

Table of Contents

Table of Contents	1
Пользователи и устройства	2
Пользователи и группы	3
Серверы аутентификации	4
Профили аутентификации	10
Настройка Captive-портала	11
Пользователи терминальных серверов	14
Профили MFA (мультифакторной аутентификации)	16
UserID-агент	18
UserID-агент для AD/WEC	29

Пользователи и группы

Product: DCFW
Version: 8.x

Политики безопасности, правила межсетевого экрана, правила веб-безопасности и многие другие возможности UserGate DCFW могут быть применены к пользователям или группам пользователей. Возможность применения политик только к тем пользователям, которым это необходимо, позволяет администратору гибко настроить свою сеть в соответствии с потребностями организации.

Идентификация пользователя — это базисная функция DCFW. Пользователь считается идентифицированным, если система однозначно связала пользователя с IP-адресом устройства, с которого пользователь подключается к сети. DCFW использует различные механизмы для идентификации пользователей:

- Идентификация по явно указанному IP-адресу.
- Идентификация по имени и паролю.
- Идентификация пользователей терминальных серверов Microsoft с помощью специального агента терминального сервиса.
- Идентификация пользователей с помощью агента авторизации (для Windows-систем).
- Идентификация с помощью протоколов NTLM, Kerberos.

Идентификация пользователей по имени и паролю возможна через Captive-портал, который, в свою очередь, может быть настроен на идентификацию пользователей с помощью каталогов Active Directory, Radius, TACACS+, NTLM, Kerberos или локальной базы пользователей.

DCFW определяет следующие типы пользователей:

Наименование	Описание
Пользователь Unknown	Представляет множество пользователей, не идентифицированных системой.
Пользователь Known	Представляет множество пользователей, идентифицированных системой. Методы идентификации пользователей могут быть различными и более подробно будут описаны далее в этой главе.
Пользователь Any	Любой пользователь является объединением множеств пользователей Known и Unknown .
Определенный пользователь	Конкретный пользователь, определенный и идентифицированный в системе, например, пользователь DOMAIN\User, идентифицированный с помощью авторизации в домене Active Directory.

Пользователи и группы пользователей могут быть заведены на самом устройстве DCFW — это так называемые **локальные пользователи и группы** или могут быть получены с внешних каталогов, например, Microsoft Active Directory.

Группы

Группы пользователей позволяют объединить пользователей для более удобного управления политиками безопасности.

Пользователи

В данном разделе можно добавить локальных пользователей. Здесь же можно временно отключить пользователей или включить их заново.

Обязательными параметрами для создания локального пользователя являются имя пользователя и логин. Остальные параметры являются необязательными, но для корректной идентификации необходимо указать:

- Логин и пароль — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
- IP-адрес или диапазон, MAC-адрес для идентификации с помощью комбинации MAC и IP-адресов. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанных MAC и/или IP-адреса.
- VLAN ID для идентификации пользователя по тегу VLAN. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанного VLAN.
- Почтовые адреса — email пользователя. Если указан, может быть использован для отсылки пользователю информации по электронной почте, например, 2-й фактор многофакторной организации.
- Номера телефонов — телефоны пользователя. Если указан, может быть использован для отсылки пользователю информации по SMS, например, 2-й фактор многофакторной организации.

В случае, если у пользователя указан и логин, и пароль, и IP/MAC/VLAN адреса, система использует идентификацию по адресу, то есть идентификация по адресу является более приоритетной.

Учетные записи пользователей LDAP здесь не отображаются, но эти пользователи также могут быть использованы в политиках безопасности.

Серверы аутентификации

Version: 8.x
Product: DCFW

Серверы аутентификации — это внешние источники учетных записей пользователей, например, LDAP-сервер, или серверы, производящие аутентификацию для DCFW, например, RADIUS, TACACS+, Kerberos, SAML. Система поддерживает следующие типы серверов аутентификации:

Серверы аутентификации RADIUS, TACACS+, NTLM, SAML могут осуществлять только аутентификацию пользователей, в то время как LDAP-коннектор позволяет также получать информацию о пользователях и их свойствах.

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA. Пользователи и группы могут быть использованы при настройке правил фильтрации.
- Осуществлять авторизацию пользователей через домены Active Directory/FreeIPA с использованием методов аутентификации Captive-портал, Kerberos, NTLM.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN контроллера домена, то DCFW получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, DCFW будет использовать резервный. В случае недоступности части контроллеров домена с площадки, где работает DCFW, следует добавить статическую запись в настройки DNS, где были бы указаны адреса доступных контроллеров, и использовать имя этой записи в коннекторе.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Срок жизни LDAP-кэша	Срок жизни LDAP-кэша (от 1 до 48 часов). Новый срок жизни применяется к новым записям, добавляемым в LDAP-кэш после того, как администратор его установит. (Доступно начиная с релиза UGOS 7.1.3).
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена. Список доменов, указанный здесь будет использован для выбора на странице авторизации Captive-портала при включении соответствующей опции. Более подробно о настройке Captive-портала смотрите раздел Настройка Captive-портала .
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.
Kerberos keytab	Здесь можно загрузить keytab-файл для аутентификации Kerberos. Подробно об аутентификации Kerberos и создании keytab-файла смотрите в разделе Метод аутентификации Kerberos .

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

ПримечаниеДля авторизации пользователей с помощью LDAP-коннектора необходимо, чтобы пользователи входили в доменную группу Domain users.

Настройка LDAP-коннектора завершена. Для авторизации LDAP-пользователей по имени и паролю необходимо создать правила Captive-портала. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Для добавления пользователя или группы пользователей LDAP в правила фильтрации необходимо нажать на **Добавить пользователя LDAP/Добавить группу LDAP**, в поле поиска указать как минимум один символ, входящий в имена искомых объектов, после чего нажать на **Поиск** и выбрать желаемые группы/пользователей.

Сервер аутентификации пользователей RADIUS

Сервер RADIUS позволяет производить аутентификацию пользователей на серверах RADIUS, то есть DCFW выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер DCFW посылает на серверы RADIUS информацию с именем и паролем пользователя, а RADIUS-сервер отвечает, успешно прошла аутентификация или нет.

Сервер RADIUS не может предоставить список пользователей в DCFW, поэтому, если пользователи не были заведены в DCFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере RADIUS) или **Unknown** (не прошедших авторизацию).

Для создания сервера аутентификации RADIUS необходимо нажать на кнопку **Добавить**, выбрать **Добавить RADIUS-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Секрет	Общий ключ, используемый протоколом RADIUS для аутентификации.
Хост	IP-адрес сервера RADIUS.
Порт	UDP-порт, на котором сервер RADIUS слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.

После создания сервера аутентификации необходимо настроить Captive-портал для использования метода RADIUS. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Сервер аутентификации пользователей TACACS+

Сервер TACACS+ позволяет производить аутентификацию пользователей на серверах TACACS+. При авторизации через TACACS+ DCFW посылает на серверы TACACS+ информацию с именем и паролем пользователя, а сервер TACACS+ отвечает, успешно прошла аутентификация или нет.

Сервер TACACS+ не может предоставить список пользователей в DCFW, поэтому, если пользователи не были заведены в DCFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере TACACS+) или **Unknown** (не прошедших авторизацию).

Для создания сервера аутентификации TACACS+ необходимо нажать на кнопку **Добавить**, выбрать **Добавить TACACS+-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.
Порт	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+.
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Сервер аутентификации пользователей SAML IDP

Сервер аутентификации SAML IDP (Security Assertion Markup Language Identity Provider) позволяет авторизовать пользователей с помощью развернутой на предприятии системе Single Sign-On (SSO), например, Microsoft Active Directory Federation Service. Это позволяет пользователю, единожды авторизовавшись в системе SSO, прозрачно проходить авторизацию на всех ресурсах, поддерживающих аутентификацию SAML. DCFW может быть настроен в качестве SAML сервис-провайдера, использующего сервера SAML IDP для авторизации клиента.

Сервер SAML IDP не может предоставить свойства пользователей в DCFW поэтому, если не настроено подключение к домену AD с помощью LDAP-коннектора, в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере SAML) или **Unknown** (не прошедших аутентификацию).

Для использования авторизации с помощью сервера SAML IDP необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать DNS-записи для DCFW.	На контроллере домена создать DNS-запись, соответствующую DCFW, для использования в качестве домена для auth.captive, например, utm.domain.loc. В качестве IP-адреса укажите адрес интерфейса DCFW, подключенного в сеть Trusted .
Шаг 2. Настроить DNS-серверы на DCFW.	В настройках DCFW в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 3. Изменить адрес Домен auth captive-портала .	Изменить адрес Домен auth captive-портала в разделе Настройки на созданную на предыдущем шаге запись DNS. Подробно об изменении адреса домена Auth Captive-портала смотрите в разделе Общие настройки .

Наименование	Описание
Шаг 4. Настроить сервер SAML IDP.	Добавить на сервере SAML IDP запись о сервис-провайдере DCFW, указывая созданное на шаге 1 FQDN имя.
Шаг 5. Создать сервер аутентификации пользователей SAML IDP.	Создать в DCFW сервер аутентификации пользователей SAML IDP.

Для создания сервера аутентификации пользователей SAML IDP необходимо в разделе **Пользователи и устройства → Серверы аутентификации** нажать на кнопку **Добавить**, выбрать **Добавить SAML IDP-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Описание	Описание сервера аутентификации.
SAML metadata URL	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML. При нажатии на кнопку Загрузить происходит заполнение необходимых полей настройки сервера аутентификации данными, полученными из xml-файла. Это предпочтительный метод настройки сервера аутентификации SAML IDP. Подробно о сервере SAML смотрите в соответствующей документации.
Сертификат SAML IDP	Сертификат, который будет использован в SAML-клиенте. Возможны варианты: - Создать новый сертификат из скачанного — если при настройке был использован метод загрузки xml- файла, то сертификат автоматически создается и ему назначается роль SAML IDP (смотрите раздел Управление сертификатами). - Использовать существующий сертификат. Сертификат уже должен быть создан или импортирован в разделе Сертификаты, и ему не должна быть назначена роль. После создания и сохранения сервера аутентификации этому сертификату будет назначена роль SAML IDP. - Не использовать сертификат.
Single sign-on URL	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single sign-on binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты POST и Redirect . Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single logout URL	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single logout binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты POST и Redirect . Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Сервер аутентификации NTLM

Аутентификация NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации с помощью NTLM DCFW работает с контроллерами домена, выполняющими проверку пользователя с целью получения доступа в Интернет.

Сервер NTLM не может предоставить список пользователей в DCFW, поэтому, если пользователи не были заведены в DCFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере NTLM) или **Unknown** (не прошедших аутентификацию).

Аутентификация NTLM может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан. Настройка DCFW не отличается от режима работы авторизации.

Для настройки авторизации с помощью NTLM необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить синхронизацию времени с контроллером домена.	В настройках DCFW включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена.
Шаг 2. Создать DNS-запись для DCFW.	На контроллере домена создать DNS-записи, соответствующие DCFW для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса DCFW, подключенного в сеть Trusted.

Наименование	Описание
Шаг 3. Изменить адрес Домен Auth Captive-портала .	Изменить адрес домена Auth Captive-портала и опционально адрес домена Logout Captive-портала в разделе Настройки. Для домена Auth Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Для домена Logout Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Подробнее об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе Настройка Captive-портала.
Шаг 4. Добавить NTLM-сервер.	В разделе Серверы аутентификации нажать на кнопку Добавить , выбрать Добавить NTLM-сервер и указать название и имя домена Windows. Для корректной работы аутентификации NTLM, необходимо, чтобы указанное здесь имя домена резолвилось в IP-адреса контроллеров домена.
Шаг 5. Создать правило Captive-портала с аутентификацией NTLM.	Настроить Captive-портал для использования метода аутентификации NTLM. Более подробно о Captive-портале рассказывается в следующих главах руководства.
Шаг 6. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM
Шаг 7. Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса DCFW в качестве адреса прокси-сервера. Важно! Вместо IP-адреса можно использовать доменное имя, но для NTLM важно, чтобы это имя было не из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos. Важно! В настройках DCFW имена, используемые в качестве домена для auth.captive и logout.captive, не должны быть из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos.
Шаг 8. Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в Панель управления → Свойства браузера → Безопасность, выберите зону Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя и установите Автоматический вход в сеть с текущим именем пользователя и паролем (Control panel → Internet options → Security, выберите зону Internet → Custom level → User Authentication → Logon и установите Automatic logon with current name and password). Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).

Метод аутентификации Kerberos

Аутентификация Kerberos позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации через Kerberos DCFW работает с контроллерами домена, которые выполняют проверку пользователя, получающего доступ в Интернет.

Аутентификация Kerberos может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан.

Для авторизации с помощью Kerberos необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-записи для DCFW.	На контроллере домена создать DNS-записи, соответствующие DCFW, для использования в качестве доменов для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc В качестве IP-адреса укажите адрес интерфейса DCFW, подключенного в сеть Trusted. Важно! Для корректной работы создайте записи типа A, не используйте CNAME-записи.
Шаг 2. Создать пользователя для DCFW.	Создать пользователя в домене AD, например, kerb @domain.loc с опцией password never expires. Установите пароль пользователю kerb. Важно! Не используйте символы национальных алфавитов, например, кириллицу, в именах пользователя kerb или в организационных единицах Active Directory, где вы планируете создать учетную запись пользователя kerb. Важно! Не используйте в качестве пользователя для Kerberos пользователя, созданного для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись.

Наименование	Описание
Шаг 3. Создать keytab-файл.	На контроллере домена, создать keytab файл, выполнив следующую команду из-под администратора (команда в одну строку!): <pre>ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC /mapuser kerb@DOMAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:\utm.keytab</pre> Введите пароль пользователя kerb. Важно! Команда чувствительна к регистру букв. В данном примере: auth.domain.loc — DNS-запись, созданная для сервера UserGate на шаге 1 DOMAIN.LOC — Kerberos realm domain, обязательно большими буквами! kerb@DOMAIN.LOC — имя пользователя в домене, созданное на шаге 2, имя realm-домена обязательно большими буквами!
Шаг 4. Настроить DNS-серверы на UserGate.	В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 5. Настроить синхронизацию времени с контроллером домена.	В настройках UserGate включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена.
Шаг 6. Изменить адрес Домен auth captive-портала .	Изменить адрес Домен auth captive-портала и опционально адрес Домен logout captive-портала в разделе Настройки на созданные на предыдущем шаге записи DNS. Подробно об изменении адресов доменов смотрите в разделе Общие настройки .
Шаг 7. Создать LDAP-коннектор и загрузить в него keytab-файл.	Создать сервер аутентификации типа LDAP-коннектор и загрузить полученный на предыдущем шаге keytab-файл. Важно! Не используйте в качестве пользователя для LDAP-коннектора, пользователя, созданного ранее для работы Kerberos. Необходимо использовать отдельную учетную запись. Подробно о настройке LDAP-коннектора смотрите раздел LDAP-коннектор.
Шаг 8. Создать правило Captive-портала с аутентификацией по Kerberos.	Настроить Captive-портал для использования метода аутентификации Kerberos. Более подробно о Captive-портале рассказывается в разделе Настройка Captive-портала .
Шаг 9. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью Kerberos.
Шаг 10. Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера в виде FQDN-имени UserGate, созданного на шаге 3.
Шаг 11. Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в Панель управления → Свойства браузера → Безопасность, выберите зону Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя и установите Автоматический вход в сеть с текущим именем пользователя и паролем (Control panel → Internet options → Security, выберите зону Internet → Custom level → User Authentication → Logon и установите Automatic logon with current name and password). Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).

Метод аутентификации HTTP Basic

Аутентификация Basic позволяет авторизовать пользователей с явно указанным прокси-сервером по базе локальных и LDAP-пользователей. Не рекомендуется использовать данный тип аутентификации поскольку имя пользователя и пароль передаются в открытом виде по сети. Аутентификация HTTP Basic можно использовать для автоматической авторизации утилит командной строки, которым необходим доступ в Интернет, например:

```
curl -x 192.168.179.10:8090 -U user:password http://www.msn.com
```

Для авторизации по HTTP Basic необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-запись для DCFW.	На контроллере домена создать DNS-записи, соответствующие DCFW для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса DCFW, подключенного в сеть Trusted.

Наименование	Описание
Шаг 2. Изменить адрес Домен Auth Captive-портала .	Изменить адрес домена Auth Captive-портала и опционально адрес домена Logout Captive-портала в разделе Настройки. Для домена Auth Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Для домена Logout Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Подробнее об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе Настройка Captive-портала.
Шаг 3. Создать правило Captive-портала с аутентификацией по HTTP Basic.	Настроить Captive-портал для использования метода аутентификации HTTP Basic. При настройке, помимо метода HTTP Basic, необходимо добавить базу пользователей, по которой будет проверяться аутентификация (например, добавить методы аутентификации Локальный пользователь или Сервер LDAP). Более подробно о Captive-портале рассказывается в следующих главах руководства.
Шаг 4. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью HTTP Basic.
Шаг 5. Настроить прокси-сервер на компьютерах пользователей	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса DCFW в качестве адреса прокси-сервера.

Профили аутентификации

Version: 8.x
Product: DCFW

Профиль аутентификации позволяет указать набор способов и параметров авторизации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах DCFW, например, Captive-портал, VPN, веб-портал и т.д. Чтобы создать профиль аутентификации, необходимо в разделе **Пользователи и устройства → Профили аутентификации** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Профиль MFA	Профиль мультифакторной аутентификации. Должен быть предварительно создан в разделе Профили MFA, если планируется использовать мультифакторную аутентификацию. Профиль определяет способ доставки одноразового пароля для второго метода аутентификации. Более подробно о настройке профиля MFA смотрите в соответствующей главе далее. Важно! Мультифакторная аутентификация возможна только с методами аутентификации, позволяющими ввести пользователю одноразовый пароль, то есть только те, где пользователь явно вводит свои учетные данные в веб-форму страницы авторизации. В связи с этим, мультифакторная аутентификация невозможна для методов аутентификации Kerberos и NTLM.
Время бездействия до отключения	Данный параметр определяет, через сколько секунд DCFW переведет пользователя из Known users в Unknown users при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя).
Время жизни авторизованного пользователя	Данный параметр определяет, через сколько секунд DCFW переведет пользователя из Known users в Unknown users . По происшествии указанного времени пользователю потребует повторно авторизоваться на Captive-портале.
Число неудачных попыток авторизации	Разрешенное количество неудачных попыток авторизации через Captive-портал до блокировки учетной записи пользователя.
Время блокировки пользователя	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации.
Методы аутентификации	Созданные ранее методы аутентификации пользователей, например, сервер аутентификации Active Directory или RADIUS. Если указано более одного метода аутентификации, то они будут использоваться в порядке, в котором они перечислены в консоли. Также возможно использование встроенных механизмов аутентификации, таких как: • Локальный пользователь — аутентификация по базе данных локально заведенных пользователей. • Принять политику — не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Данный тип аутентификации необходимо применять совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • HTTP Basic — аутентификация с помощью устаревшего метода HTTP Basic. • Аутентификация Kerberos — аутентификация по протоколу Kerberos.

Настройка Captive-портала

Version: 8.x
Product: DCFW

Captive-портал позволяет авторизовать неизвестных пользователей (**Unknown users**) с помощью методов авторизации с использованием каталогов Active Directory, Radius, TACACS+, SAML IDP, Kerberos, NTLM или локальной базы пользователей. Кроме этого, с помощью Captive-портала можно настроить самостоятельную регистрацию пользователей с подтверждением идентификации через SMS или e-mail.

Следует помнить, что:

- Идентифицированные пользователи, например, у которых в свойствах пользователя явно указан IP-адрес, идентифицированные с помощью агентов авторизации терминальных серверов или для систем Windows, не авторизуются на Captive-портале. Такие пользователи уже относятся к типу **Known users** и не требуют дополнительной идентификации.
- Авторизация с помощью Captive-портала возможна только для протоколов HTTP и HTTPS. Например, если вы создали правило межсетевого экрана, разрешающее доступ в интернет по протоколу FTP только для пользователя **Known users**, то пользователи не смогут получить доступ в интернет по этому протоколу до тех пор, пока они не станут идентифицированными, то есть не запустят у себя браузер и не пройдут авторизацию на Captive-портале.
- Для авторизации пользователей, работающих по протоколу HTTPS, необходимо настроить инспектирование SSL, иначе авторизация работать не будет.
- Если Captive-портал использует метод авторизации Active Directory, то пользователь должен указывать в качестве логина свое доменное имя в формате DOMAIN\username или username@domain.

Настройка Captive-портала сводится к следующим шагам:

Наименование	Описание
Шаг 1. Создать метод авторизации, например, авторизация с помощью домена Active Directory.	В консоли DCFW в разделе Пользователи и устройства → Серверы аутентификации нажать на кнопку Добавить и создать сервер авторизации.
Шаг 2. Создать профиль аутентификации, в котором указать необходимые методы авторизации.	В консоли DCFW в разделе Пользователи и устройства → Профили аутентификации нажать на кнопку Добавить и создать профиль авторизации, используя созданный ранее метод авторизации.
Шаг 3. Создать Captive-профиль, в котором указать необходимые профили аутентификации.	В консоли DCFW в разделе Пользователи и устройства → Captive-профили нажать на кнопку Добавить и создать Captive-профиль, используя созданный ранее профиль авторизации.
Шаг 4. Создать правило Captive-портала.	Правило Captive-портала определяет трафик, к которому должны быть применены методы идентификации пользователей, указанные в Captive-профиле. В консоли DCFW в разделе Пользователи и устройства → Captive-портал нажать на кнопку Добавить и создать правило Captive-портала.
Шаг 5. Настроить DNS для доменов auth.captive и logout.captive.	Служебные доменные имена auth.captive и logout.captive используются DCFW для авторизации пользователей. Если клиенты используют в качестве DNS-сервера DCFW то ничего делать не надо. В противном случае необходимо прописать в качестве IP-адреса для этих доменов IP-адрес интерфейса DCFW, который подключен в клиентскую сеть. Альтернативное решение — настроить параметры Домен auth captive-портала и Домен logout captive-портала . Более подробно эти параметры описаны в разделе Общие настройки .

Создание методов авторизации подробно рассматривалось в предыдущих главах. Рассмотрим более подробно создание Captive-профиля и правил Captive-портала.

Чтобы создать Captive-профиль, необходимо в разделе **Captive-профили** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название Captive-профиля.
Описание	Описание Captive-профиля.
Шаблон страницы авторизации	Выбрать шаблон страницы авторизации. Создавать страницы авторизации можно в разделе Библиотеки → Шаблоны страниц . Если необходимо настроить самостоятельную регистрацию пользователей с подтверждением по SMS или e-mail, то следует выбрать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).

Наименование	Описание
Метод идентификации	Метод, с помощью которого DCFW запомнит пользователя. Возможны 2 варианта: • Запоминать IP-адрес. После успешной авторизации пользователя через Captive-портал DCFW запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут относиться к данному пользователю. Данный метод позволяет идентифицировать данные, передаваемые по любому из протоколов семейства TCP/IP, но не будет корректно работать при наличии NAT-подключения между пользователями и DCFW. Это рекомендуемое значение, устанавливаемое по умолчанию. • Запоминать cookie. После успешной авторизации пользователя через Captive-портал DCFW добавляет в браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя. Данный метод позволяет авторизовать пользователей, находящихся за NAT-устройством, но авторизуется только протокол HTTP(S) и только в том браузере, в котором происходила авторизация через Captive-портал. Кроме этого, для авторизации HTTPS-сессий пользователя DCFW будет принудительно дешифровать все HTTPS-соединения. Для правил межсетевого экрана пользователь, идентифицированный по cookie, будет всегда определен как Unknown user.
Профиль аутентификации	Созданный ранее профиль авторизации, определяющий методы аутентификации.
Режим аутентификации	Аутентификация с помощью логина и пароля через RADIUS сервер (AAA) или посредством сертификатов (PKI).
Профиль сертификата пользователя	При выборе режима аутентификации посредством сертификатов PKI необходимо указать сконфигурированный ранее профиль пользовательских сертификатов.
URL для редиректа	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL.
Разрешить браузерам запомнить авторизацию	Включает возможность сохранить авторизацию в браузере на указанное время в часах. Для сохранения авторизационной информации используются cookie.
Предлагать выбор домена AD/LDAP на странице авторизации Captive-портала	Если в качестве метода аутентификации используется авторизация с помощью Active Directory, то при включении данного параметра пользователь сможет выбрать имя домена из списка на странице авторизации. Если данный параметр не включен, пользователь должен явно указывать домен в виде DOMAIN\username или username@domain.
Показывать CAPTCHA	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей.

Для настройки самостоятельной регистрации пользователей с подтверждением пароля с помощью SMS или e-mail необходимо настроить параметры на вкладке **Регистрация гостевых пользователей**. Следует помнить, что в этом случае необходимо использовать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).

Наименование	Описание
Профиль оповещения	Профиль оповещения, который будет использоваться для отсылки информации о созданном пользователе и его пароле. Может использоваться 2 типа — SMS и email. Более подробно о создании профиля оповещения смотрите в главе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.
Тема оповещения	Тема оповещения (только для email-оповещений).
Письмо оповещения	Тело письма сообщения. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль.
Дата и время окончания	Время, когда учетная запись временного пользователя будет отключена.
Время жизни	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена.
Длина пароля	Определяет длину пароля для создаваемого пользователя.
Сложность пароля	Определяет сложность пароля для создаваемого пользователя. Возможны варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спец. символы.

Наименование	Описание
Группы	Группа для временных пользователей, в которую будут помещены создаваемые пользователи.

Чтобы создать правило Captive-портала, необходимо нажать на кнопку **Добавить** в разделе **Captive-портал** и указать необходимые параметры:

Наименование	Описание
Название	Название правила Captive-портала.
Описание	Описание правила Captive-портала.
Captive-профиль	Выбрать Captive-профиль, созданный ранее. Доступно действие Не использовать аутентификацию , при выборе которого аутентификация не будет требоваться.
Записывать в журнал правил	При активации данной опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики.
Источник	Адреса источника. В качестве источника можно указать определенную зону, например, зону LAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (GeoIP). Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Адреса назначения. В качестве адресов можно указать определенную зону, например, зону WAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (GeoIP). Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Категории	Категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию.
URL	Списки URL, для которых будет применяться правило.
Время	Время, когда данное правило будет активно.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Таким образом, создав несколько правил Captive-портала, можно настроить различные политики идентификации пользователей для различных зон, адресов, категорий сайтов и времени.

Примечание Условия, указанные во вкладках правила, применяются согласно логике "И", то есть требуют совпадения всех указанных условий для того, чтобы правило сработало. Если необходимо использовать логику "ИЛИ", то это достигается путем создания нескольких правил.

Примечание Правила применяются в порядке, в котором они отображаются в консоли. Вы можете изменить порядок правил с помощью соответствующих кнопок.

Примечание При обработке правил применяется только первое сработавшее правило.

В случае, если необходимо сменить пользователя после его авторизации в системе или выйти из системы, необходимо перейти на URL <http://logout.captive> и нажать на кнопку **Выйти**.

Пользователи терминальных серверов

Version: 8.x
Product: DCFW

Терминальный сервер служит для удаленного обслуживания пользователя с предоставлением рабочего стола или консоли. Как правило, один терминальный сервер предоставляет свой сервис нескольким пользователям, а в некоторых случаях десяткам или даже сотням пользователей. Проблема идентификации пользователей терминального сервера состоит в том, что у всех пользователей сервера будет определен один и тот же IP-адрес, и DCFW не может корректно идентифицировать сетевые подключения пользователей. Для решения данной проблемы предлагается использование специального агента терминального сервиса. Каждому пользователю выделяется диапазон портов, с использованием которых происходит соединение пользователя, т.е. исходные порты подменяются на порты из выделенного для пользователя диапазона.

Агент терминального сервиса должен быть установлен на все терминальные серверы, пользователей которых необходимо идентифицировать. Агент представляет собой сервис, который передает на UserGate DCFW информацию о пользователях терминального сервера и об их сетевых соединениях. В силу специфики работы протокола TCP/IP, агент терминального сервиса может идентифицировать трафик пользователей, передаваемый только с помощью TCP и UDP протоколов. Протоколы, отличные от TCP/UDP, например, ICMP, не могут быть идентифицированы.

Для корректной идентификации пользователей, в случае использования на терминальных серверах авторизации Active Directory, требуется настроенный сервер Active Directory коннектор.

Чтобы начать работу с аутентификацией пользователей на терминальных серверах, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис Агент аутентификации на необходимой зоне.	В разделе Сеть → Зоны разрешить сервис Агент Аутентификации для той зоны, со стороны которой расположены серверы терминального доступа.
Шаг 2. Задать пароль агентов терминального сервера.	В консоли DCFW в разделе UserGate → Настройки → Модули напротив записи Пароль агентов терминального сервиса нажать на кнопку Настроить и задать пароль агентов терминального сервера.
Шаг 3. Установить агент терминального сервера.	Установить агент терминального сервера на все серверы, для которых необходимо идентифицировать пользователей. При установке следует задать IP-адрес DCFW и заданный на предыдущем шаге пароль.
Шаг 4. Добавить необходимые серверы в консоли DCFW.	В разделе Пользователи и устройства → Терминальные серверы необходимо добавить агентов терминального сервера, указав имя и адрес хоста. После получения данных с указанного в настройках хоста и совпадении пароля, указанного в пункте 2, аутентификация пользователей будет включена автоматически. При обновлении версии DCFW агенты терминальных серверов, которые ранее отображались в веб-консоли, будут продолжать работать.

UserGate теперь будет получать информацию о пользователях.

Агент терминального сервера позволяет аутентифицировать не только доменных, но и локальных пользователей терминального сервера. Для этого необходимо добавить в файл конфигурации (%ALLUSERSPROFILE%\Entensys\Terminal Server Agent\tsagent.cfg) следующий параметр:

LocalDomain = 1

При включении данного параметра информация о пользователях будет передаваться на DCFW в формате "имя сервера_имя пользователя" для локальных пользователей или "имя домена_имя пользователя" для доменных.

Таких пользователей также необходимо добавить в DCFW как локальных. О добавлении пользователей читайте в разделе [Пользователи](#). При добавлении необходимо указать **Логин** в приведенном выше формате; пароль указывать не нужно.

Данная опция предназначена, в основном, для терминальных серверов, не включенных в домен, вход на который осуществляется с локальными учетными данными.

После изменения файла конфигурации сервис терминального агента нужно перезапустить.

ПримечаниеИмя компьютера должно состоять из букв, цифр и знака подчёркивания; использование тире не допускается.

Параметры терминального сервера могут быть изменены путём внесения изменений в файл конфигурации агента аутентификации для терминальных серверов. После внесения изменений агент аутентификации необходимо перезапустить.

Нижепредставлен список параметров файла tsagent.cfg:

- **TimerUpdate:** периодичность отправки данных (указывается в секундах).
- **MaxLogSize:** максимальный размер журнала работы сервиса (указывается в Мбайт).
- **SharedKey:** пароль для подключения агента.
- **SystemAccounts:** может принимать значения **0** или **1**. При значении параметра **SystemAccounts=1** включает передачу информации о соединениях системных аккаунтов (system, local service, network service) и портах, используемых для соединения, на DCFW.
- **FQDN:** может принимать значения **0** или **1**. Значение параметра **FQDN=1** соответствует использованию FQDN (Fully Qualified Domain Name), например, «example.com» вместо «example».
- **ServerPort:** номер порта DCFW, принимающего соединение от агента авторизации. По умолчанию используется порт UDP:1813.
- **ServerAddress:** IP-адрес устройства UserGate, принимающего соединение от агента аутентификации.
- **UserCount:** максимальное количество пользователей.
- **BlockDNS:** может принимать значения **0** или **1**. При **BlockDNS=1** происходит замена порта источника на свободный порт из выделенного для пользователя диапазона при DNS запросе (UDP:53); при **BlockDNS=0** — отправка трафика происходит без замены порта.
- **BlockUDP:** может принимать значения **0** или **1**. Значение параметра **BlockUDP=1** соответствует замене порта источника на свободный порт из

выделенного для пользователя диапазона при отправке трафика UDP; при **BlockUDP=0** — отправка трафика происходит без замены порта.

- **ExcludeIP:** в случае, если на терминальном сервере настроены несколько IP-адресов, то все они будут использованы для аутентификации пользователей. Параметр ExcludeIP позволяет ограничить аутентификацию пользователей с определённых IP-адресов терминального сервера:
 - IP-адреса в формате x.x.x.x и/или адреса подсетей в формате x.x.x.x/n указываются через точку с запятой (например, **ExcludeIP=x.x.x.x/n; x.x.x.x**).
 - Допускается использование пробелов между адресами в списке, они игнорируются (например, **ExcludeIP=x.x.x.x/n; x.x.x.x;y.y.y.y**).
 - Если в строке есть ошибки в написании адресов, они будут отражены в логах при старте агента. Будут использованы только правильно указанные адреса. Количество используемых адресов из списка записывается в лог при старте агента.
 - Если в результате фильтрации будут исключены все адреса из рассылки, то делается запись в лог (один раз) в виде: **GetIPAddressList: IP list is blocked by ExceptIP**. Если позже будет сформирована непустая рассылка, то делается запись в лог в виде: **GetIPAddressList: IP list is not blocked by ExceptIP anymore**.
- **ExcludePorts:** диапазон, порты из которого не будут подменяться на порты из выделенного для пользователя диапазона портов (диапазон портов указывается следующим образом: **ExcludePorts=port1-port2**).
- **NAT_IP:** необходим при наличии NAT между терминальным сервером и UserGate: замена IP-адреса терминального сервера на один из адресов указанного диапазона. Адреса указываются в следующем виде: **NAT_IP="12.3.4-1.1.1;2.2.2-5.5.5"**.

Для исключения из рассылки определенных адресов и/или подсетей терминальным агентом помимо добавления параметра **ExcludeIP** в файл конфигурации tsagent.cfg он может быть активирован и в реестре сервера следующим образом:

- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать только для данного пользователя.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать для всех пользователей данной системы.

Порядок поиска настроек параметра ExcludeIP в системе следующий: сначала параметр ищется в ветке реестра [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client], затем в ветке реестра [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client], затем в файле tsagent.cfg.

Профили MFA (мультифакторной аутентификации)

Version: 8.x
Product: DCFW

Мультифакторная аутентификация — это метод идентификации и аутентификации пользователя, где используются два или более различных типа идентификационных данных. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту учетной записи от несанкционированного доступа.

DCFW поддерживает мультифакторную аутентификацию с использованием имени пользователя и пароля в качестве первого типа аутентификации и следующих типов в качестве второго:

- **TOTP** (Time-based One Time Password) токена в качестве второго. TOTP-токен создает одноразовый пароль на основе времени, то есть время является параметром; более подробно о TOTP можно прочитать в https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm. В качестве TOTP-токена могут выступать различные устройства либо программное обеспечение, установленное на смартфоны пользователей, например, Google Authenticator.
- **SMS** — получение одноразового пароля по SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в DCFW или в доменной учетной записи в Active Directory.
- **Email** — получение одноразового пароля по электронной почте. Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в DCFW или в доменной учетной записи в Active Directory.

Чтобы настроить мультифакторную аутентификацию, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить авторизацию с помощью Captive-портала.	Мультифакторная авторизация работает только при авторизации пользователей с помощью Captive-портала. Смотрите раздел для подробной информации.
Шаг 2. Создать профиль мультифакторной авторизации.	В разделе консоли Пользователи и устройства → Профили MFA создать профиль мультифакторной авторизации. При создании профиля указать необходимые настройки доставки второго фактора авторизации. Возможно создать 3 типа доставки: • MFA через TOTP — доставка второго фактора авторизации с помощью токенов TOTP. • MFA через SMS — доставка второго фактора авторизации с помощью SMS. • MFA через email — доставка второго фактора авторизации с помощью email.

Для способа доставки **MFA через TOTP** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Инициализация TOTP	Для получения токенов TOTP необходимо произвести первоначальную инициализацию устройства или ПО клиента. Для этого требуется ввести уникальный ключ в устройство или ПО клиента. Передать первоначальный код для инициализации TOTP можно следующими средствами: • Показать на странице Captive-портала после первой успешной авторизации. Для этого варианта необходимо выбрать Показать ключ на странице Captive -портала. • Выслать с помощью SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в DCFW или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки SMS (профиль SMPP). • Выслать с помощью email Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в DCFW или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки email (профиль SMTP).
Показывать QR-код	Показывать QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.

В случае, если пользователь утратил токен, администратор может потребовать повторной инициализации TOTP-токена. Для этого ему необходимо выбрать данного пользователя в списке пользователей (**Пользователи и устройства** → **Пользователи**) и выбрать действие **Сбросить ключ TOTP**. При следующей авторизации пользователю будет предложено заново проинициализировать свой токен.

Для способа доставки **MFA через SMS** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.

Наименование	Описание
Профиль отправки MFA	Профиль SMPP, который будет использован для отправки паролей с помощью сообщений SMS. Подробно о настройке профилей отсылки сообщений через SMS смотрите в разделе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.
Содержимое	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

Для способа доставки **MFA через email** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Профиль отправки MFA	Профиль SMTP, который будет использован для отправки паролей с помощью сообщений электронной почты. Подробно о настройке профилей отсылки сообщений по электронной почте смотрите в разделе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.
Тема	Тема оповещения.
Содержимое	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

Technology: Identification and Authentication

Version: 8.x

Product: DCFW

UserID — технология прозрачной аутентификации пользователей на устройствах UserGate. Источниками данных для однозначной идентификации пользователей являются журналы безопасности операционных систем доменных контроллеров, данные журналов серверов приложений и доступа, в которых пользователи уже аутентифицированы.

Для того, чтобы создавать политики, включающие пользователей и группы, межсетевому экрану необходимо сопоставить IP-адреса с пользователями, получившими эти адреса и извлечь информацию о группах, в которые они входят. UserID предоставляет несколько методов, позволяющие выполнить такое сопоставление. Например, для получения информации о пользователях UserID может просматривать журналы на серверах в поисках сообщений от служб аутентификации. Те пользователи, чьи имена не удалось сопоставить с IP-адресами, могут быть перенаправлены на специальный портал (Captive Portal) для прохождения аутентификации. Для получения информации о группах межсетевой экран подключается напрямую к серверам LDAP.

В настоящий момент в качестве источников данных для аутентификации в UserID используются журналы Microsoft ActiveDirectory, данные, полученные по syslog, или сообщения RADIUS accounting (начиная с версии ПО 7.2.0).

Для конечных пользователей работа UserID полностью прозрачна, то есть пользователям нет необходимости в явном виде проходить аутентификацию на DCFW.

Принцип работы UserID

В зависимости от сценария использования и настройки UserID агент получает данные о событиях, связанных с аутентификацией пользователей, одним из следующих способов:

1. Непосредственное получение данных узлом с UserID агентом от источников данных аутентификации с помощью настроенных коннекторов:

- UserID агент может подключаться к контроллеру домена AD через технологию WMI и считывать журналы событий безопасности.
- UserID агент может принимать со сторонних серверов сообщения по стандарту syslog.
- UserID агент может принимать со сторонних RADIUS NAS-серверов сообщения RADIUS accounting.

2. Работа с источником данных через посредника — специального программного агента, который устанавливается на контроллер домена или сервер-сборщик событий (WEC):

- Программный агент UserID для AD/WEC устанавливается на контроллер домена (AD) или сервер-сборщик событий домена (WEC), читает необходимую для идентификации пользователя информацию из журналов безопасности Windows и пересылает её в формате syslog на коллектор UserID на LogAn (подробнее об агенте читайте в статье [UserID агент для AD/WEC](#)).

Главные достоинства данного способа получения данных из домена AD:

- Не требуется предоставлять доступ извне в контроллер домена для сбора данных об аутентификации пользователей, как это требуется при доступе по технологии WMI.
- Не требуется создавать в домене специальный аккаунт с особыми привилегиями для узлов, на которых работает UserID агент.

Рассмотрим принцип работы технологии UserID на примере сценария взаимодействия с Active Directory в качестве источника данных для аутентификации пользователей через технологию WMI.

На контроллере домена AD работает аудит событий безопасности, который записывает события по настроенным категориям в специальный журнал аудита.

После создания и настройки UserID агента и коннектора "Microsoft Active Directory" на DCFW, UserID агент начинает периодически отправлять на контроллер AD WMI-запросы для извлечения следующих событий по Event ID из журнала аудита:

- 4624 — успешный вход в систему;
- 4768 — запрос билета аутентификации Kerberos TGT;
- 4769 — запрос билета аутентификации Kerberos TGS;
- 4770 — обновление билета аутентификации Kerberos TGS;
- 4627 — сведения о членстве в группах.

Данные события позволяют UserID агенту получать информацию о регистрации пользователей и членстве в группах. Полученная информация записывается в специальную системную базу данных на DCFW.

UserID агент периодически обращается к этой базе данных, извлекает из записей имя пользователя, домен, SID, IP-адрес, список групп пользователя. Эти данные кэшируются. Интервал поиска записей в базе данных можно задать в настройках UserID агента. Время жизни данных о пользователе в кэше устанавливается в настройках коннектора UserID агента на DCFW.

В случае, если список групп, в которые входит пользователь, не был получен, UserID агент обращается к контроллеру домена по протоколу LDAP в соответствии с настроенным профилем аутентификации для получения информации о группах.

При обработке сетевого трафика, в том случае, если в правилах настроены условия для определённых пользователей и групп, DCFW обращается к кэшу для поиска информации о том, какие пользователи зарегистрированы с какими IP-адресами. Эта информация используется для принятия решения о том, как будут обрабатываться пакеты.

Завершение сессий пользователей может принудительно инициироваться администратором DCFW. Для этого администратор может выполнить сброс всех пользователей или сброс отдельного пользователя:

- В веб-консоли администратора в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** на панели инструментов нажать кнопку **Сбросить аутентификацию всех пользователей**:



- В консоли CLI — [командой](#):

```
Admin@nodename# execute termination user-sessions ip <IP-address>
```

В сценарии с использованием в качестве источника данных аутентификации пользователей серверов-источников данных syslog принцип работы аналогичен, только DCFW в этом случае выступает в роли syslog listener — принимает сообщения от отправителя syslog (номер порта и протокол устанавливаются в настройках UserID агента, по умолчанию порт TCP 514) и затем отфильтровывает нужные события из потока принятых данных с помощью настроенных фильтров из библиотеки "Syslog фильтры UserID агента". В этом случае в базу данных сохраняются: имя пользователя, IP-адрес, SID (опционально). Для получения информации о группах, в которых зарегистрирован пользователь, UserID агент обращается к контроллеру домена по LDAP протоколу в соответствии с настроенным профилем аутентификации UserID агента.

В сценарии с использованием сообщений RADIUS accounting в качестве источника данных аутентификации пользователей принцип работы в целом схож. DCFW в этом сценарии выступает в роли пропускного RADIUS-сервера — принимает сообщения RADIUS accounting от серверов NAS (по порту UDP 1813) и проверяет пользователя на контроллере домена AD по LDAP в соответствии с настроенным профилем аутентификации UserID агента.

Настройка UserID агента на DCFW не является кластерной, а значит ее нужно производить на каждом узле отдельно. После настройки UserID агент будет работать самостоятельно и самостоятельно получать данные о событиях логин/логаут из журналов источников.

Помимо DCFW UserID может работать на устройствах LogAn (Log Analyzer). Подробнее о работе UserID на LogAn читайте в руководстве администратора Log Analyzer. Использование LogAn позволяет масштабировать технологию UserID на другие устройства сети. Принцип работы UserID на устройстве LogAn аналогичен принципу работы на DCFW. Найденные в собранных данных события отправляются на другие DCFW в соответствии с политикой UserID Sharing на основании настроенных профилей редистрибуции. Данная политика позволяет при необходимости отправлять разные данные на разные узлы DCFW. На DCFW отправляются только GUID пользователя, его IP-адрес и список идентификаторов групп, участником которых он является. Такая архитектура позволяет

использовать один или несколько серверов LogAn для централизованного сбора информации о пользователях с различных источников и далее централизованно и избирательно распространять эту информацию на узлы DCFW в сети.

Алгоритм настройки UserID

Для настройки работы UserID необходимо выполнить ряд действий как на стороне источников данных аутентификации, так и на DCFW.

На стороне источников данных

При работе с Active Directory в качестве источника данных об аутентификации пользователей, необходимо включить аудит событий безопасности. Потребуются следующие категории:

- Audit LogOn;
- Audit LogOff;
- Audit Kerberos Authentication Service;
- Audit Group Membership;
- Audit Kerberos Service Ticket Operations.

При работе с серверами-источниками данных syslog необходимо на них настроить отправку журналов на адрес UserID агента (то есть на IP-адрес DCFW; номер порта и протокол устанавливаются в настройках UserID агента, по умолчанию порт TCP 514).

При работе с серверами RADIUS NAS необходимо на серверах настроить отправку сообщений RADIUS accounting на адрес UserID агента (то есть на IP-адрес DCFW, порт UDP 1813).

На стороне DCFW

На стороне DCFW необходимо выполнить следующие настройки:

- Создать сервер аутентификации для UserID агента. Подробнее о создании и настройке сервера аутентификации читайте в статье [Серверы аутентификации](#).
- Создать профиль аутентификации для UserID агента. Подробнее о создании и настройке профиля аутентификации читайте в статье [Профили аутентификации](#).
- Для сценария с серверами-источниками данных syslog активировать сервис "UserID syslog collector" в настройках контроля доступа зоны, где будет находиться отправитель syslog. Для сценария с RADIUS NAS-серверами активировать сервис "Агент аутентификации" в настройках контроля доступа зон, где будет находиться серверы RADIUS NAS. Подробнее о создании и настройке зон читайте в статье [Настройка зон](#).
- Создать коннектор UserID агента в соответствии с методом получения данных аутентификации;
- Настроить общие параметры UserID агента.

Создание коннектора UserID агента

Коннектор UserID агента в веб-консоли администратора DCFW создаётся в разделе **Настройки → Пользователи и устройства → UserID агент коннекторы**. Необходимо нажать кнопку **Добавить** на панели инструментов и выбрать тип создаваемого коннектора:

- Microsoft Active Directory;
- Отправитель syslog;
- RADIUS-сервер.

Microsoft Active Directory

В случае, если в качестве источника информации выступает Microsoft Active Directory, необходимо:

1. Настроить источник событий.
2. Настроить параметры коннектора UserID агента для мониторинга AD.

Для включения аудита событий на сервере AD необходимо отредактировать **Политики Аудита** в **Политике домена** по умолчанию и **Конфигурацию расширенной политики**, как указано на следующих снимках экрана, используя оснастку gpedit.msc:



Политика Default Domain Policy [DC.LAB.LOC]

Конфигурация компьютера

Политики

Конфигурация программ

Конфигурация Windows

Политика разрешения имен

Сценарии (запуск/завершение)

Параметры безопасности

Политики учетных записей

Политика паролей

Политика блокировки учетной записи

Политика Kerberos

Локальные политики

Политика аудита

Назначение прав пользователя

Параметры безопасности

Журнал событий

Группы с ограниченным доступом

Системные службы

Реестр

Файловая система

Политики проводной сети (IEEE 802.3)

Монитор брандмауэра Защитника Windows

Политики диспетчера списка сетей

Политики беспроводной сети (IEEE 802.11)

Политики открытого ключа

Политики ограниченного использования

Политики управления приложениями

Политики IP-безопасности на "Служба"

Конфигурация расширенной политики

Политики аудита

Вход учетной записи

Управление учетными записями

Подробное отслеживание

Доступ к службе каталогов (DS)

Вход/выход

Доступ к объектам

Изменение политики

Использование привилегий

Система

Аудит доступа к глобальным объектам

Подкатегория

Аудит блокировки учетных записей

Аудит заявок пользователей или устройств на доступ

Членство в группе аудита

Аудит расширенного режима IPsec

Аудит основного режима IPsec

Аудит быстрого режима IPsec

Аудит выхода из системы

Аудит входа в систему

Аудит сервера политики сети

Аудит других событий входа и выхода

Аудит специального входа

События аудита

Не настроено

Не настроено

Успех и отказ

Не настроено

Не настроено

Не настроено

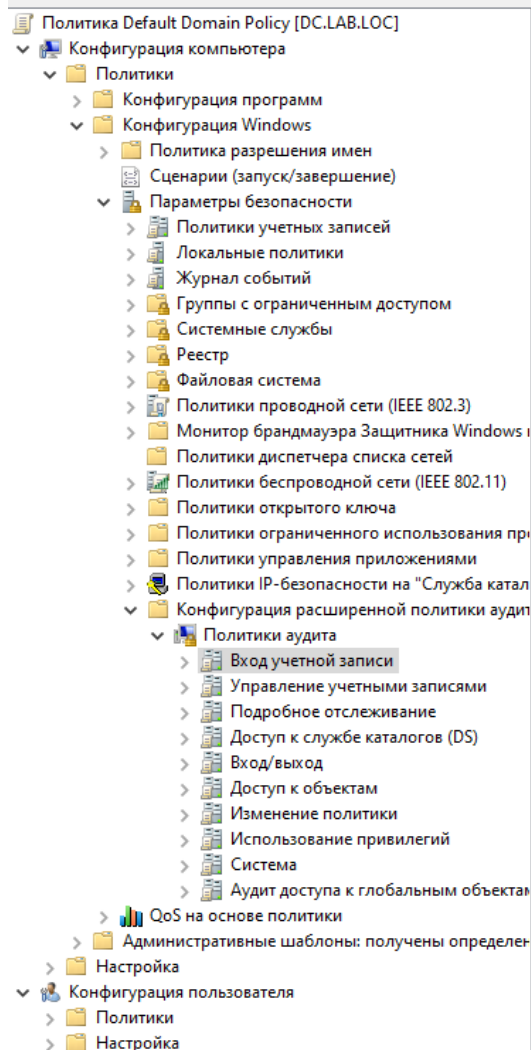
Успех и отказ

Успех и отказ

Не настроено

Не настроено

Не настроено



Подкатегория	События аудита
Аудит проверки учетных данных	Не настроено
Аудит службы проверки подлинности Kerberos	Успех и отказ
Аудит операций с билетами службы Kerberos	Успех и отказ
Аудит других событий входа учетных записей	Не настроено

Для выполнения WMI-запросов необходимо создать пользователя с соответствующими привилегиями по процедуре, указанной ниже.

Внимание! Эти настройки нужны для подключения агента по WMI посредством учётной записи с ограниченными правами.

1. Создать учётную запись пользователя на контроллере домена:

- Перейти в меню **Пуск → Диспетчер серверов → Средства → Active Directory — пользователи и компьютеры**
- В необходимом Подразделении (OU) создать **Нового пользователя** для UserID.

2. Сконфигурировать членство в группах для новой учётной записи пользователя:

- Нажать правой кнопкой мыши по новой учётной записи пользователя UserID и выбрать **Свойства**.
- Нажать на вкладку **Членство в группах**.
- Нажать **Добавить → Дополнительно → Поиск**.
- Выбрать следующие группы:
 - **Пользователи DCOM**
 - **Пользователи журналов производительности**
 - **Пользователи удалённого рабочего стола**
 - **Читатели журнала событий**
- Нажать **ОК**

3. Назначить права Distributed Component Object Model (DCOM):

- Перейти в меню Windows **Пуск → Администрирование → Службы компонентов**. Откроется окно **Службы компонентов**.
- Раскрыть **Службы компонентов → Компьютеры → Мой компьютер**.
- Нажать правой кнопкой мыши по **Мой компьютер** и выбрать **Свойства**. Откроется окно **Свойства: Мой компьютер**.
- Перейти во вкладку **Безопасность COM**.
- В области Права доступа нажать **Изменить ограничения**.
- Убедиться, что для **Пользователи DCOM** выбрано **Локальный доступ** и **Удалённый доступ**.

- Нажать **ОК**, чтобы сохранить настройки.
- В окне **Свойства: Мой компьютер** нажать в области **Разрешения на запуск и активацию** на **Изменить ограничения**.
- Убедиться, что для **Пользователи DCOM** выбрано **Локальный запуск**, **Удалённый запуск**, **Локальная активация** и **Удалённая активация**.
- Нажать **ОК**, чтобы сохранить настройки, и ещё раз нажать **ОК**, чтобы закрыть окно **Свойства: Мой компьютер**.
- Выбрать **Файл → Выход**, чтобы закрыть окно **Службы компонентов**.

4. Сконфигурировать назначения защиты пространства имён WMI:

- Перейти в меню **Пуск → Выполнить**.
- Ввести `wmicmgmt.msc` и нажать **ОК**.
- Нажать правой кнопкой мыши на **Элемент управления WMI (локальный)** и выбрать **Свойства**.
- Перейти на вкладку **Безопасность**.
- Нажать **Безопасность → Добавить → Дополнительно → Поиск**.
- Выбрать новую учётную запись пользователя, нажимать **ОК**, пока вы не вернётесь в окно **Безопасность** для Root.
- Нажать **Дополнительно** и выбрать добавленную учётную запись пользователя.
- Нажать **Изменить**.
- В меню **Применяется к:** выбрать **Данное пространство и подпространство имён**.
- Убедиться, что выбрано **Выполнение методов**, **Включить учётную запись**, **Включить удалённо** и **Прочитать безопасность**.
- Нажать **ОК**, пока вы не вернётесь в окно `wmicmgmt`.
- Выбрать **Файл → Выход**, чтобы закрыть окно `wmicmgmt`.

Внимание! Обновление Windows KB5014692 может привести к появлению ошибок доступа к WMI типа: `NTSTATUS: NT_STATUS_ACCESS_DENIED`. В этом случае можно попробовать добавить в реестр Windows следующую информацию:

Path : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat
 Value Name: "RequireIntegrityActivationAuthenticationLevel"
 Type: dword
 Value Data: 0x00000000

При использовании серверов AD в качестве источников событий UserID агент выполняет WMI-запросы для поиска событий, связанных с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627).

В веб-консоли администратора DCFW в разделе **Настройки → Пользователи и устройства → UserID агент коннекторы** необходимо нажать кнопку **Добавить** на панели инструментов и выбрать тип создаваемого коннектора: **Microsoft Active Directory**. Далее указать следующие данные:

- **Включено** — Включение/отключение получения журналов с источника.
- **Название** — Название источника.
- **Описание** — Описание источника (опционально).
- **Адрес сервера** — Адрес сервера Microsoft Active Directory.
- **Протокол** — Протокол доступа к AD (WMI).
- **Пользователь** — Имя пользователя для подключения к AD.
- **Пароль** — Пароль пользователя для подключения к AD.
- **Профиль аутентификации** — Название созданного ранее профиля аутентификации, с помощью которого производится поиск пользователей, найденных в журналах AD.
- **Время жизни аутентифицированного пользователя (сек.)** — Период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кэша на DCFW. Значение по умолчанию - 2700 секунд (45 минут).

В случае, если в качестве источника информации выступает отправитель syslog, необходимо:

1. Настроить источник событий.

Для корректной работы коннектора UserID агента syslog, необходимо настроить сервер-источник данных syslog для отправки журналов на адрес UserID агента. Подробнее см. документацию на отправитель syslog.

Параметры сервера syslog на DCFW можно посмотреть/скорректировать в [общих настройках UserID агента](#).

2. Разрешить сбор информации с удалённых устройств по протоколу syslog.

В настройках контроля доступа зоны, в которой находится отправитель syslog, разрешить сервис "UserID syslog коллектор".

3. Настроить параметры коннектора UserID агента для отправителя syslog.

В веб-консоли администратора DCFW в разделе **Настройки → Пользователи и устройства → UserID агент коннекторы** необходимо нажать кнопку **Добавить** на панели инструментов и выбрать тип создаваемого коннектора: **Отправитель syslog**. Далее указать следующие данные:

- **Включено** — Включение/отключение получения журналов с источника.
- **Название** — Название источника.
- **Описание** — Описание источника (опционально).
- **Адрес сервера** — Адрес хоста, с которого DCFW будет получать события по протоколу syslog.
- **Домен по умолчанию** — Название домена, который используется для поиска найденных в журналах syslog пользователей.
- **Часовой пояс** — Часовой пояс, установленный на источнике.
- **Профиль аутентификации** — Профиль аутентификации, с использованием которого происходит поиск пользователя, найденного в журналах syslog.
- **Время жизни аутентифицированного пользователя (сек.)** — Период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кэша на DCFW. Значение по умолчанию - 2700 секунд (45 минут).

На вкладке **Фильтры** выбираются фильтры для поиска необходимых записей журнала.



Фильтры создаются и настраиваются в разделе **Библиотеки → Syslog фильтры UserID агента**. Подробнее читайте в разделе [Syslog фильтры UserID агента](#).

RADIUS accounting

(Доступно начиная с версии ПО 7.2.0).

В случае, если источником информации выступают сообщения RADIUS accounting, необходимо:

1. Настроить источник событий.

Для корректной работы коннектора UserID агента, необходимо настроить NAS-сервер для отправки сообщений RADIUS accounting на адрес UserID агента (порт UDP 1813). Подробнее см. документацию на NAS-сервер.

2. Разрешить получение запросов RADIUS accounting от удалённых устройств.

В настройках контроля доступа зон, в которых находятся NAS-серверы, разрешить сервис "Агент аутентификации".

3. Настроить параметры коннектора UserID агента для RADIUS-сервера.

В веб-консоли администратора DCFW в разделе **Настройки → Пользователи и устройства → UserID агент коннекторы** необходимо нажать кнопку **Добавить** на панели инструментов и выбрать тип создаваемого коннектора: **RADIUS-сервер**. Далее указать следующие данные:

- **Включено** — Включение/отключение получения журналов с источника.
- **Название** — Название источника.
- **Описание** — Описание источника (опционально).
- **Время жизни аутентифицированного пользователя (сек.)** — Период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кэша на DCFW. Значение по умолчанию - 2700 секунд (45 минут).

- **Профиль аутентификации** — Профиль аутентификации, с использованием которого происходит поиск пользователя, найденного в журналах RADIUS accounting.
- **Атрибут для имени** — Номер radius attribute type, в котором находится имя пользователя. Значение по умолчанию: 1.
- **Атрибут для групп** — Номер radius attribute type, в котором находится группа пользователя, по умолчанию группа не проверяется.
- **Домен по умолчанию** — Имя домена, в котором будет производиться поиск пользователя в случае, если в запросе не было явно указано какому домену принадлежит пользователь.
- **Секретный код** — Общий ключ, используемый протоколом RADIUS для аутентификации.

На вкладке **Адреса** указываются адреса хостов (NAS-серверов), с которых UserID агент будет получать события RADIUS accounting:

Настройка UserID агента

Настройка общих параметров UserID агента производится в разделе **Настройки → Пользователи и устройства → Свойства агента UserID**. Необходимо нажать кнопку **Редактировать** на панели инструментов:



На вкладке **Общие** настраиваются интервалы опроса данных:

- **Интервал опроса WMI** — Период опроса серверов Active Directory. Значение по умолчанию - 120 секунд.

- **Интервал опроса syslog** — Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников. Значение по умолчанию - 60 секунд.
- **Интервал опроса RADIUS** — Период опроса базы данных для поиска событий начала/завершения сеанса пользователей по RADIUS-логу. Значение по умолчанию - 120 секунд. (Опция доступна начиная с релиза ПО 7.2.0).

На вкладке **Протоколы syslog** настраиваются параметры соединения с сервером syslog:

Для протокола TCP:

- **Включено** — Включение/отключение протокола TCP для приёма журналов syslog.
- **Порт** — Номер порта, используемого для сбора syslog-событий. По умолчанию — порт 514.
- **Максимальное количество сессий** — Максимальное количество устройств, подключённых одновременно с целью отправки сообщений.
- **Безопасное соединение** — Включение/отключение шифрования потока данных.
- **Файл сертификата УЦ** — Сертификат удостоверяющего центра, который используется для установления безопасного соединения.
- **Файл сертификата** — Сертификат, созданный пользователем и подписанный удостоверяющим центром.

Для протокола UDP:

- **Включено** — Включение/отключение протокола UDP для приёма журналов syslog.
- **Порт** — Номер порта, используемого для сбора syslog-событий. По умолчанию — порт 514.

На вкладке **Списки Ignore server** указываются списки IP-адресов, события от которых будут проигнорированы UserID агентом. Запись об игнорировании источника появится в журнале UserID:

Список может быть создан в разделе **Библиотеки → IP-адреса**, или при настройке UserID агента (кнопка **Создать и добавить новый объект**). Подробнее о создании и настройке списков IP-адресов читайте в разделе [IP-адреса](#).

Данная настройка является глобальной и относится ко всем источникам.

На вкладке **Списки Ignore user** указываются имена пользователей, события от которых будут проигнорированы UserID агентом. Поиск производится по Common Name (CN) пользователя AD:

Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID.

Важно! При задании имени допустимо использовать символ астериск (*), но только в конце строки.

Примечание При подключении DCFW к Log Analyzer возможна одновременная работа UserID агентов, настроенных на обоих устройствах. Агенты устройств будут работать независимо друг от друга. События журналов UserID агента, полученные DCFW, как и события других журналов, будут переданы на LogAp.

Журналирование

UserID агент периодически обращается к настроенным источникам данных. Полученные события сохраняются в служебной базе данных без каких-либо изменений. Содержимое данной базы можно посмотреть в соответствующих журналах:

- Журнал Windows AD коннектора;
- Syslog коннектор;
- RADIUS коннектор.

В веб-консоли администратора DCFW их можно посмотреть в разделе **Журналы и отчеты → Журналы → Агент UserID**:

UserID агент периодически обращается к служебной базе данных и извлекает из записей событий имя пользователя, SID, домен, IP-адрес, списки групп. Результаты обработки записей событий заносятся в журнал "UserID агент события аутентификации". Посмотреть его можно в том же разделе: **Журналы и отчеты → Журналы → Агент UserID**.

Описание журналов источников данных и UserID агента читайте в статье [Агент UserID](#) раздела "Журналы и отчёты".

Описание форматов экспорта журналов UserID находится в Приложении в статье [Описание форматов журналов](#).

Technology: Identification and Authentication

Version: 8.x

Product: DCFW

UserID-агент для AD/WEC устанавливается на сервер-контроллер домена или сервер WEC (Windows Event Collector). Агент считывает необходимую для идентификации пользователя информацию из журналов безопасности Windows и пересылает ее в формате syslog в коллектор UserID на устройстве UserGate LogAn.

Основные свойства

Основные функции UserID-агента для AD/WEC:

- работа в качестве сервиса;
- настройка параметров работы через файл конфигурации;
- чтение журналов безопасности Windows и отправка данных пользователей на UserID-коллектор через syslog;
- ведение файла журнала и его ротация. Возможность включить или отключить режим отладки журналирования.

Установка

UserID-агент для AD/WEC поставляется в формате установочного файла.

Для установки UserID-агента:

1. Скачайте последнюю версию UserID-агента [с официального сайта UserGate](#).
2. Распакуйте архив и запустите установочный файл *.msi.
3. После завершения инсталляции перейдите в рабочую папку агента (по умолчанию: C:\Program Files (x86)\UserGate\useridagent) и отредактируйте файл конфигурации useridagent.cfg, добавив параметры вашей сети. Подробнее о параметрах и формате файла конфигурации — в разделе « [Настройка](#) ».
4. Перезапустите сервис UserIDAgent через встроенное приложение Services (Службы Windows).

Настройка

Вы можете настроить следующие параметры конфигурационного файла:

- ServerAddress — IP-адрес интерфейса UserGate DCFW, на который UserID-агент передает события.
- EventFileNames — имена журналов для чтения. Значение по умолчанию: Security.
- MaxLogSize — максимальный размер файла журнала в МБ. Значение по умолчанию: 10.
- EventIDs — номера событий для пересылки. Например, 4624,4634 (ID событий входа в сеть и выхода из сети).
- DebugLogs — включение или отключение режима отладки. 0 — журналируются основные события, 1 — журналируется расширенный список событий. Значение по умолчанию: 1.
- UserExclude — список пользователей, для которых события не должны собираться.
- NetworkList — список подсетей, в которых собираются события UserID.
- GatewayList — список шлюзов (серверов LogAn), на которые отправляются найденные события.

Синтаксис конфигурационного файла:

- Разделителем между параметрами в списках является символ запятой, пробелы после запятой игнорируются.
- Строки, начинающиеся с символов: «;» и «#», являются комментариями.
- Раздел [default] является необязательным, однако при его использовании раздел должен сохранять указанное название. Перечень подсетей и шлюзов следует указывать в других разделах, названия которых могут быть произвольными. Новый раздел начинается со строки, содержащей символ «[».
- В файле конфигурации должен быть минимум один раздел с одним маршрутом и одним шлюзом.

Пример конфигурации:

```
[default]
ServerAddress=192.168.0.1:514
MaxLogSize=10
EventIDs=4634, 4624
```

```
EventFileNames=Security
DebugLogs=1
UserExclude=adm_,sys_
[net1]
NetworkList=192.168.30.0/24,172.30.250.0/24
GatewayList=192.168.45.1:514,192.168.45.2:514
[net2]
NetworkList=192.168.200.0/24,10.10.0.0/16
GatewayList=192.168.45.4:514,192.168.45.5:514
```

Пример минимальной конфигурации:

```
[net1]
NetworkList=192.168.30.0/24
GatewayList=192.168.45.1
```

Журналирование

UserID-агент записывает информацию о событиях в файл uidagent.log, размер которого контролируется параметром MaxLogSize. При достижении лимита:

- текущий файл журнала сохраняется с расширением *.bak, заменяя предыдущую версию файла;
- начинается запись нового файла журнала.

Для хранения всех записей работы сервиса рекомендуется настроить внешнее копирование файлов журнала с помощью специализированных сервисов.

