????????? ????????

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает настраиваемую парольную политику для локальных пользователей системы. Администратор может управлять требованиями к сложности паролей, сроками их действия, историей использования, блокировкой пользователей и параметрами пользовательских сессий.

??????????

Система должна обеспечивать контроль требований к паролям пользователей, предотвращать использование слабых паролей и обеспечивать защиту учётных записей от несанкционированного доступа.

Парольная политика позволяет реализовать требования организации к сложности паролей, срокам их действия и процедурам управления учётными записями пользователей.

??? ??? ???????????? ? Printum

Для локальных пользователей Printum поддерживает настраиваемые парольные политики.

Администратор может создавать несколько парольных политик и назначать их отдельным пользователям, группам пользователей или подразделениям.

В рамках парольной политики могут настраиваться:

- минимальная длина пароля;
- минимальное количество букв;
- минимальное количество цифр;
- минимальное количество специальных символов;
- срок действия пароля;
- период обязательной смены пароля;
- период запрета повторной смены пароля;
- максимальное количество неудачных попыток аутентификации;
- период блокировки после неудачных попыток входа;
- период блокировки неактивных пользователей;
- количество ранее использованных паролей, запрещённых к повторному использованию;
- период, в течение которого ранее использованные пароли считаются уникальными;

- требование смены пароля при первом входе в систему;
- запрет последовательностей одинаковых символов;
- запрет цифровых и алфавитных последовательностей;
- запрет использования визуально похожих символов («I», «l», «1»).

Printum поддерживает хранение истории паролей и может запрещать повторное использование ранее применявшихся паролей.

При изменении парольной политики пользователи, чьи пароли перестали соответствовать новым требованиям, могут быть обязаны сменить пароль при следующем входе в систему.

Для защиты учётных записей поддерживается автоматическая блокировка пользователя после заданного количества неуспешных попыток аутентификации.

Также поддерживается автоматическая блокировка пользователей, не использовавших систему в течение установленного периода времени.

???????? ???????

Пароли пользователей не хранятся в открытом виде.

Для хранения паролей используются стандартные механизмы Django на основе алгоритма PBKDF2 с HMAC-SHA256 и индивидуальной криптографической солью для каждого пароля.

В процессе аутентификации система выполняет проверку хэша пароля без хранения или передачи пароля в открытом виде.

??? ????????? ?? ??????????????

При использовании локальной аутентификации параметры парольной политики определяются администраторами Printum.

При использовании доменной аутентификации, LDAP, Active Directory, Kerberos или SAML требования к паролям, срокам их действия и блокировке пользователей определяются соответствующей службой аутентификации организации.

??????????? ? ???????????

Парольная политика применяется только к локальным пользователям Printum.

Для пользователей, аутентифицируемых через внешние службы каталогов или системы единого входа, требования к паролям определяются средствами соответствующей инфраструктуры.

Revision #1
Created 2026-06-08 19:39:00 UTC by DD
Updated 2026-06-08 19:39:00 UTC by DD