

Система анализа и мониторинга состояния ИБ DATARK

Тема 6. Настройка системы управления доступом.

Общие сведения

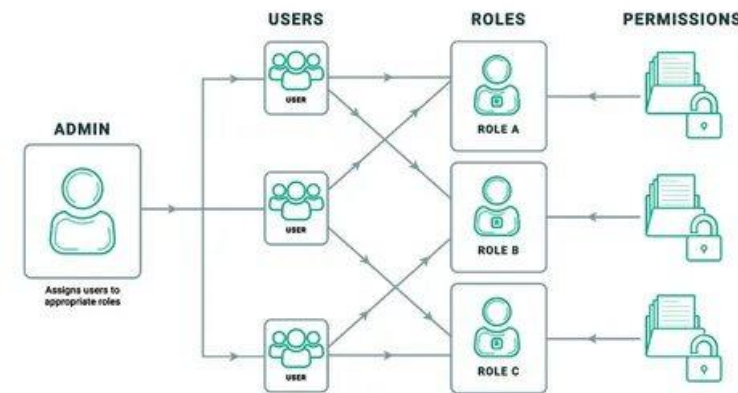
Продукт администрируется через веб-интерфейс (уровень Management).

На Supervision тоже свой веб-интерфейс (в данном курсе не рассматривается).

На сенсоре нет веб-интерфейса.

В продукте реализована ролевая модель доступа:

- **Администратор** – полный доступ
- **Инженер** – работа с активами, сетевыми соединениями, конфигурациями
- **Просмотр веб-интерфейса** – просмотр данных без возможности редактирования
- **Просмотр панели мониторинга** – только просмотр страницы «Панель мониторинга» (с бесконечным временем жизни сессии)



Таймаут по бездействию настраивается в консоли (`/usr/share/udv/datap/manager.env`, переменная **USER_SESSION_INACTIVITY_TIMEOUT** – задается в секундах (по умолчанию 600), распространяется для всех ролей, кроме «Просмотр панели мониторинга»)

Сервисный SSH-доступ здесь не рассматривается – это настраивается средствами ОС Альт СП.

Необходимо сразу внедрять DATAPK с безопасными настройками пользователей в соответствии с политикой организации – **не использовать простые пароли/пароли по умолчанию**

Учетные записи

Учетные записи в DATAPK могут быть:

- локальные
- служба каталогов (пароль проверяется LDAP-сервером), настройки LDAP – в **manager.env** переменные **LDAP_CONNECTION_STRING** (строка подключения к серверу LDAP) и **LDAP_TLS** (рекомендуется всегда ставить в **true** и использовать шифрованный LDAP), работает с MS AD и RED ADM
- централизованное управление с уровня Supervision (не рассматривается в курсе)

Создание учетной записи

Тип учетной записи *

Служба каталогов

Логин * ⓘ

test

Новый пароль *

Новый пароль

Подтверждение нового пароля *

Подтверждение нового пароля

Имя учетной записи в службе каталогов *

test@company.local

Фамилия *

Demo

Редактирование учетной записи

Тип учетной записи *

Локальная

Логин * ⓘ

datapk

Новый пароль *

.....

Подтверждение нового пароля *

.....

Имя учетной записи в службе каталогов *

example@domain.local

Фамилия *

UDV

Имя *

Demo

Отчество

Отчество

Роль пользователя *

Администратор

Парольная политика

Для локальных УЗ есть возможность настроить парольную политику и политику блокировки (Администрирование\Парольная политика).

По умолчанию парольная политика мягкая (6 символов, 1 цифра, 365 дней, 1 прошлый пароль, после 3 неуспешных попыток блокирование на 15 мин. (900 секунд)), поэтому ее надо откорректировать под нужные задачи.

Парольная политика не распространяется на учетные записи с типом «Служба каталогов» - они подчиняются настройкам контроллера домена

В централизованном управлении с Supervision подход схожий, только парольная политика и учетные записи распространяются с верхнего уровня – так же есть локальные / «служба каталогов» УЗ с доступами к определенным Managements с требуемыми ролями (и при включенном централизованном управлении локальные УЗ на данных Managements использовать нельзя).

[← Администрирование](#) | [Пользователи](#) [Парольная политика](#)

Парольная политика

Минимальная длина пароля ⓘ	12
Минимальное количество цифровых символов	2
Минимальное количество заглавных букв	3
Минимальное количество специальных символов	1
Срок действия пароля, дн ⓘ	120
Длина журнала паролей ⓘ	5
Максимальное количество попыток ввода пароля ⓘ	5
Срок блокировки при превышении попыток ввода пароля УЗ, сек ⓘ	600

Сохранить изменения

Аудит действий пользователей

Система фиксирует действия пользователей (источник **User Action Control**, типы событий **user_action_detected** и **appliance_authentication**):

- успешная/неуспешная авторизация
- успешное создание/редактирование учетных записей
- успешное редактирование парольной политики.

Дата создания	Важность	Описание
27.02.2026, 13:19:22.681	Низкая	Успешный вход в Комплекс
27.02.2026, 13:19:18.994	Низкая	Неудачная попытка входа в Комплекс
27.02.2026, 13:19:18.467	Низкая	Неудачная попытка входа в Комплекс
27.02.2026, 13:19:15.200	Низкая	Успешный выход из Комплекса
27.02.2026, 13:18:55.936	Низкая	Пользователь создан
27.02.2026, 11:44:21.663	Низкая	Успешный вход в Комплекс
27.02.2026, 11:44:16.861	Низкая	Успешный выход из Комплекса

1160001 appliance_authentication ✕
Дата создания: 27.02.2026, 10:14:21.999

Важность:

Низкая

Категория события:

—

Протокол:

—

Сообщение:

Успешный вход в Комплекс. Пользователь: Иванов Иван (datapktst); IP адрес: 10.41.56.30

[Показать полностью](#)

Действие:

—

Дополнительная информация:

—

Обоснование:

—

Идентификатор события:

04089f86-be6f-47f1-9e08-fa1543ed5bfa

Источник события:

datapk_sensor

Пользователь:

datapktst

Информация о пользователе так же фигурирует в событиях от других подсистем (редактирование инцидентов, активов, правил сессий и пр.)

Вопросы?