История изменений

Релиз 5.10

Сервис единого входа

- Исправлена ошибка, что если пользователь закрыл экран входа в момент показа ему страницы выбора аккаунта из запомненных, то при последующем запросе приложением входа в режиме prompt=none при отсутствии сессии вместо ошибки login_required показывался экран выбора аккаунта.
- Изменен разделитель, используемый в client_id, выпущенном с использованием сервиса динамической регистрации. Вместо двоеточия используется тильда.
- При входе пользователя с использованием запомненного устройства информация о запомненном устройстве обновляется в случае обновления версии ОС или браузера.
- В заголовок id_token/access_token добавлена передача идентификатора ключа подписи (kid).
- Исправлена ошибка, что если вызывать сервис /oauth/me с просроченным access_token в формате JWT, то выдается ошибка 500.
- Исправлена ошибка множественной регистрации в логах «The SCS is expired».
- Исправлена ошибка, что не срабатывал вход через внешний поставщик, если во внешнем поставщике изменился атрибут с контактом, и для этого атрибута в Blitz Identity Provider настроено правило «Мастер» для обновления при входе.
- Исправлена ошибка, что вычисляемые атрибуты не передавались в id_token после прохождения второго фактора аутентификации.

Регистрация, Личный кабинет, Восстановление пароля

- В API смены пароля (/api/v3/users/.../pswd) при использовании пользовательских access_token параметр current с текущим паролем сделан обязательным.
- Исправлена ошибка, что не работало сохранение ключа безопасности по нажатию кнопки Enter.
- Исправлено, что в личном кабинете могли отображаться не все привязки внешних поставщиков идентификации.

Консоль управления

- В настройках приложений добавлен блок «Контроль доступа», с помощью которого можно настроить правила контроля доступа пользователей в приложения. Проверка

доступа возможна на основе правил проверки значений атрибутов пользователя, членства в группах пользователей, наличия у пользователя прав доступа.

- Можно настроить передачу событий безопасности на сервер очередей Kafka.
- Можно настроить перечень событий безопасности, подлежащих регистрации.
- Добавлена поддержка запоминания в событиях безопасности геоданных по IP-адресу на основе базы данных mmdb. Можно настроить отображение геоданных в личном кабинете пользователя, а также включить геоданные в тексты писем с уведомлениями о событиях безопасности.
- Добавлена возможность администрировать группы пользователей и назначать пользователям права доступа.
- Исправлена ошибка, что при включении через процедуру входа режима select_account игнорируется параметр bip_action_hint.

Релиз 5.9

Сервис единого входа

- При входе можно показать пользователю объявление, запросить ввод атрибута, запросить предоставление согласия, запросить настройку passkey (Face ID / Touch ID).
- Добавлена возможность входа по Тинькофф ID.
- Исправлена ошибка, что был возможен вход заблокированной учетной записью при использовании метода входа по SMS как первый фактор и по ключу безопасности (passkey).
- Исправлена ошибка в работе функции принудительной смены пароля при входе.
- Исправлена ошибка, что при входе с известного устройства могло запрашиваться повторно подтверждение входа, если на первом факторе метод аутентификации отличен от входа по паролю.
- В id_token добавлена передача идентификатора сессии (sid).
- Добавлена регистрация в событиях безопасности отправки по SMS и email кодов подтверждения.
- Добавлена регистрация события безопасности о незавершенном входе, что пользователь вошел по логину и паролю, но не стал подтверждать вход и не завершил вход.
- Исправлена ошибка, что при логауте пользователю показывалась страница выхода в дизайне по умолчанию, а не в дизайне вызвавшего логаут приложения.

- Исправлена внутренняя ошибка, которая могла возникать при входе по passkey в iOS в случае, если производилась автоподстановка логина средствами iOS.
- Исправлена ошибка, что при выполнении в процедуре команды StrategyState.DENY вход в SAML-приложение завершался 500 ошибкой. Теперь показывается корректное сообщение об ошибке авторизации.
- Исправлена ошибка, что при включении пользователя в большое число групп пользователей в каталоге при входе пользователя могла возникать ошибка и-за превышения размера сессионной cookie.
- Обеспечена поддержка в Blitz Identity Provider работы с новой версией расширения Chrome для работы с электронной подписью (Blitz Smart Card Plugin, поддерживающим Chrome Manifest v.3).
- Исправлена ошибка internal error при входе по неправильному паролю с использованием OAuth 2.0 Password Credentials Flow.
- Исправлена внутренняя ошибка при входе в случае, если введенный пользователем логин не соответствует настроенным для атрибутов регулярным выражениям.
- Изменен алгоритм хранения запомненных устройств/браузеров пользователей.

Регистрация, Личный кабинет, Восстановление пароля

- В API смены пароля (/api/v3/users/.../pswd) появилась возможность сгенерировать и отправить новый пароль пользователю по SMS.

Консоль управления

- В разделе Пользователи можно просматривать настроенные пользователями ключи безопасности, создавать и отменять их привязки.
- Улучшена возможность по передаче событий аудита в SIEM.
- Обеспечена возможность делегировать хранилищу учетных записей генерации id учетной записи в процессе регистрации пользователя.
- Добавлена поддержка работы с Couchbase Server версий 6.5 и 7.0.

Релиз 5.8

Сервис единого входа

- Реализовано ограничение общего кол-ва попыток ввода кода подтверждения по SMS, HOTP, TOTP на каждую учетную запись. При превышении лимита попыток по учетной

записи выполняется временное блокирование данного способа входа / подтверждения входа для учетной записи.

- При превышении неуспешного кол-ва входов можно запросить ввод CAPTCHA.
- Для входа через внешний поставщик идентификации SAML поддержана совместимость с алгоритмом подписи, использующим SHA2-256. Поддержано использование кодировщика urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified. Поддержано использование SAML-утверждений с именами в виде URI.
- Исправлена ошибка err.selected_subject_id_not_match, которая могла возникать при входе по сеансу ОС.
- Исправлена ошибка, что мог не работать вход по платформенному ключу безопасности FIDO2 при входе с Windows Hello с некоторых ПК.
- В HTTP-сервисах аутентификации (headless) добавлена поддержка входа по QR-коду.

Регистрация, Личный кабинет, Восстановление пароля

- Реализовано ограничение общего кол-ва попыток ввода кода подтверждения по SMS, email, TOTP на каждую учетную запись при восстановлении пароля. При превышении лимита попыток по учетной записи выполняется временное блокирование данного способа подтверждения восстановления пароля для учетной записи.
- REST-сервис blitz/api/v3/users/.../audit теперь выдает события аудита, где пользователь участвует в качестве объекта, а не субъекта (те же события, что показываются пользователю в Личном кабинете).
- Исправлена ошибка, что если после успешного восстановления пользователь переправлен в приложение, а обработчик приложения долго не отвечает, то пользователь все еще видит экран восстановления пароля и может повторно нажать в нем кнопку подтверждения смены пароля.

Консоль управления

- Исправлено, что при создании не компилировалась стандартная процедура входа.
- При сохранении настроек приложения теперь можно не заполнять настройку с префиксами ссылок возврата при выходе.
- С атрибутом можно ассоциировать кастомный обработчик формата значения. Реализован обработчик для формата objectGUID в MS AD, позволяющий преобразовывать формат objectGUID в текстовый вид (например, f49dd483-0fd5-4d39-917b-2938a0b37037).

- Для метода аутентификации по ключу безопасности можно задать настройку, что вход по ключу безопасности может считаться за двухфакторную аутентификацию.
- Исправлена ошибка, что через API для регистрации нового приложения обязательно требовалось передавать заголовок If-Match со значением ETag. Теперь это делать необязательно.
- Исправлена ошибка, что не удавалось включить метод аутентификации «Подтверждение с помощью электронной почты» с помощью переключателя.

Релиз 5.7

Сервис единого входа

- Порядок отображения методов подтверждения входа можно определить с помощью «процедуры входа».
- В HTTP-сервисах аутентификации (headless) добавлена поддержка входа и подтверждения входа по SMS-коду.

Консоль управления

- Для атрибутов можно разработать собственные алгоритмы верификации.
- Добавлена возможность для обеспечения уникальности атрибута автоматически забирать его из другой учетной записи при назначении в новой.
- Добавлена возможность настраивать включение проверки PoW по HTTP-заголовку.

Релиз 5.6

Сервис единого входа

- В процедуре входа можно настроить перечень «избранных» методов входа, чтобы показывать их на странице входа, а второстепенные методы прятать среди «других» методов входа.
- Обновлены иконки социальных сетей.
- Добавлена возможность входа с помощью ключей безопасности FIDO2.
- Добавлена возможность подтверждения входа с помощью ключей безопасности FIDO2 и U2F.
- В момент входа можно запросить пользователя ввести телефон, а также подтвердить актуальность телефона.
- В процедуре входа можно получить сведения о браузере пользователя.

- Исправлена ошибка, что при повторных входах (SSO) в подключенные по SAML приложения могла возникать ошибка 500.
- Добавлена поддержка OpenID Connect Front-Channel Logout 1.0 и OpenID Connect Back-Channel Logout 1.0.
- При входе пользователя по паролю запрашивается выполнение вычислительно сложной задачи (proof of work) для защиты от подбора пароля.
- В маркер идентификации включается утверждение с идентификаторов устройства пользователя.
- При входе пользователя можно запросить его ввести или актуализировать мобильный телефон или email.
- Можно настроить вход через внешний поставщик идентификации, работающий по SAML 2.0.
- Исправлена ошибка с входом в приложения, подключенные по протоколу Simple.

Регистрация, Личный кабинет. Восстановление пароля

- Добавлена возможность запросить тест CAPTCHA в страницу регистрации.
- Добавлена возможность запросить тест CAPTCHA в страницу восстановления пароля.
- Исправлена ошибка, что могла зациклиться обработка задач отправки email при использовании некорректного значения email.
- При отображении устройств в личном кабинете теперь показывается статус устройства (запомнен ли вход на устройстве, запомнено ли прохождение двухфакторной аутентификации на устройстве) в виде цветового индикатора.
- В REST-сервис blitz/api/v3/users/.../audit добавлен опциональный параметр ua, позволяющий получать распарсенные сведения о UserAgent пользователя.

Консоль управления

- Добавлена возможность быстрого перехода из события аудита к карточке пользователя, группы пользователей или приложения, а также из карточки пользователя к событиям аудита.
- Добавлена возможность сконфигурировать порядок отображения атрибутов в карточке пользователя, а также задать вместо системных имен атрибутов пользовательские имена атрибутов.

Релиз 5.3.1

Сервис единого входа

- Добавлена возможность входа с помощью цифрового профиля ЕСИА (опция). В момент входа через госуслуги запрашивается согласие на доступ к сведениям из цифрового профиля гражданина.
- Исправлена ошибка, что при входе через Apple ID с доверенного устройства Blitz Identity Provider мог повторно запросить пользователя пройти подтверждение входа.
- Исправлена ошибка 500 при вызове подключенного по SAML приложения с использованием IdP-Initiated SSO.
- Исправлена ошибка, что при настройке внешнего метода аутентификации для первого фактора в вызов сервиса внешнего метода аутентификации передавался одинаковый идентификатор запроса. Теперь при каждом вызове генерируется уникальный идентификатор запроса.
- Исправлена ошибка с вызовов в процессе входа вспомогательного приложения, что для успешного входа приложение должно было обеспечить возврат в течение 15 секунд. Теперь время работы вспомогательного приложения можно регулировать, и по умолчанию приложению предоставляется 300 секунд.
- При обработке URL возвратов выполняется проверка, что в параметры URL возврата не встроены JS-конструкции. URL-возврата с встроенными JS теперь не обрабатываются.
- Оптимизирована работа счетчика отслеживания времени последнего входа. Теперь счетчик не обновляется при SSO-входах, чтобы избежать повышенной нагрузки на БД. Также добавлена возможность отключения регистрации счетчика отслеживания времени последнего входа (если не нужно использовать функцию автоматической блокировки учетной записи по неактивности).
- С поля ввода кода подтверждения при прохождении аутентификации убрано отображение всплывающей подсказки.
- Исправлена ошибка, что мог не работать вход в SAML-приложение при очень длинном ID пользователя (длиной более 200 символов). Такое, в частности, наблюдалось при настройке входа в Cisco ISE.
- Исправлена ошибка, что на LDAP могла создаваться избыточная нагрузка на поиск учетных записей для проверки уникальности атрибутов в результате вызова через Blitz операций регистрации учетных записей пользователей или изменения уникальных атрибутов в учетной записи.
- Исправлена ошибка, что мог не работать вход в приложения, подключенные по WS-Federation.

- Исправлена ошибка, что при вызове проверки логина/пароля через headless API по ошибке можно было различить ситуации неправильного логина и неправильного пароля. Теперь для обеих ситуаций возвращается единая ошибка invalid_credentials.

Регистрация, Личный кабинет. Восстановление пароля

- Исправлена ошибка, что если в процедуре входа, настроенной для Личного кабинета, вызывался запрет входа (DENY), то пользователю отображалась некрасивая ошибка 401 с пустым экраном. Теперь показывается страница с текстом ошибки в дизайне личного кабинета.
- Добавлена возможность проверки CAPTCHA на веб-страницу запроса восстановления забытого пароля.
- Исправлено, что привязки внешних поставщиков в личном кабинете теперь могут отображаться даже при отсутствии индекса users_fed в БД Couchbase. Оптимизация позволяет уменьшить количество нужных для работы Blitz Identity Provider индексов.
- Исправлена ошибка, что не работал REST API для привязки социальной сети (/api/v2/users/current/fa/bind). Вызов сервиса приводил к 500 ошибке.

Консоль управления

- В меню «Поставщики идентификации» появилась возможность расширенной настройки правил привязки внешних учетных записей к учетной записи в Blitz Identity Provider для выбранных типов поставщиков идентификации. В случае расширенного режима теперь можно запрограммировать через Java свою логику привязки – указать правила сопоставления учетных записей, правила маппинга атрибутов. Переключение между базовым и расширенным режимом выполняется переключателем в блоке «Связывание учетных записей».
- В меню «Сообщения» в блоке «Уведомления» появилась возможность настраивать по каждому типу уведомления используемые каналы уведомления (SMS или email).
- Исправлен перевод интерфейса на английский – добавлены недостающие строки перевода.
- Обновлены сведения, возвращаемые сервисов /oauth/.well-known/openid-configuration. Добавлена выдача блоков response_modes_supported, grant_types_supported, service_documentation, ui_locales_supported, introspection_endpoint, code_challenge_methods_supported. Все кроме service_documentation заполняется автоматически. Значение для service_documentation берется из настройки serviceDocumentationUrl из блока oauth конфигурационного файла blitz.conf.

- Появилась возможность гибко настраивать отображение кнопок дополнительных методов входа. Можно разделить методы на избранные и второстепенные. Можно настроить порядок и внешний вид отображаемых кнопок вызова внешних методов входа, используемые надписи и отображаемые иконки методов. Для экрана запроса второго фактора аутентификации можно отображать сразу все доступные пользователю методы подтверждения входа в виде кнопок.
- В меню «Пользователи» при отображении настроек найденной учетной записи добавлено отображение устройств пользователя и возможности удаления устройств из запомненных.
- С использованием процедур привязки внешних поставщиков идентификации стало возможным управлять правилами привязки не только при входе, но и при привязке через личный кабинет.
- Добавлена возможность управлять настройками приложений через REST API (опция).
- Во все уведомления, отправляемые по SMS и email, теперь можно добавить время события и имя приложения, вызвавшего событие.
- Исправлена ошибка, что при удалении SAML-приложения некорректно изменялись внутренние конфигурационные файлы attribute-filter.xml и relying-party.xml, из-за чего сервис blitz-idp мог не запуститься при перезапуске.
- Для внешних поставщиков идентификации в конфигурационном файле blitz.conf можно задать отличные от стандартных адреса вызова обработчиков внешних поставщиков. Это полезно, если вызов социальных сетей выполняется не напрямую, а через proxy-сервер.
- Исправлена ошибка, что при создании ошибочных заявок на отправку писем (например, на несуществующие адреса) могло привести к накоплению в очередях RabbitMQ избыточных заявок на отправку и многократным циклическим повторным попыткам обработки ошибочных заявок.
- Исправлена ошибка, что при работе Blitz с СУБД PostgreSQL изменение режима уровня аутентификации через консоль управления могло завершиться ошибкой.
- Исправлено, что в отправляемые уведомления теперь для ОС Windows добавляется версия ОС.
- Исправлена ошибка логирования, что в логи попадали избыточные ошибки вида «Method ... not found in the first factor state».
- Добавлена возможность настройки срока жизни токена, защищающего от CSRF-атак. Улучшено логирование ошибки «Bad CSRF token detected».

- Добавлена возможность загрузки описаний HOTP-устройств в формате Aladdin JMS Webpass. Добавлена поддержка использования HOTP с SHA-256 и длиной кода подтверждения 6-8 цифр.

Релиз 5.2.4

Сервис единого входа

- Чекбокс «Чужой компьютер» заменен на ссылку-инструкцию «Используйте инкогнито для входа с чужого устройства».
- Изменена логика запоминаний устройств. Теперь устройство входа запоминаются всегда (раньше запоминались только при убранном чекбоксе «Чужой компьютер»). После входа и прохождения двухфакторной аутентификации можно настроить запрос пользователя, доверяет ли он устройству. С доверенных устройств можно настроить, чтобы при повторных входах не запрашивалось подтверждение входа.
- Поддержан режим запоминания нескольких аккаунтов при входе (включие режима доступно через конфигурационный файл). Для переключения между аккаунтом без выхода из предыдущего аккаунта можно вызвать Authorization Endpoint с параметром prompt=select_account. При входе пользователю показывается список запомненных аккаунтов, можно выбрать любой из показанных для входа или войти новым аккаутом. С экрана выбора аккаунта для входа можно сделать выход из запомненного аккаунта или удалить запомненный аккаунт из списка.
- Изменено отображение запомненного пользователя. Теперь можно настроить отображение атрибутов запомненного аккаунта в две строки, а также включить отображение буквенного аватара, соответствующего имени аккаунта.
- Добавлена возможность входа по QR-коду. Blitz Identity Provider на странице входа отображает на ПК QR-код для подтверждения входа. Доверенное мобильное приложение (самостоятельно разрабатывается Заказчиком) может считать QR-код, запросить у пользователя подтверждение входа, и вызвать в Blitz специальное API, что позволит подтвердить вход пользователя на другом устройстве.
- Исправлены уведомления о входе с неизвестного устройства. Теперь уведомления приходят при входах любым способом (не только по логину/паролю), когда пользователь впервые входит с нового устройства. Устройства запоминаются в профиле пользователя на заданный в настройках срок. Если с устройства не будет осуществлен вход длительное время, то устройство будет удалено из запомненных.

- При сохранении в браузере ссылки на страницу входа теперь в ссылке запоминается контекст входа. При переходе по сохраненной ссылке больше не будет показываться ошибка, а пользователя направят на вход в приложение, при входе в которое первоначально была сохранена ссылка.
- Добавлена возможность входа по Apple ID.
- Реализован обработчик /oauth/logout, функционирующий в соответствии со спецификацией OpenID Connect RP-Initiated Logout 1.0 и умеющий принимать и обрабатывать переданные на вход параметры id_token_hint, post_logout_redirect_uri, state.
- В тексты уведомлений о событиях безопасности можно добавлять дату события, имя приложения, имя устройства (ОС и браузер), связанных с событием.

Консоль управления

- Исправлено отображение тэга
 при показе атрибутов пользователей в таблицах с правами пользователя.
- Исправлено распознавание браузера Microsoft Edge при регистрации событий аудита.

Релиз 5.0.0

Сервис единого входа

- Исправлена ошибка, что при вводе кода подтверждения при прохождении проверки второго фактора аутентификации, если ввод кода был сделан через нажатие Enter, а не через клик, то вход завершался ошибкой из-за дублирования отправки формы.
- Исправлена ошибка, что не работало назначение права change_role на учетную запись при вызове API с access_token, полученным на динамические client_id/client_secret.

Регистрация, Личный кабинет, Восстановление пароля

- В страницы регистрации пользователей и восстановления пароля добавлена защита от CSRF.
- Исправлено, что при открытии страницы регистрации не ставился автофокус на верхнее поле страницы.
- Доработан сервис HTTP PUT /reg/api/v1/users, что теперь по результатам успешной регистрации сервис возвращает значение cookie css, установка которой позволит обеспечить автоматический вход пользователя в приложение по результатам регистрации учетной записи.

- Исправлено, что если при восстановлении пароля настроена необходимость ввода значения проверочного атрибута, то поле сделано требующим обязательного ввода.

Консоль управления и изменения в установке

- Сделан единый установщик приложений Blitz Identity Provider (blitz.bin)
- Создан скрипт блокировки учетных записей по неактивности (lockinactive.sh)
- Добавлена возможность в «Источники данных» включать и выключать хранилища учетных записей
- Исправлены XSS при заполнении некоторых полей в формах консоли управления
- Исправлена ошибка, что не работала смена пароля учетной записи в консоли при DN учетной записи длиннее 250 символов.

Релиз 4.7.0

Сервис единого входа

- При входе по электронной подписи с использованием сертификата, выпущенного на индивидуального предпринимателя, заполняется значение ОГРНИП (из OID 1.2.643.100.5) в атрибут SUBJECT.OGRNIP.

Регистрация, Личный кабинет, Восстановление пароля

- Ко всем регистрируемым в RabbitMQ событиям добавлен параметр rpId с идентификатором приложения, инициировавшего изменение атрибута.
- Исправлена ошибка, что из Личного кабинета нельзя было отредактировать атрибут в пустое значение.
- Исправлена ошибка, что если учетная запись была зарегистрирована, то при переходе по старой ссылке на регистрацию из email выводилась 500 ошибка. Теперь выводится ошибка с корректным текстом.
- Исправлена ошибка, что через REST API v3 нельзя было поменять телефон или email в атрибутах пользователя на то же самое значение. При попытке такого вызова выдавалась ошибка нарушения уникальности атрибута. Теперь вызов отработает без ошибки (атрибут при этом меняться не будет, так как его значение остается тем же самым).
- Исправлена ошибка, что при заполнении формы регистрации в iOS для ввода кода подтверждения телефона/email не показывалась цифровая клавиатура.

Консоль управления

- Исправлена ошибка, что названия типов событий аудита «Учетная запись заблокирована» и «Учетная запись разблокирована» были перепутаны друг с другом.
- Для консоли управления можно настроить домен, отличный от используемого в сервисе единого входа.
- Для регистрируемых в СУБД Couchbase Server данных по каждому doc_type можно настроить время хранения (TTL), по истечении которого записи будут автоматически удалятся из БД. Например, можно настроить, чтобы события аудита автоматически удалялись из БД по истечении времени их хранения.

Релиз 4.6.0

Сервис единого входа

- Добавлена регистрация событий аудита, связанных с обменом маркеров доступа.
- Текст сообщения о нарушении парольной политики теперь можно настроить с использованием HTML.
- Добавлена возможность настройки порога срабатывания защиты, запрещающей прохождение одновременной аутентификации одним и тем же пользователем в течение определенного периода времени.
- Добавлена проверка CAPTCHA в экран ввода пароля при выполнении привязки учетной записи пользователя при входе через внешний поставщик идентификации.

Регистрация, Личный кабинет, Восстановление пароля

- Исправлено, что в REST API при редактировании групп пользователей нельзя было удалить атрибут. Теперь при передаче значения null для атрибута происходит его удаление.
- Исправлена ошибка, что при восстановлении пароля после подтверждения телефона и email можно было сохранить куки, и потом с помощью этих кук можно было воссоздать сессию восстановления пароля и получить возможность опять сбросить пароль от учетной записи пользователя.
- Улучшена верстка при отображении личного кабинета в смартфонах с iOS.
- Реализована функция, позволяющая настроить запрет на повторное использование идентификатора пользователя в течение определенного срока после увольнения сотрудника.

- Реализована функция, позволяющая автоматически осуществлять блокирование учетных записей пользователей после определенного периода их неактивности.

Консоль управления

- Возможность настроить вход в консоль управления через Blitz Identity Provider или иную внешнюю систему входа с поддержкой OpenID Connect.
- Исправлено, что если после логаута из консоли восстановить запомненные сессионные куки, то пользователь оказывался залогиненным в консоли.
- Добавлен новый тип уведомления пользователя о включении/выключении двухфакторной аутентификации.
- Исправлена ошибка, что при регистрации пользователя через консоль управления не создавалось событие об этом в RabbitMQ.
- Исправлено отображение чекбоксом в таблице с SAML-утверждениями в консоли управления.
- Добавлены дополнительные полномочия доступа в консоль управления. Можно отдельно настроить доступ к меню Приложения, Внешний вид, События.
- Исправлена ошибка, что после добавления новых атрибутов в настройках источников данных требовался перезапуск Blitz Identity Provider.
- При удалении учетной записи теперь пишется событие в RabbitMQ.

Релиз 4.5.0

Сервис единого входа

- Для ввода числового кода подтверждения теперь предлагается вводить только цифры. На мобильном приложении используется цифровая клавиатура.
- Выводимое на странице входа имя пользователя обрезается таким образом, чтобы умещаться в окне.
- Исправлена ошибка, что в id_token при использовании Hybrid Flow и Implicit Flow были перепутаны местами at_hash и c_hash.
- Исправлена ошибка, что не работало получение атрибута «телефон организации» из ЕСИА.

Регистрация, Личный кабинет, Восстановление пароля

- Для ввода числового кода подтверждения теперь предлагается вводить только цифры. На мобильном приложении используется цифровая клавиатура.

- Выводимое в заголовке личного кабинета имя обрезается таким образом, чтобы умещаться в окне.
- В REST API получения событий аудита добавлена поддержка использования в RQL-запросах типа Long. Необходимо для фильтрации событий аудита по диапазону времени.
- Исправлена ошибка, что при использовании СУБД PostgreSQL в личном кабинете не показывались разрешения приложений.

Консоль управления

- Исправлены ошибки безопасности в консоли управления: убрана возможность администратору консоли без достаточных прав смотреть настройки приложений через внутреннее API консоли, добавлена защиты от CSRF, исправлена ошибка парсинга XML, способная привести к зависанию консоли.
- Исправлены ошибки в верстке экрана входа, экрана отображения атрибутов в LDAP-хранилищах, экрана отображения списка сертификатов настройки входа по электронной подписи, остальных экранов с отображением таблиц в консоли.
- В настройках подключения к RabbitMQ в конфигурационном файле обеспечено хранение пароля в зашифрованном виде.
- Реализована возможность ограничить для администратора количество сессий с консолью управления до одной сессии. При входе администратором с нового устройства сессия на предыдущем устройстве сбрасывается.
- Исправлена ошибка, что при использовании СУБД PostgreSQL в консоли управления в карточке пользователя не показывались разрешения приложений.

Релиз 4.4.0

Сервис единого входа

- Можно встроить вызов внешнего вспомогательного приложения «в разрыв» в процесс входа пользователя в приложение. Встройка происходит с использованием «процедуры входа». Внешнее приложение получает контекст входа пользователя и возможность получить маркеры доступа от его имени. Внешнее приложение может быть полезно для решения следующих задач: показать пользователю объявление при входе, попросить актуализировать контакты или данные учетной записи, запросить согласие пользователя с измененной политикой конфиденциальности и др.

- Исправлена ошибка, что при вводе пользователем кода подтверждения при проверке второго фактора аутентификации если приложение, принимающее от Blitz Identity Provider код авторизации, долго отвечало, то пользователь, все еще находясь на странице подтверждения входа мог нажать кнопку подтверждения входа повторно, и тогда его вход заканчивался ошибкой. Теперь кнопка подтверждения ввода кода замораживается после отправки кода на проверку.
- Доработано API режима входа в Blitz Identity Provider без отображения страницы входа (display=script) таким образом, чтобы поддерживать сценарии проверки CAPTCHA, если проверка CAPTCHA настроена.

Регистрация, Личный кабинет, Восстановление пароля

- Исправлена ошибка, что событие о смене атрибуты группы писалось в очередь RabbitMQ при любом вызове операции редактирования любого атрибута группы, даже если изменения атрибута на самом деле не происходило (если атрибут менялся на то же самое значение).
- Исправлена ошибка, что приложение регистрации не работало, если его вызов осуществлялся пользователем в процессе входа в мобильное приложение, запрашивающее вход с использованием динамической пары client_id/client_secret.

Консоль управления

- Исправлена ошибка обработки префиксов ссылок возврата при логауте. Ранее если у приложения не были настроены префиксы ссылок возврата, то разрешался возврат на любые адреса.
- Добавлена возможность входа в консоль управления через внешний IDP, например, через сам Blitz Identity Provider. Есть следующие режимы входа: по логину/паролю из файла учетных записей, через SSO, гибридный вариант.
- Можно управлять необходимостью проверки парольной политики при входе избирательно через настройку процедуры входа или через HTTP-заголовок со значением true/false.
- В настройках просмотра событий безопасности исправлены значения фильтра «Протокол». Добавлен пункт «Другие», который позволяет смотреть все события, возникшие при взаимодействии приложения с Blitz Identity Provider иным образом, чем через SAML или OAuth 2.0.

Релиз 4.3.0

Сервис единого входа

- Добавлена возможность в момент входа выбора организации при входе сотрудником через ЕСИА. Данные выбранной организации при первом входе регистрируются в хранилище Blitz Identity Provider в виде группы пользователей с атрибутами организации, полученными из ЕСИА, а пользователь помещается в созданную группы. При последующих входах можно настроить обновление атрибутов группы актуальными значениями атрибутов из ЕСИА. Результат выбора организации пользователем в момент входа можно передавать в приложения в виде сессионного атрибута в составе id_token/access_token.
- В события аудита, регистрируемые при входе, можно добавлять дополнительные сведения из процедуры входа или из внешнего метода аутентификации. В стандартное событие входа в параметры добавлены «причина смены пароля при входе» и признак «был ли сменен пароль при входе», «использованный логин», признак того, что была временная блокировка входа, что запрашивался тест CAPTCHA, что пользователь пытался войти по старому паролю.

Релиз 4.2.0

Регистрация, Личный кабинет, Восстановление пароля

- Добавлена возможность передачи в сервер очередей RabbitMQ событий об изменении атрибутов пользователя, действий с группами пользователей (создание группы, изменение атрибутов группы, удаление группы, добавление/исключение пользователей из группы), привязок/отвязок к учетной записи внешних учетных записей (ЕСИА и соц.сети), отзыв пользователем согласия на передачу данных приложению.
- Исправлена ошибка регистрации пользователя при входе через ЕСИА, если было настроено получение из ЕСИА атрибута с типом Boolean.
- Ограничен размер данных, которые можно вводить в полях станиц входа, регистрации, восстановления пароля. Можно вводить до 100 символов.
- Можно настроить вызов внешнего приложения регистрации с передачей приложению данных контекста входа и полученных в случае входа через внешний поставщик входа сведений из него (например, передаче сведений из ЕСИА во внешнее приложение регистрации).

Релиз 4.1.0

Сервис единого входа

- При вводе логина/пароля можно запросить пользователя пройти тест CAPTCHA. Можно настроить использование Google reCAPTCHA или подключить произвольный поставщик CAPTCHA (потребуется разработать REST-коннектор к сервису поставщика CAPTCHA).
- В access_token, формируемый в формате JWT, можно включать сессионные атрибуты.
- При входе пользователя по паролю можно выполнять проверку пароля на соответствие действующей парольной политике и рекомендовать пользователю сменить пароль, если он перестал удовлетворять действующей парольной политике.
- При попытке подбора пароля можно временно блокировать для учетной записи вход по паролю. Блокировка действует до истечения срока блокирования, либо до сброса пароля через процесс восстановления забытого пароля. Другие способы входа при этом не блокируются.
- При попытке входа пользователя с паролем, который ранее был изменен пользователем, об этом пользователю выводится соответствующая ошибка, а не сообщение, что введен неправильный логин и пароль.
- Исправлена логика обработки входа в случае, если к Blitz Identity Provider подключено несколько хранилищ учетных записей, и от хранилищ в результате поиска учетной записи при входе возвращается ошибка. Если хоть в одном хранилище вход завершится успешно (или с ошибкой PasswordExpired), то ошибки остальных хранилищ будут проигнорированы. Если успешного входа ни по одному хранилищу нет, но хоть по одному хранилищу была получена ошибка InvalidCredentials, то будет возвращена эта ошибка, либо если все ошибки были отличны от InvalidCredential, то будет возвращена ошибка, полученная от последнего хранилища в списке проверок.
- Исправлена ошибка, что в составе id_token мог дублироваться атрибут sub.

Регистрация, Личный кабинет, Восстановление пароля

- Расширена поддержка проверки парольных политик средствами Blitz Identity Provider (дополнительно или вместо парольных политик LDAP). При регистрации, смене пароля в личном кабинете, в процессе входа или в результате восстановления забытого пароля можно выполнять следующие проверки пароля на соответствие парольной политике:
    - Запрет использования словарных паролей
    - Запрет использования предыдущих N паролей

    - Требовать, чтобы новый пароль отличался на X символов от предыдущего
    - Минимальный (запрет смены пароля раньше истечения минимального срока действия) и максимальный срок действия пароля
- Предусмотрено API, чтобы для указанной учетной записи можно было запретить использовать пароль для входа до момента восстановления забытого пароля и/или потребовать сменить пароль при следующем входе

Консоль управления

- В настройках шаблона приложения регистрации пользователей появилась возможность анализировать идентификатор приложения, в результате входа в который была инициирована регистрация пользователя. Для этого добавлен параметр ctx.appId.
- Добавлена поддержка возможности использования СУБД PostgreSQL (или иной реляционной СУБД, поддерживающей подключение по JDBC) в качестве альтернативы Couchbase Server. Можно использовать PostgreSQL вместо Couchbase Server как единственную СУБД или можно использовать PostgreSQL дополнительно к Couchbase Server (тогда в PostgreSQL можно хранить события аудита, а в Couchbase Server остальные данные).
- В процедуре входа можно запрашивать права текущего субъекта на объекты. Пример получения прав текущего пользователя на объект учетной записи с идентификатором testUser:

Пример получения прав текущего пользователя на объект учетной записи с идентификатором testUser:

```
final String[] rights_on_user = _ctx.rightsOnUser("testUser");
```

Пример получения прав текущего пользователя на объект группы учетных записей с идентификатором testGroup профиля orgs:

```
final String[] rights_on_group = _ctx.rightsOnGroup("orgs", "testGroup");
```

Пример получения прав текущего пользователя на объект приложения с идентификатором testSystem:

```
final String[] rights_on_app = _ctx.rightsOnRp("testSystem");
```

- Расширена поддержка разработки внешних методов аутентификации. Можно передавать во внешний метод значения настроек метода, фильтровать набор передаваемых во внешний метод утверждений о пользователе, принимать и отображать ошибки, полученные от внешнего метода аутентификации.

Релиз 3.11.3

Сервис единого входа

- Исправлена ошибка, что 2FA могла требоваться при повторных входах с известного устройства, если пользователь сначала входил в приложение, которое бы не требовало прохождение 2FA, а потом переходил в приложение, которое требует 2FA.
- На экране согласия предоставления пользователем разрешений добавлена возможность отображения блока с текстом и ссылкой, например, для возможного размещения текста «Нажимая кнопку Разрешить, вы принимаете Пользовательское соглашение». Выводимый текст определяется в message с ключом page.consent.fm.help.
- Исправлена ошибка, что мог не работать вход по долгосрочной сессии, если у учетной записи в каталоге изменился DN. В момент входа пользователь получал ошибку 500. Теперь вместо ошибки пользователю будет показан экран входа.
- Исправлена работа сервиса удаления динамических client_id/client_secret. Действия при отзыве динамического клиента приведены в соответствие с RFC 7592.
- Исправлено, что при попытке авторизации через password grant с неправильным паролем в события аудита попадала запись с некорректным prms.error. В аудит писалось internal_error вместо invalid_credentials.

Регистрация, Личный кабинет, Восстановление пароля

- Исправлена ошибка, что не срабатывала регистрация пользователя в Active Directory, если в числе атрибутов пользователя при регистрации указывался атрибут CN.

Консоль управления

- В OAuth 2.0 настройках приложения появилась возможность задать «Дополнительный секрет (client_secret)». Тогда для приложения будут действовать два возможных значения client_secret. Настройка удобна для плавной замены client_secret в приложении.

Релиз 3.10.3

Сервис единого входа

- Исправлена ошибка, что логин не мог быть длиннее 64 символов.

- При блокировании учетной записи реализовано сбрасывание действующих на момент блокирования SSO-сессий, отзыв выпущенных access_token, удаление запомненных устройств.
- Доработано, что с использованием динамически полученных client_id/client_secret мобильное приложение при запросе маркера безопасности на scope с именем native получит значение атрибута css, которое сможет использовать для сквозной веб-аутентификации в вызванном из приложения веб-браузере.
- Исправлена ошибка, что при запросе удаления динамической пары client_id/client_secret могло происходить зависание запроса на удаление.

Регистрация, Личный кабинет, Восстановление пароля

- Исправлена ошибка, что при установке внешним приложением куки из настройки portal-lang-cookie (задает возможность переключения языка приложением) язык интерфейса в Blitz Identity Provider не менялся.
- Исправлены ошибки при работе сервиса /blitz/api/v3/users при выполнении операций смены email и телефона.
- Добавлена регистрация событий безопасности по операциям с группами пользователей (добавление/редактирование/удаление групп, добавление/исключение участников в группы пользователей). В консоли управления в меню «События» в фильтре просмотра сообщений появилась новая группа событий – «Операции с группами».
- Добавлена возможность передачи в сервер очередей RabbitMQ событий о регистрации в Blitz Identity Provider нового пользователя и событий смены пароля пользователя.

Консоль управления

- В настройках подключения приложения по OAuth 2.0 можно индивидуально настроить «время жизни маркера доступа». Ранее для всех приложений действовала общая настройка.
- При задании настроек OAuth 2.0 подключения приложения по умолчанию настройка «Допустимые response type» заполняется как «code» (ранее заполнялась как «code token»).
- Поле «Пароль» в настройках сервера отправки Email-сообщений сделано необязательным для заполнения. Ранее нельзя было сохранить настройки, не заполнив пароль.

Релиз 3.9.1

Сервис единого входа

- Новый метод подтверждения входа (второй фактор аутентификации) – подтверждение входа кодом подтверждения, отправленным по email.
- Улучшена обработка ошибок входа с помощью средства электронной подписи.
- Исправлена ошибка, что при недоступности хранилища учетных записей в момент запроса приложением обновления refresh_token новый маркер обновление не может быть предоставлен из-за ошибки, а прежний маркер обновления аннулируется. Теперь в случае ошибки доступа к хранилищу прежний маркер обновления сохранится.
- Улучшена обработка ошибки, когда входит пользователь с истекшим паролем, и Blitz не может запросить у пользователя смену пароля, так как подключенное к Blitz хранилище подключено с настройкой «только чтение».
- Исправлена ошибка, что не работало удаление динамических client_id/client_secret, если они были выданы приложению с включенной настройкой «Не требовать от пользователя согласие». Улучшено логирование операций с динамическими client_id.

Регистрация, Личный кабинет, Восстановление пароля

- При использовании API создания групп теперь не обязательно передавать аргумент с id группы. Если id не передан, то он будет автоматически присвоен Blitz Identity Provider при создании группы.
- При восстановлении пароля появилась возможность для учетных записей с включенной двухфакторной аутентификацией запросить в процессе восстановления пароля прохождение дополнительной проверки.

Консоль управления

- В настройках сервиса «Восстановление доступа» можно указать необходимость в прохождении дополнительных проверок для пользователей с настроенной двухфакторной аутентификацией, и перечислить список необходимых проверок.
- Появилась возможность из консоли управления включить/выключить настройку, позволяющую информировать пользователя при запросе восстановления пароля, что для восстанавливаемой учетной записи есть связанные пользователи, которым ранее было делегировано право на изменение пароля (например, сценарий восстановления пароля ребенком, при котором его информируют, что для сброса пароля он может обратиться к родителю).

- Настройки нового метода аутентификации «Подтверждение с помощью электронной почты» – можно задать размер кода, количество секунд на проверку, количество попыток ввода кода.
- Для каждого подключенного приложения можно индивидуально настроить срок действия маркера обновления. Ранее для всех приложений действовала общая настройка.

Релиз 3.8

Сервис единого входа

- Добавлена поддержка получения маркеров доступа по спецификации RFC 8628 «OAuth 2.0 Device Authorization Grant». Возможность может быть полезна при необходимости добавления функции входа через Blitz в голосовые помощники (Алиса), Smart-TV.
- Актуализирован логотип для входа по Сбер ID.
- Исправлена ошибка с декодированием параметра post_logout_redirect_uri, что при вызове логаута и передачи в URL возврата строки с query-параметрами эти параметры терялись при обработке логаута.
- В Blitz Identity Provider появилась новая опция – Service Security. При использовании этой опции с помощью Blitz Identity Provider можно осуществлять контроль доступа к вызываемым приложениями HTTP-сервисам. Для защиты сервисов используется новый компонент – шлюз безопасности сервисов (blitz-keeper). Контроль доступа осуществляется на основе установленных в Blitz Identity Provider правил. Правила регламентируют, какие сервисы можно вызывать в зависимости от: прав доступа вызывающего приложения, прав доступа пользователя, разрешений (scope) и атрибутов (claims) в составе используемого для вызова маркера доступа. Также правила регламентируют замену маркера доступа при прохождении вызова к сервису через шлюз безопасности сервисов. Замена маркера осуществляется в соответствии со спецификацией RFC 8693 «OAuth 2.0 Token Exchange».

Регистрация, Личный кабинет, Восстановление пароля

- В поле задания пароля добавлена кнопка «глаз» для возможности включить отображение вводимого пароля.
- В поле изменения пароля добавлена кнопка «глаз» для возможности включить отображение вводимого пароля.

- Созданы REST-сервисы, позволяющие назначать и отзывать права доступа пользователей.
- Исправлена ошибка в REST-сервисе изменения пользователя, что сервис мог иногда не сработать из-за появления спец.символов в параметре instanceId.

Консоль управления

- Исправлена ошибка, что не работал чекбокс «Включить метод в качестве метода первого фактора».
- Исправлена ошибка, что могло не работать создание пользователя в консоли управления в случае, когда не настроен атрибут locked.

Релиз 3.7

Сервис единого входа

- Исправлена ошибка, что если при входе через социальную сеть в экране привязки социальной сети пользователь нажимал «Отменить», то возникала ошибка входа. Теперь в этом случае пользователь просто будет возвращен на экран входа.

Регистрация, Личный кабинет, Восстановление пароля

- Исправлена ошибка, что отправленной ссылкой на восстановление пароля можно было воспользоваться повторно.

Консоль управления

- Улучшен запуск приложений Blitz Identity Provider после аварийного перезапуска сервера. Внесены настройки, регулирующий автоматические попытки перезапуска сервисов при старте.
- Улучшено отображение пользователей, являющихся участниками групп. Корректно отображаются html-тэги, разделяющие отображение различных атрибутов пользователя.
- Унифицированы системные имена сообщений в messages-файлах, используемые для настройки отправляемых писем и SMS-сообщений.

Релиз 3.6

Сервис единого входа

- Исправлена ошибка, что не открывалась страница входа в случае, если для приложения был выключен режим входа по логину/паролю, а был разрешен только вход по соцсетям. Теперь появляется экран входа с кнопками выбора соцсетей.
- Добавлено API, позволяющее приложению отозвать ранее выпущенную динамическую пару client_id/client_secret.
- Улучшено взаимодействие с хранилищами учетных записей через REST-коннектор. Теперь можно настраивать таймаут ожидания ответа от REST-коннектора.

Регистрация, Личный кабинет, Восстановление пароля

- Созданы REST-сервисы, позволяющие выполнять следующие действия с учетной записью пользователя:
  - получать значения атрибутов
  - редактировать значения атрибутов, в т.ч. менять телефон/email с отправкой проверочного кода или без отправки
  - изменять пароль пользователя
  - проверять/изменять настройки двухфакторной аутентификации пользователя
  - получать список устройств пользователя, выданных разрешений. Удалять устройства и отзывать выданные разрешения
  - получать список событий аудита пользователя
- Доступ к сервисам регулируется с помощью разрешений (scope) OAuth 2.0. Вызов сервиса можно выполнять:
  - с использованием маркера доступа, полученного на пользователя, и тогда действия производятся с учетной записью текущего пользователя
  - с использованием маркера доступа, полученного на приложение, и тогда действия производятся с учетной записью любого пользователя
- Запрос проверочных атрибутов (например, фамилии) выполняется на той же странице, где вводится логин.
- Исправлена ошибка, что при вызове страницы восстановления пароля из страницы входа не передавался символ + в введенном пользователе логине.

Консоль управления

- Добавлена возможность из процедуры входа при неуспешной авторизации выводить пользователю на страницу входа текст ошибки входа.
  В процедуре входа для этого можно указывать имя используемой для отображения строки ошибки с помощью вызова команды

return StrategyState.DENY(msg.test.error, true);

- При отображении в консоли управления карточки пользователя в разделе отображаемых прав доступа корректно отображаются html-тэги.
- Исправлено определение мобильного браузера Chrome под iOS.

Релиз 3.5

Восстановление пароля

- Добавлена обработка ошибки попытки пользователя при восстановлении пароля задать значение ранее использованного пароля в ситуации, когда парольная политика запрещает использовать ранее использованный пароль.

Консоль управления

- Добавлено отображение наличия у пользователей прав в отношении других учетных записей.
- Добавлена возможность редактировать процедуру входа без ее предварительной деактивации.
- В настройках приложений можно задавать присвоенные приложению значения ключа шифрования идентификаторов. Приложения с общим ключом получают в составе id_token и в сервисе /oauth/me общие идентификаторы пользователя (sub) при входе.
- При настройке федеративного входа через внешнюю систему входа на основе Blitz Identity Provider теперь можно раздельно сконфигурировать URL обработчиков Authorization Endpoint, Token Endpoint, Userinfo Endpoint.
- В настройках правил сопоставления учетных записей при входе через внешние поставщики входа добавлена возможность отключить требование задавать пользователю пароль для подтверждения связи учетных записей.

Релиз 3.4

Сервис единого входа

- Добавлена возможность входа через учетную запись Mail ID.
- При смене пользователем пароля реализовано принудительное завершение запомненных сессий пользователей на других устройствах, отзыв выпущенных маркеров, удаление запомненных устройств.

Регистрация, Личный кабинет, Восстановление пароля

- При восстановлении пользователем пароля можно запросить ввод пользователем значений заданных атрибутов (например, фамилии) и проверку совпадения введенных значений с данными учетной записи. Продолжить восстановление пароля можно только при вводе правильного значения атрибута.

Консоль управления

- Добавлен новый пункт меню «Группы», позволяющий просматривать группы в хранилищах учетных записей, и членство пользователей в группах.

Релиз 3.3

Сервис единого входа

- При принудительной смене пользователем пароля при входе при задании нового пароля пользователь теперь должен заполнять также поле «Подтвердите новый пароль».

Консоль управления

- Добавлена возможность реализовать собственный метод аутентификации первого или второго фактора и настроить его использование Blitz Identity Provider.
- Из процедуры входа можно создавать сессионные claims и помещать их в формируемый маркер идентификации (id_token).

Релиз 3.2

Сервис единого входа

- Добавлена возможность отображения на странице входа элемента выбора языка интерфейса.
- Для подключенных хранилищ MS AD улучшена обработка ситуации принудительной смены пользователем пароля при входе в случае, если сервисной учетной записи Blitz Identity Provider не предоставлены права на изменение учетных записей в MS AD.
- Улучшена обработка LDAP-пула в ситуации, когда происходит полное исчерпание доступных коннектов в пуле.

Регистрация, Личный кабинет, Восстановление пароля

- Добавлена возможность отображения на странице регистрации элемента выбора языка интерфейса.
- Исправлена ошибка, что в некоторых браузерах (Chrome на Android) могла произойти повторная отправка на сервер заполненной регистрационной формы.
- Добавлена возможность отображения на странице восстановления пароля элемента выбора языка интерфейса.

Консоль управления

- Улучшено отображение событий безопасности в таблице.
- Добавлена возможность управлять настройками пула коннектов к БД Couchbase Server.
- Исправлена ситуация, что сервер мог не запуститься при недоступности LDAP-хранилищ в момент запуска сервера аутентификации.
- Исправлено указание дат привязки к учетной записи пользователя установок мобильных приложений при использовании Dynamic Client Registration.
- Обновлены иконки социальной сети Facebook/Google в консоли управления.
- Добавлена возможность из процедуры регистрации очищать атрибут создаваемой учетной записи – добавлен метод clearIdAttr().
- Заданные для атрибута правила преобразования входных значений теперь не препятствуют возможность через REST API удалить у учетной записи значение атрибута.

Релиз 3.1

Сервис единого входа

- Оптимизирована производительность работы SAML-сервисов.
- Добавлена поддержка OpenID Connect Implicit Flow, а также опционального параметра response_mode вызова Authorization Endpoint.
- Исправлена ошибка, что в id_token, полученном с помощью OpenID Connect Hybrid Flow, не заполнялись кастомные claims, которые согласно заданной настройке приложения должны были бы включаться в состав id_token.
- Улучшена обработка ситуации входа по электронной подписи, когда у пользователя не установлен браузерный плагин или установлен плагин не правильной версии. Теперь пользователю предлагается загрузить плагин именно для его операционной системы. В случае macOS Catalina проверяется, что пользователю необходимо обновить плагин до последней версии, обеспечивающей поддержку macOS Catalina.

- Добавлена возможность аутентификации с использованием Единой Биометрической Системы как метода второго фактора аутентификации. Используется биометрическая аутентификация по лицу.
- Обновлен логотип социальной сети Facebook на актуальный на кнопке входа через Facebook.
- Исправлена ошибка с проверкой подписи SAML-запроса, если вызов Blitz Identity Provider производится через HTTP-POST.
- Исправлена ошибка, что при входе с использованием динамически полученных client_id/client_secret срабатывала дефолтная процедура входа, а не процедура входа, заданная для этого приложения.

Регистрация, Личный кабинет, Восстановление пароля

- Появились REST API для работы с группами пользователей (LDAP-группы). Можно создавать, редактировать, удалять группы. Можно помещать пользователей в группы и исключать их из групп. В сервисе /blitz/oauth/me можно получать список групп, в которые включен пользователь. Доступ к новым сервисам регулируется новыми scope с именами bitz_groups и usr_grps.

Консоль управления

- В настройках методов аутентификации «Вход по логину и паролю» и «Вход по сеансу ОС» появилась возможность настроить правила роутинга хранилищ учетных записей. Можно в зависимости от того, какой пользователь ввел логин или в какое приложение входит, настроить, чтобы для поиска учетной записи использовались не все подключенные хранилища учетных записей, а только указанные в заданных администратором правилах.

Релиз 2.30

Сервис единого входа

- Улучшена работа функции «Войти с помощью Сбербанк ID» при выполнении входа на смартфонах. Если у пользователя установлено мобильное приложение «Сбербанк ID», то при входе в Blitz Identity Provider через Сбербанк ID для подтверждения входа будет вызвано мобильное приложение. Предусмотрена особая обработка ситуации для случая входа в инкогнито, входа через ссылки в мобильных приложениях, входа через нестандартные браузеры.

- Исправлена ошибка, что в момент входа через социальную сеть при выполнении первичной привязки учетной записи социальной сети к учетной записи пользователя могла возникнуть ошибка при проверке пароля, если ввод пароля подтверждался не нажатием кнопки Войти, а через кнопку Enter.

Регистрация, Личный кабинет, Восстановление пароля

- При переходе к восстановлению пароля со страницы входа если на странице входа пользователем был заполнен логин, то логин предзаполняется на странице восстановления пароля.
- Время на привязку социальной сети из Личного кабинета увеличено с 1 минуты до 10 минут.
- Исправлена ошибка, что при переходе по просроченной ссылке из email, отправленном для подтверждения регистрации учетной записи, выводилась «внутренняя ошибка». Теперь пользователю показывается корректная ошибка, информирующая его о том, что ссылка более недействительна.
- Исправлена ошибка, что в Личном кабинете можно было удалить последний настроенный метод второго фактора аутентификации, и при этом не выключить настройку «Требовать проверку 2FA при входе».

Консоль управления

- Добавлена возможность задавать (через редактирование blitz.conf) специальные настройки подключения Blitz Identity Provider к Couchbase Server для хранения данных – можно задать другие названия используемым buckets и определить свои правила маппинга сохраняемых Blitz Identity Provider объектов на используемые для их хранения buckets.
- При изменении настроек через консоль управления теперь в конфигурационном файле (blitz.conf) сохраняются сведения о том, какой администратор и когда сделал изменение настроек.

Релиз 2.29

Сервис единого входа

- Появилась возможность настроить отправку кодов подтверждения при двухфакторной аутентификации через push-уведомления в мобильное приложение.

Регистрация, Личный кабинет, Восстановление пароля

- Добавлено REST-API, позволяющее управлять правами доступа одних учетных записей в отношении других учетных записей, а также REST-API, позволяющий от имени основной учетной записи осуществить смену пароля в зависимой учетной записи.

Консоль управления

- Добавлена поддержка работы Blitz Identity Provider Enterprise Edition в ОС.

Релиз 2.28

Сервис единого входа

- Обработка входа пользователя при передаче параметра prompt=login при вызове Authorization Endpoint (/oauth/ae) приведена в соответствии со спецификацией OpenID Connect. При форсированной аутентификации пользователь должен осуществить вход именно под своей учетной записью. Если будет произведен вход под другой учетной записью, то Blitz Identity Provider вернет приложению ошибку login_required. Если для приложения при использовании prompt=login нужна именно возможность входа под другим пользователем, то это можно обеспечить через задание приложению специальной процедуры входа с поведением LOGOUT_THEN_MORE.
- Появилась возможность сквозного входа на сайт (без запроса логина/пароля) при вызове в WebView из мобильного приложения и наличии установленной приложением cookie с именем cookieShortSession.

Регистрация, Личный кабинет, Восстановление пароля

- Добавлена возможность отправить пользователям по SMS или по email уведомление об успешной регистрации учетной записи.

Консоль управления

- Исправлена ошибка, что при отключении в «Сервисы самообслуживания» функции «Личный кабинет» приложение все равно продолжало работать.
- Расширены функциональные возможности процедур входа:
    - Добавлена возможность анализировать переданные при вызове Authorization Endpoint параметры. Например, можно переопределить логику работу процедуры входа при наличии в параметре вызова /oauth/ae параметра prompt=login.

- К возможным возвратам метода begin добавлен StrategyState.LOGOUT_THEN_MORE, определяющий, что при попытке входа пользователя в приложение нужно принудительно прекратить текущую действующую сессию и провести новую идентификацию и аутентификацию пользователя. При этом допускается, что идентификация и аутентификация могут быть пройдены в отношении иного пользователя.

Релиз 2.27

Сервис единого входа

- Исправлена ошибка, что в некоторых случаях пользователям отправлялись лишние уведомления о входе с неизвестного устройства.

Регистрация, Личный кабинет, Восстановление пароля

- Встроена защита от CSRF-атаки (межсайтовая подделка запросов).

Консоль управления

- Убрана возможность посмотреть заданные в настройках пароли подключения к LDAP, к SMS-шлюзу, к SMTP, к социальным сетям. Вместо поля «Пароль» предусмотрена ссылка «Изменить значение». Заданный пароль можно только заменить на новый. Возможность посмотреть пароли сохранена только для настроек приложений (можно посмотреть заданный для приложения client_secret, нажав кнопку с изображением глаза).
- Добавлена возможность настроить максимально разрешенное количество попыток ввода кода подтверждения, направленного в SMS. Ранее было жестко ограничено 10 попытками.

Релиз 2.26

Сервис единого входа

- Добавлена возможность входа с использование Сбербанк ID.

Релиз 2.25

Сервис единого входа

- Добавлена поддержка проверки электронной подписи по ГОСТ Р 34.10-2012 в случае, если проверка электронной подписи в Blitz Identity Provider выполняется без использования вызова внешнего сервиса проверки электронной подписи.
- В записях аудита для входов с использованием OAuth 2.0 Resource Owner Password Credentials Flow теперь фиксируется client_id.
- Для сервиса Authorization Endpoint (/oauth/ae) добавлен опциональный режим prompt=login. При запросе входа в таком режиме пользователю будет показан экран входа, даже если он уже входил или у него есть долгосрочная сессия.
- Обеспечена поддержка спецификации PKCE в соответствии с RFC 7636.
- Возврат ошибок обработчика Token Endpoint (/oauth/te) приведен в соответствии с RFC 6748:
    - Код возврата при ошибке – 400 Bad Request, а не 200 OK.
    - При ошибке проверки username/password при вызове в режиме grant_type=password теперь возвращается ошибка invalid_grant, а не access_deny.

Консоль управления

- Добавлена возможность просматривать привязанные к учетным записям пользователей выпущенные динамические client_id привязанных мобильных приложений.
- В OAuth 2.0 настройках приложений теперь можно регулировать необходимость задействовать для приложения PKCE, ограничить доступные для приложения способы аутентификации, разрешенные приложению Flow (grant type и response type).

Релиз 2.24

Сервис единого входа

- Добавлена защита от атаки подбора пароля. При попытке подбора пароля к учетной записи включается задержка на вход, а также блокируется возможность входа данной учетной записью в параллельной сессии.
- Обеспечен вывод красивого сообщения об ошибке, если при принудительной смене пароля при входе пользователь вводит пароль из числа ранее использованных, и парольная политика в LDAP запрещает это.
- Улучшена работа с пулом LDAP-соединений для обработки ситуации недоступности LDAP-каталога или аварийного прерывания каталогом соединения.
- HTTP-код редиректа с обработчика Authorization Endpoint изменен с 303 на 302.

- Добавлена поддержка OAuth0 Dynamic Client Registration в соответствии с RFC 7591 и специальных возможностей по интеграции для мобильных приложений.

Регистрация, Личный кабинет, Восстановление пароля

- Ссылки на установку TOTP-приложений при настройке второго фактора аутентификации теперь открываются в новом окне.
- При изменении номера мобильного телефона теперь показывается обратный отсчет времени, доступного для ввода кода. Также ограничено количество попыток ввода кода подтверждения при смене телефона.
- Исправлено, что при открытии меню «Безопасность» всегда по умолчанию теперь будет открыта самая левая вкладка (обычно «Смена пароля»).
- Добавлено отображение на вкладке «Разрешения» выданных явно пользователем разрешений и привязанных к учетной записи пользователя установок мобильных приложений.

Консоль управления

- Исправлена работа задания SAML-настроек приложения для случая, что в названии SAML-атрибута присутствовал дефис.
- В настройка метода аутентификации «Логин и пароль» добавлена настройка для включения защиты от подбора пароля. Возможно включить как защиту от перебора пароля на конкретную учетную запись, так и подбора пароля на множество разных учетных записей.
- В OAuth0 настройках приложения можно на новой вкладке «Динамические клиенты» включить режим OAuth 2.0 Dynamic Client Registration и задать его настройки.

Релиз 2.23

Сервис единого входа

- Если обнаружено, что пользователю необходимо сменить пароль при входе, то теперь проверяется тип источника учетной записи пользователя. Для источников с пометкой «Только для чтения» пользователю не предлагается сменить пароль, а просто выводится сообщение об ошибке входа с пояснением.

Регистрация, Личный кабинет, Восстановление пароля

- Появилась вкладка «Разрешения», на которой показываются выданные пользователем разрешений на вход в приложения. В списке появляются только те разрешения, которые явно выдавал пользователь (у приложений в настройках OAuth не включен чекбокс «Не требовать от пользователя согласие на предоставление доступа к данным о себе».

Релиз 2.22

Восстановление пароля

- На экране восстановления пароля теперь не нужно выбирать, производится ли восстановление пароля по email или по телефону. Достаточно просто ввести логин – если введен email, будет запущено восстановление по email, если телефон – то по телефону, если же введен какой-то иной логин, то будет проверено, что у пользователя по этому логину есть email и/или телефон, и пользователю будет предложено выбрать из доступных для него каналов восстановления (показанные для выбора телефон и email при этом будут частично маскированы).

Релиз 2.21

Регистрация, личный кабинет, восстановление пароля

- Поле для задания пароля при регистрации, смене пароля в личном кабинете, задании нового пароля при восстановлении пароля снабжено индикатором стойкости и соответствия парольной политике.
- Предотвращена ситуация, при которой можно было добиться регистрации двух учетных записей с одинаковым мобильным телефоном несмотря на установленный признак уникальности мобильного телефона.

Релиз 2.20

Сервис единого входа

- Страница ошибки «Ваша сессия просрочена» (если больше часа находится на экране входа, а потом попробовать войти) выдается теперь не на белом экране, а в дизайне страницы входа.

Консоль управления

- Добавлена возможность в настройках самообслуживания включить/выключить отображение в Личном кабинете вкладок с событиями, а также ограничить период, за который пользователем доступен поиск/просмотр событий аудита с их учетной записью.

Релиз 2.19

Регистрация, Личный кабинет, Восстановление пароля

- Добавлена проверка парольной политики (по длине и допустимым символам) при смене в личном кабинете и при восстановлении пароля (парольная политика задается в blitz.conf в блоке password-policy). Проверка выполняется до отправки в LDAP, позволяет пользователя предупредить о неподходящем пароле еще до момента, когда сработает парольная политика внутри LDAP.

Релиз 2.18

Сервис единого входа

- Увеличена производительность входа по логину/паролю, если в качестве логина учетной записи используется дополнительный атрибут (хранимый внутри Blitz, а не во внешнем источнике).
- Оптимизирована работа Blitz с oauth bucket. Исключено использование индексов. Добавлен TTL 1 год для refresh tokens.
- Переделан механизм работы с долгосрочными сессиями. Создан метод аутентификации 1 фактора «Вход с известного устройства», позволяющий провести автоматический вход в случае, если:
    - ранее пользователь успешно вошел с этого же устройства с явно выключенным признаком «чужой компьютер» и с момента такого входа не прошел период «Срок действия долгосрочной сессии»;
    - вычисленный в момент входа цифровой отпечаток устройства не изменился с момента первичного входа;
    - пользователь не делал логаут и не очищал куки;
    - пользователь не удалял устройство в личном кабинете на вкладке «Устройства»;
    - учетная запись пользователя не заблокирована.

- Если пользователь входил в Blitz методом аутентификации, отличным от «Логин и пароль» и «SMS-код подтверждения», то долгосрочная сессия не создается. Например, для тех, кто входит по «Вход с рабочего компьютера», «Вход с помощью электронной подписи» или через внешний поставщик идентификации, вход будет проходить каждый раз после перезапуска браузера.

Регистрация, Личный кабинет, Восстановление пароля

- Исправлено отображение в личном кабинете событий аудита и устройств при большом кол-ве записей в БД.
- Исправлена работа личного кабинета на смартфоне в вертикальной ориентации:
  - кнопки привязки и удаления соц.сетей не налезают друг на друга.
  - добавлена горизонтальная прокрутка устройств и событий.
- Исправлена ошибка, что при смене пароля при установленной настройке «Уведомлять пользователя о событиях – Смена пароля») пользователю приходило два уведомления вместо одного.

Консоль управления

- Исправлено, что измененный вручную в конфиге credentials пароль администратора не зашифровывался при перезапуске blitz-console.
- Исправлена ошибка, что в консоли управления можно было создать более одной учетной записи администратора с одинаковым логином.
- Ускорен поиск событий аудита в Blitz Console. Но теперь при поиске нужно обязательно задать поисковое условие в поле Субъект или Объект.
- Включить и выключить метод «Вход с известного устройства» можно без перезапуска Blitz Identity Provider.
- В аудите вход по методу «Вход с известного устройства» протоколируется как «вход с известного устройства (...)», где вместо ... указывается тот метод входа, который был использован в первый раз в момент создания сессии. Например, «вход с известного устройства (пароль)».
- Настройка длительности долгосрочной сессии перенесена в консоли управления из экрана общий настроек аутентификации в экран нового метода «Вход с известного устройства».

Релиз 2.17

Сервис единого входа

- Новые способы входа: Яндекс, Одноклассники.
- Изменен дизайн страницы входа:
    - Кнопки входа через социальные сети всегда показываются в одну строку. Если настроено до 2 социальных сетей, то кнопки широкие с иконкой и надписью. Если 3 и более социальные сети, то кнопки в виде иконок.Кнопка входа через ЕСИА отображается в виде широкой кнопки с логотипом «Госуслуги».
    - Ссылка «Другие способы входа» заменена на кнопку и отображается только в случае, если кол-во альтернативных способов входа больше 3. Иначе другие способы входа отображаются сразу в виде кнопок.
    - На экранах входа с помощью электронной подписи, входа с помощью сеанса ОС, входа с помощью СМС-кода, убран список других способов входа – оставлена только кнопка «Другие способы входа», ведущая на основной экран страницы входа.
    - Добавлена возможность просмотра введенного/подставленного пароля на странице входа (кнопка «глаз» внутри поля «Пароль»).
    - Добавилась возможность через настройки шаблона внешнего вида регулировать начальное состояние чекбокса «Чужой компьютер».
- Улучшения программных интерфейсов (API) сервера аутентификации и механизмов интеграции:
    - Добавлено API для возможности запроса аутентификации по логину/паролю из фрейма/модального окна приложения заказчика.
    - Повышена надежность взаимодействия Blitz Identity Provider с LDAP-серверами. Теперь Blitz Identity Provider можно подключить к кластеру LDAP-серверов, прописав в DNS для хоста LDAP несколько IP-адресов каждой из нод кластера. Blitz Identity Provider будет распределять коннекты среди работающих нод LDAP-кластера.
- Оптимизирована регистрация событий аудита. Теперь на одно событие входа генерируется одна запись аудита.
- Оптимизирована работа сервиса /oauth/me в случае использования нескольких источников данных. Теперь сервис для получения данных обращается только к тому хранилищу, в котором был найден пользователь в момент выпуска access_token.
- Исправлены ошибки:

- При входе через социальную сеть при вводе неправильного логина/пароля для привязки аккаунта социальной сети к аккаунту пользователя выводилась «внутренняя ошибка», а не «неправильный логин или пароль»
- В выпущенном id_token утверждение exp указывалось в миллисекундах с момента выпуска токена, а не с 1970 года, как это должно быть в соответствии со спецификацией.
- При повторном входе через социальную сеть все время крутился спиннер входа.
- Ошибка с привязкой аккаунта к социальной сети при входе, если пользователь 3 раза неправильно ввел пароль.
- Зацикливание при смене пароля при входе, что при каждом новом входе опять запрашивалась смена пароля.

Регистрация, Личный кабинет, Восстановление пароля

- Добавлено API привязки/отвязки социальных сетей для встраивания функции в приложение заказчика.

Консоль управления

- Появилась настройка «Режим выдачи маркеров доступа по умолчанию». Если она в значении offline, то приложение получает refresh_token, если online, то не получает. Также приложение может само регулировать, получать или нет refresh_token, если в обращении к OAuth 2.0 Authorization Endpoint будет указывать опциональный параметр access_type=online/offline
- В настройках подключения к LDAP появилась возможность задать параметры балансировки соединений к LDAP-кластеру.
- Улучшена настройка процедур входа:
  - из процедуры входа можно обращаться к cookie
  - из процедур входа можно делать вызовы внешних сервисов.
- Добавлены настройки подключения социальных сетей Яндекса и Одноклассников.
- В настройках сервисов самообслуживания для «Личный кабинет» теперь можно сконфигурировать URL возврата при логауте.
- В просмотре событий безопасности убрана настройка сортировки событий аудита по датам. Сортировка теперь всегда по убыванию даты в целях повышения производительности. Ускорен поиск событий аудита в случае большого кол-ва событий.
- Исправлен перевод интерфейса на английский язык, а также переход к экрану настроек лицензий в интерфейсе консоли на английском языке.

Релиз 2.16

Сервис единого входа

- Улучшен процесс связывания учетных записей при входе через социальные сети. Если не прошел автоматический маппинг учетки при входе, то пользователь может:
    - сообщить, что у него уже есть учетная запись и ввести от нее логин/пароль;
    - пройти регистрацию.
- Исправлена 500-ошибка «No idp login context available» при взаимодействии по SAML систем с Blitz Identity Provider.

Восстановление пароля

- Ссылку на восстановление пароля теперь можно вызывать в сессии авторизованного пользователя (если пользователь хочет восстановить пароль, не выполняя логаут).
- Ссылка на восстановление пароля добавлена на экран смены пароля в личном кабинете (если пользователь хочет сменить пароль от учетной записи, но не помнит текущее значение пароля).
- Улучшено отображение приложений в Internet Explorer.

Консоль управления

- Настройки приложений:
    - Установка допустимых URL-возврата после логаута.
    - Указание, какие атрибуты пользователя/сессии должны передаваться в id_token.
- Настройки источников данных:
    - Изменен дизайн экрана настроек. Теперь раздельно задаются настройки хранимых атрибутов, настройки вычисляемых атрибутов, правила преобразования атрибутов из входящих значений (вводимых пользователем или переданных в API) и выходящих значений (подготовленных Blitz Identity Provider для передачи подключенным приложениям).
    - Появилась возможность выполнять преобразования над multi-value-атрибутами.
- Настройки социальных сетей:
    - Добавлена возможность настроить обновление в источниках данных интересующих атрибутов учетной записи значениями атрибутов из социальной сети или ЕСИА при каждом входе пользователя. Регулируется колонкой «Мастер» в таблице настроек сопоставления атрибутов учетной записи Blitz Identity

Provider атрибутам, полученным из социальной сети, в настройках «Поставщики идентификации».
    - Добавлена настройка «Предлагать пользователю ввести логин и пароль для привязки, если учетная запись не была идентифицирована».
- Механизмы безопасности консоли управления:
    - Добавлено ролевое разграничение доступа в консоль управления.
    - Добавлена возможность заведения учетных записей администраторов через консоль управления (меню «Администраторы»).
    - При длительной неактивности администратора в консоли управления его теперь просят войти повторно.

Релиз 2.15

Сервис единого входа

- Создан сервис метаданных /oauth/.well-known/openid-configuration. Сервис соответствует спецификации OpenID Connect Discovery0.
- Изменения в работе функции логаута:
    - При логауте выполняется проверка, что URL возврата в числе разрешенных.
    - При вызове сервиса единого логаута ссылку на URL-возврата теперь можно передавать в параметре с именем post_logout_redirect_uri в соответствии со спецификацией OpenID Connect Session Management 1.0.
    - Улучшена обработка ошибок на странице единого выхода.

Консоль управления

- Добавлена возможность указывать разрешенные приложению OAuth-scope.
- В настройках аутентификации с помощью сеанса операционной системы теперь можно задать подключение одновременно к нескольким Kerberos-серверам и задать несколько SPN/keytab.

Релиз 2.14

Сервис единого входа

- При входе по электронной подписи теперь можно вызывать проверку действительности сертификата через внешний сервис проверки.

- Приложение может вызывать сервис единого входа с использованием Hybrid Flow по спецификации OpenID Connect.
- Улучшена поддержка работы с LDAP-хранилищами, расположенными на удаленных площадках, сетевые соединения с которыми нестабильны. Blitz Identity Provider обеспечивает поддержание соединений с такими LDAP в рабочем состоянии и автоматически возобновляет соединения при необходимости. Этот режим рекомендуется использовать при подключении Blitz Identity Provider к Azure AD Domain Services.

Консоль управления

- В настройках приложения client-secret и пароль приложения теперь хранятся в зашифрованном виде. В консоли добавлена возможность по нажатию на изображение «глаза» посмотреть значения этих параметров.
- Настройки источников данных:
  - Для REST-хранилищ добавлена возможность указать подмножество атрибутов, управляемых REST-хранилищем. Прочие атрибуты в этом случае обрабатываются Blitz Identity Provider самостоятельно.
  - Уточнены встроенные справки-описания по настройке подключения хранилищ учетных записей через REST-API.
- Работа с процедурами входа добавлена в редакцию Standard Edition.

Релиз 2.13

Сервис единого входа

- В Standard Edition добавлен режим входа по сеансу ОС (Kerberos). Ранее этот режим был доступен только в Enterprise Edition.

Регистрация, личный кабинет, восстановление пароля

- Сделана HTML-верстка стандартных писем, отправляемых при регистрации, смене и восстановлении пароля, изменении email.

Консоль управления

- Во вкладке «Процедуры входа» созданы процедуры входа для распространенных сценариев контроля доступа пользователей в приложения.

- Много эргономических улучшений: исправление верстки, исправления текстов подсказок, повышение отзывчивости интерфейса.

Релиз 2.12

Сервис единого входа

- Новый режим входа – «долгосрочная сессия». При входе с доверенного компьютера пользователь остается залогиненным на длительный срок – сессия не прекращается в случае перезапуска браузера.

Регистрация, личный кабинет, восстановление пароля

- Пользователь может зарегистрироваться с использованием средства электронной подписи. Атрибуты предзаполняются из сертификата пользователя либо дополнительно вводятся пользователем на отдельной странице ввода.
- При регистрации через социальную сеть теперь пользователь может задать значения недостающих для регистрации атрибутов (если для регистрации нужно больше атрибутов, чем получено из социальной сети).
- При регистрации теперь может вызываться проверка введенных пользователем данных во внешней системе (например, кадровой системе), и получения из внешней системы дополнительных сведений.

Консоль управления

- Администрирование пользователей:
    - можно изменить пользователю пароль
    - можно блокировать/разблокировать учетную запись. С помощью заблокированной учетной записи нельзя войти в приложения.
- Настройки источников данных:
    - Можно пометить хранилище признаком «только для чтения». Для учетных записей из такого хранилища не будут доступны операции регистрации, смены атрибутов учетной записи и пароля.
    - При регистрации учетных записей можно настроить их хранение в разных DN.
- Назначенная приложению процедура входа начинает действовать сразу. Перезапускать сервер Blitz Identity Provider для применения настройки теперь не нужно.

Релиз 2.11

Сервис единого входа

- Новый способ входа (1-й фактор) – пользователь указывает номер телефона и полученный по SMS на этот телефон разовый пароль.

Регистрация, Личный кабинет, Восстановление пароля

- Для активации учетной записи можно использовать мобильный телефон и подтверждение регистрации по SMS.
- При заполнении значений атрибутов можно использовать атрибуты со списками значений.
- Добавлен режим восстановления пароля с использованием привязанного номера телефона и отправки проверочной SMS.

Консоль управления

- Администрирование пользователей – можно редактировать атрибуты с типом «массив строк» (раньше можно было редактировать только single-value атрибуты)
- Настройки источников данных:
    - Можно подключить несколько LDAP-хранилищ с разным набором атрибутов, разными названиями атрибутов, разным форматом значений атрибутов.
    - Упрощена настройка атрибутов. Теперь если атрибут учетной записи не хранится во внешнем хранилище, то он хранится во внутренней БД Blitz Identity Provider. Отдельно это настраивать для атрибута не нужно.

Релиз 2.10

Сервис единого входа

- В случае успешной аутентификации теперь запоминается логин. При повторных входах пользователю его вводить не нужно. Если пользователь входит с чужого ПК и не хочет, чтобы информация о его входе сохранилась на этом устройстве, то он может отметить чекбокс «Чужой компьютер».
- При включенном режиме аутентификации «Вход с известного устройства» если у пользователя активирована двухфакторная аутентификация, то она будет запрашиваться только при первом входе с новых (незнакомых) устройств. Устройство становится знакомым, если пользователь с него успешно вошел и в процессе входа снял чекбокс «Чужой компьютер».

- Новый способ двухфакторной аутентификации с помощью Duo Mobile.

Регистрация, Личный кабинет, Восстановление пароля

- Появилась возможность настраивать привязку устройств Duo Mobile.

Консоль управления

- Добавлены разделы настроек «Duo push-аутентификация», «Вход с известного устройства».
- Добавлена возможность просмотреть доступные лицензии Blitz Identity Provider.
- Исправлена ошибка, что созданные атрибуты с источником «Хранилище доп. атрибутов» нельзя было получать и редактировать через REST API.
- Исправлена ошибка, что при переименовании в «Хранилище» атрибута некоторые экраны консоли могли перестать работать, если в указанных на этих экранах настройках использовался переименованный атрибут.
- В разделе «Пользователи» появилась возможность задать настройки привязки Duo-аутентификаторов, а также привязки аппаратных TOTP-генераторов.
- В разделе «Устройства» появилась возможность загружать файлы описаний аппаратных TOTP-генераторов. Появилась поддержка загрузки файлов формата PSKC XML.
- В Standard Edition появилась функция резервного копирования и восстановление внутренней БД через консоль управления, а также настройки по автоматическому выполнению резервного копирования.
- Настройки Twirl-шаблонов для Регистрации и для Личного кабинета унифицированы.
- Предусмотрена возможность в Twirl-шаблонах использовать строки с поддержкой переводов.
- Улучшена работа с LDAP. Теперь заданные настройки подключения к LDAP вступают немедленно и не требуют перезапуска сервера Blitz Identity Provider.
- Улучшены возможности настройки входа через Госуслуги (ЕСИА). Добавлены возможности привязки по СНИЛС, email, телефону, ИНН, паспортным данным и ФИО.

Релиз 2.9

Сервис единого входа

- При отмене входа через социальную сеть или через сеанс ОС пользователь теперь сразу возвращается на главный экран входа.

- Поддержана возможность входа по электронной подписи в Firefox v.52 и новее.
- При входе по электронной подписи теперь не разрешается пытаться входить с помощью просроченного сертификата электронной подписи.
- Добавлена возможность входа через социальные сети в Standard Edition.
- Добавлено протоколирование событий входа при использовании OAuth 2.0 Resource Owner Password Credentials Flow.

Регистрация, Личный кабинет, Восстановление пароля

- При регистрации теперь можно задать не только email и пароль, но и другие атрибуты учетной записи. Например, можно настроить, чтобы при регистрации пользователи указывали ФИО.
- Приложение «Профиль пользователя» переименовано в «Личный кабинет».
- В личном кабинете добавлена возможность редактировать атрибуты пользователя (с возможностью подтверждения по email и SMS).
- В личном кабинете теперь нельзя включить двухфакторную аутентификацию, если не настроен ни один метод второго фактора аутентификации.
- Отвязка аккаунта социальной сети теперь протоколируется в журнале событий безопасности.
- Переименованы названия устройств (MAC на Mac, WINDOWS на Windows PC, IPHONE на iPhone и т.д.).
- Когда привязаны все социальные сети, пользователю теперь не выдается надпись, что доступные для привязки аккаунты социальных сетей не найдены.

Консоль управления

- Добавлен раздел «Сервисы самообслуживания», позволяющий настроить работу приложений «Регистрация», «Личный кабинет», «Восстановление доступа», а также включить и выключить размещение на них ссылок в окне входа.
- Незначительные изменения пользовательского интерфейса (исправлены названия некоторых пунктов меню и текстовые подсказки в интерфейсе).
- Расширены возможности настроек метода аутентификации TOTP.
- Обеспечена возможность работать с аппаратными TOTP-генераторами и загрузки файлов их описаний в разделе «Устройства».
- Исправлена ошибка с тем, что не работало изменение названий темы внешнего вида страниц входа и имени шаблона.

Технические изменения

- Повышена надежность и производительность Blitz Identity Provider. Выполнена замена СУБД Riak KV на СУБД Couchbase Server, используемой в качестве внутренней СУБД в Blitz Identity Provider. Производительность повышена до ~1000 запросов в секунду для одного сервера с Blitz Identity Provider при среднем времени отклика ~100 мс.
- Добавлены экраны-заглушки в дизайне Blitz Identity Provider для стандартных ошибок HTTP (страница не найдена, шлюз не отвечает, внутренняя ошибка).