

Различные способы удаленной аутентификации

Существует два типа удаленной аутентификации, которая управляется константой **KB_AUTH_TYPE**:

1. Добавление/обновление данных удаленного пользователя в KBPublisher и аутентификация пользователя.
2. Аутентификация существующего пользователя KBPublisher.

Добавление/обновление данных удаленного пользователя в KBPublisher и аутентификация

KB_AUTH_TYPE = 1

При успешной аутентификации функция **remoteDoAuth** должна вернуть ассоциативный массив со следующими ключами:

- first_name – имя
- last_name – фамилия
- email – электронный адрес
- username – имя пользователя
- password – пароль в не зашифрованном виде
- remote_user_id – уникальный идентификатор пользователя, хранящийся в вашей системе
- role_id – уникальный идентификатор роли. Не обязателен
- priv_id – уникальный идентификатор привилегии пользователя. Не обязателен. Обладая привилегией, пользователь имеет доступ к Панели администратора.

Аутентификация существующего пользователя KBPublisher

KB_AUTH_TYPE = 2

При успешной аутентификации функция **remoteDoAuth** возвращает:

- user_id – уникальный идентификатор пользователя в таблице KBPublisher с именем USER (kbp_user)
или
- ассоциативный массив с ключами (user_id, username). Например: array('user_id'=>7, 'username'=>'Test').

Существуют также другие переменные конфигурации

- **KB_AUTH_AREA**
1 – включено только для Публичного раздела, удаленная аутентификация разрешена на странице входа в Публичный раздел.
2 – включено для Публичного раздела и Панели администратора.
- **KB_AUTH_LOCAL**
0 – никогда не пытаться аутентифицировать с помощью KBPublisher, встроенного в аутентификацию.
1 – сначала всегда пытаться выполнить аутентификацию с помощью KBPublisher, встроенного в аутентификацию.
2 – пытаться выполнить аутентификацию с помощью KBPublisher, встроенного в аутентификацию, если удаленная проверка не удалась.
- **KB_AUTH_LOCAL_IP**
Только пользователи с указанными IP-адресами могут аутентифицироваться с помощью встроенной аутентификации KBPublisher.
Это имеет значение только тогда, когда для параметра **KB_AUTH_LOCAL** установлено значение **1** или **2**.
Вы можете установить определенный IP-адрес или диапазон IP-адресов. Используйте символ "-" для разделения диапазонов IP и символ ";" для разделения отдельных IP-адресов.
Например: 127.0.0.1;210.234.12.15;192.168.1.1-192.168.255.255
- **KB_AUTH_REFRESH_TIME**
Время в секундах для перезаписи пользовательских данных (3600*24*30=30 дней) работает, если для параметра **KB_AUTH_TYPE** установлено значение **1**.
0 – никогда. После создания пользователя данные в таблице KBPublisher никогда не обновляются по сценарию.
1 – при каждом запросе аутентификации пользовательские данные в базе будут синхронизированы с данными, предоставленными скриптом.
- **KB_AUTH_RESTORE_PASSWORD_LINK**
Здесь вы можете указать ссылку, по которой удаленные пользователи могут восстановить свой пароль.
Установите значение **false**, чтобы скрыть ссылку для восстановления пароля.
KBPublisher определит, следует устанавливать вашу ссылку или встроенную.
- **KB_AUTH_AUTO** ([с использованием автоматической аутентификации](#))
Эта переменная отвечает за то, видит ли пользователь страницу для входа в систему и должен ли войти в KBPublisher, или он автоматически входит в систему.
0 – отключено. Пользователь видит страницу для входа в систему.
1 – включено. Пользователь не видит страницу для входа в систему.

2 – включено, в режиме отладки. Пользователь не видит страницу для входа в систему. Это позволяет не блокировать "Auto Auth" (автоматическую аутентификацию), если проверка не удалась.
Используйте только для отладки и не забудьте вернуть в значение **1** или **0**, когда аутентификация заработает.

ID статьи: 377

Последнее обновление: 29 нояб., 2017

Обновлено от: Leontev E.

Ревизия: 4

Руководство пользователя v8.0 -> Единый вход -> Удаленная аутентификация -> Различные способы удаленной аутентификации

<https://www.kbpublisher.ru/kb/entry/377/>