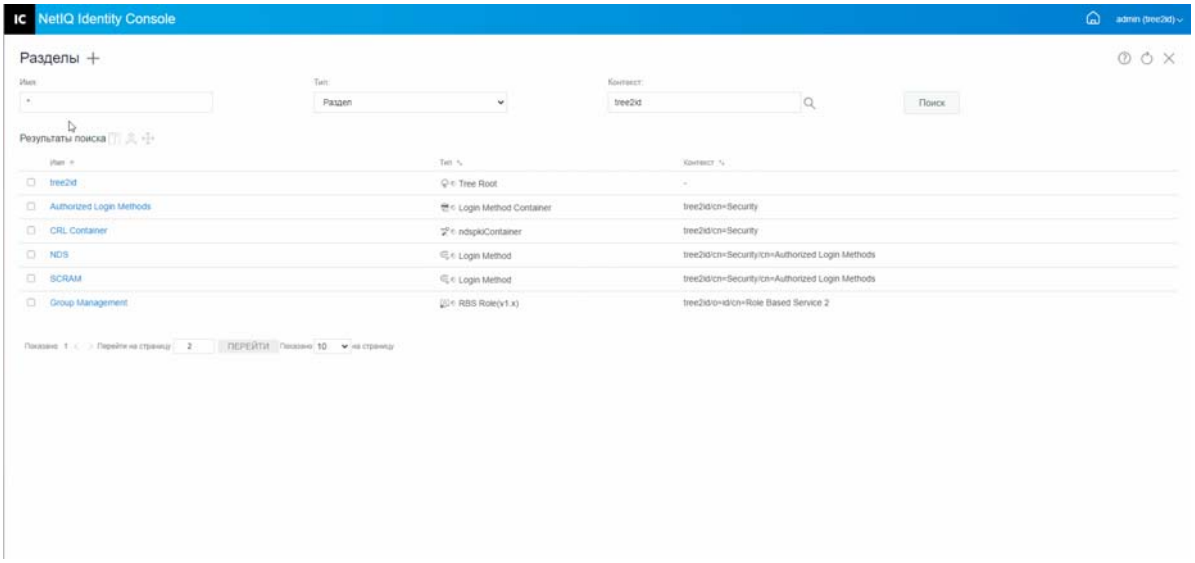
4 Выберите объект — контейнер назначения, в который необходимо переместить указанный раздел, и щелкните **ОК**.

ПРИМЕЧАНИЕ. Если задать параметр **Создать псевдоним на месте перемещенного раздела**, будет создан указатель на новое расположение раздела. Это позволит выполнять все операции, зависящие от старого расположения, до тех пор, пока операции не будут обновлены в соответствии с новым расположением. Благодаря этому пользователи смогут по-прежнему регистрироваться в сети и находить объекты в старом расположении каталога.

---

5 Появится сообщение, подтверждающее операцию перемещения раздела.

Рисунок 14-4 *Перемещение раздела*



15 Управление индексами

Менеджер индексов является атрибутом объекта "Сервер", который позволяет осуществлять управление индексами базы данных. Эти индексы позволяют eDirectory существенно повысить производительность запросов.

К NetIQ eDirectory прилагается набор индексов, которые обеспечивают базовую функциональность запросов. Эти индексы по умолчанию предназначены для указанных ниже атрибутов.

Модуль индексов позволяет выполнить следующие задачи:

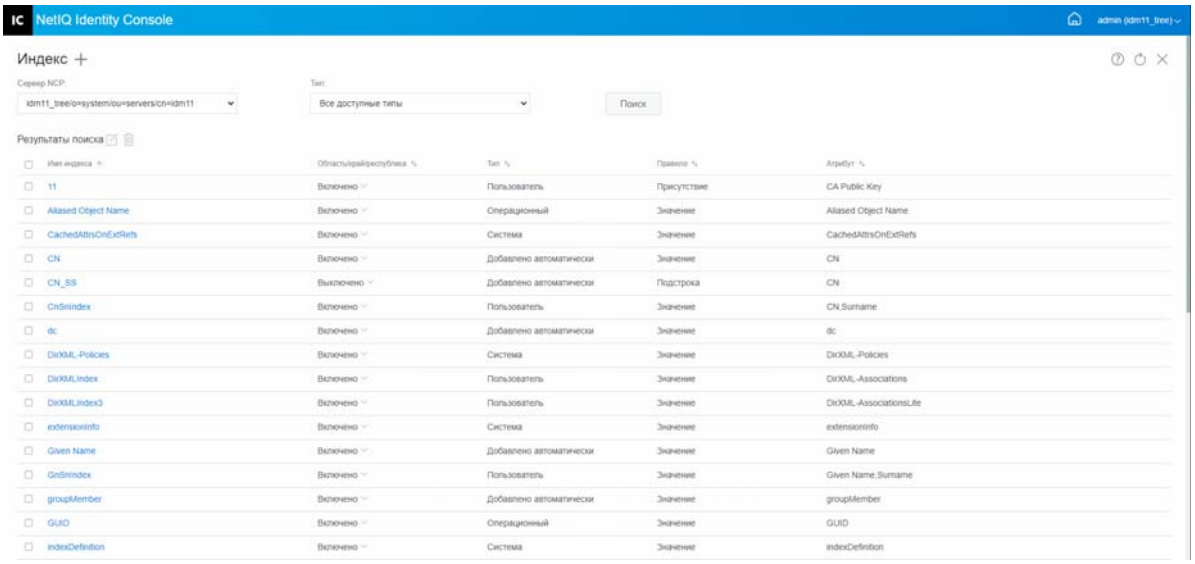
- "Создание индекса" на стр. 83
- "Удаление индекса" на стр. 84
- "Копирование индекса" на стр. 85
- "Изменение состояния индекса" на стр. 85

Создание индекса

Порядок создания нового индекса

1. На целевой странице Identity Console щелкните параметр **Управление индексами**.
2. Щелкните значок +.
3. Введите имя индекса.
4. Выберите серверы из списка доступных серверов NCP.
5. Выберите требуемые атрибуты.
6. Выберите правило индекса:
   - 6a **Подстрока.** Это правило соответствует подмножеству строки значения атрибута. Например, запрос на поиск "LastName" (Фамилия) с подстрокой "ани" вернет записи со значениями "Данилова", "Анисимов" и "Иоселиани". Для создания и обработки индекса подстроки требуется больше всего ресурсов.
   - 6b **Присутствие.** При использовании этого правила требуется только наличие атрибута, а не конкретных значений для него. Например, поиск всех записей с атрибутом "Login Script" (Сценарий входа в систему) можно выполнить с помощью индекса присутствия.
   - 6c **Значение.** При использовании этого правила сопоставляется все значение или первая часть значения атрибута. Например, правило "Значение" можно использовать для поиска элементов, у которых значение атрибута "LastName" (Фамилия) равно "Иванов", а также записей, у которых значение атрибута "LastName" начинается на "Иван".
7. Щелкните кнопку Создать.
8. Появится сообщение, подтверждающее создание индекса.

Рисунок 15-1 *Создание нового индекса*

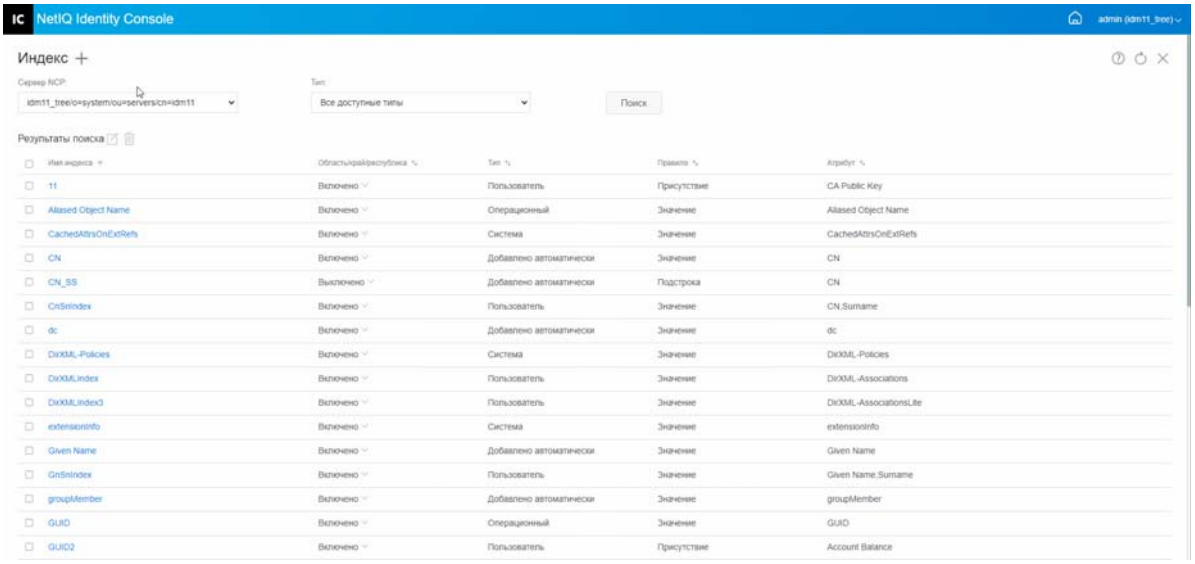


Удаление индекса

Порядок удаления индекса

1. На целевой странице Identity Console щелкните параметр **Управление индексами**.
2. Выберите сервер NCP и введите индекс, затем щелкните кнопку Поиск.
3. Выберите индекс в списке поиска и щелкните значок 🗑.
4. Появится сообщение, подтверждающее удаление индекса.

Рисунок 15-2 *Удаление индекса*



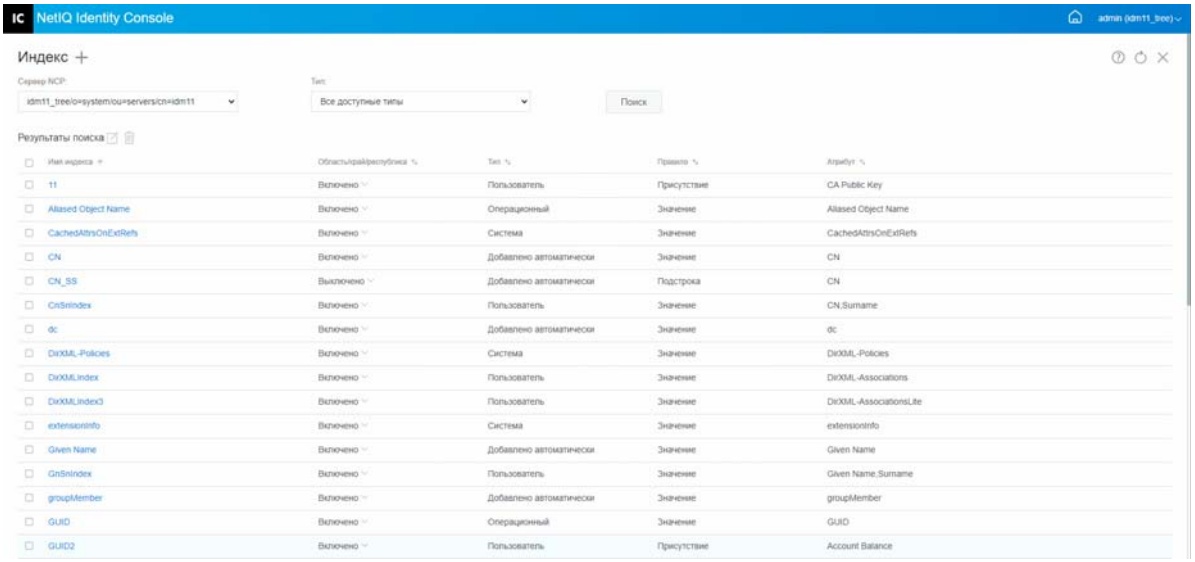
Копирование индекса

Если вы считаете, что тот или иной индекс нужен на данном сервере и может понадобиться на другом сервере, можно скопировать определение индекса с одного сервера на другой. При анализе данных предиката вы также можете обнаружить противоположное: индекс, который удовлетворяет потребность для нескольких серверов, больше не нужен на одном из них. В этом случае можно удалить индекс с того сервера, на котором он не нужен.

Порядок копирования индекса

1. На целевой странице Identity Console щелкните параметр **Управление индексами**.
2. Выберите сервер NCP и введите индекс, затем щелкните кнопку Поиск.
3. Выберите индекс в списке поиска и щелкните значок .
4. Выберите серверы NCP, на которые необходимо скопировать индекс, и щелкните кнопку Сохранить.
5. Появится сообщение, подтверждающее изменение индекса.

Рисунок 15-3 *Копирование индекса*



Изменение состояния индекса

Во время пиковых нагрузок, возможно, вам понадобится временно отключить индексы для оптимизации производительности. Например, для повышения скорости групповой загрузки можно приостановить все индексы, определенные пользователем. Если все индексы активны,

это может привести к замедлению групповой загрузки данных из-за того, что для каждого добавления или изменения объекта необходимо обновлять заданные индексы. По окончании групповой передачи индексы снова можно включить.

Порядок выключения индекса

1 На целевой странице Identity Console щелкните параметр **Управление индексами**.

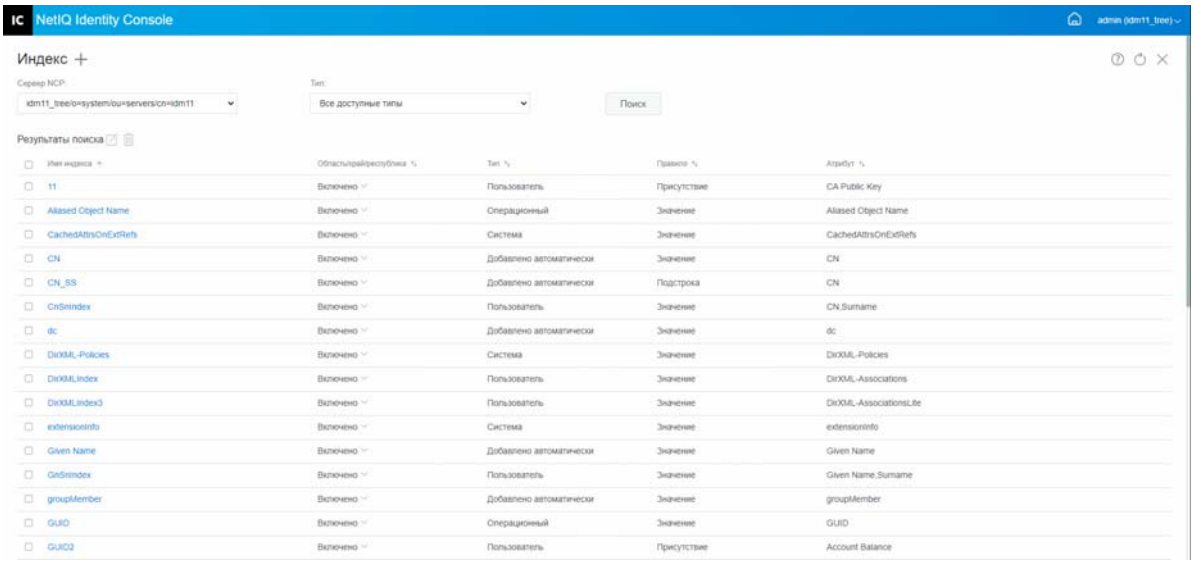
2 Выберите сервер NCP и введите индекс, затем щелкните кнопку Поиск.

3 В списке индексов щелкните раскрывающийся список **Состояние**. Индекс может иметь следующие состояния:

- **Включено:** в настоящий момент выполняется.
- **Выключено:** приостановлен. Индекс можно запустить заново.

ПРИМЕЧАНИЕ. Невозможно изменить состояние индекса типа "Системный" или "Операционный". Кроме того, такие индексы невозможно удалить.

Рисунок 15-4 *Выключение индекса*



16 Настройка объектов LDAP

При установке eDirectory создается объект LDAP "Сервер" и объект LDAP "Группа". Конфигурация служб LDAP по умолчанию расположена в каталоге в этих двух объектах. Конфигурацию по умолчанию можно изменить, используя задачу управления LDAP в Identity Console.

Объект LDAP "Сервер" представляет данные конфигурации, относящиеся к серверу. cОднако объект LDAP "Группа" содержит информацию о конфигурации, которой можно удобно поделиться с разными серверами LDAP. Этот объект предоставляет общие данные конфигурации и представляет группу серверов LDAP. Серверы имеют общие данные.

С одним объектом LDAP "Группа" можно связать несколько объектов LDAP "Сервер". Все связанные серверы LDAP получают специфичную для них конфигурацию из соответствующего им объекта LDAP "Сервер", а общую информацию — из объекта LDAP "Группа".

Модуль LDAP позволяет выполнить следующие задачи:

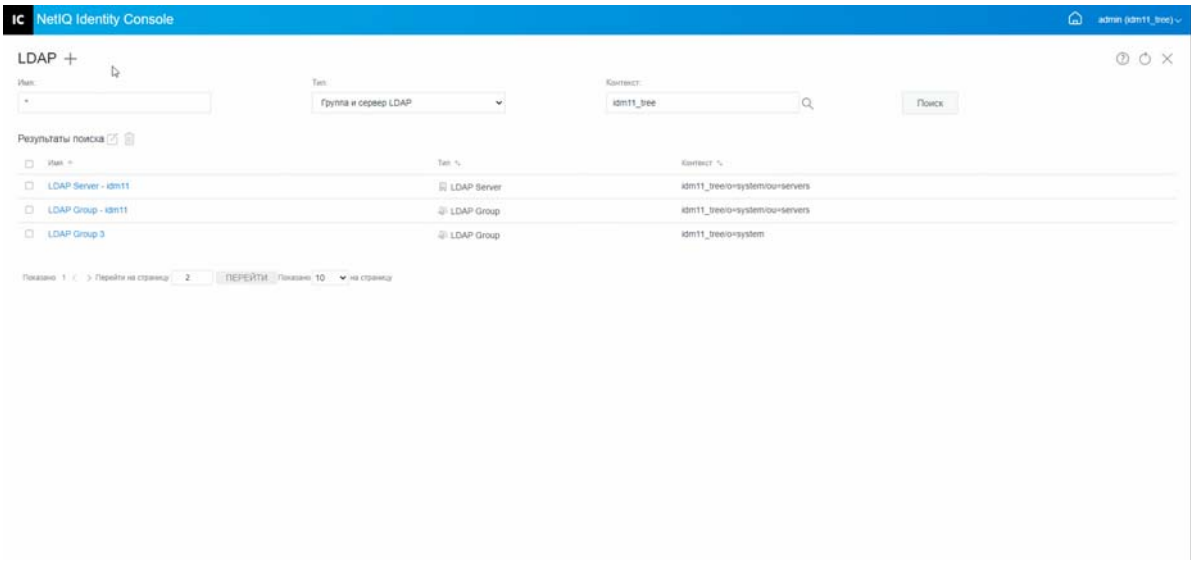
- "Создание объектов LDAP" на стр. 87
- "Удаление объектов LDAP" на стр. 88
- "Изменение объектов LDAP" на стр. 89

Создание объектов LDAP

Порядок создания объекта LDAP

1. На целевой странице Identity Console щелкните **Конфигурация LDAP**.
2. Щелкните значок +.
3. На странице "Создать объект LDAP" укажите имя, тип и контекст или используйте значок "Контекст поиска" для его поиска, затем щелкните **Создать**.
4. Появится сообщение, подтверждающее создание объекта LDAP.

Рисунок 16-1 *Создание нового объекта LDAP*

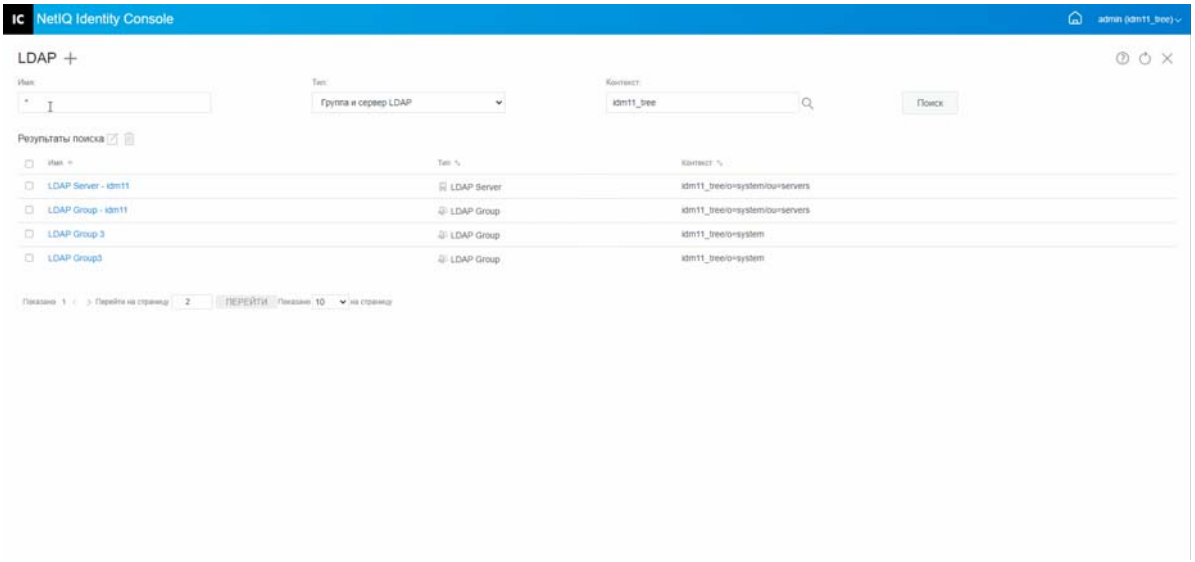


Удаление объектов LDAP

Порядок удаления объектов LDAP

1. На целевой странице Identity Console щелкните **Конфигурация LDAP**.
2. Укажите имя, тип и контекст объекта LDAP, затем щелкните кнопку Поиск.
3. Выберите объекты LDAP в списке поиска и щелкните значок 🗑.
4. Появится сообщение, подтверждающее удаление объектов LDAP.

Рисунок 16-2 *Удаление объектов LDAP*

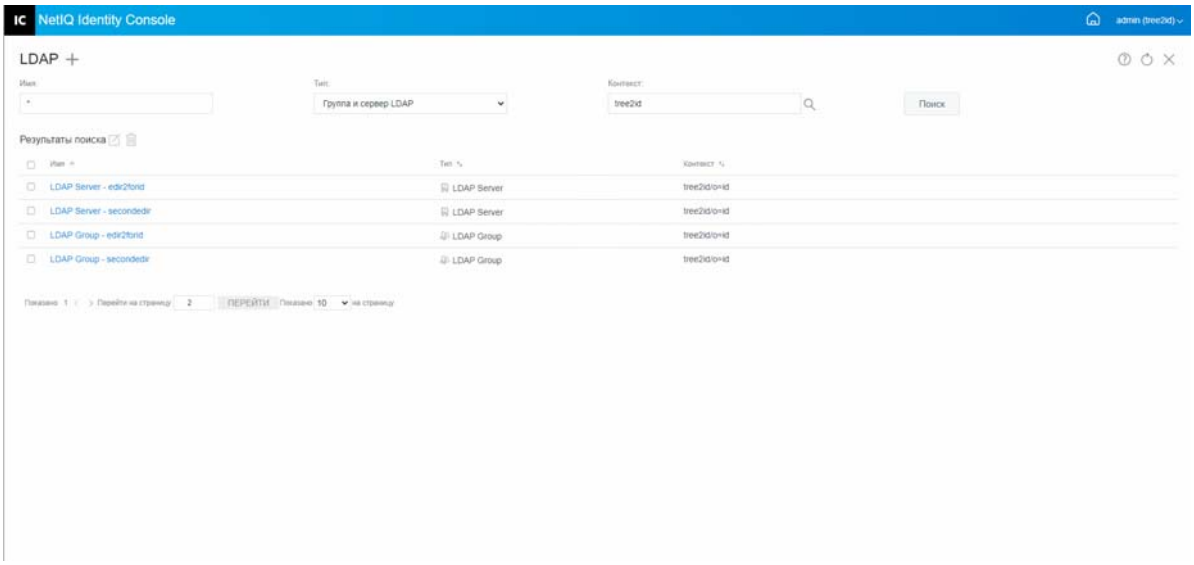


Изменение объектов LDAP

Порядок изменения объектов LDAP

1. На целевой странице Identity Console щелкните **Конфигурация LDAP**.
2. Введите имя, тип и контекст объекта LDAP, затем щелкните кнопку Поиск.
3. Выберите объект LDAP в списке поиска и щелкните значок .
4. Измените атрибуты и информацию для определенного объекта LDAP и щелкните кнопку Сохранить. Дополнительную информацию об атрибутах для объектов LDAP см. в разделе Configuring LDAP Server and LDAP Group Objects on Linux (Настройка объектов LDAP "Сервер" и "Группа" в Linux) документа *NetIQ eDirectory Administration Guide* (Руководство по администрированию NetIQ eDirectory).
5. Появится сообщение, подтверждающее изменение объекта LDAP.

Рисунок 16-3 *Изменение объектов LDAP*



17 Управление сертификатами

NetIQ Certificate Server автоматически устанавливается при установке eDirectory. Сервер сертификатов предоставляет сервисы шифрования открытым ключом, которые изначально встроены в eDirectory и позволяют создавать, издавать сертификаты пользователей и сервера и управлять ими. Этот сервис позволяет защитить конфиденциальную информацию, передаваемую по общественным каналам связи, например, по Интернету.

ПРИМЕЧАНИЕ. Если нужно использовать модуль "Управление сертификатами" с Identity Console, необходимо обновить сервер eDirectory до версии 9.2.4 HF2.

Identity Console позволяет выполнить следующие задачи управления сертификатами:

- "Управление сертифицирующей организацией (CA)" на стр. 91
- "Управление сертификатами сервера" на стр. 95
- "Управление сертификатами пользователя" на стр. 97
- "Управление доверенным корнем и контейнерами" на стр. 99
- "Создание объектов "Сертификат сервера по умолчанию"" на стр. 101
- "Выпуск сертификата открытого ключа" на стр. 102
- "Управление объектом "SAS Service"" на стр. 105

Управление сертифицирующей организацией (CA)

По умолчанию в ходе установки NetIQ Certificate Server для вас создается корпоративная сертифицирующая организация (CA). Вам будет предложено указать ее имя. После щелчка кнопки "Готово" корпоративная сертифицирующая организация (CA) будет создана (с использованием параметров по умолчанию) и помещена в контейнер безопасности. Чтобы получить более широкий контроль при создании корпоративной сертифицирующей организации (CA), можно создать ее вручную на портале Identity Console. Кроме того, если корпоративная сертифицирующая организация (CA) удалена, ее необходимо будет создать заново.

Модуль "Сертифицирующая организация (CA)" позволяет выполнить следующие задачи:

- "Создание объекта "Корпоративная сертифицирующая организация (CA)"" на стр. 92
- "Резервное копирование сертификатов корпоративной сертифицирующей организации (CA)" на стр. 92
- "Восстановление корпоративной сертифицирующей организации (CA)" на стр. 93
- "Проверка сертификатов сертифицирующей организации (CA)" на стр. 94
- "Замена сертификатов корпоративной сертифицирующей организации (CA)" на стр. 94
- "Отзыв сертификатов корпоративной сертифицирующей организации (CA)" на стр. 94

Создание объекта "Корпоративная сертифицирующая организация (CA)"

Порядок создания объекта "Корпоративная сертифицирующая организация (CA)"

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление серт. орг.**.
2. При отсутствии объекта "Корпоративная сертифицирующая организация (CA)" откроется соответствующее диалоговое окно и мастер создания объекта "Корпоративная сертифицирующая организация (CA)". Следуйте инструкциям мастера по созданию объекта.

   ПРИМЕЧАНИЕ. Убедитесь, что указанный здесь путь к файлу списка аннулированных сертификатов соотносится с путем установки eDirectory.

   ---
3. По окончании создания сертифицирующей организации (CA) мы рекомендуем создать резервную копию пары из открытого и закрытого ключей и сохранить ее в безопасном месте. Дополнительную информацию см. в разделе "Резервное копирование сертификатов корпоративной сертифицирующей организации (CA)" на стр. 92.

Резервное копирование сертификатов корпоративной сертифицирующей организации (CA)

Рекомендуем создать резервную копию закрытого ключа и сертификатов корпоративной сертифицирующей организации (CA) на тот случай, если на ее хост-сервере произойдет неустранимый сбой. При возникновении сбоя можно использовать файл резервной копии для восстановления корпоративной сертифицирующей организации (CA) на любой сервер в дереве.

ПРИМЕЧАНИЕ. Возможность создать резервную копию корпоративной сертифицирующей организации (CA) доступна только для корпоративной сертифицирующей организации (CA), созданной Certificate Server версии 9.0 и более поздних. Если закрытый ключ корпоративной сертифицирующей организации (CA) создан в предыдущих версиях Certificate Server, его экспорт невозможен.

Файл резервной копии содержит закрытый ключ сертифицирующей организации (CA), самоподписанный сертификат, сертификат открытого ключа и несколько других сертификатов, необходимых для его работы. Эта информация сохраняется в формате PKCS #12 (также известен как PFX).

Выполнять резервное копирование корпоративной сертифицирующей организации (CA) нужно тогда, когда она работает должным образом.

Порядок создания резервной копии корпоративной сертифицирующей организации (CA)

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление серт. орг.**.
2. Откройте вкладку **Сертификаты**.
3. Выберите **Самоподписанный сертификат** или **Сертификат открытого ключа**. При выполнении операции резервного копирования оба сертификата записываются в файл. Рекомендуем выбрать самоподписанный сертификат для RSA отдельно от сертификатов ECDSA.

4 Щелкните значок .

5 Выберите экспорт закрытого ключа, укажите пароль длиной не менее 6 символов (буквенно-цифровых), который будет использоваться для шифровки файла PFX, для формата экспорта выберите PKCS12 и щелкните **ОК**.

6 Зашифрованный файл резервной копии будет записан в указанное расположение. Теперь он готов для сохранения в безопасном расположении для использования при возникновении аварийной ситуации.

Восстановление корпоративной сертифицирующей организации (CA)

Если объект "Корпоративная сертифицирующая организация (CA)" удален или поврежден или на хосте-сервере корпоративной сертифицирующей организации произошел неустранимый сбой, корпоративную сертифицирующую организацию (CA) можно полностью восстановить из файла резервной копии, созданного согласно процедуре, описанной в "Резервное копирование сертификатов корпоративной сертифицирующей организации (CA)" на стр. 92.

Порядок восстановления корпоративной сертифицирующей организации (CA)

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление серт. орг.**.

2 Чтобы удалить существующую корпоративную сертифицирующую организацию (CA), щелкните в верхней части экрана (рядом с **Управление сертифицирующей организацией (CA)**).

3 Будет предложено настроить новую корпоративную сертифицирующую организацию (CA). Откроется диалоговое окно создания объекта "Корпоративная сертифицирующая организация (CA)" и окно соответствующего мастера для создания этого объекта.

4 В диалоговом окне создания укажите сервер для корпоративной сертифицирующей организации (CA) и имя объекта "Корпоративная сертифицирующая организация (CA)".

5 Выберите **Импорт**.

6 Выберите сертификаты RSA и ECDSA. Certificate Server требует, чтобы оба сертификата имели одно имя субъекта. Однако Certificate Server не поддерживает импорт внешних самоподписанных сертификатов сертифицирующей организации (CA). При этом он поддерживает импорт сертификатов подчиненной сертифицирующей организации (CA).

7 На последующих экранах найдите и выберите имя файла для RSA и ECDSA.

8 Введите пароль, использованный для шифрования файла при создании резервной копии, и щелкните **ОК**.

9 Закрытый ключ и сертификаты корпоративной сертифицирующей организации (CA) будут восстановлены, а сертифицирующая организация станет полностью функциональной. Этот файл теперь можно сохранить для использования в будущем.

Проверка сертификатов сертифицирующей организации (CA)

Если есть подозрения, что сертификат имеет проблемы или может быть недействительным, его можно легко проверить средствами Identity Console. Проверить можно любой сертификат в дереве eDirectory, включая сертификаты, изданные внешними сертифицирующими организациями (CA).

Процесс проверки сертификата включает в себя проверки данных в сертификате, а также данных в цепочке сертификатов. Цепочка сертификатов состоит из корневого сертификата сертифицирующей организации (CA) и (необязательно) сертификатов одной или нескольких промежуточных сертифицирующих организаций (CA).

Порядок проверки сертификата

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление серт. орг.**.
2. Откройте вкладку **Сертификаты**.
3. Выберите **Самоподписанный сертификат** или **Сертификат открытого ключа**.
4. Щелкните , чтобы проверить выбранные сертификаты сертифицирующей организации (CA).

Замена сертификатов корпоративной сертифицирующей организации (CA)

Если сертификаты по определенной причине повреждаются или становятся недействительными либо необходимо заменить имеющиеся сертификаты, выполните указанные ниже действия:

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление серт. орг.**.
2. Откройте вкладку **Сертификаты**.
3. Выберите **Самоподписанный сертификат** или **Сертификат открытого ключа**.
4. Щелкните , чтобы заменить выбранный сертификат сертифицирующей организации (CA).
5. Импортируйте сертификат сертифицирующей организации в формат (CA) `.pfx` или `.p12` и укажите пароль для шифрования закрытого ключа.
6. Щелкните **ОК**.

Отзыв сертификатов корпоративной сертифицирующей организации (CA)

Порядок отзыва сертификата

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление серт. орг.**.
2. Откройте вкладку **Сертификаты**.
3. Выберите **Самоподписанный сертификат** или **Сертификат открытого ключа**.

4 Щелкните значок ⊘.

5 Внимательно ознакомьтесь с предупреждением о риске, связанном с отзывом сертификатов сервера.

6 В раскрывающемся списке выберите подходящую причину отзыва, затем выберите дату истечения срока действия и укажите комментарии (если нужно).

7 Щелкните **ОК**, чтобы завершить отзыв.

Управление сертификатами сервера

Модуль "Управление сертификатом сервера" позволяет администратору выполнить следующие задачи:

- "Создание объектов "Сертификат" сервера" на стр. 95
- "Экспорт объектов "Сертификат" сервера" на стр. 95
- "Проверка объектов "Сертификат" сервера" на стр. 96
- "Замена объекта "Сертификат" сервера" на стр. 96
- "Отзыв объектов "Сертификат" сервера" на стр. 96
- "Удаление объектов "Сертификат" сервера" на стр. 97

Создание объектов "Сертификат" сервера

Порядок создания объекта "Сертификат" сервера

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом сервера**.

2 Щелкните значок +.

3 На странице **Создать сертификат сервера** укажите **Псевдоним**, сервер и выберите один из следующих параметров:

- **Стандартный (параметры по умолчанию).** Позволяет создать объект "Сертификат" сервера типа RSA или ECDSA по умолчанию.
- **Настраиваемый (параметры указываются пользователем).** Позволяет указать пользовательские параметры для объекта "Сертификат" сервера.
- **Импорт (позволяет импортировать файл PKCS12).** Позволяет импортировать файл `PKCS12` в формат `.pfx` или `.p12`.

4 После ввода параметров щелкните **Далее**, чтобы просмотреть сводную информацию сертификата.

5 На экране **Сводка** щелкните **ОК** для создания объекта "Сертификат" сервера.

Экспорт объектов "Сертификат" сервера

Порядок экспорта объектов "Сертификат" сервера

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом сервера**.

2 В раскрывающемся списке выберите соответствующий сервер.

3 Выберите соответствующий сертификат сервера в списке и щелкните значок .

4 На следующем экране установите флажок **Экспортировать закрытый ключ** и укажите пароль для защиты закрытого ключа. Подтвердите пароль и выберите формат экспорта.

ПРИМЕЧАНИЕ. Сертификаты сервера можно экспортировать только в формат `PKCS12`.

5 Щелкните **ОК**, чтобы экспортировать объект "Сертификат" сервера.

Проверка объектов "Сертификат" сервера

Порядок проверки объекта "Сертификат" сервера

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом сервера**.

2 В раскрывающемся списке выберите соответствующий сервер.

3 Выберите соответствующий сертификат сервера в списке и щелкните значок .

4 Появится сообщение, подтверждающее проверку для объекта "Сертификат" сервера.

Замена объекта "Сертификат" сервера

Если сертификаты сервера по определенной причине повреждаются или становятся недействительными либо необходимо заменить имеющиеся сертификаты по умолчанию, выполните указанные ниже действия:

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом сервера**.

2 В раскрывающемся списке выберите соответствующий сервер.

3 Выберите соответствующий сертификат сервера в списке и щелкните значок .

4 Внимательно ознакомьтесь с предупреждением о риске, связанном с заменой сертификатов сервера, и щелкните **ОК**.

5 На следующем экране найдите и выберите новый сертификат сервера в формате `.pfx` или `.p12` и укажите пароль.

6 Щелкните **ОК**, чтобы заменить сертификат сервера.

Отзыв объектов "Сертификат" сервера

Порядок отзыва объектов "Сертификат" сервера

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом сервера**.

2 В раскрывающемся списке выберите соответствующий сервер.

3 Выберите соответствующий сертификат сервера в списке и щелкните значок .

4 Внимательно ознакомьтесь с предупреждением о риске, связанном с отзывом сертификатов сервера, и щелкните **ОК**.

5 На следующем экране в раскрывающемся списке выберите подходящую причину отзыва, затем выберите дату истечения срока действия и укажите комментарии (если нужно).

6 Щелкните **ОК**, чтобы завершить отзыв.

Удаление объектов "Сертификат" сервера

Порядок удаления объектов "Сертификат" сервера

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом сервера**.
2. В раскрывающемся списке выберите соответствующий сервер.
3. Выберите соответствующий сертификат сервера в списке и щелкните значок  .
4. На следующем экране щелкните **ОК**.
5. Появится сообщение, подтверждающее удаление для объекта "Сертификат" сервера.

Управление сертификатами пользователя

Модуль "Управление сертификатом пользователя" позволяет выполнить следующую задачу:

- "Создание объектов "Сертификат" пользователя" на стр. 97
- "Экспорт объектов "Сертификат" пользователя" на стр. 97
- "Проверка объектов "Сертификат" пользователя" на стр. 98
- "Отзыв объектов "Сертификат" пользователя" на стр. 98
- "Удаление объектов "Сертификат" пользователя" на стр. 98

Создание объектов "Сертификат" пользователя

Чтобы создать объект сертификата пользователя, выполните следующие действия.

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом пользователя**.
2. Щелкните значок  .
3. На странице **Создать сертификат пользователя** укажите **Псевдоним**, сервер и выберите один из следующих параметров:
   - **Стандартный (параметры по умолчанию).** Позволяет создать объект "Сертификат" пользователя типа RSA или ECDSA по умолчанию.
   - **Настраиваемый (параметры указываются пользователем).** Позволяет указать пользовательские параметры для объекта "Сертификат" пользователя.
   - **Импорт.** Позволяет импортировать файл сертификата в формат `CERT` или `PKCS12`.
4. После ввода параметров щелкните **Далее**, чтобы просмотреть сводную информацию сертификата.
5. На экране **Сводка** щелкните **ОК** для создания объекта "Сертификат" пользователя.

Экспорт объектов "Сертификат" пользователя

Порядок экспорта объектов "Сертификат" пользователя

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом пользователя**.
2. В раскрывающемся списке выберите соответствующий сервер.

3 Выберите соответствующий сертификат пользователя в списке и щелкните значок .

4 На следующем экране установите флажок **Экспортировать закрытый ключ** и укажите пароль для защиты закрытого ключа. Подтвердите пароль и выберите формат экспорта.

ПРИМЕЧАНИЕ. Сертификаты пользователя можно экспортировать только в формат `PKCS12`.

---

5 Щелкните **ОК**, чтобы экспортировать объект "Сертификат" пользователя.

Проверка объектов "Сертификат" пользователя

Порядок проверки объектов "Сертификат" пользователя

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом пользователя**.

2 В раскрывающемся списке выберите соответствующий сервер.

3 Выберите соответствующий сертификат пользователя в списке и щелкните значок .

4 Появится сообщение, подтверждающее проверку для объекта "Сертификат" пользователя.

Отзыв объектов "Сертификат" пользователя

Порядок отзыва объектов "Сертификат" пользователя

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом пользователя**.

2 В раскрывающемся списке выберите соответствующий сервер.

3 Выберите соответствующий сертификат пользователя в списке и щелкните значок .

4 Внимательно ознакомьтесь с предупреждением о риске, связанном с отзывом сертификатов пользователя.

5 В раскрывающемся списке выберите подходящую причину отзыва, затем выберите дату истечения срока действия и укажите комментарии (если нужно).

6 Щелкните **ОК**, чтобы завершить отзыв.

Удаление объектов "Сертификат" пользователя

Порядок удаления объектов "Сертификат" пользователя

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление сертификатом пользователя**.

2 В раскрывающемся списке выберите соответствующий сервер.

3 Выберите соответствующий сертификат пользователя в списке и щелкните значок .

4 На следующем экране щелкните **ОК**.

5 Появится сообщение, подтверждающее удаление для объекта "Сертификат" пользователя.

Управление доверенным корнем и контейнерами

Доверенный корень предоставляет основу для доверия в инфраструктуре открытого ключа. Доверенные корни используются для проверки сертификатов, подписанных другими сертифицирующими организациями. Доверенные корни обеспечивают безопасность для SSL, безопасную электронную почту и аутентификацию на основе сертификата.

Модуль "Управление доверенным корнем" позволяет выполнить следующие задачи:

Создание контейнера доверенного корня

Порядок создания доверенного корня

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление доверенным корнем**. Флажок **Контейнер доверенного корня** будет установлен по умолчанию.
2. Щелкните значок +, чтобы создать новый контейнер доверенного корня.
3. Укажите имя контейнера доверенного корня.
4. Выберите соответствующий контейнер с помощью селектора объектов.
5. Щелкните **ОК**.
6. Появится сообщение, подтверждающее создание контейнера доверенного корня.

Создание объекта "Сертификат доверенного корня"

Порядок создания объекта "Сертификат доверенного корня"

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление доверенным корнем**. Флажок **Контейнер доверенного корня** будет установлен по умолчанию. Установите флажок **Доверенный корень**.
2. Щелкните значок +, чтобы создать новый объект "Доверенный корень".
3. Укажите имя объекта "Доверенный корень".
4. В раскрывающемся списке выберите соответствующий контейнер доверенного корня.
5. Найдите и выберите соответствующий файл сертификата в формате `.der` или `.b64`.

   ПРИМЕЧАНИЕ. В объекте "Доверенный корень" можно сохранить сертификаты любого типа (сертификаты сертифицирующей организации (CA), промежуточные сертификаты сертифицирующей организации (CA) или сертификаты пользователя).
6. Щелкните **ОК**.
7. Появится сообщение, подтверждающее создание объекта "Доверенный корень".

Экспорт объектов "Сертификат доверенного корня"

Порядок экспорта объектов "Сертификат доверенного корня"

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление доверенным корнем**. Флажок **Контейнер доверенного корня** будет установлен по умолчанию. Установите флажок **Доверенный корень**.
2. Выберите соответствующий сертификат доверенного корня в списке и щелкните значок  .
3. На следующем экране установите флажок **Экспортировать закрытый ключ** и укажите пароль для защиты закрытого ключа. Подтвердите пароль и выберите формат экспорта.

   ПРИМЕЧАНИЕ. Сертификаты доверенного корня можно экспортировать только в форматах `DER` или `BASE64`.
4. Щелкните **ОК** для экспорта объекта "Сертификат доверенного корня".

Проверка объектов "Сертификат доверенного корня"

Порядок проверки объектов "Сертификат доверенного корня"

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление доверенным корнем**. Флажок **Контейнер доверенного корня** будет установлен по умолчанию. Установите флажок **Доверенный корень**.
2. Выберите соответствующий сертификат доверенного корня в списке и щелкните значок  .
3. Появится сообщение, подтверждающее проверку для объекта "Сертификат доверенного корня".

Удаление объектов "Сертификат доверенного корня"

Порядок удаления объектов "Сертификат доверенного корня"

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление доверенным корнем**. Флажок **Контейнер доверенного корня** будет установлен по умолчанию. Установите флажок **Доверенный корень**.
2. Выберите соответствующий сертификат доверенного корня в списке и щелкните значок  .
3. На экране предупреждения щелкните **ОК**.
4. Появится сообщение, подтверждающее удаление объекта "Сертификат доверенного корня".

Удаление контейнеров доверенного корня

Порядок удаления контейнера доверенного корня

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Управление доверенным корнем**. Флажок **Контейнер доверенного корня** будет установлен по умолчанию.
2. Выберите соответствующий контейнер доверенного корня в списке и щелкните значок  .
3. На экране предупреждения щелкните **ОК**.
4. Появится сообщение, подтверждающее удаление контейнера доверенного корня.

Создание объектов "Сертификат сервера по умолчанию"

При установке Certificate Server создаются объекты "Сертификат сервера по умолчанию".

- SSL CertificateDNS - *имя_сервера*
- Сертификат для каждого IP-адреса, настроенного на данном сервере (IPAG*xxx.xxx.xxx.xxx - имя_сервера*)
- Сертификат для каждого имени DNS, настроенного на данном сервере (DNSAG*www.example.com - имя_сервера*)

ПРИМЕЧАНИЕ. eDirectory автоматически не создает SSL CertificateIP. Имя DNS сертификата SSL содержит все IP-адреса, указанные в альтернативном имени субъекта. При создании или восстановлении сертификатов по умолчанию в Identity Console сертификат SSL CertificateIP не создается и не восстанавливается по умолчанию. Однако в интерфейсе подключаемого модуля есть флажок, который можно выбрать для переопределения поведения по умолчанию и принудительного создания/восстановления сертификата SSL CertificateIP.

Если корпоративная сертифицирующая организация (CA) имеет сертификат ECDSA, eDirectory 9.0 и более поздних версий автоматически создает сертификаты ECDSA.

Если эти сертификаты по определенной причине повреждаются или становятся недействительными либо необходимо заменить имеющиеся сертификаты по умолчанию, можно использовать мастер создания сертификатов сервера по умолчанию, как описано в следующей процедуре:

1. На целевой странице Identity Console щелкните **Управление сертификатом** > **Сертификаты по умолчанию**.
2. Выберите сервер или серверы, для которых необходимо создать сертификаты по умолчанию, и щелкните **Далее**.
3. Выберите "Да", если нужно перезаписать существующие сертификаты сервера по умолчанию. Выберите "Нет", если нужно перезаписать существующие сертификаты сервера по умолчанию, только если они недействительны.
4. (Только один сервер) Чтобы использовать существующий адрес DNS, выберите этот параметр. Чтобы использовать другой адрес DNS, выберите этот параметр и укажите новый адрес DNS.
5. (Только для одного сервера) Чтобы использовать существующий IP-адрес по умолчанию, выберите этот параметр. Чтобы использовать другой IP-адрес, выберите этот параметр и укажите новый IP-адрес.

6 Щелкните кнопку **Далее**.

7 Просмотрите страницу сводной информации и щелкните **Готово**.

Чтобы получить более широкий контроль при создании объекта "Сертификат" сервера, его можно создать вручную. Дополнительную информацию см. в разделе "Создание объектов "Сертификат" сервера" на стр. 95.

Выпуск сертификата открытого ключа

Ваша корпоративная сертифицирующая организация (CA) работает так же, как и внешняя сертифицирующая организация (CA). Это означает, что она может издавать сертификаты на основе запросов на подпись сертификата (CSR). Когда пользователь отправит запрос на подпись сертификата (CSR), вы можете издать для него сертификат с использованием корпоративной сертифицирующей организации (CA). Пользователь, запрашивающий сертификат, может затем импортировать выданный сертификат непосредственно в приложение с активированным шифрованием.

Эта задача позволяет сгенерировать сертификаты для приложений, которые поддерживают шифрование, но не распознают объекты "Сертификат" сервера.

Порядок издания сертификата

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Издать сертификаты**.

2 Найдите и выберите файл CSR.

3 В разделе "Спецификации использования ключа" задайте значение параметров "Тип ключа" и "Использование ключа". Эти параметры позволяют выбрать тип ключа. С каждым типом ключа сопоставлены предопределенные значения использования ключа:

   3a **Не определено.** Этот параметр используется по умолчанию; он не активирует использование ключа в сертификате.

   3b **Сертифицирующая организация (CA).** Этот параметр активирует использования ключа "Подпись сертификата" и "Подпись CRL".

   3c **Шифрование.** Этот параметр включает использование ключа для шифрования ключом.

   3d **Подпись.** Этот параметр включает использование ключа для цифровой подписи.

   3e **SSL или TSL.** Этот параметр настраивает ключ для использования в транзакциях SSL или TLS.

   3f **Настраиваемый.** Этот параметр позволяет вручную выбрать отдельный параметр использования ключа или все его параметры.

   3g **Задать критическое расширение использования ключа.** При выборе любого типа ключа, кроме "Не определено", можно помечать продление использования ключа как критическое. Любое критическое расширение должно распознаваться получающей программой до начала использования сертификата с любой целью. Таким образом, пометка расширения как критического создает некоторый риск, поскольку не все приложения смогут работать с сертификатом. Но для хорошо известных расширений, таких как использование ключей, риск минимален. В общем случае, если указывается использование ключа, расширение должно быть помечено как критическое.

4 Можно определить в сертификате расширение **Расширенное использование ключа**. Для этого выберите параметр **Активировать использование расширенных ключей**:

4a **Сервер.** Этот параметр активирует расширенное использование ключа "Аутентификация сервера".

4b **Пользователь.** Этот параметр активирует расширенные использования ключа "Аутентификация пользователя" и "Защита электронной почты".

4c **Настраиваемый.** Этот параметр позволяет выбрать любое расширенное использование ключа или все из них.

4d **Любой.** Позволяет применять ключ для любого расширенного использования ключа.

4e **Задайте расширение расширенного использования ключа как критическое.**

Любое критическое расширение должно распознаваться получающей программой до начала использования сертификата с любой целью. Таким образом, пометка расширения как критического создает некоторый риск, поскольку не все приложения смогут работать с сертификатом. Так как множество приложений не распознают расширение использования расширенных ключей, пометка данного расширения как критического создает значительный риск того, что сертификат не будет принят тем или иным приложением. Поэтому устанавливать критическое расширение следует только в случае необходимости.

5 Выберите значение для **Базовые ограничения**:

5a **Тип сертификата**

5a1 **Не определено.** Выберите этот параметр, если не хотите добавлять к сертификату расширение основного ограничения.

5a2 **Сертифицирующая организация (CA).** Выберите этот параметр, чтобы добавить к сертификату расширение основного ограничения "Сертифицирующая организация". Этот параметр необходимо установить, если сертификат относится к сертифицирующей организации (CA).

5a3 **Конечный объект.** Выберите этот параметр, чтобы добавить к сертификату расширение основного ограничения, указывающее на то, что это сертификат конечного объекта (а не сертифицирующей организации). Если сертификат имеет тип "Конечный объект", для параметра "Длина пути" должно быть установлено значение "Не определено".

5b **Длина пути.**

5b1 **Не определено.** Установите этот параметр, если не хотите указывать, сколько уровней подчиненных сертифицирующих организаций (CA) может быть создано для данной сертифицирующей организации (CA).

ПРИМЕЧАНИЕ. Если сертификат имеет тип "Конечный пользователь", для параметра длины пути должно быть установлено значение "Не определено".

5b2 **Определенный.** Выберите этот параметр, если необходимо указать, сколько уровней подчиненных сертифицирующих организаций (CA) может быть создано для данной сертифицирующей организации. Чтобы задать длину пути, воспользуйтесь стрелками вверх и вниз.

ПРИМЕЧАНИЕ. Если созданный сертификат является подчиненной сертифицирующей организацией (CA), то его длина пути должна быть согласована с длиной пути вышестоящей сертифицирующей организации (CA). Например, если вышестоящая сертифицирующая организация (CA) имеет длину пути 3, то длина пути подчиненной сертифицирующей организации (CA) не

должна быть больше 2. Если длина пути для вышестоящей сертифицирующей организации (CA) не определена, то подчиненная сертифицирующая организация (CA) может иметь любую длину пути, в том числе неопределенную.

5c Задать расширение основных ограничений как критическое. В общем случае расширение основных ограничений для сертификатов сертифицирующей организации (CA) должно быть установлено как критическое. Любое критическое расширение должно распознаваться получающей программой до начала использования сертификата с любой целью. Таким образом, пометка расширения как критического создает некоторый риск, поскольку не все приложения смогут работать с сертификатом. Но для хорошо известных расширений, таких как основные ограничения, риск минимален.

6 Укажите следующие параметры сертификата:

6a Имя субъекта. Отображает полнотиповое имя дерева eDirectory.

6b Имя субъекта. Отображает полнотиповое имя дерева eDirectory.

6c Период действия. С помощью раскрывающегося списка задайте период, в течение которого будет действовать сертификат. Минимальный срок действия сертификата — 6 месяцев, максимальный — до 2036 года (это ограничение определяется 32-разрядным значением времени). Если выбрать параметр "Определение дат", можно изменить значения полей "Действителен с" и "Дата завершения срока действия" и таким образом задать собственный срок действия сертификата. Максимальная заданная дата не должна превышать даты истечения срока действия сертифицирующей организации (CA).

6c1 Дата вступления в действие. В этом поле указываются дата и время начала действия сертификата, которые можно изменить.

6c2 Дата окончания срока действия. В этом поле указываются дата и время окончания действия сертификата, которые можно изменить.

6d Настраиваемые расширения. Эта функция позволяет задавать поддержку сервером сертификатов любых стандартных или настраиваемых расширений при создании сертификата. Расширения должны быть созданы заранее и храниться в файлах (одно расширение на файл). Все расширения должны быть закодированы по стандарту языка ASN.1, как определено в разделе 4.2 IETF RFC 2459/3280.

Если в создаваемый сертификат необходимо включить поддержку одного или нескольких настраиваемых расширений, нажмите кнопку "Новый", укажите путь к файлу с настраиваемым расширением и добавьте его к сертификату. Повторяя эти действия, к сертификату можно добавить несколько расширений.

Для удаления файла настраиваемых расширений выберите его и щелкните значок  .

7 Выберите параметр для соответствующего формата сертификата:

7a Файл в двоичном формате DER. Этот параметр позволяет сохранить или экспортировать сертификат в файл, который отображается в поле "Имя файла". По умолчанию файл сертификата экспортируется с расширением `.DER` в корень диска C: рабочей станции Identity Console под управлением Windows или в личный каталог рабочей станции Identity Console под управлением Linux.

7b Файл в формате Base64. Этот параметр позволяет сохранить запрос на подпись сертификата (CSR) или экспортировать сертификат в файл, который отображается в поле "Имя файла". По умолчанию файлы сертификата и запроса на подпись

сертификата (CSR) экспортируются с расширением .B64 в корень диска C: рабочей станции Identity Console под управлением Windows или в личный каталог рабочей станции Identity Console на базе Linux.

7c **Файл в формате CER.** Этот параметр позволяет сохранить запрос на подпись сертификата (CSR) или экспортировать сертификат в файл, который отображается в поле "Имя файла". По умолчанию файлы сертификата и запроса на подпись сертификата (CSR) экспортируются с расширением .CER в корень диска C: рабочей станции Identity Console под управлением Windows или в личный каталог рабочей станции Identity Console на базе Linux.

8 Просмотрите сводную информацию о сертификате на следующем экране и щелкните **ОК**.

9 Появится сообщение, подтверждающее выпуск сертификата.

Управление объектом "SAS Service"

Объект "SAS Service" упрощает обмен данными между сервером и его сертификатами. При удалении сервера из дерева eDirectory необходимо также удалить объект сервиса SAS, сопоставленный с этим сервером. При возвращении сервера в дерево необходимо создать для этого сервера объект "SAS Service". В противном случае невозможно будет создать новые сертификаты сервера.

Объект "SAS Service" автоматически создается в процессе проверки состояния сервера. Нет необходимости создавать его вручную.

Объект "SAS Service" можно создать только в том случае, если в одном контейнере с объектом "Сервер" нет объекта "SAS Service" с правильным именем. Например, для сервера с именем "WAKE" создается объект "SAS Service" с именем "SAS Service - WAKE". Утилита добавит указатели DS из объекта "Сервер" в объект SAS и из объекта SAS в объект "Сервер", а также установит правильные элементы списка контроля доступа (ACL) в объекте "SAS Service".

Если объект "SAS Service" с правильным именем уже существует, новый объект не создается. Указатели DS старого объекта "SAS Service" могут быть неправильными или отсутствовать. Кроме того, списки контроля доступа (ACL) могут быть неправильными. В этом случае можно удалить поврежденный объект "SAS Service" и создать новый на портале Identity Console.

Создание или удаление объекта "SAS Service"

Порядок создания или удаления объекта "SAS Service"

1 На целевой странице Identity Console щелкните **Управление сертификатом** > **Объект "SAS Service"**.

2 Если для существующего сервера не создан объект "SAS Service", создайте его, щелкнув значок +.

3 Появится сообщение, подтверждающее создание объекта "SAS Service".

4 Чтобы удалить объект "SAS Service", щелкните значок  .

5 На экране подтверждения щелкните **ОК**, чтобы удалить объект "SAS Service".

18 Управление Authentication Framework

Модуль "Аутентификация" позволяет выполнить следующие задачи:

- "Управление методами входа и послевходовыми методами, а также последовательностями команд при входе в систему и после входа в нее" на стр. 107
- "Управление политиками паролей" на стр. 114
- "Управление набором удостоверяющих вопросов" на стр. 119

Управление методами входа и послевходовыми методами, а также последовательностями команд при входе в систему и после входа в нее

NMAS поддерживает ряд методов входа и послевходовых методов от NetIQ и сторонних разработчиков решений для аутентификации. Для некоторых методов требуется дополнительное оборудование и программное обеспечение. Для методов, которые планируется использовать, должно быть в наличии все необходимое оборудование и программное обеспечение.

В этом разделе описан порядок установки, начальной настройки и конфигурации методов входа и послевходовых методов, а также последовательностей команд при входе в систему и после входа в нее для NMAS.

- "Установка метода входа или метода после входа" на стр. 107
- "Обновление существующего метода входа или послевходового метода" на стр. 108
- "Удаление методов входа и послевходовых методов" на стр. 109
- "Создание новой последовательности команд при входе в систему для данного метода" на стр. 110
- "Изменение последовательности команд при входе в систему для данного метода" на стр. 111
- "Авторизация и отмена авторизации для последовательности команд при использовании этого метода входа в систему" на стр. 111
- "Настройка последовательности команд при входе в систему для данного метода" на стр. 112
- "Удаление последовательностей команд при входе в систему для данного метода" на стр. 113

Установка метода входа или метода после входа

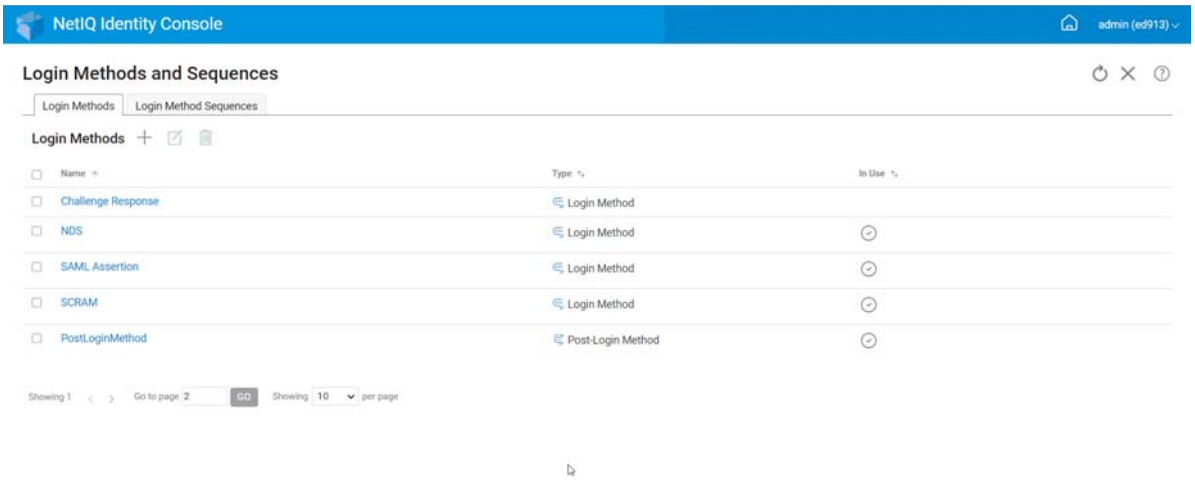
Порядок установки метода входа

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Методы входа и последовательность команд при входе в систему**.
2. Щелкните значок + для установки нового метода входа.

3 Найдите и выберите файл нужного метода входа (.zip) и щелкните **Далее**.

4 Следуйте инструкциям в мастере установки, чтобы выполнить установку метода входа.

Рисунок 18-1 *Установка нового метода входа*



Обновление существующего метода входа или послевходового метода

Порядок обновления существующего метода входа

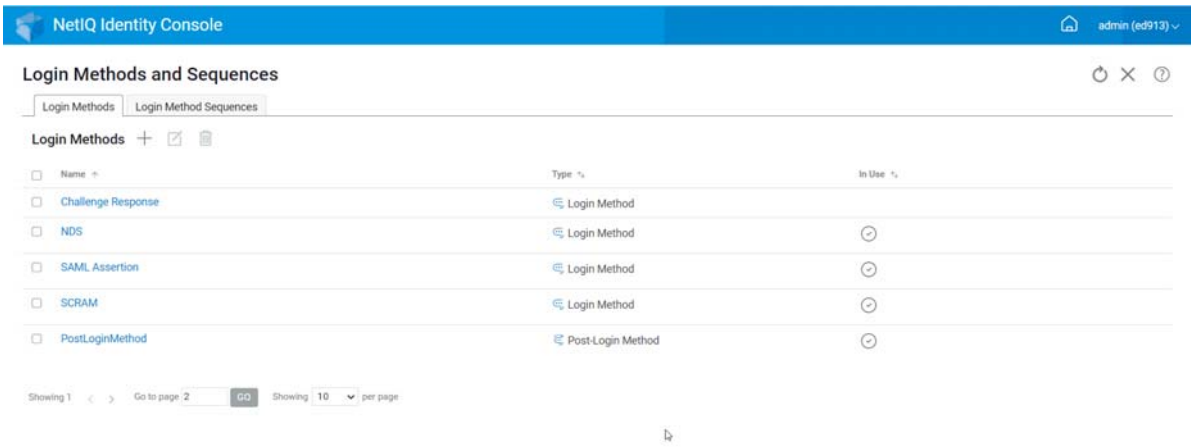
1 На целевой странице Identity Console щелкните **Управление аутентификацией** > **Методы входа и последовательность команд при входе в систему**.

2 В списке выберите метод входа для обновления и щелкните значок ☑.

3 Найдите и выберите файл нужного метода входа (.zip) и щелкните **Далее**.

4 Следуйте инструкциям в мастере обновления, чтобы обновить метод входа.

Рисунок 18-2 *Обновление существующего метода входа*

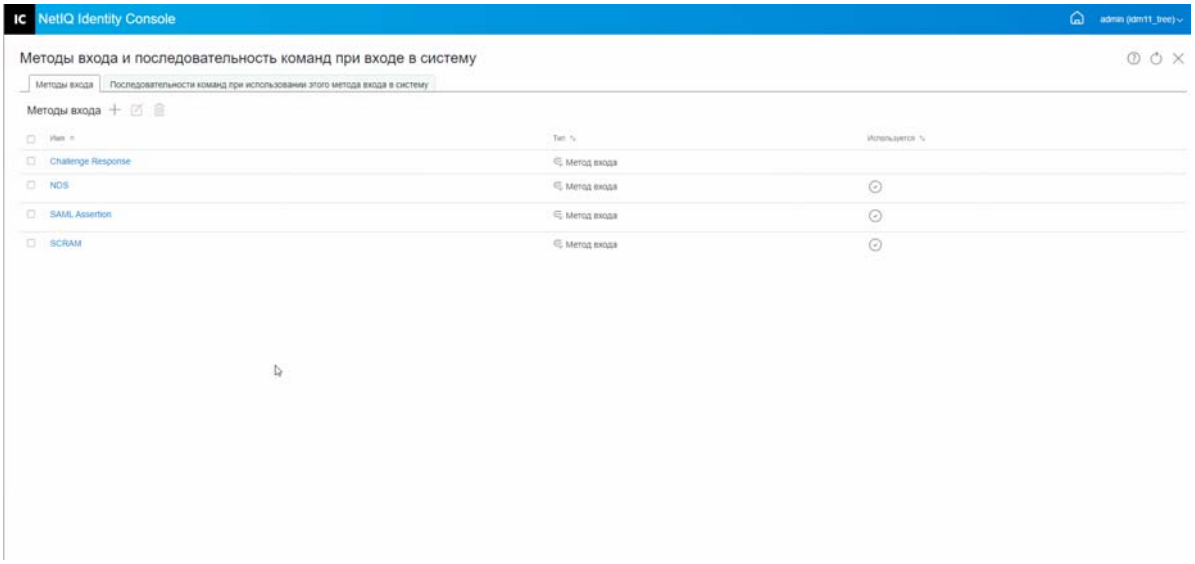


Удаление методов входа и послевходовых методов

Порядок удаления методов входа и послевходовых методов

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Методы входа и последовательность команд при входе в систему**.
2. В списке выберите методы входа для удаления и щелкните значок 🗑.
3. На следующем экране щелкните **ОК**.
4. Появится сообщение, подтверждающее удаление методов входа.

Рисунок 18-3 *Удаление метода входа*



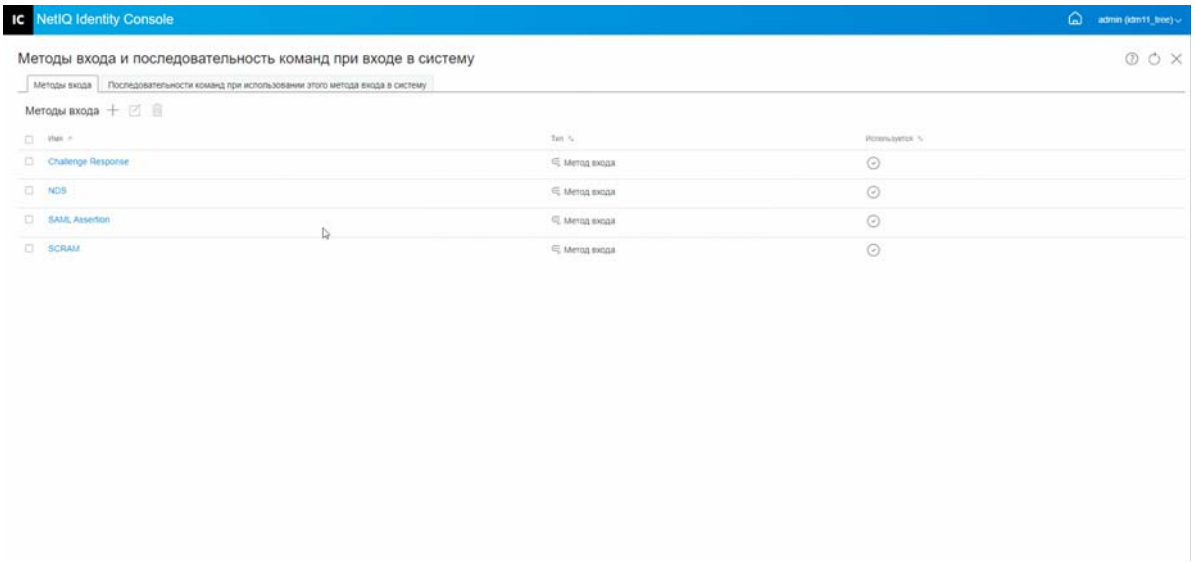
Создание новой последовательности команд при входе в систему для данного метода

После создания различных методов входа для вашей среды можно решить, в каком порядке их использовать. Порядок создания новой последовательности команд при входе в систему для данного метода

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Методы входа и последовательность команд при входе в систему**.
2. Откройте вкладку **Последовательности команд при использовании этого метода входа в систему**.
3. Щелкните значок + для создания новой последовательности команд при входе в систему.
4. Укажите **имя** и выберите **Тип последовательности**.
5. Выберите нужные методы входа и послевходовые методы из списка доступных методов.

   ПРИМЕЧАНИЕ. Чтобы задать порядок использования методов входа, воспользуйтесь стрелками вверх и вниз, которые отображаются на объектах метода входа.
6. Щелкните кнопку **Создать**.
7. Появится сообщение, подтверждающее создание новой последовательности команд при входе в систему для данного метода.

Рисунок 18-4 *Создание последовательности команд при входе в систему для данного метода*

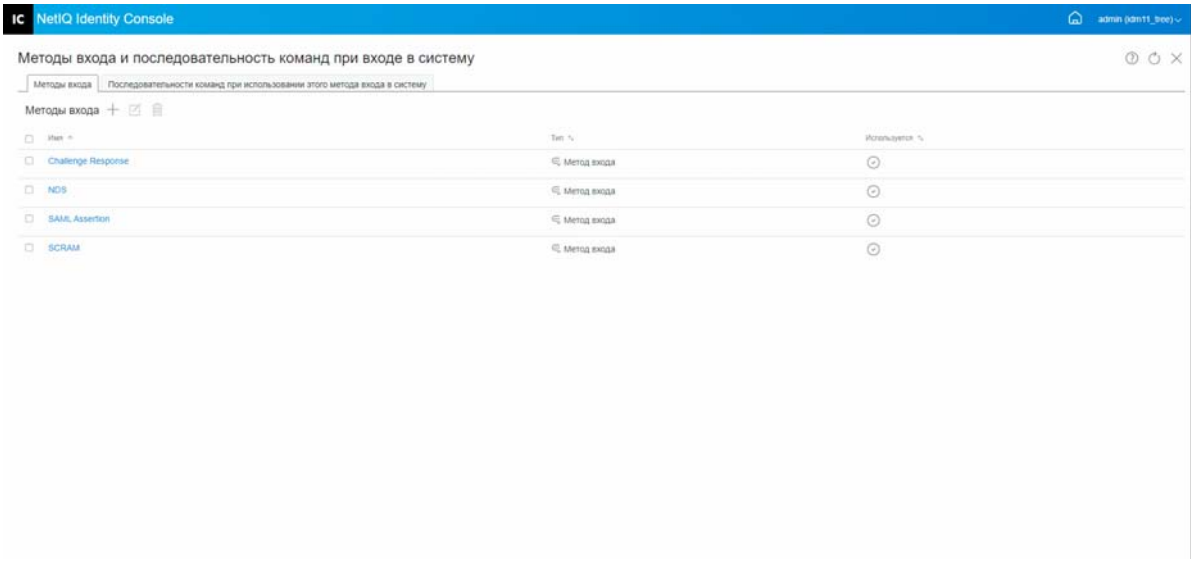


Изменение последовательности команд при входе в систему для данного метода

Порядок изменения существующей последовательности команд при входе в систему для данного метода

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Методы входа и последовательность команд при входе в систему**.
2. Откройте вкладку **Последовательности команд при использовании этого метода входа в систему**.
3. Щелкните значок ☑, чтобы изменить последовательность команд при входе в систему.
4. Внесите необходимые изменения на странице **Изменить последовательность команд при использовании этого метода входа в систему** и щелкните **Сохранить**.
5. Появится сообщение, подтверждающее изменение последовательности команд при входе в систему.

Рисунок 18-5 *Изменение последовательности команд при входе в систему для данного метода*



Авторизация и отмена авторизации для последовательности команд при использовании этого метода входа в систему

Чтобы связать последовательность команд при входе в систему для данного метода с пользователями, контейнерами и разделами, ее необходимо авторизовать и задать для нее значение по умолчанию. Порядок авторизации последовательности команд при входе в систему для данного метода

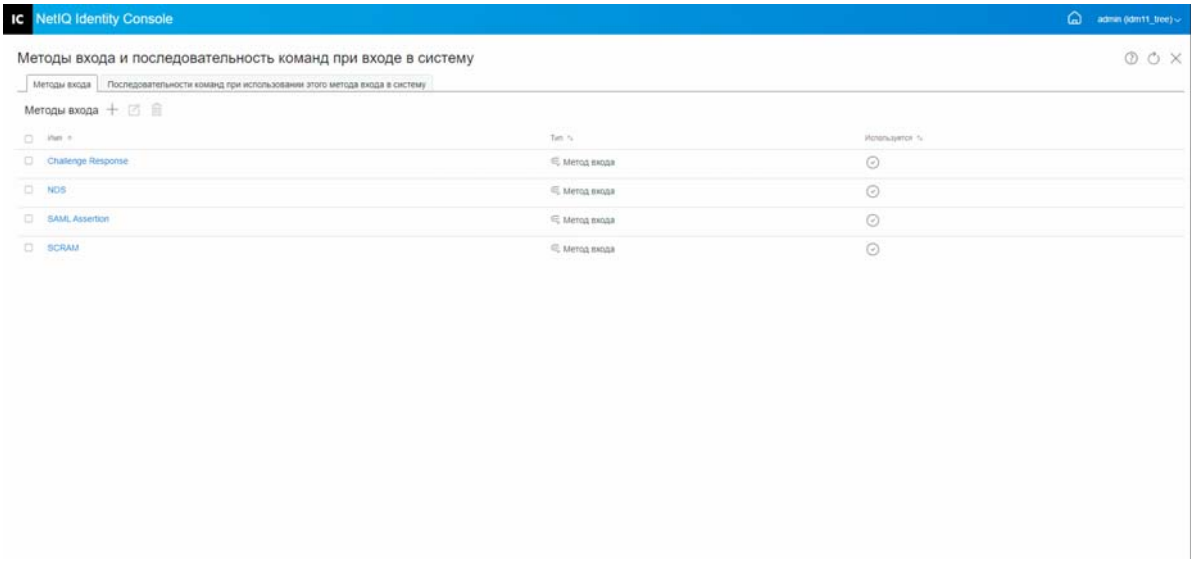
1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Методы входа и последовательность команд при входе в систему**.
2. Откройте вкладку **Последовательности команд при использовании этого метода входа в систему**.

3 В списке выберите последовательность команд при использовании этого метода входа в систему и щелкните значок ⊙.

4 Чтобы отменить авторизацию последовательности команд при использовании этого метода входа в систему, выберите ее и щелкните значок ⊗.

5 Как вариант, для авторизации последовательности команд при использовании этого метода входа в систему и отмены такой авторизации можно использовать раскрывающееся меню в столбце **Авторизовано** списка "Последовательности команд при использовании этого метода входа в систему".

Рисунок 18-6 *Авторизация и отмена авторизации для последовательности команд при использовании этого метода входа в систему*



Настройка последовательности команд при входе в систему для данного метода

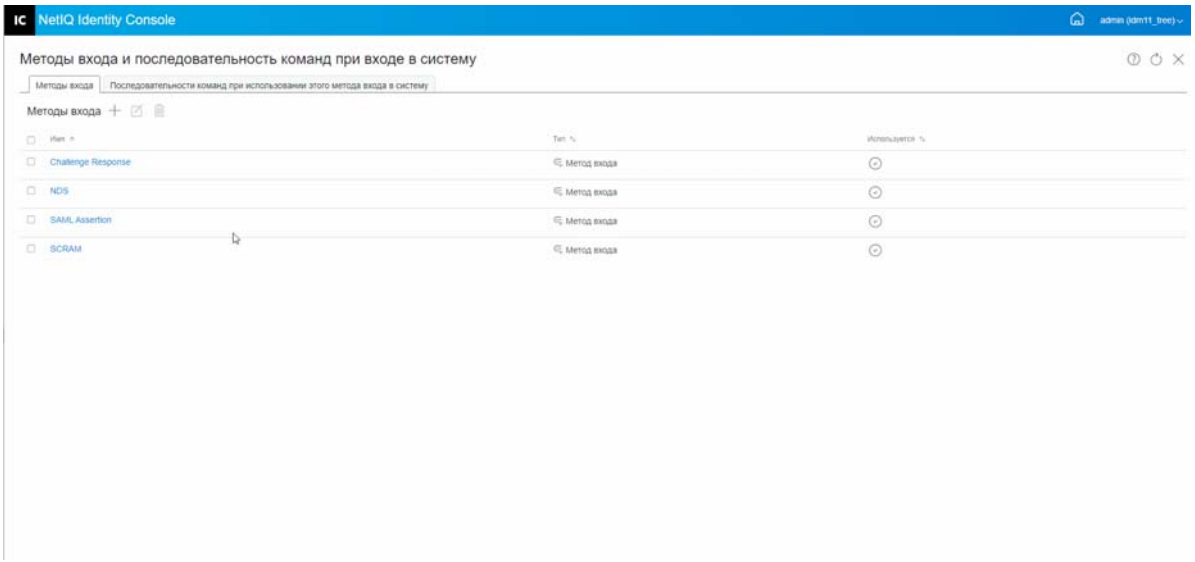
Можно задать последовательность команд при входе в систему по умолчанию, чтобы пользователям не нужно было при каждом входе в систему указывать ее:

1 На целевой странице Identity Console щелкните **Управление аутентификацией** > **Методы входа и последовательность команд при входе в систему**.

2 Откройте вкладку **Последовательности команд при использовании этого метода входа в систему**.

3 Активируйте переключатель ⊗, чтобы использовать разрешенную последовательность команд при входе в систему для данного метода по умолчанию.

Рисунок 18-7 *Настройка последовательности команд при входе в систему для данного метода*

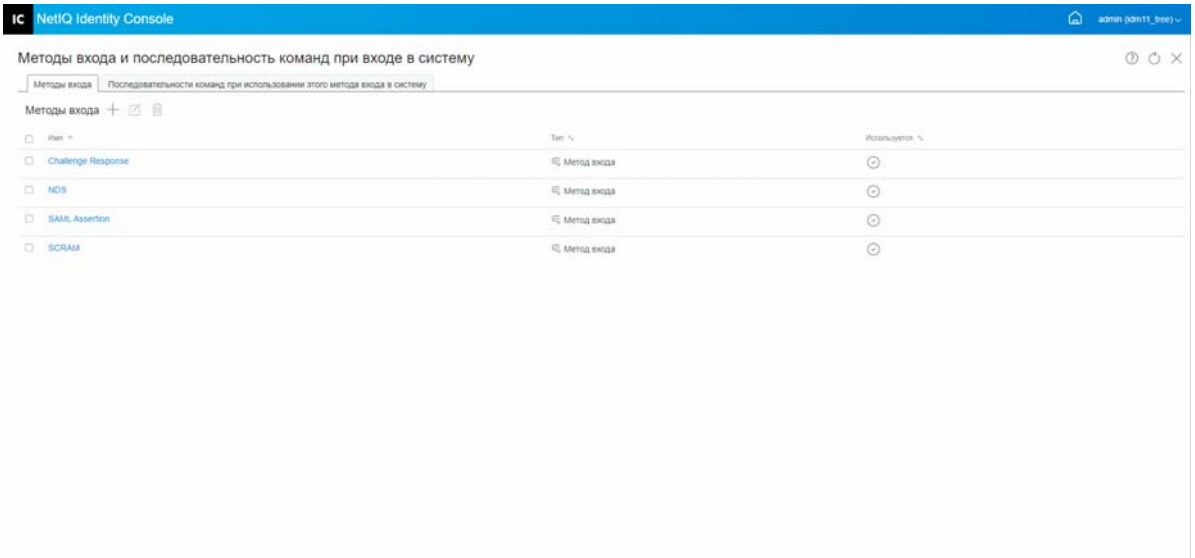


Удаление последовательностей команд при входе в систему для данного метода

Порядок удаления последовательности команд при входе в систему для данного метода

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Методы входа и последовательность команд при входе в систему**.
2. Откройте вкладку **Последовательности команд при использовании этого метода входа в систему**.
3. В списке выберите последовательность команд при использовании этого метода входа в систему и щелкните значок .
4. На следующем экране подтверждения щелкните **ОК**.

Рисунок 18-8 *Удаление последовательности команд при входе в систему для данного метода*



Управление политиками паролей

Политика паролей — это набор заданных администратором правил, которые определяют критерий создания и замены паролей конечных пользователей. NMAS позволяет применить политики паролей, которые назначаются пользователям в eDirectory. В политики паролей также можно включить функции самообслуживания "Забытый пароль", чтобы уменьшить количество обращений в службу поддержки по поводу восстановления забытых паролей. Еще одна функция самообслуживания — "Сбросить пароль" — позволяет пользователям менять пароли при просмотре правил, заданных администратором для политики паролей. Пользователи получают доступ к этим функциям в пользовательском приложении Identity Manager или Identity Console.

Модуль "Политика паролей" позволяет выполнить следующие задачи:

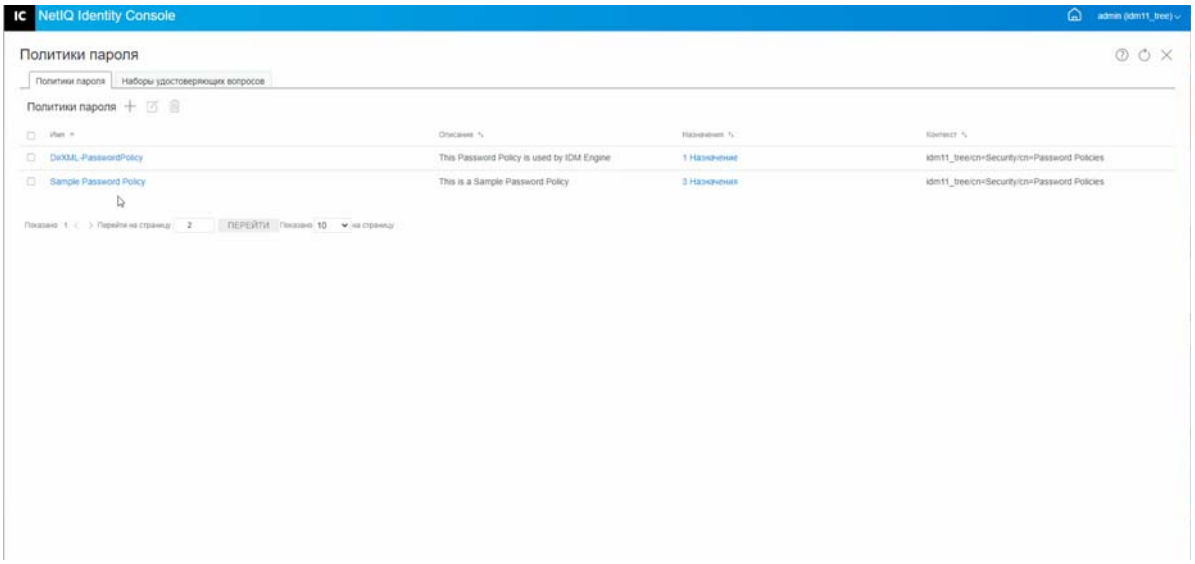
- "Создание политики паролей с настройками по умолчанию" на стр. 114
- "Создание политики паролей с пользовательскими настройками" на стр. 115
- "Изменение политики паролей" на стр. 118
- "Удаление политики паролей" на стр. 119

Создание политики паролей с настройками по умолчанию

Порядок создания политики паролей

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Политики паролей**.
2. Чтобы создать новую политику паролей, щелкните значок +.
3. На следующем экране укажите имя, контекст, описание и сообщение об изменении пароля.
4. Чтобы создать политику паролей с настройками по умолчанию, установите флажок **Создать новую политику на основе настроек по умолчанию** и щелкните **Далее** для просмотра страницы **Сводка**.
5. Проверьте данные на странице **Сводка** и щелкните **Создать**.
6. Появится сообщение, подтверждающее создание политики паролей.

Рисунок 18-9 *Создание политики паролей с настройками по умолчанию*



Создание политики паролей с пользовательскими настройками

Порядок создания политики паролей с пользовательскими настройками

1 На целевой странице Identity Console щелкните **Управление аутентификацией** > **Политики паролей**.

2 Чтобы создать новую политику паролей, щелкните значок +.

3 На следующем экране укажите имя, контекст, описание и сообщение об изменении пароля.

4 Чтобы создать политику паролей с пользовательскими настройками, щелкните **Далее**.

5 На странице **Конфигурация** выполните указанные ниже действия:

5a **Включение универсального пароля.** Включение универсального пароля для политики позволяет использовать параметры в функции "Политики паролей". Однако прежде чем включать универсальный пароль для политики, необходимо убедиться в том, что в среде выполнены необходимые предварительные действия для его использования.

5b **Включение дополнительных правил для паролей.** Этот параметр разрешает использование подробных правил, описанных на вкладке "Дополнительные правила для паролей". Эти правила помогают обеспечить безопасность вашей среды, предоставляя контроль по критериям, таким как срок действия пароля и его содержимого (буквы, цифры, прописные и строчные буквы, а также специальные символы). Можно также исключить заведомо "небезопасные" пароли, например, запретить использовать в качестве пароля название своей компании.

5c **Синхронизация паролей.** Эти параметры задают условия синхронизации универсального пароля в eDirectory с другими типами паролей хранилища объектов и отношений. Функция синхронизации пароля имеет следующие параметры:

5c1 **Удалить пароль NDS при установке пароля.** Если этот параметр выбран, то при установке универсального пароля пароль NDS будет отключен. Пользователи не смогут использовать более ранние методы или утилиты, в которых реализован

прямой вход с паролем NDS (в отличие от обращения к NMAS). Если этот параметр задан, следующий параметр **Синхронизировать пароль NDS при установке пароля** будет отключен по умолчанию.

5c2 **Синхронизировать пароль NDS при установке пароля.** Если этот параметр выбран, то установка универсального пароля в таких приложениях, как Identity Console, также приведет к изменению пароля NDS.

5c3 **Синхронизировать простой пароль при установке пароля.** Этот параметр обеспечивает совместимость с NetIQ и сторонними клиентами, которые используют простой пароль и обеспечение пользователей правами доступа.

5c4 **Синхронизировать пароль распространения при установке пароля.** Этот параметр определяет способность ядра метакаталога получить или установить универсальный пароль пользователя в eDirectory.

5d **Получение универсального пароля.** Доступны следующие параметры:

5d1 **Разрешить пользователю получать пароль.** Разрешает агенту пользователя получать пароль. Этот параметр определяет, может ли сервис самообслуживания "Забытый пароль" восстановить пароль от имени пользователя, чтобы можно было отправить этот пароль пользователю по электронной почте. Если этот параметр не выбран, соответствующая функция будет затенена на вкладке "Забытый пароль" в разделе политики паролей.

5d2 **Разрешить администратору получать пароли.** Установите этот флажок, если соответствующая возможность необходима для работы конкретного сервиса. В Identity Manager для администраторов нет необходимости получать пароли. Однако этот параметр может обеспечить преимущества для определенных сторонних сервисов.

5d3 **Разрешить следующим пользователям получать пароли.** Щелкните значок + и выберите соответствующего пользователя, который должен получить пароль.

5e **Аутентификация:**

5e1 **Проверять соответствие существующих паролей политике паролей (проверка выполняется при входе).** Этот параметр обычно применяется при развертывании новой политики паролей или когда меняются дополнительные правила для паролей в существующей политике и необходимо убедиться в том, что существующие пароли соответствуют новым или измененным правилам.

Если выбран этот параметр, то при входе пользователей их пароли анализируются на соответствие дополнительным правилам для паролей в новой или измененной политике паролей. Если существующий пароль не соответствует правилам, пользователю будет предложено изменить его.

По окончании щелкните **Далее**.

6 **Расширенные правила пароля** позволяют лучше защитить среду, предоставляя возможности контроля таких параметров пароля, как срок действия, частота изменения и содержимое.

Специальные символы — это символы, отличные от цифр (0–9) и букв.

На странице "Расширенные правила пароля" можно выполнить следующие действия:

6a Изменить настройки синтаксиса пароля, используя политику сложности Microsoft (в системах, предшествующих Microsoft Windows Server 2008), политику паролей Microsoft Server 2008 или синтаксис Novell.

6b Указать требуемые настройки для параметров "Изменить пароль", "Срок действия пароля", "Длина и состав пароля" и "Исключения пароля" в мастере и щелкнуть **Далее**.

7 Сервис самообслуживания **Забытый пароль** для пользователей, забывших пароль, позволяет сократить расходы на службу поддержки. Эти функции самообслуживания доступны для пользователей на портале Identity Console. На странице "Забытый пароль" можно выполнить следующие действия:

ПРИМЕЧАНИЕ. При включении сервиса "Забытый пароль" необходимо также указать, должен ли пользователь отвечать на набор удостоверяющих вопросов при входе.

7a Наборы удостоверяющих вопросов. Если включено использование набора удостоверяющих вопросов, пользователи смогут воспользоваться сервисом самообслуживания "Забытый пароль" только после ответа на все вопросы. Чтобы требовать у пользователей указывать такую информацию при входе на портал Identity Console, выберите параметр **Требовать набор удостоверяющих вопросов**.

7b Действие. Параметры, доступные на этой вкладке, позволяют вашим пользователям сбрасывать пароли, ответив на вопросы набора удостоверяющих вопросов и указав универсальный пароль, включить отправку текущего пароля или подсказки о пароле по электронной почте, а также вывести подсказку о пароле.

7c Аутентификация. Чтобы требовать от пользователей указать набор удостоверяющих вопросов или подсказку о пароле, установите флажок **Требовать от пользователя задать удостоверяющий вопрос и (или) подсказку при аутентификации**.

По окончании щелкните **Далее**.

8 Политика не вступает в силу, пока она не будет назначена одному или нескольким объектам. Для упрощения администрирования мы рекомендуем назначать политики объектам, расположенным как можно выше в дереве. Политику паролей можно назначить следующим объектам:

8a Объект "Политика входа". Рекомендуем создать политику паролей по умолчанию для всех пользователей в дереве и назначить объект "Политика входа", который расположен в контейнере безопасности.

8b Контейнер, который является корнем раздела. Если назначить политику контейнеру, который является корнем раздела, все пользователи данного раздела, включая пользователей во вложенных контейнерах, наследуют назначенную политику.

8c Контейнер, который не является корнем раздела. Если назначить политику контейнеру, который не является корнем раздела, назначенная политика наследуется только пользователями из данного контейнера. Пользователи во вложенных контейнерах не наследуют политику.

Чтобы применить политику ко всем пользователям ниже уровня контейнера, который не является корнем раздела, назначьте политику каждому вложенному контейнеру отдельно.

8d Пользователь. Можно назначить политику одному или нескольким пользователям.

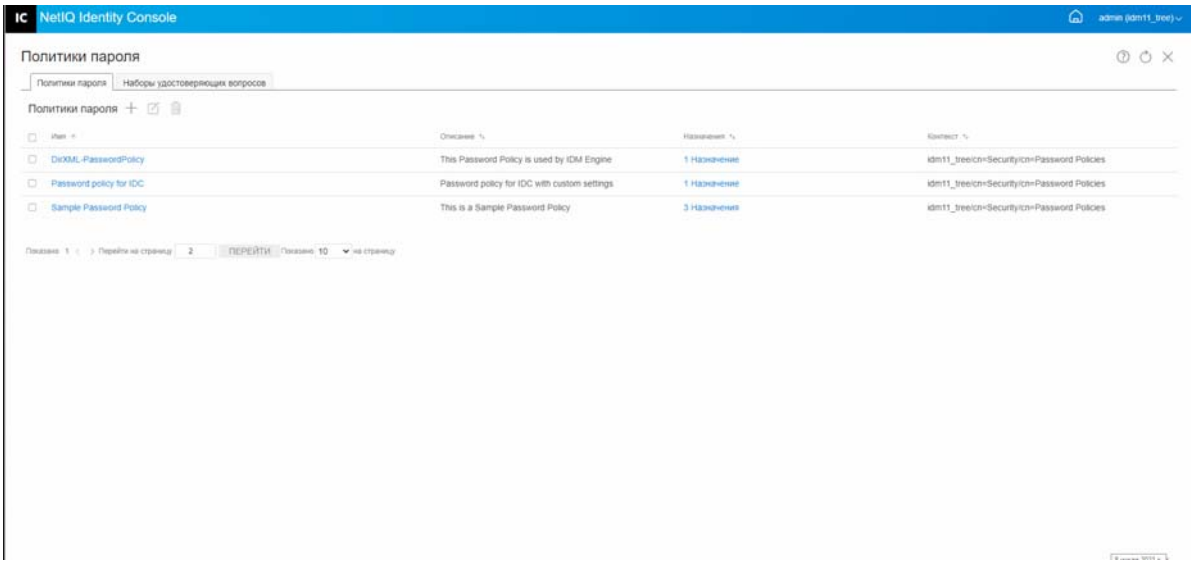
Чтобы назначить политику, щелкните значок +. После этого найдите и выберите соответствующий объект для назначения политики паролей.

Чтобы удалить ассоциацию политики, выберите политику в списке и щелкните значок 🗑.

9 Проверьте данные на странице **Сводка** и щелкните **Создать**.

10 Появится сообщение, подтверждающее создание политики паролей.

Рисунок 18-10 *Создание политики паролей с пользовательскими настройками*

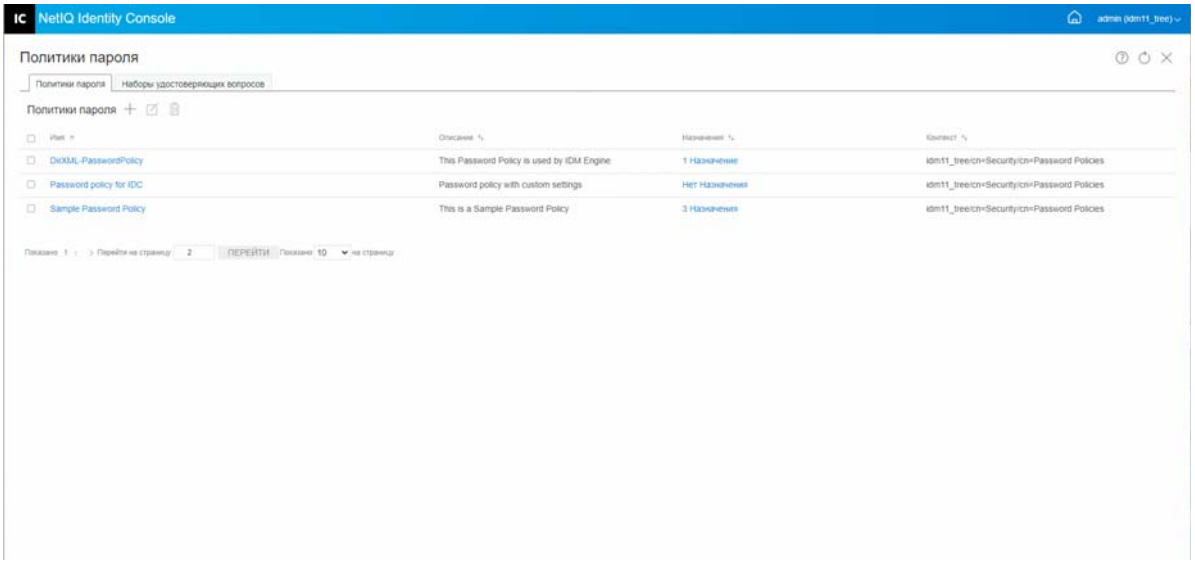


Изменение политики паролей

Порядок изменения существующей политики паролей

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Политики паролей**.
2. Выберите соответствующую политику паролей в списке и щелкните значок ☑.
3. Внесите необходимые изменения на странице **Изменить политику паролей** и щелкните **Сохранить**.

Рисунок 18-11 *Изменение политики паролей*

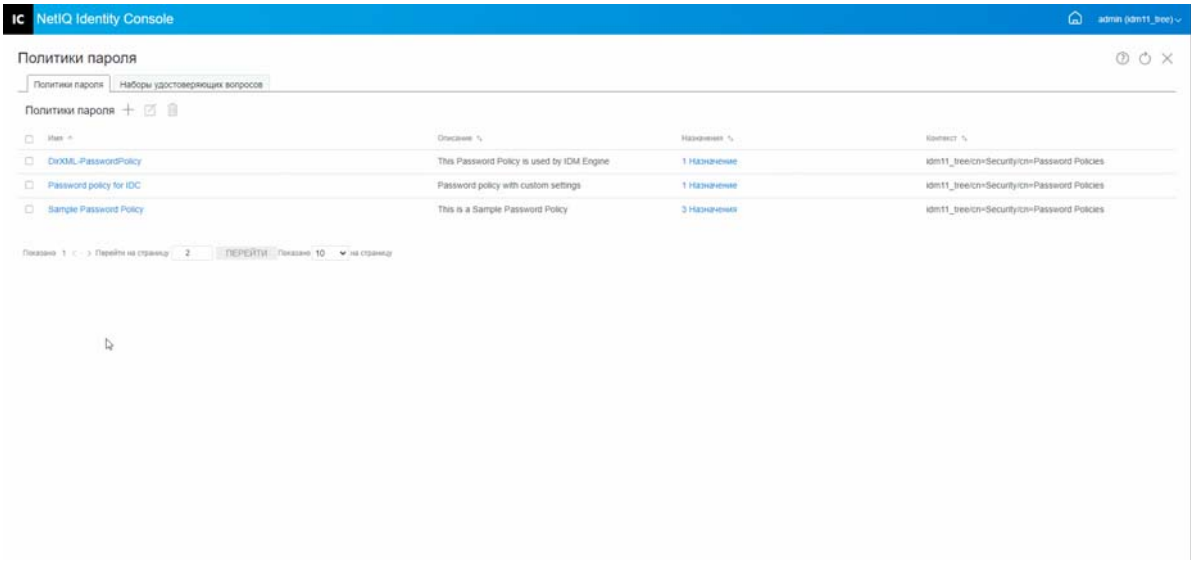


Удаление политики паролей

Порядок удаления политик паролей

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Политики паролей**.
2. Выберите соответствующие политики паролей в списке и щелкните значок .
3. На следующем экране предупреждения щелкните **ОК**.
4. Появится сообщение, подтверждающее удаление политик паролей.

Рисунок 18-12 *Удаление политики паролей*



Управление набором удостоверяющих вопросов

Набор удостоверяющих вопросов — это один или несколько вопросов, на которые пользователь должен ответить для проверки идентификации. Набор удостоверяющих вопросов является частью сервиса самообслуживания паролей.

Если пользователь забудет пароль или возникнут проблемы с его использованием, можно будет воспользоваться сервисом самообслуживания паролей, а не обращаться в службу поддержки. Набор удостоверяющих вопросов позволяет пользователю подтвердить идентификацию, а затем получить подсказку или пароль по электронной почте или сбросить пароль в веб-браузере.

Можно разрешить пользователям настроить собственные вопросы или требовать от них ответа на указанные вами вопросы.

На странице "Набор удостоверяющих вопросов" можно искать существующие наборы удостоверяющих вопросов и вносить в них изменения, а также создавать новые наборы удостоверяющих вопросов.

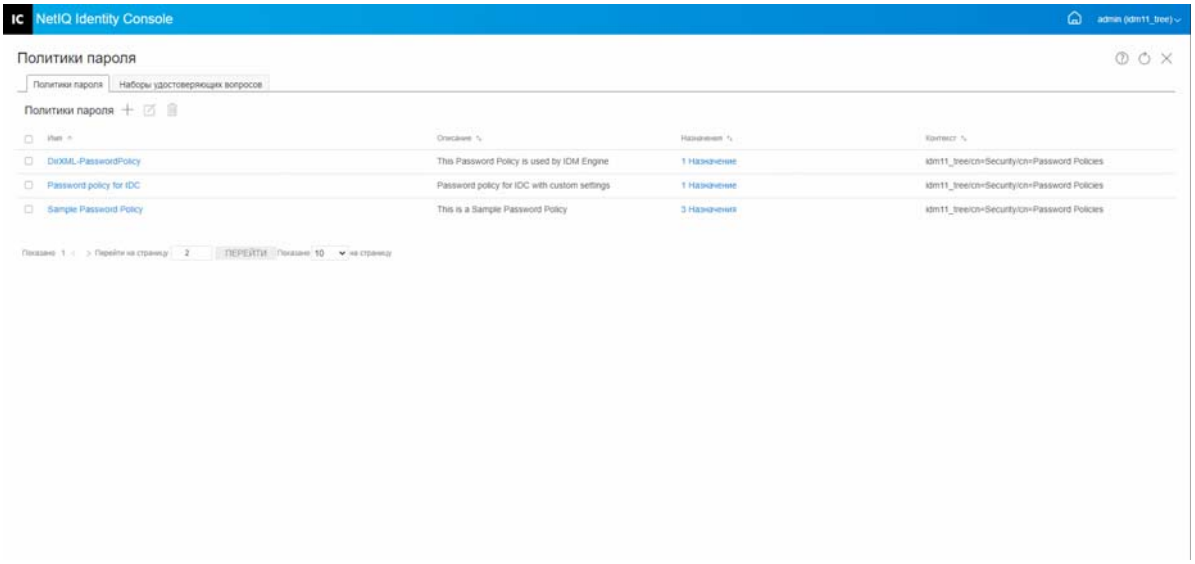
- "Создание нового набора удостоверяющих вопросов" на стр. 120
- "Изменение набора удостоверяющих вопросов" на стр. 120
- "Удаление наборов удостоверяющих вопросов" на стр. 121

Создание нового набора удостоверяющих вопросов

Порядок создания набора удостоверяющих вопросов

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Политики паролей** > **Наборы удостоверяющих вопросов**.
2. Щелкните значок +, чтобы создать новый набор удостоверяющих вопросов.
3. Укажите имя объекта "Набор удостоверяющих вопросов" и выберите контейнер или вложенный контейнер, в котором должен быть создан данный объект.
4. Создайте новый набор вопросов, на которые пользователю нужно будет ответить при получении пароля. Можно также выбрать один из существующих случайных вопросов.
5. Укажите количество задаваемых вопросов и щелкните **Создать**.
6. Появится сообщение, подтверждающее создание набора удостоверяющих вопросов.

Рисунок 18-13 *Создание набора удостоверяющих вопросов*

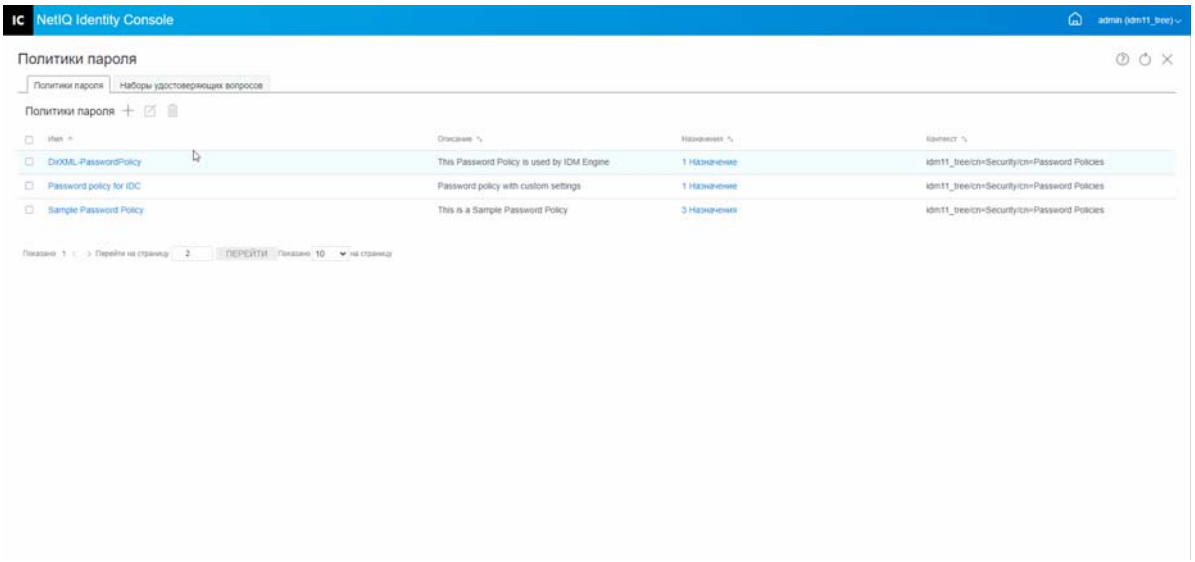


Изменение набора удостоверяющих вопросов

Порядок изменения существующего набора удостоверяющих вопросов

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Политики паролей** > **Наборы удостоверяющих вопросов**.
2. Выберите соответствующий набор удостоверяющих вопросов в списке и щелкните значок ☑.
3. Внесите необходимые изменения на странице "Изменить наборы удостоверяющих вопросов" и щелкните **Сохранить**.
4. Появится сообщение, подтверждающее изменение набора удостоверяющих вопросов.

Рисунок 18-14 *Изменение набора удостоверяющих вопросов*

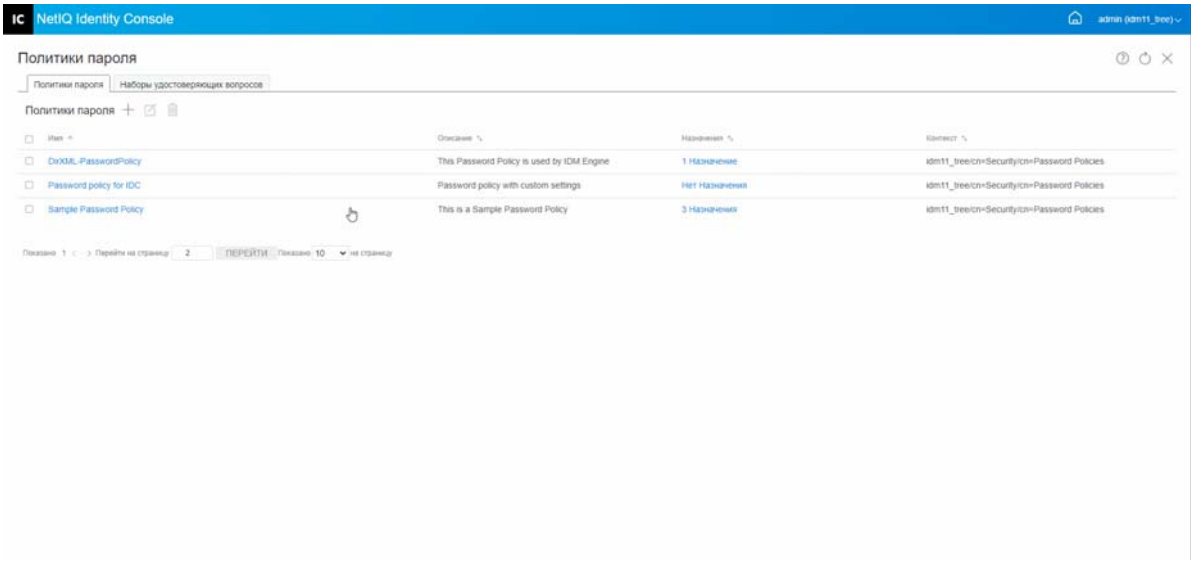


Удаление наборов удостоверяющих вопросов

Порядок удаления наборов удостоверяющих вопросов

1. На целевой странице Identity Console щелкните **Управление аутентификацией** > **Политики паролей** > **Наборы удостоверяющих вопросов**.
2. Выберите нужный набор удостоверяющих вопросов в списке и щелкните значок .
3. На экране подтверждения щелкните **ОК**.
4. Появится сообщение, подтверждающее удаление набора удостоверяющих вопросов.

Рисунок 18-15 *Удаление набора удостоверяющих вопросов*



19 Управление объектами "Группа SNMP"

Протокол Simple Network Management Protocol (SNMP) — это интернет-протокол стандартных и обслуживающих операций для обмена управляющей информацией между приложениями консоли управления и управляемыми устройствами.

Модуль SNMP позволяет выполнить следующие задачи:

- "Создание объектов "Группа SNMP"" на стр. 123
- "Изменение объектов "Группа SNMP"." на стр. 123
- "Удаление объектов "Группа SNMP"" на стр. 123

Создание объектов "Группа SNMP"

Порядок создания объектов "Группа SNMP"

1. На целевой странице Identity Console выберите модуль **SNMP**.
2. Щелкните значок +, чтобы создать новый объект "Группа SNMP".
3. Укажите имя и выберите контекст для создания нового объекта "Группа SNMP".
4. Щелкните кнопку **Создать**.
5. На экране появится сообщение, подтверждающее создание объекта "Группа SNMP".

Изменение объектов "Группа SNMP".

Порядок изменения объектов "Группа SNMP"

1. На целевой странице Identity Console выберите модуль **SNMP**.
2. Выберите объект "Группа SNMP" для изменения и щелкните значок  .
3. Измените настраиваемые параметры на странице **Общие**/**Ловушки**.
4. После этого щелкните кнопку **Сохранить**.
5. На экране появится сообщение, подтверждающее изменение объекта "Группа SNMP".

Удаление объектов "Группа SNMP"

Порядок удаления объектов "Группа SNMP"

1. На целевой странице Identity Console выберите модуль **SNMP**.
2. Выберите объект "Группа SNMP" для изменения и щелкните значок  .
3. На следующем экране щелкните **OK**.
4. На экране появится сообщение, подтверждающее удаление объекта "Группа SNMP".

20 Управление расширенной фоновой аутентификацией Enhanced Background Authentication (EBA)

Для доступа к eDirectory из подключаемого модуля EBA системы Identity Console сертификат CA EBA должен находится в хранилище доверенных сертификатов EBA в Identity Console. На сервере должно быть дерево eDirectory с поддержкой EBA. Сведения о том, как включить EBA для дерева eDirectory, см. в разделе Enabling EBA on an eDirectory Tree (Включение EBA для дерева eDirectory) документа *NetIQ eDirectory Administration Guide* (Руководство по администрированию NetIQ eDirectory).

ПРИМЕЧАНИЕ. Если необходимо использовать модуль EBA с Identity Console, потребуется обновить сервер eDirectory до версии 9.2.4 HF2.

Чтобы открыть страницу управления CA EBA, войдите на портал Identity Console и щелкните модуль **EBA**.

Страница управления CA EBA содержит перечисленные ниже вкладки для управления различными аспектами работы этого модуля.

- **Общие.** Отображается IP-адрес ЦС EBA и его сертификат.
- **Сертификат выдан:** Отображаются сертификаты ЦС EBA вместе с их IP-адресом и портом.

  Чтобы отозвать сертификат, выберите его и щелкните ⊘. Используйте эту функцию только в крайних ситуациях, так как после отзыва сервер, которому принадлежит сертификат CA NCP, потеряет работоспособность. Как правило, сертификат отзывается в случае компрометации сервера.
- **CSR:** список запросов на подпись сертификатов, ожидающих утверждения администратором. Чтобы утвердить запрос на подпись сертификата, выберите его и щелкните **Утвердить**.

II Управление Identity Manager с использованием Identity Console

В этом разделе описаны различные задачи по управлению серверами Identity Manager с использованием портала Identity Console.

- Глава 21 на стр. 129: "Управление драйверами и наборами драйверов"
- Глава 22 на стр. 135: "Управление свойствами набора драйверов"
- Глава 23 на стр. 145: "Управление свойствами драйвера"
- Глава 24 на стр. 171: "Управление статистикой набора драйверов"
- Глава 25 на стр. 173: "Проверка объектов Identity Manager"
- Глава 26 на стр. 175: "Управление потоком данных"
- Глава 27 на стр. 177: "Управление получателями наделения правами"
- Глава 28 на стр. 179: "Управление порядками работ"
- Глава 29 на стр. 183: "Управление состоянием и синхронизацией пароля"
- Глава 30 на стр. 187: "Управление библиотеками"

21 Управление драйверами и наборами драйверов

Набор драйверов — это контейнер, в котором хранятся драйверы Identity Manager. На сервере одновременно может быть активен только один набор драйверов. Поэтому все активные драйверы сгруппированы в одном наборе драйверов. Набор драйверов можно создать с использованием инструмента Designer. Дополнительную информацию см. в разделе Configuring Driver Sets (Настройка наборов драйверов) документа *NetIQ Designer for Identity Manager Administration Guide* (Руководство по администрированию NetIQ Designer для Identity Manager).

- "Добавление и удаление серверов" на стр. 129
- "Активация набора драйверов с использованием ключа активации продукта" на стр. 130
- "Просмотр информации об активации наборов драйверов" на стр. 131
- "Запуск и останов драйверов" на стр. 132
- "Поиск драйверов" на стр. 132
- "Фильтрация драйверов и наборов драйверов" на стр. 133
- "Удаление набора драйверов" на стр. 134
- "Действия с драйверами" на стр. 134

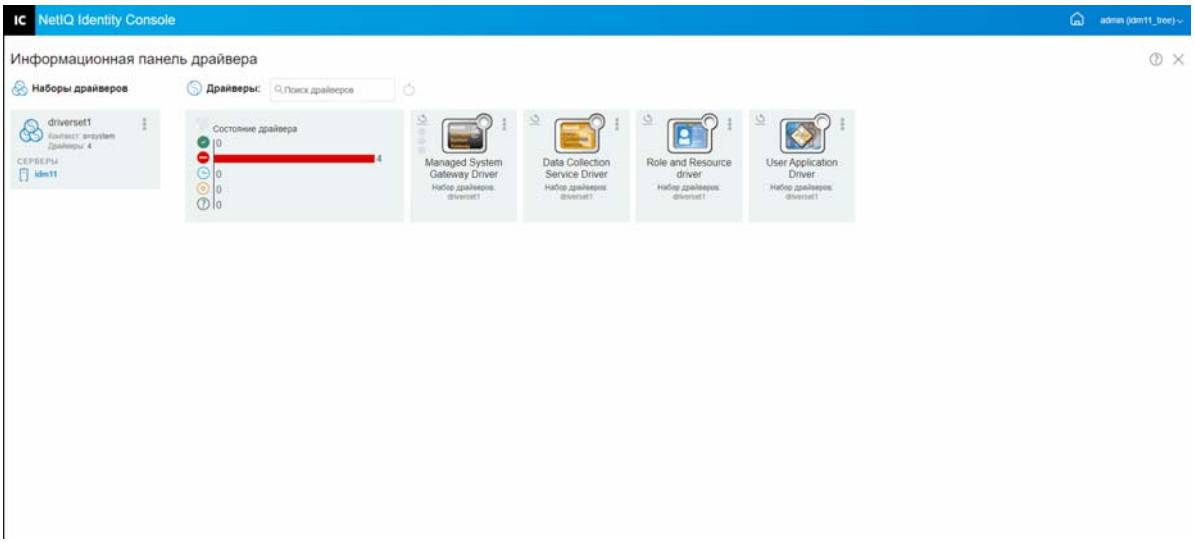
Добавление и удаление серверов

Набор драйверов одновременно может быть связан с одним или несколькими серверами. Однако в зависимости от конкретных требований с доступным сервером можно связать другой объект "Набор драйверов".

Чтобы добавить новый сервер, щелкните значок на объекте определенного набора драйверов, выберите **Добавить серверы** и укажите соответствующий сервер в контекстном браузере.

Чтобы удалить существующий сервер, выберите **Удалить сервер**.

Рисунок 21-1 *Добавление сервера в набор драйверов*

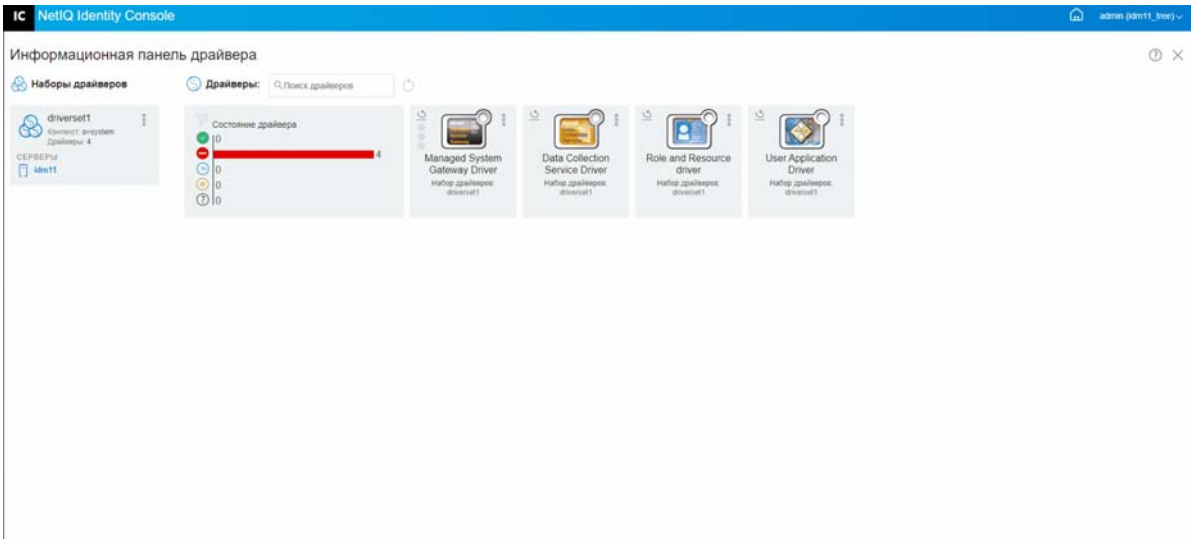


Активация набора драйверов с использованием ключа активации продукта

Перед использованием любого набора драйверов, а также тех или иных драйверов из данного набора драйверов сначала необходимо активировать его, указав код активации, отправленный на электронную почту. После покупки лицензии вы получите ключ активации от NetIQ. Порядок активации набора драйверов с использованием ключа активации

1. На главном экране Identity Console откройте вкладку **Администрирование IDM**.
2. В поле набора драйверов, который необходимо активировать, щелкните значок "Действия" , а затем щелкните **Установка активации**.
3. Если файл активации загружен на компьютер, установите флажок **Выберите файл с учетными данными**.
4. Найдите и выберите файл активации и щелкните **Передать**.
5. Как вариант, можно активировать набор драйверов, используя содержимое файла активации. Установите флажок **Введите учетные данные**.
   - **5a** Откройте файл учетных данных активации продукта и скопируйте их в буфер обмена.
   - **5b** При копировании содержимого нужно удалить все лишние строки и пробелы. Скопируйте содержимое, начиная от первого дефиса (-) учетных данных (----BEGIN PRODUCT ACTIVATION CREDENTIAL) до последнего дефиса (-) учетных данных (END PRODUCT ACTIVATION CREDENTIAL-----), и щелкните **Готово**.
6. Появится сообщение, подтверждающее активацию набора драйверов.

Рисунок 21-2 *Активация наборов драйверов*

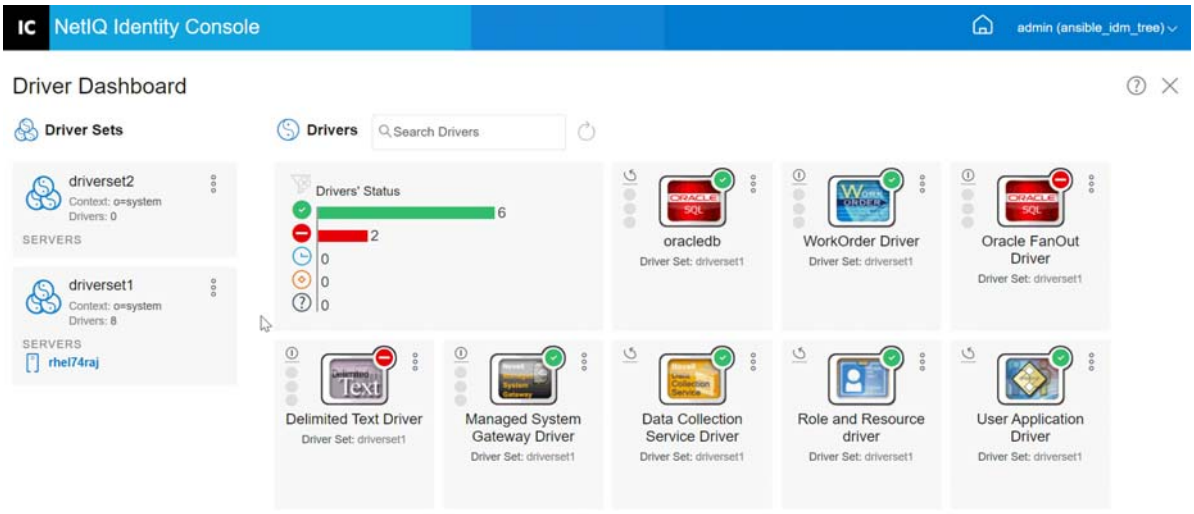


Просмотр информации об активации наборов драйверов

После активации набора драйверов необходимо проверить ее статус. Порядок проверки статуса активации набора драйверов

1. На главном экране Identity Console откройте вкладку **Администрирование IDM**.
2. В объекте "Набор драйверов", для которого необходимо проверить статус активации, щелкните значок "Действия" ⋮, а затем щелкните **Информация об активации**.
3. Откроется всплывающее окно с информацией об активации. В этом окне можно проверить информацию об активации для данного набора драйверов.

Рисунок 21-3 *Просмотр информации об активации наборов драйверов*

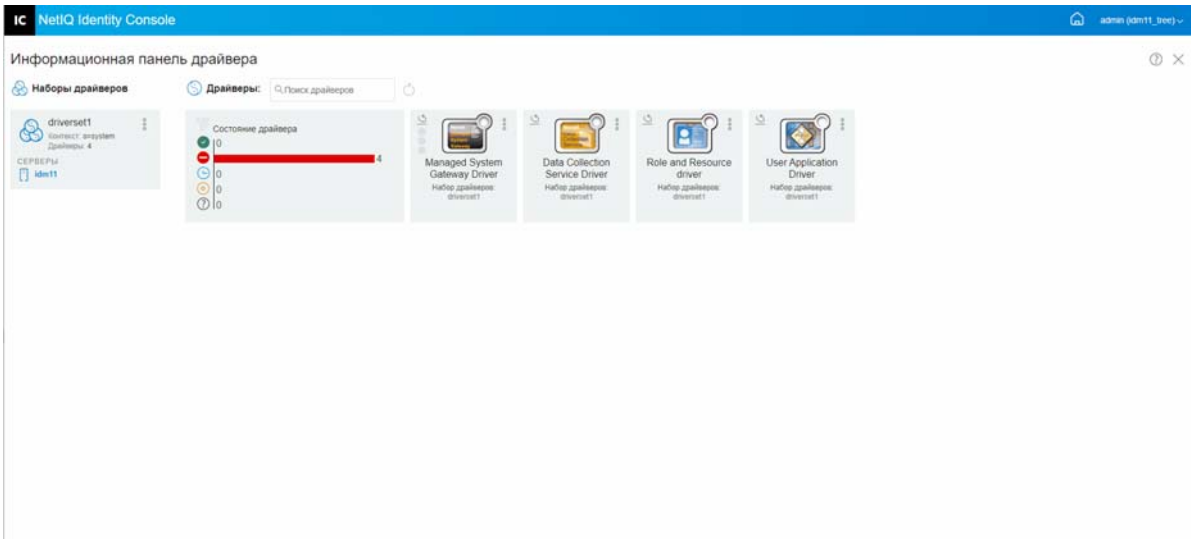


Запуск и останов драйверов

После создания драйвера он остановлен по умолчанию. Чтобы драйвер начал работать, его необходимо запустить. Identity Manager — это система, реагирующая на события, поэтому после запуска драйвера она продолжит простаивать до возникновения какого-либо события. Порядок запуска/останова драйверов.

1. На главном экране Identity Console откройте вкладку **Администрирование IDM**.
2. На правой стороне экрана щелкните объект "Набор драйверов", для которого необходимо показать все связанные с ним драйверы.
3. Щелкните значок "Действия" для нужного драйвера и выберите пункт **Запустить драйвер**.
4. Чтобы остановить объект "Драйвер", щелкните значок "Действия" для нужного драйвера и выберите пункт **Остановить драйвер**.
5. (Зависит от условий) Как вариант, можно одновременно запустить и остановить все драйверы в одном объекте "Набор драйверов". Щелкните значок "Действия" в объекте "Набор драйверов" и выберите пункт **Запустить все драйверы** или **Остановить все драйверы**.

Рисунок 21-4 *Запуск и останов драйверов*

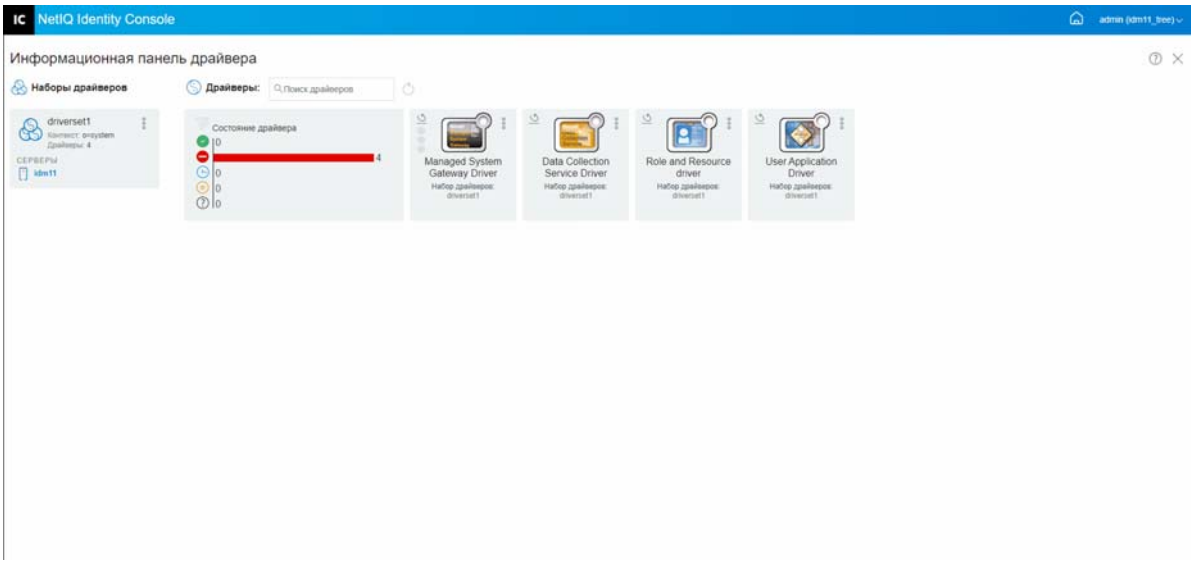


Поиск драйверов

Identity Console предоставляет возможность поиска драйверов на сервере. Порядок поиска драйвера

1. На главном экране Identity Console откройте вкладку **Администрирование IDM**.
2. Укажите имя драйвера в поле **Поиск**. На экране появится соответствующий объект "Драйвер". Чтобы обновить список драйверов, также можно щелкнуть значок .

Рисунок 21-5 *Поиск драйверов*



Фильтрация драйверов и наборов драйверов

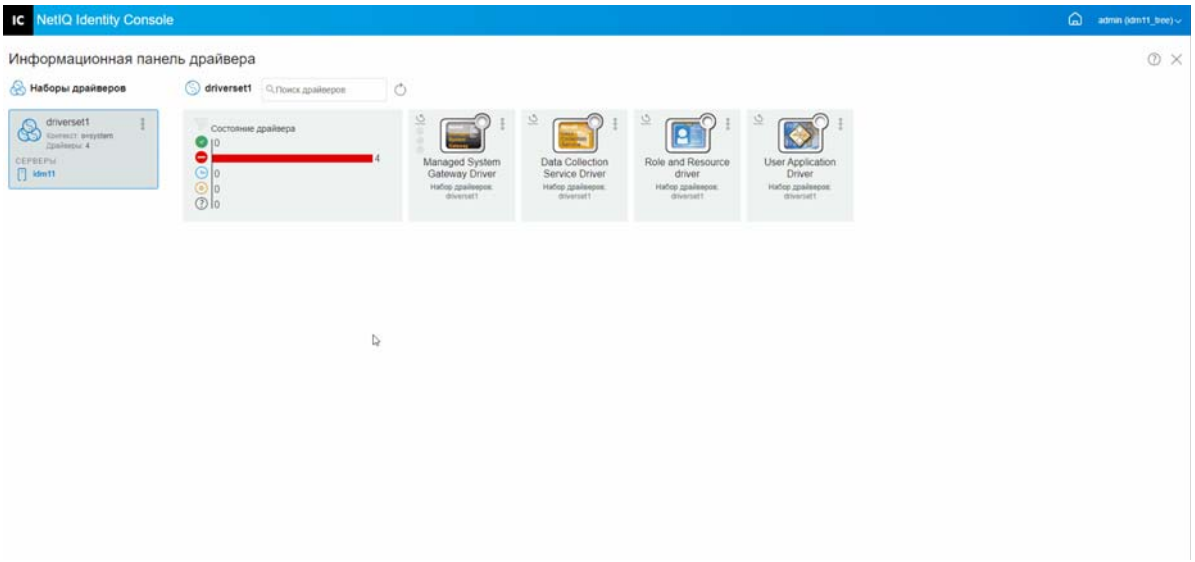
Драйверы можно отфильтровать по их состоянию на странице **Администрирование IDM**.
Порядок фильтрации драйверов

1. На главном экране Identity Console откройте вкладку **Администрирование IDM**.
2. Для фильтрации драйверов по состоянию воспользуйтесь указанными ниже значками на плитке **Состояние драйверов**:

   - Щелкните значок , чтобы показать все драйверы, запущенные на сервере.
   - Щелкните значок , чтобы показать все остановленные драйверы на сервере.
   - Щелкните значок , чтобы показать все драйверы, которые запускаются.
   - Щелкните значок , чтобы показать все драйверы, которые останавливаются.
   - Щелкните значок , чтобы показать те драйверы, которые не имеют определенного состояния. Если набор драйверов не имеет связанного с ним сервера, то для драйверов из этого набора будет отображаться состояние **Неизвестно**.

   Чтобы снять фильтр, примененный к драйверам, щелкните значок на плитке **Состояние драйверов**.
3. Наборы драйверов также можно отфильтровать на портале Identity Console. По умолчанию на портале Identity Console отображаются все драйверы, относящиеся ко всем наборам драйверов на вашем сервере. Чтобы вывести драйверы конкретного набора драйверов, необходимо выбрать соответствующий набор драйверов в списке наборов драйверов на левой стороне портала Identity Console. Чтобы отменить выбор набора драйверов, еще раз щелкните выбранный набор.

Рисунок 21-6 Фильтрация драйверов и наборов драйверов



Удаление набора драйверов

Чтобы удалить набор драйверов, выполните указанные ниже действия.

1. На главном экране Identity Console откройте вкладку **Администрирование IDM**.
2. Нажмите кнопку действий для набора драйверов, который хотите удалить.
3. Выберите **Удалить**.

Действия с драйверами

При щелчке по значку действий для определенного драйвера доступны перечисленные ниже операции.

- **Запустить драйвер**: запуск драйвера.
- **Остановить драйвер**: остановка драйвера.
- **Перезапустить драйвер**: перезапуск драйвера.
- **Удалить драйвер**: удаление драйвера.
- **Статистика**: просмотр статистики работы драйвера.
- **Копировать данные**: копирование данных драйвера с одного сервера на другой. Эта команда доступна только для многосерверных сред.

22 Управление свойствами набора драйверов

В этом разделе содержится информация о свойствах, которые являются общими для всех наборов драйверов. Это касается всех свойств ("Поименованный пароль", "Уровень протоколирования", "Инспектор набора драйверов" и т. д.).

Этот раздел содержит следующие темы:

- "Настройка наборов драйверов" на стр. 135
- "Настройка заданий и наборов драйверов" на стр. 137
- "Управление библиотеками для определенного набора драйверов" на стр. 138
- "Настройка уровней протоколирования и трассировки для наборов драйверов" на стр. 139
- "Управление инспектором набора драйверов и статистикой" на стр. 142

Настройка наборов драйверов

Порядок изменения конфигурации набора драйверов

1. Щелкните **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов**.
2. По умолчанию откроется страница **Конфигурация набора драйверов**. Параметры конфигурации набора драйверов подразделяются на следующие категории:

- "Поименованный пароль" на стр. 135
- "Значения глобальной конфигурации" на стр. 136
- "Настройка параметров среды Java" на стр. 136
- "Управление списком атрибутов со значениями" на стр. 137

Поименованный пароль

Identity Manager позволяет безопасно хранить несколько паролей для набора драйверов. Эта функциональность называется "поименованные пароли". Каждый конкретный пароль доступен до ключу или имени.

Поименованные пароли можно добавить в набор драйверов или в отдельные драйверы. Поименованные пароли для набора драйверов доступны для всех драйверов в наборе.

Чтобы использовать поименованный пароль в политике драйверов, достаточно сослаться на него по имени (а не указывать сам пароль), и ядро Identity Manager отправит пароль драйверу. Описанный в этом разделе метод хранения и извлечения поименованных паролей можно использовать с любым драйвером, не внося изменений в оболочку совместимости драйвера.

Чтобы получить доступ к поименованному паролю, выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** > **Поименованный пароль** в разделе **Конфигурация набора драйверов**.

Чтобы добавить новый поименованный пароль, щелкните значок . Чтобы удалить существующий поименованный пароль, выберите соответствующий пароль и щелкните значок .

Значения глобальной конфигурации

Отображает упорядоченный список объектов глобальной конфигурации. Объекты содержат определения расширения GCV для драйвера, который Identity Manager загружает при запуске драйвера. Объекты глобальной конфигурации можно добавить или удалить. Кроме того, можно изменить порядок исполнения объектов. Щелкните значок для сохранения значений глобальной конфигурации. Чтобы обновить список значений глобальной конфигурации, щелкните значок .

Настройка параметров среды Java

Порядок настройки параметров среды Java

1. В Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов**.
2. В разделе **Конфигурация набора драйверов** щелкните **Параметры среды Java**, чтобы показать страницу свойств, которая содержит параметры среды Java.
3. Измените следующие настройки по своему усмотрению:

   Добавления пути к классу. Укажите дополнительные пути, которые JVM будет использовать для поиска файлов пакета (`.jar`) и файлов класса (`.class`). Использование этого параметра идентично использованию команды `java -classpath`. При вводе разных путей к классу используйте в качестве разделителя точку с запятой (;) для Windows JVM и двоеточие (:) для UNIX или Linux JVM.

   Параметры JVM. Укажите дополнительные параметры для использования с JVM. Допустимые параметры см. в документации по JVM.

   Соответствующая переменная среды —`DHOST_JVM_OPTIONS`. Она указывает аргументы для JVM 1.2. Пример:

   ```
   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
   ```

   Между строками параметра в качестве разделителя используется пробел. Если пробел есть в самой строке параметра, его нужно заключить в двойные кавычки.

   Атрибут набора драйверов имеет более высокий приоритет по сравнению с переменной среды `DHOST_JVM_OPTIONS`. Эта переменная среды присоединяется к концу атрибута набора драйверов.

   Начальный размер кучи. Укажите начальный (минимальный) размер кучи, доступный для JVM. Увеличение начального размера кучи может снизить время запуска и повысить производительность. Используйте числовое значение с буквами G, M или K. Если размер не определен буквой, по умолчанию считается, что он задан в байтах. Использование этого параметра идентично использованию команды `java -Xms`.

   Соответствующая переменная среды — `DHOST_JVM_INITIAL_HEAP`. Она указывает начальный размер кучи десятичным числом байтов. Она имеет приоритет над параметром атрибута набора драйверов.

   Информацию о начальном размере кучи по умолчанию см. в документации по JVM.

Максимальный размер кучи. Укажите максимальный размер кучи, доступный для JVM. Используйте числовое значение с буквами G, M или K. Если размер не определен буквой, по умолчанию считается, что он задан в байтах. Использование этого параметра идентично использованию команды `java -Xmx`.

Соответствующая переменная среды — `DHOST_JVM_MAX_HEAP`. Она указывает максимальный размер кучи JVM десятичным числом байтов. Она имеет приоритет над параметром атрибута набора драйверов.

Информацию о максимальном размере кучи по умолчанию см. в документации по JVM.

4 Щелкните , чтобы сохранить изменения.

5 Перезапустите хранилище объектов и отношений, чтобы применить изменения.

Управление списком атрибутов со значениями

Чтобы добавить атрибуты в список атрибутов со значениями для определенного набора драйверов, выполните указанные ниже действия.

1 В Identity Console выберите модуль **Управление объектами**.

2 Выберите из раскрывающегося списка тип **DirXML-DriverSet** и нажмите кнопку "Поиск".

3 Нажмите на соответствующий набор драйверов в списке результатов.

4 Чтобы добавить добавить атрибуты без значений в список атрибутов со значениями, нажмите на значок рядом с элементом **Атрибуты со значениями** и выберите из списка соответствующие атрибуты без значений.

5 Когда все будет готово, нажмите **OK**.

Настройка заданий и наборов драйверов

Identity Console позволяет запланировать события с использованием параметра "Задания" для всех драйверов соответствующего набора драйверов.

На странице "Задания" содержится следующая информация: имя задания, его состояние (включено или отключено), время запланированного запуска и описание задания. Чтобы вывести страницу "Задания", щелкните имя задания. Щелкните значок включения/отключения в столбце "Включено", чтобы включить или отключить задание. Чтобы просмотреть полное описание задания, щелкните его имя.

Чтобы открыть страницу "Задания", на главной странице Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** и откройте вкладку **Расширенный**. Вкладка "Задания" содержит таблицу с существующими объектами задания для выбранного драйвера, для которого в записи "Драйвер" указано полное характерное имя.

На странице Job Scheduler (Планировщик задания) можно выполнить следующие задачи:

- **Запустить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .
- **Остановить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .
- **Включить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .

- **Отключить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .
- **Получить состояние**. Выберите задание, установив флажок слева от него, затем щелкните значок .
- **Удалить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .

Управление библиотеками для определенного набора драйверов

В объектах библиотеки хранятся политики и другие ресурсы, которые совместно используются одним или несколькими драйверами. Объект библиотеки можно создать в объекте набора драйверов или любого контейнера eDirectory. В дереве eDirectory может быть несколько библиотек. Драйверы могут ссылаться на любую библиотеку в дереве, пока сервер, на котором выполняется драйвер, содержит реплику чтения/записи или главную реплику объекта библиотеки.

В библиотеке могут храниться таблицы стилей, политики, правила и другие объекты "Ресурс". На них может ссылаться один драйвер или несколько драйверов.

Модуль "Управление библиотекой" позволяет выполнить следующие задачи:

- "Просмотр и удаление существующей библиотеки" на стр. 138
- "Просмотр и удаление объектов в библиотеке" на стр. 138

Просмотр и удаление существующей библиотеки

Порядок просмотра и удаления существующей библиотеки

1. В Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** > **Расширенный** > **Библиотеки**.
2. Выберите соответствующую библиотеку из списка.
3. Щелкните значок . Щелкните **ОК** для подтверждения.

Просмотр и удаление объектов в библиотеке

Можно просмотреть и удалить политики и таблицы назначений из объектов библиотеки.
Порядок удаления объектов

1. В Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** > **Расширенный** > **Библиотеки**.
2. Выберите соответствующую библиотеку из списка.
3. Чтобы удалить политики, откройте вкладку **Политики**.
4. Выберите соответствующую политику в списке и щелкните значок .
5. Чтобы удалить таблицы назначений, откройте вкладку **Таблицы назначений**.

6 Выберите соответствующую таблицу назначений в списке и щелкните значок  .

7 Щелкните **ОК** для подтверждения.

Настройка уровней протоколирования и трассировки для наборов драйверов

Чтобы настроить уровни протоколирования и трассировки для наборов драйверов, на главной странице Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** и откройте вкладку **Конфигурация протоколирования и отслеживания**. Этот раздел содержит следующие темы:

- "Настройка уровня протоколирования" на стр. 139
- "Настройка уровня трассировки" на стр. 140
- "Отслеживание сценария DirXML" на стр. 141

Настройка уровня протоколирования

Для каждого набора драйверов есть поле уровня протоколирования, в котором можно определить уровень ошибок для отслеживания. Указанный таким образом уровень определяет сообщения, которые будут доступны в журналах. По умолчанию для уровня протоколирование задано отслеживание сообщений об ошибке. (Сюда также входят сообщения о неустранимых сбоях). Для отслеживания сообщений других типов, измените уровень протоколирования. Чтобы настроить уровень протоколирования, в Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** > **Конфигурация протоколирования и отслеживания** > **Уровень протоколирования**. В представленной ниже таблице описаны настройки уровня протоколирования.

Параметр	Описание
Выключите протоколирование в журналы "Набор драйверов", "Подписчик" и "Издатель"	Отключает протоколирование для всех драйверов в объекте "Набор драйверов", подписочном канале и издательском канале.
Максимальное количество записей в журнале (50–500)	Количество записей в журнале. Значение по умолчанию: 50.

Параметр	Описание
Уровни протоколирования	Для выбора доступны следующие уровни протоколирования: ◆ **Ошибки протоколирования**. Записывать в журнал только ошибки. ◆ Ошибки и предупреждения протоколирования. Записывать в журнал ошибки и предупреждения. ◆ **Особые события протоколирования**. Записывать выбранные события. Выбор этого параметра позволяет активировать запись для следующих событий: ◆ **События ядра метакаталога** ◆ **События состояния** ◆ **События операции** ◆ **События преобразования** ◆ **События обеспечения прав доступа** ◆ **Обновлять только время последней записи в журнал**. Обновлять время последней записи в журнал. ◆ **Отключение протоколирования**. Отключить протоколирование для драйвера.

Настройка уровня трассировки

Можно настроить трассировку для конкретного набора драйверов. В зависимости от уровня трассировки, указанного для набора драйверов, в данных трассировки отображаются события, относящиеся к драйверу за период времени, когда ядро обрабатывает события. Уровень трассировки драйвера влияет только на драйвер или набор драйверов, для которых настроена трассировка. Если используется удаленный загрузчик, файл трассировки удаленного загрузчика задается непосредственно в удаленном загрузчике и содержит только данный трассировки модуля сопряжения драйвера.

Чтобы настроить трассировку для набора драйверов, выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** > **Конфигурация протоколирования и отслеживания** > **Отследить**. Настройки трассировки описаны в следующей таблице:

Параметр	Драйвер
Уровень трассировки	С повышением уровня трассировки драйвера увеличивается объем информации, которая отображается на вкладке "Отследить". Если для трассировки задан первый уровень, отображаются ошибки, но не их причины. Чтобы просмотреть данные о синхронизации пароля, задайте для уровня трассировки пятый уровень. Если выбрать параметр **Использовать настройку из набора драйверов**, значение будет взято из набора драйверов.

Параметр	Драйвер
Уровень трассировки XSL	В данных трассировки отображаются события XSL. Этот уровень трассировки следует задавать только при поиске и устранении проблем с таблицами стилей XSL. Чтобы не отображать данные XSL, задайте нулевой уровень.
Порт отладки Java	Разрешает разработчикам подключать отладчик Java. Перезапустите хранилище объектов и отношений после подключения отладчика Java.
Файл трассировки.	Укажите имя и расположение файла, в который записывается информация Identity Manager для выбранного драйвера. Если выбрать параметр **Использовать настройку из набора драйверов**, значение будет взято из набора драйверов.
Кодировка файла трассировки	Файл трассировки использует системную кодировку по умолчанию. При необходимости можно указать другую кодировку. Если выбрать параметр **Использовать настройку из набора драйверов**, значение будет взято из набора драйверов.
Ограничение по размеру для файла трассировки	Позволяет задать ограничение для файла трассировки Java. Если задать для файла неограниченный размер, его размер будет расти до тех пор, пока есть место на диске. **ПРИМЕЧАНИЕ.** Если для файла указано ограничение размера, файл трассировки будет разбиваться на несколько файлов. Identity Manager автоматически делит максимальный размер файла на десять и создает десять отдельных файлов. Общий размер этих файлов равен максимальному размеру файла трассировки. Если выбрать параметр **Использовать настройку из набора драйверов**, значение будет взято из набора драйверов.

Отслеживание сценария DirXML

Параметр отслеживания сценариев DirXML позволяет выбрать уровень трассировки для набора драйверов. Выбранный параметр применяется ко всем политикам в наборе драйверов. Для выбора доступны следующие параметры отслеживания сценария DirXML:

- Включить все отслеживания для сценария Dirxml Script
- Выключить все отслеживания для сценария Dirxml
- Включить отслеживание правила для сценария Dirxml
- Выключить отслеживание правила для сценария Dirxml

Щелкните , чтобы сохранить изменения.

Управление инспектором набора драйверов и статистикой

Для просмотра подробной информации об объектах, связанных с набором драйверов, можно использовать средство "Инспектор набора драйверов". Этот раздел содержит следующие темы:

- "Просмотр статистики набора драйверов" на стр. 142
- "Просмотр информации о версии" на стр. 143
- "Просмотр статистики по ассоциациям" на стр. 143

Просмотр статистики набора драйверов

На портале Identity Console можно просмотреть различную статистику для одного драйвера или для всего набора драйверов. Это относится к следующей статистике: размер файла кэша, размер необработанных транзакций в файле кэша, самые старые и самые последние транзакции, а также общее количество необработанных транзакций по категориям (добавление, удаление, изменение и т. д.). Порядок просмотра статистики для набора драйверов

1. В Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** > **Инспектор и статистика** > **Статистика**.
2. В раскрывающемся списке выберите соответствующий сервер.

   Откроется страница, на которой можно просмотреть статистику для всех драйверов в наборе драйверов.

   - Чтобы обновить статистику, щелкните значок .
   - Чтобы закрыть статистику для драйвера, щелкните кнопку в верхнем правом углу окна статистики драйвера.
   - Чтобы открыть статистику для всех драйверов, щелкните **Действия** > **Показать все**.
   - Чтобы свернуть список необработанных транзакций для драйвера, щелкните кнопку , расположенную над списком. Чтобы свернуть список необработанных транзакций для всех драйверов, щелкните **Действия** > **Сверните все транзакции**.
   - Чтобы развернуть список транзакций, щелкните кнопку . Чтобы развернуть список необработанных транзакций для всех драйверов, щелкните **Действия** > **Развернуть все транзакции**.
   - Чтобы закрыть информационную панель отключенных драйверов, щелкните **Действия**, затем выберите **Закрыть отключенные драйверы**.

Просмотр информации о версии

Ядро программы Identity Manager, модули сопряжения драйвера и файлы конфигурации драйвера содержат разные номера версий. Параметр "Обнаружение версии" в Identity Console помогает найти версии ядра программы Identity Manager и модулей сопряжения драйвера. Файлы конфигурации драйвера содержат собственные соглашения об именовании. Чтобы просмотреть информацию о версии, выполните следующие действия:

1. В Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** > **Инспектор и статистика** > **Обнаружение версии**.
2. Просмотрите информацию о версиях самого высокого уровня:
   - Дерево eDirectory, в котором вы выполнили аутентификацию.

     ПРИМЕЧАНИЕ. Когда сервис eDirectory используется в Identity Manager, он называется хранилищем объектов и отношений.
   - Выбранный набор драйверов.
   - Серверы, связанные с набором драйверов.

     Если набор драйверов связан с несколькими серверами, можно просмотреть информацию об Identity Manager на каждом сервере.
   - Драйверы.
3. Щелкните значок **Просмотреть**  , чтобы показать текстовое представление той же информации, которая содержится в представлении верхнего уровня.
4. Нажмите кнопку "Экспорт"  , чтобы экспортировать и сохранить текст в файл на локальном или сетевом диске.

Просмотр статистики по ассоциациям

Функция Identity Manager Association Statistics (Статистика по ассоциациям Identity Manager) позволяет найти подробную информацию об ассоциациях для удостоверений, которые управляются Identity Manager. Identity Manager использует статистику ассоциаций для получения количества ассоциаций для драйверов Identity Manager.

Чтобы получить информацию об активных, неактивных и управляемых системой объектах, запустите задание сбора статистики по ассоциациям. Можно запланировать задание сбора статистики по ассоциациям ежедневно, еженедельно, ежемесячно или ежегодно. По умолчанию запланирован еженедельный запуск задания.

На информационной панели "Статистика по ассоциациям" отображается подробная информация об ассоциациях. Как вариант, можно просмотреть подробную информацию, экспортировав ассоциации в файл.

ПРИМЕЧАНИЕ

- Количество ассоциаций для драйверов указано для конкретного сервера. Если объект связан с несколькими драйверами, количество ассоциаций отдельно рассчитывается для каждого драйвера.
- Если ассоциаций больше 200 000, рекомендуем установить для максимального размера кучи для набора драйверов значение 2 ГБ или больше. Информацию о настройке размера кучи см. в разделе "Настройка параметров среды Java" на стр. 136.

Порядок просмотра статистики по ассоциациям

1. В Identity Console выберите **Администрирование IDM** > **щелкните контекстное меню (троеточие) соответствующего набора драйверов** > **Свойства набора драйверов** > **Инспектор и статистика** > **Статистика по ассоциациям**.
2. Выберите сервер, для которого необходимо выполнить статистику по ассоциациям.
3. В поле количества ассоциаций отображается ранее рассчитанный результат.

   Identity Console показывает количество ассоциаций для активных, неактивных и управляемых системой объектов для всех драйверов, связанных с набором драйверов.

   Identity Console обрабатывает группы и подразделения как объекты, управляемые системой. В Identity Console объект считается неактивным, если атрибуту `Вход отключен` в этом объекте задано значение true и в объект не вносились изменения на протяжении последних 120 дней. Все оставшиеся объекты рассматриваются как активные управляемые объекты.
4. Чтобы получить обновленные результаты, щелкните значок .

   Когда драйвер отключен на сервере, Identity Console не отображает драйвер на панели мониторинга.
5. Щелкните значок , чтобы экспортировать подробную информацию о системе и информацию о количестве ассоциаций для драйверов, связанных с сервером.
6. Чтобы экспортировать объекты, связанные с определенным драйвером, щелкните рядом с нужными объектами и сохраните файл.

   ПРИМЕЧАНИЕ. Для разветвляющих драйверов экспортируются только уникальные объекты. Если объект связан с несколькими экземплярами разветвляющего драйвера, Identity Console отображает все счетчики ассоциаций на информационной панели. Однако если выбрать экспорт объектов в файл, Identity Console экспортирует только уникальные объекты.
7. Щелкните **Действия** и выберите нужный параметр, чтобы упорядочить информационную панель счетчиков ассоциаций.

23 Управление свойствами драйвера

В этом разделе содержится информация о свойствах, которые являются общими для всех драйверов. Это касается всех свойств ("Поименованный пароль", "Значения, присвоенные элементу управления ядром", "Уровень протоколирования" и т. д.).

Порядок изменения конфигурации драйвера

1. На главном экране Identity Console откройте вкладку **Драйверы**.
2. Щелкните соответствующую плитку драйвера для просмотра страницы конфигурации драйвера.

   По умолчанию откроется страница **Параметры подключения**. Параметры конфигурации драйвера подразделяются на следующие категории:

- "Параметры подключения" на стр. 145
- "Конфигурация драйвера" на стр. 146
- "Преобразование и синхронизация данных" на стр. 153
- "Дополнительные параметры" на стр. 158
- "Настройка уровней протоколирования и трассировки для драйверов" на стр. 160
- "Просмотр подробной информации о драйверах" на стр. 162

Параметры подключения

Параметры подключения позволяют выбрать режим выполнения драйвера (локально или удаленно).

- **Java.** Этот параметр позволяет указать имя класса Java, экземпляр которого создается для компонента сопряжения драйвера. Этот класс может находиться в каталоге классов в виде файла класса или в каталоге `lib` в виде файла `.jar`. Выберите этот параметр, чтобы запустить драйвер локально. Необходимо также указать пароль объекта "Драйвер" и предельный размер кэша драйвера. Задать новый пароль можно по ссылке **Задать пароль**.

  Например, `com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim`
- **Собственный.** Этот параметр используется для указания имени файла `.dll`, который разработан на "родном" языке (например, C++) для драйвера. Необходимо также указать пароль объекта "Драйвер" и предельный размер кэша драйвера. Задать новый пароль можно по ссылке **Задать пароль**.

  Например, `addriver.dll`
- **Подключиться к удаленному загрузчику.** Этот параметр используется, когда драйвер удаленно подключается к подключенной системе. Если этот параметр выбран, необходимо указать следующие подпараметры:
  - **Параметры подключения удаленного загрузчика**. Сюда входит подробная информация о среде удаленного загрузчика, например, имя хоста, порт подключения и т. д.

- **Пароль удаленного загрузчика**. Пароль удаленного загрузчика.
- **Пароль объекта "Драйвер":**. Пароль объекта "Драйвер". Если используется удаленный загрузчик, на этой странице необходимо ввести пароль. Удаленный загрузчик использует этот пароль для аутентификации в модуле сопряжения драйвера.

- **Аутентификация**. Эти параметры используются для аутентификации ядра программы Identity Manager Engine и серверов Remote Loader. Укажите следующие параметры:
  - **ИД аутентификации**. Укажите идентификатор аутентификации пользователя. Этот идентификатор используется для передачи информации о подписке хранилища объектов и отношений в приложении.
  - **Контекст аутентификации**. Укажите IP-адрес или имя сервера, к которому должна подключиться оболочка совместимости программы.
  - **Пароль приложения**. Параметр, который позволяет задать пароль аутентификации приложения.

После этого щелкните значок , чтобы сохранить конфигурацию.

Конфигурация драйвера

В разделе конфигурации драйвера можно настроить его параметры, например "Значения, присвоенные элементу управления ядром", "Значения глобальной конфигурации" и т. д. Изменение параметров драйвера позволяет настроить поведение драйвера в соответствии с сетевой средой. Этот раздел содержит следующие темы:

- "Параметры драйвера" на стр. 146
- "Значения глобальной конфигурации" на стр. 147
- "Значения, присвоенные элементу управления ядром" на стр. 147
- "Параметры запуска" на стр. 151
- "Поименованный пароль" на стр. 152
- "Эквиваленты по правам" на стр. 152
- "Исключенные объекты" на стр. 152
- "Управление списком атрибутов со значениями" на стр. 153

Параметры драйвера

Параметры драйвера имеют три категории — "Настройки драйвера", "Настройки подписчика" и "Параметры издателя". Эти настройки заполняются в зависимости от конфигурации драйвера. Дополнительную информацию о параметрах драйвера см. в руководстве по конкретному драйверу в документации по драйверам Identity Manager.

По окончании можно сохранить параметры, щелкнув . Чтобы задать для параметров значение по умолчанию, щелкните значок . Чтобы изменить конфигурацию драйвера с использованием файла xml, щелкните значок .

Значения глобальной конфигурации

Отображает упорядоченный список объектов глобальной конфигурации. Объекты содержат определения расширения GCV для драйвера, который Identity Manager загружает при запуске драйвера. На вкладке **Значения глобальной конфигурации** можно просмотреть или изменить объекты, используя редактор XML. Щелкните значок  для сохранения значений глобальной конфигурации. Чтобы обновить список значений глобальной конфигурации, щелкните значок  . Чтобы удалить значения глобальной конфигурации, выберите соответствующий объект GCV и щелкните значок  .

Значения, присвоенные элементу управления ядром

Значения, присвоенные элементу управления ядром — это способ для изменения определенных моделей поведения по умолчанию ядра программы Identity Manager. К этим значениям можно получить доступ, только если сервер связан с объектом "Набор драйверов".

Параметр	Описание
Subscriber channel retry interval in seconds (Интервал повторных попыток подписочного канала в секундах)	Интервал повторных попыток подписочного канала определяет частоту, с которой ядро программы Identity Manager должно заново обрабатывать кэшированную транзакцию после того, как объект "Подписочный канал" оболочки совместимости приложения вернет статус повтора.
Qualified form for DN-syntax attribute values (Полная форма для значений атрибута DN-syntax)	Полная спецификация для значений атрибута DN-syntax определяет тип представления значений атрибута DN-syntax (в полной или неполной форме с использованием косой черты). Значение ture означает, что значения представлены в полной форме.
Qualified form from rename events (Полная форма для событий переименования)	Полная форма для событий переименования позволяет указать, будет ли часть new-name событий переименования (поступает из хранилища объектов и отношений) представлена в подписочном канале с квалификаторами типа. Например, CN=. Значение ture означает, что имена представлены в полной форме.
Maximum eDirectory replication wait time in seconds (Максимальное время ожидания репликации eDirectory в секундах)	Эта настройка определяет максимальное время, в течение которого ядро программы Identity Manager ожидает репликации конкретного изменения между локальной и удаленной репликой. Это влияет только на те операции, для выполнения которых ядру программы Identity Manager необходимо связаться с удаленным сервером eDirectory в том же дереве и, возможно, дождаться завершения репликации некоторых изменений на удаленный сервер или с него. Примеры: объект перемещается, когда на сервере нет основной реплики перемещенного объекта; операции с правами в отношении файловой системы для пользователей, созданных на основе шаблона.

Параметр	Описание
Use non-compliant backwards-compatible mode for XSLT (Использовать несовместимый режим XSLT с обратной совместимостью)	Этот элемент управления определяет обработчик XSLT, используемый ядром программы Identity Manager для реализации режима с обратной совместимостью. Режим обратной совместимости приводит к тому, что процессор XSLT использует одну или несколько моделей поведения, которые несовместимы со стандартами XPath 1.0 и XSLT 1.0. Это происходит из-за необходимости обеспечить обратную совместимость с существующими таблицами стилей, которые зависят от нестандартных моделей поведения. Пример: поведение оператора XPath “!=”, когда один операнд задан узлом, а второй операнд задан не узлом, будет неправильным в выпусках DirXML в Identity Manager версии 2.0 или более ранних. Это поведение исправлено, однако исправленное поведение отключено по умолчанию этим элементом управления для обратной совместимости с существующими таблицами стилей DirXML.
Maximum application objects to migrate at once (Максимальное количество объектов приложения для разовой миграции)	Этот элемент управления используется для ограничения количества объектов приложения, которые ядро программы Identity Manager запрашивает из приложения при выполнении единичного запроса входе операции миграции объектов из приложения. Если при выполнении операции переноса из программы возникают ошибки java.lang.OutOfMemoryError, для этого параметра должно быть задано значение, которое будет меньше значения по умолчанию. По умолчанию установлено значение 50. **ПРИМЕЧАНИЕ.** Этот элемент управления не ограничивает количество объектов приложения, которые можно перенести, он просто ограничивает размер пакета.
Set creatorsName on objects created in Identity Vault (Установить creatorsName в отношении объектов, созданных в хранилище объектов и отношений)	Этот элемент управления указывает ядру программы Identity Manager, нужно ли задавать атрибуту creatorsName характерное имя этого драйвера в отношении всех объектов, созданных в хранилище объектов и отношений этим драйвером. Атрибут creatorsName позволяет легко идентифицировать объекты, созданные этим драйвером, однако это может привести к снижению производительности. Если атрибут creatorsName не задан, то по умолчанию для него задается характерное имя объекта "Сервер NCP", на котором размещен этот драйвер.
Write pending associations (Записывать отложенные ассоциации)	Этот элемент управления определяет, записывает ли ядро программы Identity Manager отложенные ассоциации в отношении объекта при обработке подписочного канала. Запись отложенных ассоциаций практически не дает преимуществ, но приводит к снижению производительности. Тем не менее этот параметр доступен для обратной совместимости.

Параметр	Описание
Use password event values (Использовать значения события пароля)	Этот элемент управления определяет источник значения, которое возвращается для атрибута nspmDistributionPassword для подписочного канала. Если этому элементу управления задано значение false, текущее значение nspmDistributionPassword получается и возвращается как значение события атрибута. Это означает, что доступно только текущее значение пароля. Это поведение по умолчанию. Если этому элементу управления задано значение true, то значение, записанное вместе с событием eDirectory, дешифруется и возвращается как значение события атрибута. Это означает, что во время события доступно старое значение пароля (если существует) и значение пароля замены. Это полезно для синхронизации паролей с определенными приложениями, которые требуют старого пароля для включения настройки нового пароля.
Retry Out of Band events (Повторные попытки синхронизации по внешнему каналу)	Этот элемент управления определяет, нужно ли выполнять повторные попытки синхронизации по внешнему каналу при получении состояния **retry** для события синхронизации по внешнему каналу. Если этому элементу управления задано значение false, не будет предприниматься повторных попыток синхронизация по внешнему каналу. Если же для него задано значение true, попытки синхронизации по внешнему каналу будут продолжаться до успешной синхронизации.
Use Rhino ECMAScript engine (Использовать ядро Rhino ECMAScript)	Позволяет задать использование ядра Rhino ECMAScript в ядре программы Identity Manager. Ядро использует Rhino в качестве ядра ECMAScript по умолчанию. По умолчанию этот элемент управления имеет значение **true**. Если задать ему значение **false**, ядро будет использовать сценарий Nashorm.
Enable Subscriber Service Channel (Включить канал сервиса подписчика)	Позволяет задать обработку ядром программы Identity Manager внешних запросов в канале службы подписчика данного драйвера. Распространенные примеры таких запросов: обновление карты кода, сбор данных и запросы от dxcmd. Если этому элементу управления задано значение true, канал отдельно обрабатывает эти запросы без вмешательства в обычную обработку событий. В настоящий момент этот элемент управления доступен только для использования с разветвляющим драйвером (включен по умолчанию).
Enable password synchronization status reporting (Включить отчеты о состоянии синхронизации пароля)	Этот элемент управления определяет, будет ли ядро программы Identity Manager сообщать состояния для событий изменения пароля в подписочном канале. Возврат сообщений о состоянии событий изменения пароля в подписочном канале позволяет таким программам, как приложение Identity Manager, отлеживать ход выполнения синхронизации изменения пароля, который должен быть синхронизирован с подключенной программой.

Параметр	Описание
Combine values from template object with those from add operation (Объединить значения из объекта шаблона со значениями из операции добавления)	Это значение определяет, будет ли ядро программы Identity Manager объединять подобные значения из шаблона создания и операции добавления при выполнении операции добавления. Если задать значение true для этого элемента управления, значения атрибута с множественными значениями шаблона будут дополнять значения того же атрибута, которые указаны в операции добавления. Если задать значение false для этого элемента управления, значения из шаблона будут игнорироваться, если для данного атрибута имеются значения в поле операции добавления.
Allow event loopback from publisher to subscriber channel (Разрешить событию замыкаться на себя из издательского канала в подписочный канал)	Это значение определяет, будет ли ядро программы позволять событию замыкаться на себя из издательского канала в подписочный канал. Если этому элементу управления задано значение false, то ядро программы Identity Manager не позволяет замыкание событий на себя. Если этому элементу управления задано значение true, ядро программы Identity Manager разрешает событиям замыкаться на себя из издательского канала в подписочный канал.
Revert to calculated membership value behavior (Сбросить до рассчитанного поведения значения членства)	Это значение определяет метод, который используется ядром Identity Manager при выполнении операций чтения и поиска, связанных с членством группы. Если этому элементу управления задано значение false (настройка по умолчанию), то ядро программы Identity Manager при чтении или поиске атрибутов "Участник" или "Членство в групп" объектов хранилища объектов и отношений будет возвращать только те значения, которые являются "статическими". Статические значения — это объекты, которые получили членство в группе путем прямого назначения через вложенную группу. Если этому элементу управления задано значение true, ядро программы Identity Manager возвращается к методу, который использовался до выпуска Identity Manager 3.6. В версиях, выпущенных до версии 3.6, при поиске ядром программы Identity Manager атрибутов "Участник" и "Участник группы". Рассчитанные значения включают в себя объекты, которым членство назначено 1) статически или 2) динамически на основании расчетов иерархии вложенной группы, используемых eDirectory. Поиск атрибутов "Участник группы" группы возвращает все объекты, непосредственно назначенные группе, или все объекты, которым назначено членство посредством вложенной группы.
Maximum time to wait for driver shutdown in seconds (Максимальное время ожидания для выключения драйвера)	Эта настройка задает максимальное время, в течение которого ядро программы Identity Manager ожидает отключения издательского канала драйвера. Если драйвер не выключится в течение указанного интервала времени, ядро программы Identity Manager прервет выполнение драйвера.

Параметр	Описание
Regular Expression escape meta-characters (Метасимволы для отграничения в регулярном выражении)	Этот элемент управления определяет метасимволы, которые будут отграничиваться при расширении локальной переменной, когда она используется в контексте регулярного выражения. Все символы, которые необходимо отграничить, должны быть добавлены в значение этого элемента управления в виде списка с разделителями-запятыми. Все метасимволы, которые отсутствуют в значении элемента управления, не будут отграничиваться при расширении локальной переменной с регулярным выражением. При использовании этого элемента управления убедитесь, что выполнены следующие условия: ◆ Значение не оставлено пустым. По умолчанию оно содержит символ ***$***. Этот символ требуется для расширения локальной переменной. ◆ Значение должно быть в виде действительного списка с разделителями-запятыми. В противном случае при оценке политики возникнут ошибки. ◆ Чтобы отграничивать все метасимволы, в значении элемента управления укажите "\,$,^,.,?,*,+,[,],(,),|". ◆ Если тот или иной метасимвол не нужно отграничивать, удалите его из значения. ◆ Чтобы отграничивать все экземпляры того или иного метасимвола, укажите искомый метасимвол с косой обратной чертой в конце (\).
Ignore Entitlement Changes of other drivers (Пропускать изменения наделения правами других драйверов)	Этот элемент управления определяет, будет ли ядро программы Identity Manager игнорировать или обрабатывать изменения наделения правами других драйверов. По умолчанию используется значение true. Это означает, что драйвер автоматически игнорирует изменения наделения правами других драйверов. Если этому элементу управления задать значение false, то изменения наделения правами других драйверов кэшируются и обрабатываются этим драйвером.
Allow Entitlement event loopback from cprs to subscriber channel (Разрешить событию "Наделение правами" замыкаться на себя из cprs в подписочный канал)	Этот элемент управления определяет, разрешает ли ядро Identity Manager событию наделения правами, сгенерированному назначением CPRS, замыкаться на себя в канал подписчика драйвера. По умолчанию задано значение false. Это означает, что событие не замыкается на себя в подписочном канале. Если для этого элемента управления задано значение true, поток событий отправляется в подписочный канал драйвера.

Параметры запуска

В разделе "Параметры запуска" можно задать состояние драйвера при запуске сервера Identity Manager.

- **Автоматический запуск**. Если выбран этот параметр, драйвер запускается при каждом запуске сервера Identity Manager.
- **Ручной**. Если выбран этот параметр, драйвер не запускается при запуске сервера Identity Manager. Драйвер необходимо запустить с портала Identity Console.
- **Отключенные**. Драйвер имеет файл кэша, в котором хранятся все события. Если драйверу задается состояние "Отключенные", этот файл удаляется и никакие новые события не записываются, пока состояние не будет изменено на "Ручной" или "Автоматический запуск".

После настройки предпочтительного параметра запуска щелкните значок для сохранения. Чтобы сбросить параметр запуска, щелкните значок .

Поименованный пароль

Identity Manager позволяет безопасно хранить несколько паролей для драйвера. Эта функциональность называется "поименованные пароли". Каждый конкретный пароль доступен до ключу или имени.

Поименованные пароли можно добавить в набор драйверов или в отдельные драйверы. Поименованные пароли для набора драйверов доступны для всех драйверов в наборе. Поименованные пароли для отдельного драйвера доступны только для данного драйвера.

Чтобы использовать поименованный пароль в политике драйверов, достаточно сослаться на него по имени (а не указывать сам пароль), и ядро Identity Manager отправит пароль драйверу. Описанный в этом разделе метод хранения и извлечения поименованных паролей можно использовать с любым драйвером, не внося изменений в оболочку совместимости драйвера.

Чтобы добавить новый поименованный пароль, щелкните значок . Чтобы удалить существующий именованный пароль, щелкните значок . Чтобы сохранить список, щелкните значок .

Эквиваленты по правам

На странице "Эквиваленты по правам" можно просмотреть или изменить список объектов, для которых драйвер является эквивалентом по правам через явное назначение. Данный объект в действительности имеет все права перечисленных объектов.

Можно добавить новый объект в список эквивалентов по правам, щелкнув значок . При добавлении объекта в список или его удалении из списка система автоматически добавляет его в свойство "Эквивалент меня по правам" данного объекта или удаляет его из этого свойства. Не нужно добавлять в список опекуна [Public] или родительские контейнеры данного объекта, поскольку данный объект уже является их неявным эквивалентом по правам.

Чтобы удалить существующий объект из этого списка, щелкните значок . Чтобы сохранить список, щелкните значок .

Исключенные объекты

Этот параметр позволяет создать список объектов, которые не будут реплицироваться в приложении. Рекомендуется добавить в список все объекты, представляющие административную функцию (например, объект Admin). Можно добавить новый объект в этот список, щелкнув значок . Чтобы удалить существующий объект из этого списка, щелкните значок . Чтобы сохранить список, щелкните значок .

Управление списком атрибутов со значениями

Чтобы добавить атрибуты в список атрибутов со значениями для определенного драйвера, выполните указанные ниже действия.

1. В Identity Console выберите модуль **Управление объектами**.
2. Выберите из раскрывающегося списка тип **Dir-XML-Driver** и нажмите кнопку "Поиск".
3. Нажмите на соответствующий драйвер в списке результатов.
4. Чтобы добавить добавить атрибуты без значений в список атрибутов со значениями, нажмите на значок + рядом с элементом **Атрибуты со значениями** и выберите из списка соответствующие атрибуты без значений.
5. Когда все будет готово, нажмите **OK**.

Преобразование и синхронизация данных

Этот раздел содержит следующие темы:

- "Представление синхронизации данных" на стр. 153
- "Фильтры атрибута класса" на стр. 155
- "ECMA Script" на стр. 156
- "Назначение обратного атрибута" на стр. 156

Представление синхронизации данных

Страница обзора драйвера подразделяется на следующие три категории:

- "Все политики" на стр. 153
- "Миграция данных в хранилище объектов и отношений" на стр. 154
- "Миграция данных из хранилища объектов и отношений" на стр. 154
- "Синхронизация объектов" на стр. 154
- "Отслеживание сценария DirXML" на стр. 154

Все политики

По умолчанию открывается страница "Все политики". Существующую политику можно импортировать в контейнер, щелкнув значок  . Кроме того, можно удалить любую политику, которая не нужна. Чтобы выбрать уровень трассировки для драйвера, щелкните значок  . Для перемещения политик вверх и вниз по списку используйте значки  и  .

ПРИМЕЧАНИЕ. Добавление и развертывание новых политик для драйверов в Identity Console не поддерживается. Мы рекомендуем вам использовать iManager и Identity Designer для добавления и развертывания новых политик.

Миграция данных в хранилище объектов и отношений

Эта задача позволяет определить критерии, которые Identity Manager использует для миграции объектов из приложения в хранилище объектов и отношений. При миграции объекта ядро метакаталога применяет к объекту все политики сопоставления, размещения и создания, а также фильтр "Издатель". Объекты переносятся в хранилище объектов и отношений с использованием порядка, указанного в списке "Класс". Этот параметр позволяет выполнить следующие задачи:

1. **Добавить класс и атрибуты**. Чтобы добавить и удалить класс и атрибуты, которые необходимо перенести, щелкните значок  . После этого выберите класс и соответствующие атрибуты, которые необходимо добавить. После выбора классов и атрибутов, щелкните **Добавить**, чтобы сохранить изменения.
2. **Изменить значение атрибута**. Чтобы изменить значение атрибута миграции, указанное при изменении списка, щелкните значок "Изменить атрибут"  .
3. **Изменить порядок в списке класса**. Чтобы изменить порядок классов в списке, воспользуйтесь кнопками  и . Объекты переносятся в хранилище объектов и отношений с использованием порядка, указанного в списке "Класс".
4. **Обновить.** Чтобы обновить список, щелкните значок  .

Миграция данных из хранилища объектов и отношений

На вкладке **Экспорт** можно выбрать контейнеры или объекты, которые необходимо перенести из хранилища объектов и отношений в программу. При миграции объекта ядро метакаталога применяет к объекту все политики сопоставления, создания и размещения, а также фильтр "Издатель".

Чтобы выполнить миграцию объектов и контейнеров из хранилища объектов и отношений в другую программу, щелкните значок  . Найдите и выберите объект для миграции, затем щелкните **ОК** для добавления объекта в список миграции. Чтобы удалить объект из списка миграции, щелкните значок  .

После выбора объектов для миграции щелкните  , чтобы начать миграцию. Ход миграции будет отображаться на экране. Чтобы остановить миграцию, нажмите кнопку  .

Синхронизация объектов

В ходе операции синхронизации выполняется поиск объектов, в которые внесены изменения, и их синхронизация. Чтобы запустить синхронизацию немедленно, выберите **Проверить все объекты**. Как вариант, можно задать дату и время запуска синхронизации.

Отслеживание сценария DirXML

Параметр отслеживания сценариев позволяет выбрать уровень трассировки для драйвера. Он также применяет настройки трассировки ко всем издательским каналам и подписочным каналам. Для выбора доступны следующие параметры отслеживания сценария DirXML:

- Включить все отслеживания для сценария Dirxml Script
- Выключить все отслеживания для сценария Dirxml

- Включить отслеживание правила для сценария Dirxml
- Выключить отслеживание правила для сценария Dirxml

Щелкните , чтобы сохранить изменения.

Фильтры атрибута класса

Фильтры атрибута класса позволяют указать классы и атрибуты, которые приложение сможет отправлять в хранилище объектов и отношений и получать из него. Если нужно, чтобы тот или иной класс был обработан ядром метакаталога, необходимо добавить класс в фильтр соответствующего канала. Кроме того, у вас есть возможность отфильтровать объекты по определенному значению атрибута. Этот параметр позволяет выполнить следующие действия:

- **Задать шаблон**. Это действие позволяет задать параметры по умолчанию для всех атрибутов, добавленных в фильтр. Щелкните значок рядом с меткой "Фильтры атрибута класса".
- **Изменить XML**. Измените настройки фильтра атрибута и классов, используя значок изменения файла XML .
- **Добавить новый класс**. Добавьте новый класс, щелкнув значок .
- **Добавить новый атрибут**. Добавьте новый атрибут, щелкнув значок .
- **Удалить класс или атрибуты**. Удалите любой класс или атрибут, щелкнув значок рядом с соответствующим классом или атрибутом.

Можно задать следующие параметры для значения класса и атрибута для обоих каналов (издательского канала и подписочного канала):

- Синхронизировать
- Игнорировать
- Оповещение
- Сбросить

Полномочия на слияние

Если атрибут не синхронизируется ни в одном канале, слияние не выполняется.

Если атрибут синхронизируется только в одном канале, то существующие значения в назначении этого канала удаляются и заменяются значениями из источника для данного канала. Если источник имеет несколько значений, а назначение может вместить только одно значение, то на стороне назначения используется только одно значение.

Если атрибут синхронизируется в обоих каналах и обе стороны могут вместить только одно значение, подключенная программа получает значения, которые хранятся в хранилище объектов и отношений (при наличии). В этом сценарии хранилище объектов и отношений получает значения из подключенного приложения.

Если атрибут синхронизируется в обоих каналах, но только одна сторона вмещает несколько значений, значение из канала с одним значением добавляется в канал с несколькими значениями (если оно еще там не присутствует). Если на одной из сторон нет значения, можно выбрать значение для добавления. Для объединения организации можно установить перечисленные ниже параметры.

- По умолчанию
- Хранилище объектов и отношений
- Приложение
- Нет

Щелкните  , чтобы сохранить изменения.

ECMA Script

Отображает упорядоченный список файлов ресурса ECMAScript. Файлы содержат функции расширения для драйвера, который загружается Identity Manager во время выполнения операции запуска драйвера. Чтобы импортировать дополнительные файлы, щелкните  , чтобы удалить существующие —  . Кроме того, можно изменить порядок исполняемых файлов. Сценарии также можно перемещать вверх и вниз по списку. Чтобы сохранить список сценариев ECMA, щелкните значок  .

Назначение обратного атрибута

Назначения обратного атрибута позволяют создавать обратные или обычные ссылки между объектами. Например, объект "Группа" включает в себя атрибут "Участники", который ссылается на все объекты "Пользователь", которые принадлежат данной группе. Аналогичным образом, каждый объект "Пользователь" включает в себя атрибут "Членство в группе", который ссылается на те объекты "Группа", в который входит этот пользователь. Чтобы ядро метакаталога обеспечивало синхронизацию атрибута "Участники" (объекта "Группа") с атрибутом "Членство в группе" (объекта "Пользователь") для всех объектов "Группа" и "Пользователь" в хранилище объектов и отношений, эти атрибуты должны быть связаны. Такие ссылки между атрибутами объекта называются назначениями обратного атрибута.

Этот модуль позволяет выполнить следующие действия:

- "Создание настраиваемых назначений обратных атрибутов" на стр. 157
- "Добавление нового назначения обратного атрибута" на стр. 157
- "Удаление назначения обратного атрибута" на стр. 157
- "Удаление атрибута из списка назначения обратных атрибутов" на стр. 157
- "Изменения порядка назначенных атрибутов" на стр. 158
- "Удаление настраиваемого назначения обратного атрибута" на стр. 158
- "Изменение XML обратного атрибута" на стр. 158

Создание настраиваемых назначений обратных атрибутов

Процедура, описанная в этом разделе, применима только в том случае, если на странице "Назначение обратного атрибута" отображается **Драйвер не содержит настраиваемых назначений обратных атрибутов. Чтобы создать основные назначения обратных атрибутов, щелкните значок "+" выше**.

1. Щелкните значок +, чтобы создать новое настраиваемое значение обратных атрибутов.
2. Отобразятся назначения атрибута драйвера по умолчанию. Теперь можно добавить назначения, изменить существующие назначения или удалить их.

Добавление нового назначения обратного атрибута

При создании назначения обратного атрибута сначала необходимо добавить один из атрибутов в список назначений обратных атрибутов.

1. Щелкните значок + рядом с раскрывающимся меню "Действия".
2. При вводе нового атрибута выберите нужный атрибут в раскрывающемся списке.
3. Укажите подробную информацию о назначениях обратных атрибутов:
   - 3a **Класс источника**. Указывает имя класса, с которым связан атрибут в списке назначений. Например, если атрибут "Членство в группе" помещен в список назначений обратных атрибутов, то связанным классом источника будет "Пользователь".
   - 3b **Класс назначения**. Указывает имя класса, связанного с атрибутом, для которого вы планируете создать обратное назначение. Например, если атрибут "Членство в группе" помещен в список назначений обратных атрибутов, то связанным классом назначения будет "Группа".
   - 3c **Обратный атрибут**. Указывает имя атрибута, для которого вы планируете создать обратное назначение.
4. Чтобы назначить атрибут другому обратному атрибуту, щелкните значок + справа от имени атрибута.

   В конец списка атрибутов добавится новый раздел для атрибута. Выберите класс источника, класс назначения и обратный атрибут.

Удаление назначения обратного атрибута

Порядок удаления назначения обратного атрибута

1. Установите флажок для назначения обратного атрибута, который необходимо удалить, перед **классом источника**.
2. Щелкните значок рядом с раскрывающимся список атрибутов.

Удаление атрибута из списка назначения обратных атрибутов

Порядок удаления атрибута из списка назначения обратных атрибутов

1. Выберите атрибут для удаления, установив флажок перед атрибутом.
2. Щелкните значок рядом с раскрывающимся списком **Действия**.

Изменения порядка назначенных атрибутов

Назначения атрибутов разрешаются в указанном порядке (сверху вниз). Назначенные атрибуты можно переместить вверх или вниз по списку, чтобы обеспечить их разрешение в правильном порядке. В общем, чем более конкретными являются назначения, тем выше они должны быть в списке. Например, назначение для атрибута "Участник" по отношению к объекту "Группа" должно быть указано перед назначением для атрибута "Участник" по отношению ко всем объектам (параметр <Any Class>).

Установите флажок перед назначенным атрибутом, который необходимо переместить, затем щелкните ↑, чтобы переместить атрибут вверх, или ↓, чтобы переместить его вниз.

Удаление настраиваемого назначения обратного атрибута

Созданные настраиваемые назначения атрибута можно удалить. Это приведет к тому, что ядро метакаталога будет использовать назначения атрибута по умолчанию для драйвера.

Чтобы удалить настраиваемое назначение обратного атрибута, щелкните значок в верхней части экрана.

Изменение XML обратного атрибута

При желании можно напрямую изменить XML для обратного атрибута. Для этого на странице "Настраиваемые назначения обратных атрибутов" щелкните значок "Изменить XML". Откроется основной редактор XML, который позволяет изменить XML. По окончании щелкните "OK" или "Отмена" для закрытия редактора XML.

Дополнительные параметры

Дополнительные параметры подразделяются на следующие категории:

- "Управление наделения правами" на стр. 158
- "Управление таблицей назначений объектов" на стр. 159
- "Управление заданиями для драйверов" на стр. 159

Управление наделения правами

Страница "Наделение правами" содержит таблицу со всеми назначениями прав, которые в настоящий момент определены в выбранном драйвере (указаны их полные характерные имена). На этой странице разрешено выполнять следующие действия:

- **Редактирование в XML**. Для изменения назначения прав в файле XML, выберите назначение прав в списке и щелкните значок. После этого установите флажок **Enable XML Editing** (Включить редактирование XML).
- **Удаление**. Чтобы удалить наделение правами, установите флажок слева от имени наделения правами, затем щелкните значок. Отобразится сообщение о необратимости операции с вопросом том, действительно ли нужно удалять выбранное наделение правами. Чтобы удалить наделение правами, щелкните **OK**. Чтобы остановить операцию,

щелкните **Отмена**. Чтобы удалить несколько наделений правами, установите несколько соответствующих флажков. Чтобы удалить все наделения правами, установите верхний левый флажок.

Управление таблицей назначений объектов

Политики Identity Manager используют таблицы назначений для назначения набора значений другому набору соответствующих значений. При установке пакета наделения правами политики этого пакета добавляются в набор политик запуска драйвера. Драйвер выполняет эти политики только один раз при запуске. Дополнительную информацию см. в разделе Mapping Table Objects (Объекты таблицы назначений) документа *NetIQ Identity Manager Driver Administration Guide* (Руководство по администрированию драйвера NetIQ Identity Manager).

Таблица назначений объектов позволяет выполнить следующие действия:

- **Изменение существующего назначения.** Чтобы внести изменения в существующую таблицу назначений объектов, щелкните нужное назначение в списке. В открывшемся экране выполните указанные ниже действия:
  - Добавьте новый столбец.

    Укажите значение для столбца, затем выберите, будет ли оно регистрозависимым или числовым.
  - Добавьте новую строку и укажите значения для нее.
  - Щелкните значок .
- **Удаление назначения**. Чтобы удалить назначение из списка, выберите нужное назначение и щелкните значок .
- **Редактирование в XML**. Чтобы изменить назначение в файле XML, выберите нужное назначение в списке и щелкните значок . После этого установите флажок **Enable XML Editing** (Включить редактирование XML).

Управление заданиями для драйверов

Identity Console позволяет запланировать события с использованием параметра "Задания" для всех отдельных драйверов.

На странице Job Scheduler (Планировщик задания) содержится следующая информация: имя задания, его состояние (включено или отключено), время запланированного запуска и описание задания. Чтобы вывести страницу задания, щелкните его имя. Щелкните значок включения/отключения в столбце "Включено", чтобы включить или отключить задание. Чтобы просмотреть полное описание задания, щелкните его имя.

Вкладка "Задания" содержит таблицу с существующими объектами задания для выбранного драйвера, для которого в записи "Драйвер" указано полное характерное имя.

На странице Job Scheduler (Планировщик задания) можно выполнить следующие задачи:

- **Запустить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .
- **Остановить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .

- **Включить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .
- **Отключить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .
- **Получить состояние**. Выберите задание, установив флажок слева от него, затем щелкните значок .
- **Удалить задание**. Выберите задание, установив флажок слева от него, затем щелкните значок .

Настройка уровней протоколирования и трассировки для драйверов

Чтобы настроить уровни протоколирования и трассировки для драйверов, на главной странице Identity Console выберите **Драйверы** > **Конфигурация протоколирования и отслеживания**. Этот раздел содержит следующие темы:

- "Настройка уровня протоколирования" на стр. 160
- "Настройка уровня трассировки" на стр. 161

Настройка уровня протоколирования

Для каждого драйвера есть поле уровня протоколирования, в котором можно определить уровень ошибок для отслеживания. Указанный таким образом уровень определяет сообщения, которые будут доступны в журналах. По умолчанию для уровня протоколирование задано отслеживание сообщений об ошибке. (Сюда также входят сообщения о неустранимых сбоях). Для отслеживания сообщений других типов, измените уровень протоколирования. Чтобы настроить уровень протоколирования, выберите **Конфигурация протоколирования и отслеживания** и откройте вкладку **Уровень протоколирования**. В представленной ниже таблице описаны настройки уровня протоколирования.

Параметр	Описание
Использовать параметры протоколирования из набора драйверов	Если выбрана эта настройка, события журналов драйверов основываются на параметрах протоколирования объекта "Набор драйверов".
Выключите протоколирование в журналы "Набор драйверов", "Подписчик" и "Издатель"	Отключает протоколирование для этого драйвера в объекте "Набор драйверов", подписочном канале и издательском канале.
Максимальное количество записей в журнале (50–500)	Количество записей в журнале. Значение по умолчанию: 50.

Параметр	Описание
Уровни протоколирования	Для выбора доступны следующие уровни протоколирования: ◆ **Ошибки протоколирования**. Записывать в журнал только ошибки. ◆ Ошибки и предупреждения протоколирования. Записывать в журнал ошибки и предупреждения. ◆ **Особые события протоколирования**. Записывать выбранные события. Выбор этого параметра позволяет активировать запись для следующих событий: ◆ **События ядра метакаталога** ◆ **События состояния** ◆ **События операции** ◆ **События преобразования** ◆ **События обеспечения прав доступа** ◆ **Обновлять только время последней записи в журнал**. Обновлять время последней записи в журнал. ◆ **Отключение протоколирования**. Отключить протоколирование для драйвера.

Настройка уровня трассировки

Можно настроить трассировку для конкретного драйвера. В зависимости от уровня трассировки, указанного для драйвера, в данных трассировки отображаются события, относящиеся к драйверу за период времени, когда ядро обрабатывает события. Уровень трассировки драйвера влияет только на драйвер или набор драйверов, для которых настроена трассировка. Если используется удаленный загрузчик, файл трассировки удаленного загрузчика задается непосредственно в удаленном загрузчике и содержит только данный трассировки модуля сопряжения драйвера.

Чтобы настроить трассировку для драйвера, выберите **Конфигурация протоколирования и отслеживания** и откройте вкладку **Отследить**. Настройки трассировки описаны в следующей таблице:

Параметр	Драйвер
Уровень трассировки	С повышением уровня трассировки драйвера увеличивается объем информации, которая отображается на вкладке "Отследить". Если для трассировки задан первый уровень, отображаются ошибки, но не их причины. Чтобы просмотреть данные о синхронизации пароля, задайте для уровня трассировки пятый уровень. Если выбрать параметр **Использовать настройку из набора драйверов**, значение будет взято из набора драйверов.

Параметр	Драйвер
Файл трассировки.	Укажите имя и расположение файла, в который записывается информация Identity Manager для выбранного драйвера. Если выбрать параметр **Использовать настройку из набора драйверов**, значение будет взято из набора драйверов.
Имя трассировки	В начало сообщений трассировки драйвера добавляется введенное значение вместо имени драйвера. Используйте этот параметр, если имя драйвера слишком длинное.
Кодировка файла трассировки	Файл трассировки использует системную кодировку по умолчанию. При необходимости можно указать другую кодировку.
Ограничение по размеру для файла трассировки	Позволяет задать ограничение для файла трассировки Java. Если задать для файла неограниченный размер, его размер будет расти до тех пор, пока есть место на диске. **ПРИМЕЧАНИЕ.** Если для файла указано ограничение размера, файл трассировки будет разбиваться на несколько файлов. Identity Manager автоматически делит максимальный размер файла на десять и создает десять отдельных файлов. Общий размер этих файлов равен максимальному размеру файла трассировки. Если выбрать параметр **Использовать настройку из набора драйверов**, значение будет взято из набора драйверов.

Просмотр подробной информации о драйверах

Для просмотра подробной информации об объектах, связанных с драйвером, можно использовать средство "Инспектор драйвера". Этот раздел содержит следующие темы:

- "Инспектор драйвера" на стр. 162
- "Инспектор кэша драйвера" на стр. 163
- "Инспектор кэша синхронизации по внешнему каналу" на стр. 164
- "Манифест драйвера" на стр. 165
- "Мониторинг работоспособности драйвера" на стр. 165

Инспектор драйвера

Порядок просмотра объектов, связанных с драйвером

1. В Identity Console выберите **Драйверы** > **Инспектор** и откройте вкладку **Инспектор драйвера**.
2. В поле **Драйвер** укажите полное характерное имя драйвера, который необходимо проверить, или щелкните значок обзора для поиска и выбора нужного драйвера.
3. После выбора драйвера для проверки щелкните **ОК**, чтобы показать страницу "Инспектор драйвера".

На этой странице отображается информация об объектах, связанных с выбранным драйвером. Можно выполнить любое из указанных ниже действий:

- **Удалить.** Удаляет ассоциацию между драйвером и объектом. Установите флажок перед объектом, с которым больше не должен быть связан драйвер, и щелкните значок  . Для подтверждения удаления щелкните **OK**.
- **Обновить.** Выберите значок обновления для этого параметра, чтобы заново считать все объекты, связанные с драйвером, и обновить информацию.
- **Показать.** Выберите количество ассоциаций, которые будут отображаться на одной странице. Можно выбрать предопределенное количество (25, 50 или 100) или указать другое количество по собственному усмотрению. По умолчанию на одной странице отображается 10 ассоциаций. Если количество ассоциаций больше отображаемого количества, для перехода между страницами ассоциаций можно воспользоваться кнопками со стрелками.
- **Действия.** Позволяет выполнить действия по отношению к объектам, связанным с драйвером. Щелкните **Действия**, затем выберите один из следующих параметров:
  - **Показать все ассоциации.** Показывает все объекты, связанные с драйвером.
  - **Показать только ассоциации "Отключенные".** Показывает все объекты, связанные с драйвером, который имеет состояние "Отключенные".
  - **Показать только ассоциации "Ручные".** Показывает все объекты, связанные с драйвером, который имеет состояние "Ручные".
  - **Показать только ассоциации "Миграция".** Показывает все объекты, связанные с драйвером, который имеет состояние "Миграция".
  - **Показать только ассоциации "Отложенные".** Показывает все объекты, связанные с драйвером, которые имеют состояние "Отложенные".
  - **Показать только ассоциации "Обработанные".** Показывает все объекты, связанные с драйвером, которые имеют состояние "Обработанные".
  - **Показать только ассоциации "Неопределенные".** Показывает все объекты, связанные с драйвером, которые имеют состояние "Неопределенные".
  - **Сводка по ассоциациям.** Показывает состояние всех объектов, связанных с драйвером.
- **Характерное имя объекта.** Показывает характерные имена связанных объектов.
- **Состояние.** Показывает состояние ассоциации объекта.
- **ИД объекта.** Показывает значение ассоциации.

Инспектор кэша драйвера

В Identity Console можно просмотреть транзакции в файле кэша драйвера. На вкладке **Инспектор кэша драйвера** отображается информация о файле кэша, включая список событий, которые подлежат обработке драйвером.

1. В Identity Console выберите **Драйверы** > **Инспектор** и откройте вкладку **Инспектор кэша драйвера**.
2. В поле **Драйвер** укажите полное характерное имя драйвера, кэш которого необходимо проверить, или щелкните значок обзора для поиска и выбора нужного драйвера. После этого щелкните **OK**, чтобы показать страницу "Инспектор кэша драйвера".

   Файл кэша драйвера можно считать только тогда, когда драйвер не запущен. Если драйвер остановлен, на странице "Инспектор кэша драйвера" будет отображаться кэш. Если драйвер выполняется, на месте записей кэша страница отображает уведомление

`Driver not stopped, cache cannot be read` (Драйвер не остановлен. Кэш невозможно прочитать). Чтобы остановить драйвер, щелкните кнопку . После этого кэш будет считан и выведен.

- **Кэш драйвера на сервере.** Здесь показан сервер, который содержит этот экземпляр файла кэша. Если драйвер выполняется на нескольких серверах, можно выбрать другой сервер в списке для просмотра файла кэша драйвера для данного сервера.
- **Значки "Запустить/Остановить драйвер"** Отображают текущее состояние драйвера и позволяют запустить или остановить его. Кэш можно считать только в то время, когда драйвер остановлен.
- **Удалить.** Выберите записи в кэше, затем щелкните значок , чтобы удалить их из файла кэша.
- **Действия.** Позволяет выполнить действия с записями в файле кэша. Щелкните **Действия**, чтобы развернуть меню, затем выберите один из следующих параметров:
  - **Очистить все кэшированные события.** Позволяет очистить все кэшированные события.
  - **Сводка кэша.** Сводка всех событий, сохраненных в файле кэша.

Просмотр сведений о подключенных системах для драйверов

Чтобы просмотреть сведения о подключенных системах для определенного драйвера, выполните указанные ниже действия.

1. В Identity Console выберите модуль **Инспектор объектов**.
2. Найдите и выберите объект драйвера, для которого хотите просмотреть подключенные системы.
3. На компьютере отобразятся сведения обо всех подключенных системах для выбранного объекта драйвера.

Инспектор кэша синхронизации по внешнему каналу

Порядок просмотра событий кэша синхронизации по внешнему каналу

1. В Identity Console выберите **Драйверы** > **Инспектор** > **Инспектор кэша синхронизации по внешнему каналу**.
2. В поле **Драйвер** укажите полное характерное имя драйвера, кэш которого необходимо проверить, или щелкните значок обзора для поиска и выбора нужного драйвера. После этого щелкните **OK**.

   Файл кэша драйвера можно считать только тогда, когда драйвер не запущен. Если драйвер остановлен, на странице "Инспектор кэша драйвера" будет отображаться кэш. Если драйвер выполняется, на месте записей кэша страница отображает уведомление `Driver not stopped, cache cannot be read` (Драйвер не остановлен. Кэш невозможно прочитать). Чтобы остановить драйвер, щелкните кнопку . После этого кэш будет считан и выведен.

   - **Имя файла кэша.** Отображает имя файл кэша.
   - **Кэш драйвера на сервере.** Здесь показан сервер, который содержит этот экземпляр файла кэша. Если драйвер выполняется на нескольких серверах, можно выбрать другой сервер в списке для просмотра файла кэша драйвера для данного сервера.

- **Значки "Запустить/Остановить драйвер"** Отображают текущее состояние драйвера и позволяют запустить или остановить его. Кэш можно считать только в то время, когда драйвер остановлен.
- **Удалить.** Выберите записи в кэше, затем щелкните значок  , чтобы удалить их из файла кэша.
- **Действия.** Позволяет выполнить действия с записями в файле кэша. Щелкните **Действия**, чтобы развернуть меню, затем выберите один из следующих параметров:
  - **Сводка кэша.** Сводка всех событий, сохраненных в файле кэша.
  - **Очистить все кэшированные события.** Позволяет очистить все кэшированные события.

Манифест драйвера

Манифест драйвера — это подобие аннотации. В нем приведена информация о том, что поддерживает драйвер, а также некоторые настройки конфигурации. Манифест драйвера должен предоставляться разработчиком драйвера. Администратору сети, как правило, не нужно менять манифест драйвера. Если администратору нужно будет изменить манифест драйвера, это можно сделать, выбрав параметр **Драйверы** > **Инспектор** > **Манифест драйвера** > **Enable XML Editing** (Включить редактирование XML).

Мониторинг работоспособности драйвера

Мониторинг работоспособности драйвера позволяет просматривать текущее состояние драйвера (зеленое, желтое или красное) и задавать действия, которые будут выполняться в ответ на переход в каждое из этих состояний.

Можно создать условия (критерии), которые определяют каждое из состояний работоспособности. Кроме того, можно задать действия, которые будут выполняться при каждом изменении состояния работоспособности драйвера. Например, если состояние работоспособности драйвера меняется с зеленого на желтое, можно перезапустить драйвер, выключить его, отправить электронное письмо лицу, которое уполномочено разрешать проблемы с драйвером.

Этот модуль позволяет выполнить следующие задачи:

- "Изменение условий, связанных с состоянием работоспособности драйвера" на стр. 165
- "Изменение действий, связанных с состоянием работоспособности драйвера" на стр. 168
- "Создание настраиваемого состояния" на стр. 169
- "Изменение настраиваемого состояния" на стр. 170

Изменение условий, связанных с состоянием работоспособности драйвера

Вы управляете условиями, которые определяют каждое состояние работоспособности драйвера. Состояние, обозначенное зеленым цветом, означает работоспособный драйвер, а состояние, обозначенное красным цветом — неисправный драйвер.

Сначала проводится оценка условий для зеленого состояния. Если они не удовлетворены, проводится оценка условий для желтого состояния. Если и они не удовлетворены, драйверу автоматически присваивается нерабочее состояние (красное).

Порядок изменения условий для состояния

1 В Identity Console откройте страницу "Конфигурация работоспособности драйвера" для драйвера, условия состояния которого необходимо изменить.

1a Откройте главную страницу Identity Console.

1b Выберите **Драйверы** > **выберите соответствующий драйвер в списке** > **Инспектор** > **Конфигурация работоспособности драйвера**.

2 Откройте вкладку для состояния ("Зеленый" или "Желтый"), в условия которого необходимо внести изменения.

На вкладке отображаются текущие условия для данного состояния работоспособности. Условия упорядочены по группам. Все группы и все условия составлены с использованием оператором И или ИЛИ. Рассмотрим следующий пример для зеленого состояния:

```
GROUP1
Condition1 and
Condition2
Or
GROUP2
Condition1 and
Condition2 and
Condition3
```

В этом примере драйверу назначается зеленое состояние, если условия GROUP1 или GROUP2 получили оценку true. Если ни одна из групп условий не получила оценку true, оцениваются условия желтого состояния.

Могут оцениваться следующие условия:

- **Состояние драйвера.** Выполняется, остановлен, запускается, не выполняется или выключается. Например, выполнение драйвера является одним из условий для зеленого состояния работоспособности драйвера.
- **Переполнение кэша драйвера.** Состояние кэша, который используется для хранения транзакций драйвера. Если драйвер находится в состоянии переполнения кэша, используется весь доступный кэш. Например, условие по умолчанию для зеленого состояния работоспособности — значение false для "Переполнение кэша драйвера", для желтого состояния — значение true для "Переполнение кэша драйвера".
- **Самые новые.** Возраст самых новых транзакций в кэше.
- **Самые старые.** Возраст самых старых транзакций в кэше.
- **Общий размер.** Размер кэша.
- **Размер необработанных.** Размер всех необработанных транзакций в кэше.
- **Необработанные транзакции.** Количество необработанных транзакций в кэше. Можно указать все типы транзакций или определенные типы транзакций (например, добавления, удаления или переименования).
- **Журнал транзакций.** Количество транзакций, обработанных на разных этапах в подписочном канале или издательском канале за определенный период времени. Это условие использует несколько элементов в следующем формате:

  <*тип транзакции*> <*расположение и период времени транзакции* > <*оператор отношения*> <*количество транзакций*>.

  - <*тип транзакции*>: определяет тип оцениваемой транзакции. Это могут быть все транзакции, добавления, удаления, переименования и т. д.

- <*расположение и период времени транзакции*>: указывает расположение в подписочном канале или издательском канале и период времени для оценки. Например, вы можете оценить общее количество транзакций, обработанных как события от издателя за последние 48 часов. По умолчанию данные истории транзакции хранятся две недели. Это означает, что нельзя указать период времени, который превышает две недели, если не изменить значение настройки Transaction Data Duration (Срок хранения данных транзакции).
- <*оператор отношения*>: задает отношение указанных транзакций к значению <количество транзакций> (равно, не равно, меньше, меньше или равно, больше, больше или равно).
- <*количество транзакций*>: указывает количество транзакций, которые используются при оценке.

Ниже приведен пример условия "Журнал транзакций".

```
<количество добавлений> <как команды издателя> <за последние 10 минут>
<меньше или равно> <1000>
```

- **Доступный журнал.** Объем данных истории транзакций, которые доступны для оценки. Основная цель этого условия — обеспечить, чтобы условие "Журнал транзакций" не вызывало сбой текущего состояния из-за недостатка данных журнала транзакций, собранных за оцениваемый период времени.

  Например, предположим вы планируете использовать условие "Журнал транзакций" для оценки количества добавлений команд издателя за последние 48 часов (пример, показанный в разделе "Журнал транзакций" выше). Однако вам нужно избежать сбоя условия, пока еще не собраны данные за 48 часов. Это может иметь место после начальной настройки конфигурация работоспособности драйвера или при перезапуске сервера драйвера (поскольку данные истории транзакции хранятся в памяти). Поэтому вы создаете группы условия, подобные указанным ниже:

  ```
  Доступный журнал группы1 <меньше> <48 часов> или Доступный журнал группы2
  <больше или равно> <48 часов> и "Журнал транзакций" <количество добавлений>
  <как команды издателя> <за последние 48 часов> <меньше> <1000>
  ```

  Данное состояние оценивается как true, если одно из условий оцениваются как true, что означает а) наличие данных менее чем за 48 часов или б) наличие данных как минимум за 48 часов и количество добавлений по команде издателя за последние 48 часов меньше 1000.

  Данное состояние оценивается как false, если оба условия оцениваются как false, что означает а) наличие данных как минимум за 48 часов и б) количество добавлений по команде издателя за последние 48 часов превышает 1000.

3 Измените критерий по своему усмотрению.

- Чтобы добавить новую группу, щелкните значок + рядом с **Группы условий**.
- Чтобы добавить условие, щелкните значок + рядом с логическими операторами (И/ИЛИ). Как вариант, можно перейти по ссылке **Добавить новое условие**.
- Чтобы изменить порядок групп условия или отдельных условий, установите флажок рядом с группой или условием, которое необходимо переместить, затем щелкните кнопки со стрелкой для его перемещения вверх и вниз. Можно использовать кнопки со стрелками для перемещения условия из одной группы в другую.

4 По окончании сохраните изменения, щелкнув кнопку **Сохранить**.

5 Чтобы изменить действия, связанные с заданными условиями, см. соответствующую процедуру в разделе "Изменение действий, связанных с состоянием работоспособности драйвера" на стр. 168.

Изменение действий, связанных с состоянием работоспособности драйвера

Можно определить действия, которые будут выполнятся при изменении состояния работоспособности драйвера. Например, если состояние меняется с зеленого на желтое, можно выключить или перезапустить драйвер, сгенерировать событие или запустить поток операций. Если же состояние меняется с желтого на зеленое, выполняются все действия, связанные с зеленым состоянием.

Действия при изменении состояния работоспособности выполняются однократно при выполнении указанных условий. В те периоды времени, когда состояние остается неизменным, никаких действий не выполняется. Если состояние меняется по причине несоответствия условиям, действия выполняются заново тогда, когда нарушенные условия снова будут удовлетворены.

1. В Identity Console откройте страницу конфигурации "Конфигурация работоспособности драйвера" для драйвера, действия которого необходимо изменить.
   1a. Откройте главную страницу Identity Console.
   1b. Выберите **Драйверы** > **выберите соответствующий драйвер в списке** > **Инспектор** > **Конфигурация работоспособности драйвера**.
2. Откройте вкладку **Зеленый**, **Желтый** или **Красный** для состояния, для которого необходимо изменить действия.
3. Щелкните значок (+) рядом с заголовком **Действия** для добавления действия, а затем выберите нужный тип действия:
   - **Запустить драйвер.** Запускает драйвер.
   - **Остановить драйвер.** Останавливает драйвер.
   - **Перезапустить драйвер.** Останавливает, а затем запускает драйвер.
   - **Очистить кэш драйвера.** Удаляет из кэша все транзакции, включая необработанные.
   - **Отправить электронное письмо.** Отправляет электронное письмо одному или нескольким получателям. Шаблон, который вы планируете использовать в электронном письме, уже должен существовать. Чтобы включить в электронное письмо имя драйвера, имя сервера и данные о текущем состоянии работоспособности, добавьте маркеры `$Driver$`, `$Server$` и `$HealthState$` в шаблон электронного письма и включите их в текст сообщения. Пример:

     ```
     The current health state of the $Driver$ driver running on $Server$ is
     $HealthState$.
     ```

     ЗАМЕЧАНИЕ. Чтобы отправить электронные письма нескольким пользователям, в качестве разделителя между их адресами используйте запятую (,). Не используйте двоеточие вместо запятой.
   - **Написать сообщение для отслеживания.** Записывает сообщение в файл журнала работоспособности драйвера или файл журнала набора драйверов, если файл трассировки не настроен для задания "Работоспособность драйвера".
   - **Сгенерировать событие.** Генерирует событие, которое может использоваться в Audit и Sentinel.
   - **Выполнить ECMAScript.** Выполняет существующий ECMAScript.

Информацию о создании сценариев ECMA см. в разделе Using ECMAScript in Policies (Использование ECMAScript в политиках) документа *NetIQ Identity Manager - Using Designer to Create Policies* (NetIQ Identity Manager: использование Designer для создания политик).

- **Запустить рабочий поток.** Запускает рабочий поток обеспечения правами доступа.
- **При ошибке.** При сбое действия определяет дальнейшие процедуры в отношении оставшихся действий, текущего состояния работоспособности и задания "Работоспособность драйвера".
  - **Изменять действия при.** Можно продолжить выполнять оставшиеся действия, остановить их выполнение или сбросить настройки до текущих. Текущая настройка применяется, только если есть несколько действий "При ошибке", и при этом вы задаете "Изменять действия при" через параметр в одном из предшествующих действий "При ошибке".
  - **Изменять состояние при.** Можно изменить текущее состояние, отклонить его или сбросить настройки до текущих. При сохранении состояния его условия продолжают оцениваться как true. При отказе от состояния его условия оцениваются как false. Текущая настройка применяется, только если есть несколько действий "При ошибке", и при этом вы задаете "Изменять состояние при" через параметр в одном из предшествующих действий "При ошибке".
  - **Изменять состояние работоспособности драйвера при.** Можно продолжить выполнять задание, прервать или отключить его или сбросить настройки до текущих. Продолжение выполнения задания приводит к тому, что задание прекращает оценивать условия для определения состояния работоспособности драйвера и выполнять какие-либо действия, связанные с этим состоянием. Прерывание или отключение задания приводит к остановке текущей активности задания и его выключению. Задание не будет запускаться снова, пока оно не будет включено. Текущая настройка применяется, только если есть несколько действий "При ошибке", и при этом вы задаете "Изменять состояние работоспособности драйвера при" через настройку в одном из предшествующих действий "При ошибке".

4 По окончании сохраните изменения, щелкнув кнопку **Сохранить**.

Создание настраиваемого состояния

Можно создать одно или несколько настраиваемых состояний для выполнения действий, независимых от текущего состояния работоспособности драйвера (зеленый, желтый, красный). При выполнении условий настраиваемого состояния, его действия выполняются независимо от текущего состояния работоспособности.

Так же, как и при изменении состояний (зеленый, желтый и красный), действия настраиваемого состояния выполняются однократно при выполнении указанных условий. В те периоды времени, когда состояние остается неизменным, никаких действий не выполняется. Если состояние меняется по причине несоответствия условиям, действия выполняются заново тогда, когда нарушенные условия снова будут удовлетворены.

1 В Identity Console откройте страницу конфигурации "Конфигурация работоспособности драйвера" для драйвера, для которого необходимо создать настраиваемое состояние:

1a Откройте главную страницу Identity Console.

1b Выберите **Драйверы** > **выберите соответствующий драйвер в списке** > **Инспектор** > **Конфигурация работоспособности драйвера**.

2 Щелкните значок + рядом со значками состояния работоспособности драйвера (зеленый, желтый и красный).

3 Следуйте инструкциям в разделах "Изменение условий, связанных с состоянием работоспособности драйвера" на стр. 165 и "Изменение действий, связанных с состоянием работоспособности драйвера" на стр. 168, чтобы определить условия и действия настраиваемого состояния.

Изменение настраиваемого состояния

Порядок изменения настраиваемых состояний

1 В Identity Console откройте страницу конфигурации "Конфигурация работоспособности драйвера" для драйвера, для которого необходимо создать настраиваемое состояние:

1a Откройте главную страницу Identity Console.

1b Выберите **Драйверы** > **выберите соответствующий драйвер в списке** > **Инспектор** > **Конфигурация работоспособности драйвера**.

2 Щелкните значок  рядом со значками состояния работоспособности драйвера (зеленый, желтый и красный).

3 Следуйте инструкциям в разделах "Изменение условий, связанных с состоянием работоспособности драйвера" на стр. 165 и "Изменение действий, связанных с состоянием работоспособности драйвера" на стр. 168, чтобы определить условия и действия настраиваемого состояния.

24 Управление статистикой набора драйверов

На портале Identity Console можно просмотреть различную статистику для одного драйвера или для всего набора драйверов. Это относится к следующей статистике: размер файла кэша, размер необработанных транзакций в файле кэша, самые старые и самые последние транзакции, а также общее количество необработанных транзакций по категориям (добавление, удаление, изменение и т. д.). Порядок просмотра статистики для набора драйверов

1. В Identity Console откройте страницу **Статистика по набору драйверов**.
2. В раскрывающемся списке выберите соответствующий сервер.

   Откроется страница, на которой можно просмотреть статистику для всех драйверов в наборе драйверов.

   - Чтобы обновить статистику, щелкните значок .
   - Чтобы закрыть статистику для драйвера, щелкните кнопку в верхнем правом углу окна статистики драйвера.
   - Чтобы открыть статистику для всех драйверов, щелкните **Действия** > **Показать все**.
   - Чтобы свернуть список необработанных транзакций для драйвера, щелкните кнопку , расположенную над списком. Чтобы свернуть список необработанных транзакций для всех драйверов, щелкните **Действия** > **Сверните все транзакции**.
   - Чтобы развернуть список транзакций, щелкните кнопку . Чтобы развернуть список необработанных транзакций для всех драйверов, щелкните **Действия** > **Развернуть все транзакции**.
   - Чтобы закрыть информационную панель отключенных драйверов, щелкните **Действия**, затем выберите **Закрыть отключенные драйверы**.

25 Проверка объектов Identity Manager

Для просмотра подробной информации об участии объекта в отношениях Identity Manager можно использовать инспектор объектов. Эти отношения включают в себя подключенные системы, которые связаны с объектом, способ передачи данных между хранилищем объектов и отношений и подключенными системами, значения атрибута, которые в текущий момент хранятся в хранилище объектов и отношений и в подключенных системах, конфигурации драйвера подключенной системы и т. д.

Чтобы проверить объекты Identity Manager, на главной странице Identity Console щелкните параметр **Инспектор объектов**. Укажите полное характерное имя объекта, который необходимо проверить, или щелкните значок обзора для поиска и выбора нужного объекта.

В разделе "Подключенные системы" отображаются все подключенные системы, с которыми связан данный объект. На странице **Инспектор объектов** можно выполнить следующие действия:

- **Добавить ассоциацию**: чтобы добавить новую ассоциацию с подключенной системой, щелкните значок +. Найдите и выберите **объект драйвера интеграции** и укажите **ИД связанного объекта**.
- **Удалить ассоциацию**: чтобы удалить ассоциацию с подключенной системой, установите флажок слева от ассоциации и щелкните значок . Чтобы удалить все ассоциации, установите флажок под столбцом "Удалить" и щелкните значок .

26 Управление потоком данных

Поток данных показывает подписочные и издательские каналы для нескольких драйверов в одном представлении. Этот параметр позволяет просмотреть и обновить владение данными для всех драйверов.

Чтобы получить доступ к табличному представлению потока данных, на главной странице Identity Console щелкните модуль **Поток данных (табличное представление)**. После этого выберите соответствующий контейнер для отображения списка драйверов.

Для управления владением данных для конкретных драйверов, выполните указанные ниже действия:

1 Каждый драйвер имеет две кнопки для управления потоком данных по подписочному каналу и издательскому каналу. Кнопка с левой стороны предназначена для управления потоком данных в издательском канале, а кнопка справа — в подписочном канале.

   1a **Синхронизировать**. Этот параметр позволяет синхронизировать определенный атрибут. После выбора этого параметра в издательском канале этот значок меняется на ↑, а в канале подписчика — на ↓.

   1b **Игнорировать**. Этот параметр позволяет остановить синхронизацию конкретного атрибута. После выбора этого параметра значок изменяется на ⊘.

   1c **Оповестить**. Этот параметр позволяет получать уведомления обо всех изменениях конкретного атрибута. Но данное изменение не синхронизируется автоматически. После выбора этого параметра значок изменяется на 🔔.

   1d **Сбросить**. Выберите этот параметр для сброса значения атрибута к значению, указанному другим каналом. После выбора этого параметра значок изменяется на ↻.

   ПРИМЕЧАНИЕ. Это значение можно задать либо для издательского канала, либо для подписочного канала. Это значение невозможно задать одновременно для обоих каналов.

   ---

27 Управление получателями наделения правами

Ссылки и результаты наделения правами поддерживаются в отношении объектов, для которых предоставлено или отозвано наделение правами. Ссылки и результаты наделения правами содержат информацию о том, предоставлено ли или отозвано наделение правами в отношении этого объекта. Получатели наделения правами — это любые объекты, которые содержат ссылки на наделение правами.

Ссылки наделения правами

Чтобы просмотреть ссылки и результаты наделения правами, на главной странице Identity Console щелкните параметр **Получатели наделения правами** и выберите "Ссылка наделения правами". Затем заполните полное характерное имя объекта, которые имеет тип `DirXML-EntitlementRecipient`. Для выбора объекта можно воспользоваться кнопкой  выбора объекта.

Результаты наделения правами

В таблице результатов наделения правами Identity Console перечислены результаты, связанные с выбранным объектом. Чтобы просмотреть связанное наделение правами, выберите характерное имя при наделении правами. Чтобы просмотреть результаты наделения правами в формате XML, выберите соответствующий идентификатор результата.

- **Заголовки столбцов в таблице результатов наделения правами**: заголовки столбцов включают полное характерное имя для наделения правами, его текущее состояние (предоставлено или отозвано), источник результатов, статус результата, сопровождающие результат сообщения, отметку времени результата и его идентификатор.
  - **Характерное имя при наделении правами**: щелкните полное характерное имя наделения правами для объекта, чтобы открыть страницу "Изменение объекта". На этой странице можно просмотреть назначенные объекту атрибуты eDirectory. Здесь также можно изменить атрибуты данного объекта. Количество категорий, отображаемых на странице "Изменение объекта", зависит от выбранного объекта.
  - **Состояние**: текущее состояние наделения правами (предоставлено или отозвано). Если подключаемый модуль найдет в тексте XML какое-то другое значение, оно будет отображено.
  - **Сообщение**: сообщение, связанное со статусом результата в DirXML. Эти данные хранятся в разделе <msg></msg> файла результатов XML. Нажмите на значение идентификатора результата, чтобы просмотреть сведения о данном результате на странице средства просмотра XML.

- **Отметка времени**: время обработки и записи результата подсистемой наделения правами. Нажмите на значение идентификатора результата, чтобы просмотреть сведения о данном результате на странице средства просмотра XML.
- **ИД результата**: нажмите на значение идентификатора результата, чтобы просмотреть сведения о данном результате на странице средства просмотра XML. Завершив просмотр результатов, нажмите кнопку "Закрыть".

Чтобы удалить запись из списка результатов наделения правами, щелкните флажок слева от нее и выберите "Удалить".

28 Управление порядками работ

Драйверы Identity Manager могут создавать порядки работ по результатам событий, обработанных драйверами. Например, если используется драйвер Human Resource (SAP HR, PeopleSof и т. д.), можно задать, чтобы он создавал порядок работ при каждом добавлении нового пользователя.

Identity Console можно использовать для создания порядков работ и управления ими для разных драйверов, которые поддерживают определенную функциональность.

- "Создание нового порядка работ" на стр. 179
- "Удаление существующего порядка работ" на стр. 180
- "Фильтрация списка порядка работ" на стр. 180

Создание нового порядка работ

Процедура создания нового порядка работ

1. На целевой странице Identity Console щелкните **Порядок работ**.
2. Чтобы создать новый порядок работ, щелкните значок +.
3. Укажите имя порядка работ и щелкните **ОК**.

   Это имя используется для объекта WorkOrder в хранилище объектов и отношений.
4. Заполните указанные ниже поля.

   Состояние. Новый порядок работ может иметь следующие состояния: **Отложенный** или **На удержании**. Как правило, порядок работ имеет состояние **На удержании**. Порядок работ можно остановить, выбрав **На удержании**. После обработки порядка работ в этом поле будет отображаться его новое состояние.

   Дата выполнения. Можно указать немедленное выполнение порядка работ драйвером или запланировать выполнение порядка работ. Чтобы запланировать дату выполнение, щелкните значок календаря. Выберите дату в календаре. Для выбора месяца, года и времени используйте стрелки.

   Повторить порядок работ. Выберите этот параметр, чтобы порядок работ мог обрабатываться несколько раз. Укажите интервал времени между повторными обработками порядка работ. Для этого выберите количество недель, дней, часов или минут. При наступлении даты удаления повторная обработка порядка работ прекратится за исключением случаев, когда он удален, изменен, или драйвер вернет сообщение об ошибке.

   Дата удаления. Используйте элемент управления календаря для выбора даты удаления порядков работ, которые настроены. Порядки работ, для которых возвращена ошибка, не удаляются, если не выбран параметр **Удалить порядок работ, даже если он с ошибкой**.

   Зависимые порядки работ. При создании нового порядка работ можно сделать его зависимым от одного или нескольких порядков работ. Щелкните , чтобы выполнить обзор и выбрать зависимые порядки работ. Чтобы удалить порядок работ из списка, выберите порядок работ и щелкните .

Тип. Это поле позволяет указать тип порядка работ. Драйвер не меняет этот атрибут. Атрибут передается через объект WorkToDo при обработке порядка работ.

Номер порядка работ. Уникальный номер порядка работ. Это значение может быть назначено сторонней корпоративной системой порядка работ (не NetIQ eDirectory), например, базой данных порядка работ.

Контактная информация. Контактная информация лица, ответственного за порядок работ.

Журнал обработки порядка работ. После обработки порядка работ журналы драйвер записывает в это поле результаты порядка работ (включительно с состоянием). Это позволит проверить текущий статус порядка работ и выявить любые проблемы, которые возникли для драйвера при попытке настроить порядок работ.

Атрибут состояния порядка работ продолжает обрабатываться, пока обрабатывается прядок работ. Порядок работ обрабатывается по истечении установленного срока. Драйвер сообщает о результатах обработки, задавая атрибуту состояния значение "Настроено", "Предупреждение" или "Ошибка". Если порядок работ имеет состояние "На удержании", порядок работ пропускается.

- **Отложенный.** Драйвер выполнит порядок работ при наступлении даты выполнения.
- **Настроено.** Порядок работ обработан.
- **Ошибка.** Драйверу не удалось выполнить порядок работ.
- **Предупреждение.** В отношении порядка работ есть предупреждение. Например, если для порядка работ есть зависимый порядок работ с более поздней датой выполнения, драйвер отправляет предупреждение.

Описание. Описание порядка работ.

Содержимое порядка работ. Данные, указанные в этом поле, используются правилами драйвера для обработки порядка работ. Например, преобразование Command Transformation может использовать XML для обработки порядка работ.

Удаление существующего порядка работ

Процедура удаления существующего порядка работ

1. На целевой странице Identity Console щелкните **Порядок работ**.
2. Выберите порядок работ для удаления.
3. Щелкните значок  .

Фильтрация списка порядка работ

Порядок фильтрации списка порядка работ

1. На целевой странице Identity Console щелкните **Порядок работ**.
2. В разделе "Управление порядком работ" щелкните **Действие**.
3. В раскрывающемся меню выберите тип фильтра:
   - **Показать все.** Выводятся все порядки работ, связанные с драйвером.
   - **Настроено.** Выводятся только настроенные порядки работ, связанные с драйвером.
   - **Ошибка.** Выводятся только порядки работ с ошибкой.
   - **На удержании.** Выводятся только те порядки работ, которых находятся на удержании.

- **Отложенный.** Выводятся те порядки работ, которые еще не обработаны.

29 Управление состоянием и синхронизацией пароля

На портале Identity Console можно проверить синхронизацию пароля и его состояние для отдельных драйверов. Для проверки на целевой странице Identity Console выберите модуль **Синхронизация пароля**.

Этот модуль позволяет выполнить следующие действия:

- "Проверка состояния синхронизации пароля" на стр. 183
- "Проверка настроек синхронизации пароля" на стр. 184

Проверка состояния синхронизации пароля

Можно определить, будет ли пароль для рассылки для определенного пользователя совпадать с паролем в подключенной системе. Выполните следующие действия для проверки состояния синхронизации пароля:

1. В Identity Console выберите пункты **Синхронизация пароля** > **Состояние пароля**.
2. Найдите и выберите пользователя, для которого нужно проверить состояние пароля.
3. Пароль может иметь следующие состояния:
   - Пароли синхронизированы.
   - Пароли НЕ синхронизированы.
   - Состояние пароля неизвестно, поскольку подключенная система недоступна для отправки запроса на проверку пароля.
   - Произошла ошибка.

ПРИМЕЧАНИЕ. Для просмотра подробных данных о каждом из вышеперечисленных состояний необходимо навести указатель мыши на состояние в столбце **Состояние пароля**.

Задача "Состояние пароля" предусматривает выполнение действия "Проверить пароль объекта". Не все драйверы поддерживают проверку пароля. Те драйверы, которые поддерживают проверку пароля, должны содержать возможность проверки пароля в манифесте драйвера. Identity Console не разрешает отправлять операции проверки пароля драйверам, в манифесте которых нет такой возможности.

Действие "Проверить пароль объекта" проверяет пароля для рассылки. Если пароль для рассылки не обновляется, то при выполнении действия "Проверить пароль объекта" может вернуться сообщение о том, что пароли не синхронизированы.

Пароль для рассылки не обновляется, если имеет место одно из следующих условий:

- Используется метод синхронизации с использованием пароля NDS для синхронизации или универсального пароля для синхронизации. Дополнительную информацию см. в разделе "Создание политики паролей с пользовательскими настройками" на стр. 115.

ПРИМЕЧАНИЕ. Действие "Состояние пароля" проверяет пароль NDS вместо универсального пароля для хранилища объектов и отношений. Поэтому если политикой паролей пользователя не определена синхронизация пароля NDS с универсальным паролем, пароли всегда будут иметь состояние несинхронизированных. Пароль для рассылки и пароль в подключенной системе могут быть синхронизированы, но состояние проверки пароля не будет точным, пока пароль NDS и пароль для рассылки не будут синхронизированы с универсальным паролем.

Проверка настроек синхронизации пароля

Синхронизация пароля позволяет синхронизировать пароли в подключенных системах с использованием Identity Manager. Чтобы просмотреть настройки синхронизации пароля для подключенных систем, выберите соответствующий набор драйверов в раскрывающемся списке.

Используя функцию синхронизации паролей, можно настроить подключенные системы для выполнения следующих действий:

- Публиковать пароли в Identity Manager.
- Подписываться на пароли из Identity Manager или других подключенных систем.
- Применять политики паролей на подключенных системах.
- Отправлять оповещения по электронной почте.

Выполните следующие действия для проверки настроек синхронизации пароля:

1. В Identity Console выберите пункты **Синхронизация пароля** > **Синхронизация пароля**.
2. Выберите набор драйверов с драйвером, настройки которого необходимо проверить.
3. Щелкните имя драйвера из списка.

   ПРИМЕЧАНИЕ. Включенные и отключенные настройки зависят от конкретного драйвера. Доступны только те настройки для функций, которые поддерживаются драйвером.

4. Проверьте, что настройки правильно заданы.

   Identity Manager принимает пароли (издательский канал). Если этот параметр включен, Identity Manager позволит перенос паролей с подключенной системы в хранилище объектов и отношений. Если этот параметр отключен, это означает, что никакие элементы `<пароля>` не разрешено переносить в Identity Manager. При чтении XML они не учитываются политикой синхронизации паролей в издательском канале.

   Эта настройка применяется к паролям пользователей, которые указаны самой подключенной системой, а также значениям пароля, которые созданы политикой в издательском канале.

   Если этот параметр включен, но параметр "Пароль для рассылки" под ним отключен, значение `<пароль>`, исходящее из подключенной системы, записывается непосредственно в универсальный пароль в хранилище объектов и отношений. Если политика паролей пользователя не активирует универсальный пароль, то пароль записывается в пароль NDS.

   Использовать пароль для рассылки для синхронизации паролей. Эта настройка доступна, только если включена настройка **Identity Manager принимает пароли (издательский канал)**.

   Если этот параметр включен, то значение пароля, исходящее из подключенной системы, записывается в пароль для рассылки. Пароль для рассылки обратим, что означает, что его можно извлечь из хранилища данных для синхронизации пароля. Он используется Identity

Manager для двунаправленной синхронизации пароля с подключенными системами. Чтобы Identity Manager мог распространять пароли с этой системы на другие системы, этот параметр должен быть включен.

Принимать пароль, только если он соответствует политике паролей пользователя.

Эта настройка доступна, только если включена настройка **Использовать пароль для рассылки для синхронизации паролей**.

Если этот параметр выбран, Identity Manager не записывает пароль из этой подключенной системы в пароль для рассылки в хранилище объектов и отношений или не публикует его в подключенные системы, если пароль не соответствует политике паролей пользователя.

Если пароль не соответствует политике паролей, включите настройку **Reset the user's password to the Distribution Password** (Сбросить пароль пользователя до пароля для рассылки), чтобы сбросить пароль пользователя в подключенной системе. Это позволяет применить политику паролей на подключенной системе, а также в хранилище объектов и отношений. Если этот параметр не выбран, пароли пользователей могут рассинхронизироваться на подключенных системах. При принятии решения о целесообразности использования этого параметра необходимо принять во внимание политики паролей подключенной системы. На некоторых подключенных системах может быть запрещено сбрасывать пароли из-за запрета повторять пароли.

Параметр **Notify the user of password synchronization failure via e-mail setting** (Уведомить пользователя о сбое синхронизации пароля по электронной почте) позволяет уведомлять пользователей о сбое установки и сброса пароля. Уведомление особенно полезно при использовании этого параметра. Если новый пароль пользователя разрешен подключенной системой, но отклонен Identity Manager из-за политики паролей, пользователь не будет знать о том, что пароль сброшен до того, пока не получит уведомление или не попытается войти на подключенную систему со старым паролем.

Всегда принимать пароль. Игнорировать политики паролей. Эта настройка доступна, только если включена настройка **Использовать пароль для рассылки для синхронизации паролей**.

Если выбран этот параметр, Identity Manager не применяет политику паролей пользователя для этой подключенной системы. Identity Manager записывает пароль с этой подключенной системы в пароль для рассылки в хранилище объектов и отношений и рассылает его другим подключенным системам независимо от соответствия политике паролей.

Приложение принимает пароли (подписочный канал). Если этот параметр включен, драйвер отправляет пароли с хранилища объектов и отношений этой подключенной системе. Это также означает, что если пользователь меняет пароль на другой подключенной системе, которая публикует пароли в пароль для рассылки в хранилище объектов и отношений, пароль меняется на этой подключенной системе.

По умолчанию для пароля для рассылки используется универсальный пароль в хранилище объектов и отношений, поэтому изменения, внесенные в универсальный пароль в хранилище объектов и отношений, распространяются и на подключенную систему.

Notify the user of password synchronization failure via e-mail (Уведомить пользователя о сбое синхронизации пароля по электронной почте). Если этот параметр включен, пользователю будет отправляться электронное письмо с уведомление о том, что пароль не синхронизирован, не задан или не сброшен. Электронное письмо, которое отправляется пользователю, основано на шаблоне. Этот шаблон предоставлен программой синхронизации паролей. Однако для работы этого шаблона необходимо настроить его и указать почтовый сервер для отправки уведомлений. Инструкции см. в

разделе Configuring E-Mail Notification (Настройка оповещения электронной почтой) документа *NetIQ Identity Manager Password Management Guide* (Руководство по управлению паролями в NetIQ Identity Manager).

5 По окончании щелкните **Сохранить** для сохранения изменений. Настройки сохраняются как глобальные конфигурационные значения.

30 Управление библиотеками

В объектах библиотеки хранятся политики и другие ресурсы, которые совместно используются одним или несколькими драйверами. Объект библиотеки можно создать в объекте набора драйверов или любого контейнера eDirectory. В дереве eDirectory может быть несколько библиотек. Драйверы могут ссылаться на любую библиотеку в дереве, пока сервер, на котором выполняется драйвер, содержит реплику чтения/записи или главную реплику объекта библиотеки.

В библиотеке могут храниться таблицы стилей, политики, правила и другие объекты "Ресурс". На них может ссылаться один драйвер или несколько драйверов.

Модуль "Управление библиотекой" позволяет выполнить следующие задачи:

- "Просмотр и удаление существующей библиотеки" на стр. 187
- "Просмотр и удаление объектов в библиотеке" на стр. 187

Просмотр и удаление существующей библиотеки

Порядок просмотра и удаления существующей библиотеки

1. В Identity Console на главной странице выберите модуль **Библиотеки**.
2. Выберите соответствующую библиотеку из списка.
3. Щелкните значок . Щелкните **ОК** для подтверждения.

Просмотр и удаление объектов в библиотеке

Можно просмотреть и удалить политики и таблицы назначений из объектов библиотеки.
Порядок удаления объектов

1. В Identity Console на главной странице выберите модуль **Библиотеки**.
2. Выберите соответствующую библиотеку из списка.
3. Чтобы удалить политики, откройте вкладку **Политики**.
4. Выберите соответствующую политику в списке и щелкните значок .
5. Чтобы удалить таблицы назначений, откройте вкладку **Таблицы назначений**.
6. Выберите соответствующую таблицу назначений в списке и щелкните значок .
7. Щелкните **ОК** для подтверждения.