Table of Contents

Table of Contents 1
Пользователи и устройства 2
- Пользователи и группы 3
- Серверы аутентификации 4
- Профили аутентификации 9
- Настройка Captive-портала 10
- Пользователи терминальных серверов 13
- Профили MFA 15
- UserID 17
- Radius accounting 25
- UserID-агент для серверов AD, WEC 26
- Работа с доверенными браузерами 29

Пользователи и устройства

Product: SWG
Version: 7.5.x

Политики безопасности, правила межсетевого экрана, правила веб-безопасности и многие другие возможности UserGate SWG 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 UserGate SWG. Пользователь считается идентифицированным, если система однозначно связала пользователя с IP-адресом устройства, с которого пользователь подключается к сети. UserGate SWG 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.

UserGate SWG определяет следующие типы пользователей:

Тип	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 UserGate SWG — 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.

Version: 7.5.x
Product: SWG

Серверы аутентификации — это внешние источники учетных записей пользователей, например LDAP-сервер, или серверы, производящие аутентификацию для UserGate SWG, например RADIUS, TACACS+, Kerberos, SAML.

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 в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить LDAP-коннектор** и укажите параметры коннектора.

Параметр	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 UserGate SWG получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate SWG будет использовать резервный. В случае недоступности части контроллеров домена с площадки, где работает UserGate SWG, 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
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. При наличии поддоменов, в которых может происходить авторизация пользователей, на вкладке **Домены LDAP** необходимо указывать все варианты таких поддоменов. 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. Подробнее о настройке Captive-портала — в разделе «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. Подробнее об аутентификации Kerberos и создании keytab-файла — в разделе «Метод аутентификации Kerberos»

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

ПримечаниеДля аутентификации 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. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

Для добавления пользователя или группы пользователей LDAP в правила фильтрации нажмите **Добавить пользователя LDAP**/**Добавить группу LDAP**, в поле поиска укажите как минимум один символ, входящий в имена искомых объектов, после чего нажмите **Поиск** и выберите желаемые группы или пользователей.

Сервер аутентификации пользователей RADIUS

Сервер RADIUS позволяет производить аутентификацию пользователей на серверах RADIUS, то есть UserGate SWG выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер UserGate SWG 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 UserGate SWG, поэтому, если пользователи не были заведены в UserGate SWG 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 аутентификацию).

Для создания сервера аутентификации RADIUS в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить RADIUS-сервер** и укажите параметры сервера.

Параметр	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 настройте Captive-портал для использования метода RADIUS. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

Сервер аутентификации пользователей TACACS+

Сервер TACACS+ позволяет производить аутентификацию пользователей на серверах TACACS+. При аутентификации через TACACS+ UserGate SWG 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 UserGate SWG, поэтому, если пользователи не были заведены в UserGate SWG 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 аутентификацию).

Для создания сервера аутентификации TACACS+ в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить TACACS+-сервер** и укажите параметры сервера.

Параметр	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	Порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт TCP 49
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+ **Важно!** Чтобы эта опция работала, необходимо настроить ее также на стороне сервера 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 аутентифицировать 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 аутентификацию на всех ресурсах, поддерживающих аутентификацию SAML. UserGate SWG может быть настроен в качестве сервис-провайдера SAML, использующего сервера SAML IdP для авторизации клиента.

Сервер SAML IdP не может предоставить свойства пользователей в UserGate SWG 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 аутентификации с помощью сервера SAML IdP:

1. На контроллере домена создайте DNS-запись, соответствующую UserGate SWG, для использования в качестве домена для auth.captive. В качестве IP-адреса укажите адрес интерфейса UserGate SWG, принадлежащего зоне Trusted.

2. Настройте DNS-серверы на UserGate SWG. В параметрах UserGate SWG в качестве системных DNS-серверов укажите IP-адреса контроллеров домена.

3. Измените адрес домена auth captive-портала в разделе **Настройки → UserGate → Настройки** на созданную на предыдущем шаге запись DNS. Подробнее об изменении адреса домена auth Captive-портала — в разделе «Общие настройки».

4. Настройте сервер SAML IdP. Добавьте на сервере SAML IdP запись о сервис-провайдере UserGate SWG, указывая созданное на шаге 1 FQDN-имя.

5. В разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить SAML IdP-сервер** и укажите параметры сервера.

Параметр	Описание
Включен	Включение или отключение использования данного сервера аутентификации
Название сервера	Название сервера аутентификации
Описание	Описание сервера аутентификации
SAML metadata URL	URL на сервере SAML IdP, откуда можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML. При нажатии **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. Возможные 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 (подробнее — в разделе «Управление сертификатами»). • Использовать существующий сертификат. Сертификат уже должен быть создан или импортирован в разделе **Настройки → UserGate → 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, используемый 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. Возможные 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. Возможные 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 аутентификации с помощью NTLM UserGate SWG работает с контроллерами домена, выполняющими проверку пользователя с целью получения доступа в интернет.

Сервер NTLM не может предоставить список пользователей в UserGate SWG, поэтому, если пользователи не были заведены в UserGate SWG 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 UserGate SWG не отличается от режима работы аутентификации.

Для настройки аутентификации с помощью NTLM:

1. Настройте синхронизацию времени с контроллером домена. В настройках UserGate SWG в разделе **Настройки → UserGate → Настройки** включите синхронизацию времени с серверами NTP, в качестве основного и (опционально) запасного NTP-сервера укажите IP-адреса контроллеров домена.

2. На контроллере домена создайте DNS-записи, соответствующие UserGate SWG для использования в качестве домена для auth.captive и logout.captive..В качестве IP-адреса укажите адрес интерфейса UserGate SWG, принадлежащего зоне Trusted.

3. Для домена auth Captive-портала укажите созданную на предыдущем шаге запись DNS. Для домена logout Captive-портала укажите созданную на предыдущем шаге запись DNS. Подробнее об изменении адресов доменов auth Captive-портала и logout Captive-портала — в разделе «Настройка Captive-портала».

4. Добавьте NTLM-сервер. В разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить NTLM-сервер** и укажите название и имя домена Windows. Для корректной работы аутентификации NTLM, необходимо, чтобы указанное здесь имя домена определялось в IP-адреса контроллеров домена.

5. Создайте правило Captive-портала с аутентификацией NTLM. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

6. Разрешите доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM.

7. Для аутентификации в стандартном режиме настройте обязательное использование прокси-сервера на компьютерах пользователей. Укажите IP-адрес интерфейса UserGate SWG 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 UserGate SWG 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.

8. Для аутентификации в прозрачном режиме настройте 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 текущем 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 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) аутентифицировать пользователей домена Active Directory. При аутентификации через Kerberos UserGate SWG 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 аутентификации с помощью Kerberos:

1. На контроллере домена создайте DNS-записи UserGate SWG для использования в качестве доменов для auth.captive и logout.captive. В качестве IP-адреса укажите адрес интерфейса UserGate SWG, принадлежащего зоне Trusted.

Важно! Для корректной работы создайте записи типа A, не используйте CNAME-записи.

2. Создайте учетную запись в домене AD и отключите для нее требование смены пароля.

Важно! Не используйте символы национальных алфавитов, например кириллицу, в имени учетной записи или в организационных единицах Active Directory, где вы планируете создать учетную запись.
Важно! Не используйте в качестве учетной записи для Kerberos запись, созданную для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись.

3. На контроллере домена создайте keytab-файл, выполнив команду вида:

ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC /mapuser kerb@DOMAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:\utm.keytab

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 учетной записи в домене, созданное на шаге 2 (имя realm-домена обязательно большими буквами).

4. Настройте DNS-серверы на UserGate SWG. В качестве системных DNS-серверов укажите IP-адреса контроллеров домена.

5. Включите на UserGate SWG в разделе **Настройки → UserGate → Настройки** синхронизацию времени с серверами NTP, в качестве основного и (опционально) запасного NTP-сервера укажите IP-адреса контроллеров домена.

6. Измените адрес домена auth captive-портала и опционально адрес домена logout captive-портала в разделе **Настройки → UserGate → Настройки** на созданные ранее записи DNS. Подробнее об изменении адресов доменов — в разделе «Общие настройки».

7. Создайте сервер аутентификации LDAP и загрузите полученный на предыдущем шаге keytab-файл. Подробнее о настройке LDAP-коннектора — разделе «LDAP-коннектор».

Важно! Не используйте в качестве учетной записи для LDAP-коннектора запись, созданную ранее для работы Kerberos. Необходимо использовать отдельную учетную запись.

8. Создайте правило Captive-портала для использования метода аутентификации Kerberos. Подробнее о Captive-портале — в разделе « Настройка Captive-портала».

9. Откройте доступ к сервису HTTP(S)-прокси в свойствах контроля доступа зоны, к которой подключены пользователи, авторизующиеся с помощью Kerberos.

10. Для аутентификации в стандартном режиме настройте обязательное использование прокси-сервера на компьютерах пользователей. Укажите FQDN UserGate SWG в качестве адреса прокси-сервера.

11. Для аутентификации в прозрачном режиме настройте 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 текущем 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 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 этот тип аутентификации для пользователей, поскольку имя пользователя и пароль передаются в открытом виде по сети. Аутентификацию 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 аутентификации с помощью HTTP Basic:

1. На контроллере домена создайте DNS-записи, соответствующие UserGate SWG, для использования в качестве домена для auth.captive и logout.captive. В качестве IP-адреса укажите адрес интерфейса UserGate SWG, принадлежащего зоне Trusted.

2. Измените адрес домена auth Captive-портала и (опционально) адрес домена logout Captive-портала в разделе **Настройки → UserGate → Настройки** на созданные на предыдущем шаге записи DNS. Подробнее об изменении адресов доменов — в разделе « Общие настройки».

3. Создайте правило Captive-портала для использования метода аутентификации HTTP Basic. Подробнее о Captive-портале — в разделе « Настройка Captive-портала».

4. Откройте доступ к сервису HTTP(S)-прокси в свойствах контроля доступа зоны, из которой происходит авторизация с помощью HTTP Basic.

5. На устройствах, с которых выполняется авторизация, укажите обязательное использование прокси-сервера. Укажите IP-адрес зоны Trusted интерфейса UserGate SWG в качестве адреса прокси-сервера.

Профили аутентификации

Version: 7.5.x
Product: SWG

Профиль аутентификации позволяет указать набор способов и параметров аутентификации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах UserGate SWG, например Captive-портал, веб-портал и т. д. Чтобы создать профиль аутентификации, в разделе **Настройки → Пользователи и устройства → Профили аутентификации** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Название	Название профиля
Описание	Описание профиля
Профиль MFA	Профиль многофакторной аутентификации. Должен быть предварительно создан в разделе **Профили MFA**, если планируется использовать многофакторную аутентификацию. Профиль определяет способ доставки одноразового пароля для дополнительного метода аутентификации. Подробнее о настройке профилей MFA — в разделе «Профили MFA» **Важно!** Многофакторная аутентификация возможна только с методами аутентификации, позволяющими ввести пользователю одноразовый пароль, то есть только с теми, где пользователь явно вводит свои учетные данные в веб-форму страницы аутентификации. В связи с этим, многофакторная аутентификация невозможна для методов аутентификации Kerberos и NTLM.
Время бездействия до отключения	Этот параметр определяет, через сколько секунд UserGate SWG переведет пользователя из состояния Known users в состояние Unknown users при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя)
Время жизни авторизованного пользователя	Этот параметр определяет, через сколько секунд UserGate SWG переведет пользователя из состояния Known users в состояние Unknown users. По прошествии указанного времени пользователю потребуется повторно аутентифицироваться на Captive-портале
Число неудачных попыток авторизации	Разрешенное количество неудачных попыток аутентификации через Captive-портал до блокировки учетной записи пользователя
Время блокировки пользователя	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток аутентификации
Методы аутентификации	Созданные ранее методы аутентификации пользователей, например сервер аутентификации Active Directory или RADIUS. Если указано более одного метода аутентификации, 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. Этот тип аутентификации необходимо применять совместно с профилем Captive-портала, в котором используется страница аутентификации Captive portal policy. • **HTTP Basic** — аутентификация с помощью устаревшего метода HTTP Basic. • **Аутентификация Kerberos** — аутентификация по протоколу Kerberos

Настройка Captive-портала

Version: 7.5.x
Product: SWG

Captive-портал позволяет аутентифицировать неизвестных пользователей с помощью методов аутентификации 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 пользователи, у которых в свойствах явно указан IP-адрес, или пользователи, идентифицированные с помощью агентов авторизации терминальных серверов, не аутентифицируются на Captive-портале. Такие пользователи уже относятся к типу Known users и не требуют дополнительной идентификации.
- Аутентификация с помощью Captive-портала возможна только для протокола HTTPS. Например, если вы создали правило межсетевого экрана, разрешающее доступ в интернет по протоколу FTP только для пользователей 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 аутентификацию на Captive-портале.
- Необходимо настроить инспектирование SSL, иначе аутентификация по протоколу HTTPS работать не будет.
- Если Captive-портал использует метод аутентификации Active Directory, то пользователь должен указывать в качестве логина свое доменное имя в формате DOMAIN\username или username@domain.

Для настройки Captive-портала:

1. Создайте метод аутентификации, например аутентификацию с помощью домена Active Directory. В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить** и создайте сервер аутентификации.

2. Создайте профиль аутентификации, в котором укажите необходимые методы аутентификации. В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Профили аутентификации** нажмите **Добавить** и создайте профиль аутентификации, используя созданный ранее метод аутентификации.

3. Создайте Captive-профиль, в котором укажите необходимые профили аутентификации. В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Captive-профили** нажмите **Добавить** и создайте Captive-профиль, используя созданный ранее профиль аутентификации.

4. Создайте правило Captive-портала. Правило Captive-портала определяет трафик, к которому должны быть применены методы аутентификации пользователей, указанные в Captive-профиле. В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Captive-портал** нажмите **Добавить** и создайте правило Captive-портала.

5. Настройте DNS для доменов auth.captive и logout.captive. Служебные доменные имена auth.captive и logout.captive используются в UserGate SWG для аутентификации пользователей. Если клиенты не используют UserGate SWG в качестве DNS-сервера необходимо прописать в качестве IP-адреса для этих доменов IP-адрес интерфейса UserGate SWG, который подключен в клиентскую сеть. Альтернативное решение — настроить параметры «Домен auth captive-портала» и «Домен logout captive-портала». Подробнее об этих параметрах — в разделе «Общие настройки».

При создании Captive-профиля укажите следующие параметры.

Параметр	Описание
Название	Название Captive-профиля
Описание	Описание Captive-профиля
Шаблон страницы авторизации	Выбор шаблона страницы аутентификации. Создавать страницы аутентификации можно в разделе **Настройки → Библиотеки → Шаблоны страниц**. Если необходимо настроить самостоятельную регистрацию пользователей с подтверждением по SMS или e-mail, следует выбрать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth)
Метод идентификации	Метод, с помощью которого UserGate SWG сохраняет данные о пользователе. Возможные варианты: • **Запоминать IP-адрес**. После успешной аутентификации пользователя через Captive-портал UserGate SWG запоминает IP-адрес пользователя. Все последующие соединения с этого IP-адреса будут относятся к данному пользователю. Такой метод позволяет идентифицировать данные, передаваемые по любому из протоколов семейства TCP/IP, но не будет корректно работать при наличии NAT-подключения между пользователями и UserGate SWG. Это рекомендуемое значение параметра, устанавливаемое по умолчанию. • **Запоминать cookie**. После успешной аутентификации пользователя через Captive-портал UserGate SWG добавляет в браузер пользователя cookie, с помощью которых идентифицирует последующие соединения данного пользователя. Такой метод позволяет аутентифицировать пользователей, находящихся за NAT-устройством, но аутентифицируется только протокол HTTP(S) и только в том браузере, в котором происходила аутентификация через Captive-портал. Кроме этого, для аутентификации HTTPS-сессий пользователя UserGate SWG 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 аутентификации, 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 необходимо указать сконфигурированный ранее профиль пользовательских сертификатов

Параметр	Описание
URL для редиректа	URL, куда будет перенаправлен пользователь после успешной аутентификации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL
Разрешить браузерам запомнить авторизацию	Разрешение сохранять аутентификацию в браузере на указанное время в часах. Для сохранения аутентификационной информации используются cookie
Предлагать выбор домена AD/LDAP на странице авторизации Captive-портала	Если в качестве метода аутентификации используется аутентификация с помощью Active Directory, то при включении данного параметра пользователь сможет выбрать имя домена из списка на странице аутентификации. Если этот параметр не включен, пользователь должен явно указывать домен в виде DOMAIN\username или username@domain
Показывать CAPTCHA	При включении этой опции пользователю будет предложено ввести код, который ему будет показан на странице аутентификации 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).

Параметр	Описание
Профиль оповещения	Профиль оповещения, который будет использоваться для отсылки информации о созданном пользователе и его пароле. Может использоваться два типа профилей — SMS и email. Подробнее о создания профилей оповещения — в разделе «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 аутентификации временного пользователя, по истечении которого его учетная запись будет отключена
Длина пароля	Длина пароля для создаваемого пользователя
Сложность пароля	Сложность пароля для создаваемого пользователя. Возможные варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спец. символы
Группы	Группа для временных пользователей, в которую будут помещены создаваемые пользователи

При создании правила Captive-портала укажите следующие параметры.

Параметр	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 этой опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики

Параметр	Описание
Источник	Адреса источника. В качестве источника можно указать определенную зону, например зону LAN и диапазон адресов IP. Могут быть использованы 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 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 правило будет активно
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, отметьте правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу

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

ПримечаниеУсловия, указанные на вкладках правила, применяются согласно логике "И", то есть требуют совпадения всех указанных условий для того, чтобы правило сработало. Если необходимо использовать логику "ИЛИ", необходимо создать несколько правил.
ПримечаниеПравила применяются в порядке, в котором они отображаются в консоли. Вы можете изменить порядок правил, нажав соответствующие значки в консоли.
ПримечаниеПри обработке правил применяется только первое сработавшее правило.

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

Пользователи терминальных серверов

Version: 7.5.x
Product: SWG

Терминальный сервер служит для удаленного обслуживания пользователей 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 аутентификации пользователей терминального сервера состоит в том, что у всех пользователей сервера будет определен один и тот же IP-адрес, и UserGate SWG не может корректно идентифицировать сетевые подключения пользователей. Для решения этой 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 SWG 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 протоколов TCP и UDP. Протоколы, отличные от TCP и UDP, например ICMP, не могут быть идентифицированы.

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

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

1. Разрешите сервис **Агент аутентификации** в свойствах контроля доступа зоны, со стороны которой расположены серверы терминального доступа.

2. Установите пароль агентов терминального сервера. В веб-консоли UserGate SWG в разделе **Настройки → UserGate → Настройки → Модули** нажмите **Настроить** напротив строки **Пароль агентов терминального сервиса** и установите пароль агентов терминального сервера.

3. Установите агент терминального сервера на все серверы, для которых необходимо идентифицировать пользователей. При установке укажите адрес UserGate SWG и установленный на предыдущем шаге пароль.

4. В веб-консоли UserGate SWG. в разделе **Настройки → Пользователи и устройства → Терминальные серверы** добавьтеь агентов терминального сервера, указав имя и адрес узла. После получения данных с указанного в настройках узла и совпадении пароля, указанного на шаге 2, аутентификация пользователей будет включена автоматически. При обновлении версии ПО UserGate SWG 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 этого параметра информация о пользователях будет передаваться на UserGate SWG в формате « имя сервера_имя пользователя» для локальных пользователей или «имя домена_имя пользователя» для доменных.

Таких пользователей также необходимо добавить в UserGate SWG как локальных. О добавлении пользователей — в разделе « Пользователи». При добавлении необходимо указать логин в приведенном выше формате; пароль указывать не нужно.

Эта 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 подчеркивания. Использование тире в имени компьютера возможно только в том случае, если используются только доменные пользователи.

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

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 учетных записей (system, local service, network service) и портах, используемых для соединения, на UserGate SWG.
- 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 UserGate SWG, принимающего соединение от агента авторизации. По умолчанию используется порт UDP:1813.
- ServerAddress: адрес устройства UserGate, принимающего соединение от агента аутентификации. Начиная с версии агента 6.2.0.49 поддерживается возможность работы с несколькими UserGate SWG одновременно. Строка ServerAddress может содержать несколько элементов, разделенных символом ";". Это могут быть как IP-адреса, так и FQDN (например, ServerAddress=testtermserver.net;15.0.0.203).Все адреса определяются в момент старта и в момент изменений в настройках сетевых адаптеров. Рассылки о пользователях дублируются на все адреса.
- 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 определенных 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="12.3.4-1.1.1.1;2.2.2.2-5.5.5.5".

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

Version: 7.5.x
Product: SWG

Многофакторная аутентификация (MFA) — 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.

UserGate SWG поддерживает многофакторную аутентификацию с использованием имени пользователя и пароля в качестве первого типа аутентификации, одноразового токена или пароля — в качестве второго. Доступны следующие методы получение одноразовых токенов или паролей:

- **TOTP** (Time-based One Time Password) — получение одноразового токена. TOTP-токен создает одноразовый пароль на основе времени, то есть время является параметром. 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 UserGate SWG 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 SWG или в доменной учетной записи в Active Directory.

Чтобы настроить многофакторную аутентификацию:

1. Настройте аутентификацию с помощью Captive-портала. Многофакторная аутентификация работает только при аутентификации пользователей с помощью Captive-портала. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

2. Создайте профиль многофакторной аутентификации. В веб-консоли UserGate SWG перейдите в раздел **Настройки → Пользователи и устройства → Профили MFA** создайте профиль многофакторной аутентификации. При создании профиля укажите метод доставки второго фактора аутентификации. Доступны три метода доставки:

- **MFA через TOTP** — доставка второго фактора аутентификации с помощью токенов TOTP.
- **MFA через SMS** — доставка второго фактора аутентификации с помощью SMS.
- **MFA через email** — доставка второго фактора аутентификации с помощью email.

Параметры для настройки метода **MFA через TOTP**.

Параметр	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 аутентификации. Для этого варианта выберите **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 UserGate SWG или в доменной учетной записи в Active Directory. Для этого варианта выберите 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 UserGate SWG или в доменной учетной записи в Active Directory. Для этого варианта выберите 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 пользователя в списке (**Настройка → Пользователи и устройства → Пользователи**) и выбрать действие **Сбросить ключ TOTP**. При следующей аутентификации пользователю будет предложено заново инициализировать свой токен.

Параметры для настройки метода **MFA через SMS**.

Параметр	Описание
Название	Название профиля MFA
Описание	Описание профиля MFA
Профиль отправки MFA	Профиль SMPP, который будет использован для отправки паролей с помощью сообщений SMS. Подробнее о настройке профилей отсылки сообщений через SMS — в разделе «Профили оповещений»
От	Указать автора отправки сообщения

Параметр	Описание
Содержимое	Тело сообщения. В сообщении можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль
Время жизни MFA кода	Срок действия одноразового пароля

Параметры для настройки метода **MFA через email**.

Параметр	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. Подробнее о настройке профилей отсылки сообщений по электронной почте — в разделе «Профили оповещений»
От	Указать автора сообщения
Тема	Тема сообщения
Содержимое	Тело сообщения. В сообщении можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль
Время жизни MFA кода	Срок действия одноразового пароля

Technology: Identification and Authentication

Version: 7.5.x

Product: SWG

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

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, позволяющих 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 качестве источников данных для аутентификации в UserID используются журналы Microsoft Active Directory, данные, полученные по syslog или сообщения RADIUS accounting.

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

Принцип работы UserID

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

- Непосредственное получение данных узлом с UserID-агентом от источников данных аутентификации с помощью настроенных коннекторов:
  - UserID-агент может подключаться к контроллеру домена AD с помощью технологии WMI и считывать журналы событий безопасности;
  - UserID-агент может принимать со сторонних серверов сообщения по протоколу syslog;
  - UserID-агент может принимать со сторонних RADIUS NAS-серверов сообщения RADIUS accounting.

- Получение данных через посредника — специального программного агента, который устанавливается на контроллер домена или сервер-сборщик событий (WEC).

  Программный агент UserID для AD- и WEC-серверов устанавливается на контроллер домена (AD) или сервер-сборщик событий домена (WEC), считывает необходимую для идентификации пользователя информацию из журналов безопасности Windows и пересылает ее в формате syslog на коллектор UserID на UserGate Log Analyzer или UserGate SWG (подробнее об агенте — в разделе «UserID-агент для AD/WEC»).

  Главные достоинства такого 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 специальную учетную запись 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 UserGate SWG, 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 UserGate SWG.

Информация из Microsoft AD о выходе пользователя из системы в настоящий момент не обрабатывается.

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

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 определенных пользователей и групп, UserGate SWG обращается к кеш-памяти 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 UserGate SWG. Для этого администратор может выполнить сброс всех пользователей или сброс отдельного пользователя:

- В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** на панели инструментов нажмите **Сбросить аутентификацию всех пользователей**.
- В консоли CLI — выполните команду:

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

В сценарии с использованием серверов-источников данных syslog в качестве источника данных аутентификации пользователей принцип работы аналогичен, только UserGate SWG 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. Нужные события фильтруются в потоке 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. UserGate SWG 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 UserGate SWG 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 UserGate SWG UserID может работать на устройствах UserGate Log Analyzer. Подробнее о работе UserID на Log Analyzer читайте в руководстве администратора UserGate Log Analyzer. Использование UserGate Log Analyzer позволяет масштабировать технологию UserID на другие устройства сети. Принцип работы UserID на устройстве UserGate Log Analyzer аналогичен принципу работы на UserGate SWG. Найденные в собранных данных события отправляются на другие узлы UserGate SWG в соответствии с политикой UserID Sharing, настроенной с помощью профилей редистрибуции. При необходимости можно отправлять разные данные на разные узлы UserGate SWG. На SWG отправляются только GUID пользователя, его IP-адрес и список идентификаторов групп, участником которых он является. Такая архитектура позволяет использовать один или несколько серверов UserGate Log Analyzer для централизованного сбора информации о пользователях с различных источников и далее централизованно и избирательно распространять эту информацию на узлы UserGate SWG в сети.

ПримечаниеВ инфраструктурах с серверами Active Directory и высоким потоком событий аутентификации (свыше 50 событий в секунду) для корректной работы функции UserID рекомендуется применять сценарий сбора событий через AD/WEC-агент вместо сценария с технологией WMI. Это связано с ограниченной производительностью технологии WMI, которая может вызывать ошибки при получении данных и приводить к некорректной работе правил

фильтрации.

Алгоритм настройки UserID

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

Настройка на стороне источников данных:

- При работе с Active Directory в качестве источника данных об аутентификации пользователей включите 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 настройте отправку журналов на адрес UserID-агента (то есть на IP-адрес UserGate SWG; номер порта и протокол устанавливаются в настройках UserID-агента, по умолчанию порт TCP 514).
- При работе с серверами RADIUS NAS настройте отправку сообщений RADIUS accounting на адрес UserID-агента (то есть на IP-адрес UserGate SWG, порт UDP 1813).

Настройка на стороне UserGate SWG:

- Создайте сервер аутентификации для UserID-агента. Подробнее о создании и настройке серверов аутентификации — в разделе « Серверы аутентификации».
- Создайте профиль аутентификации для UserID-агента. Подробнее о создании и настройке профилей аутентификации — в разделе « Профили аутентификации».
- Для сценария с серверами-источниками данных syslog активируйте сервис **UserID syslog collector** в параметрах контроля доступа зоны, где будет находиться отправитель syslog. Для сценария с RADIUS NAS-серверами активируйте сервис **Агент аутентификации** в настройках контроля доступа зон, где будет находиться серверы RADIUS NAS. Подробнее о создании и настройке зон — в разделе «Настройка зон».
- Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.
- Настройте общие параметры UserID-агента.

Создание коннектора UserID-агента

Коннектор UserID-агента в веб-консоли UserGate SWG создается в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы**. Нажмитеь **Добавить** на панели инструментов и выберите тип создаваемого коннектора:

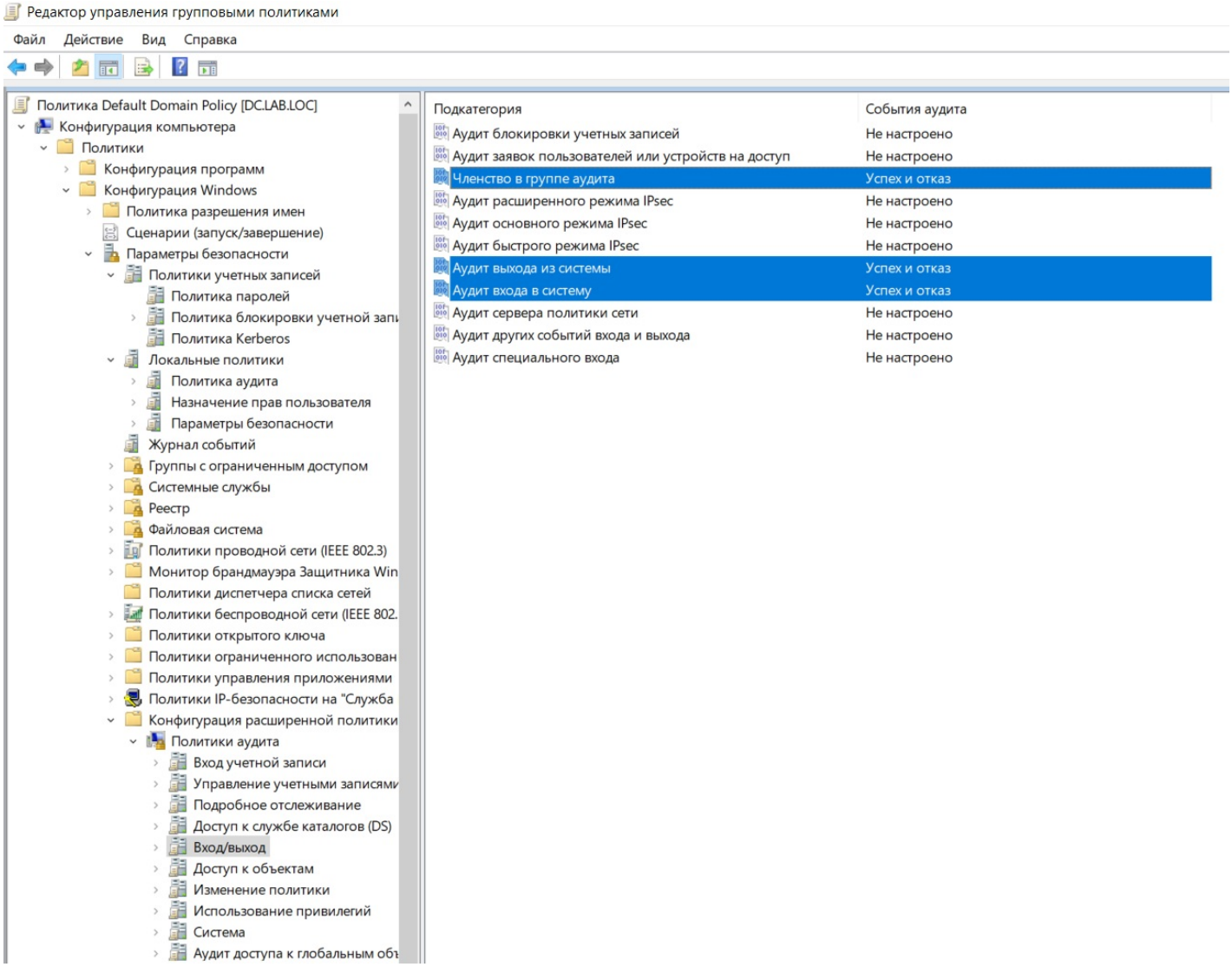
- Microsoft Active Directory;
- Отправитель syslog;
- RADIUS-сервер.

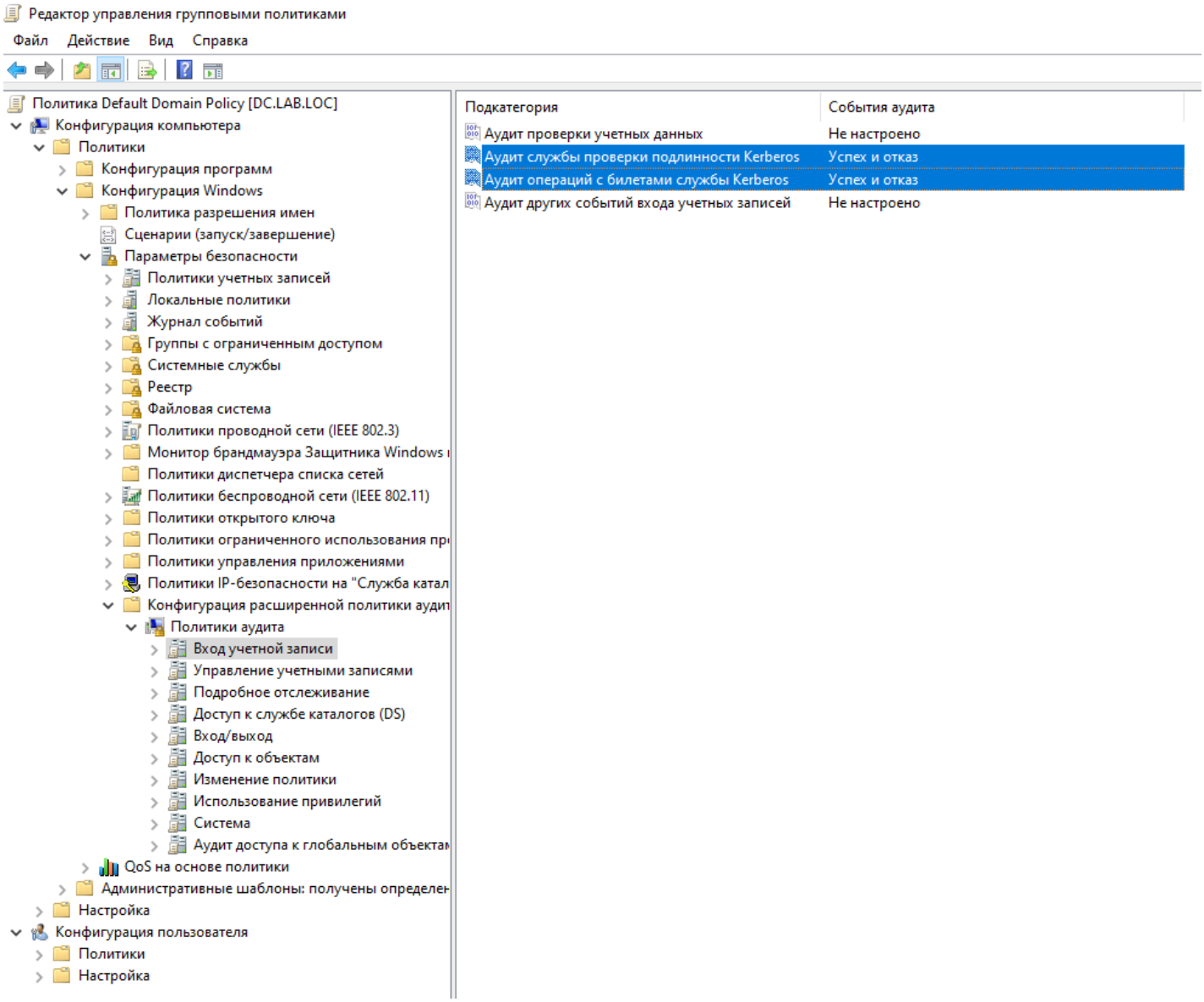
Microsoft Active Directory

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

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

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


Редактор управления групповыми политиками
Файл Действие Вид Справка
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 запи
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 Win
Политики диспетчера списка сетей
Политики беспроводной сети (IEEE 802.
Политики открытого ключа
Политики ограниченного использован
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 об
Подкатегория
События аудита
Аудит блокировки учетных записей
Не настроено
Аудит заявок пользователей или устройств на доступ
Не настроено
Членство в группе аудита
Успех и отказ
Аудит расширенного режима IPsec
Не настроено
Аудит основного режима IPsec
Не настроено
Аудит быстрого режима IPsec
Не настроено
Аудит выхода из системы
Успех и отказ
Аудит входа в систему
Успех и отказ
Аудит сервера политики сети
Не настроено
Аудит других событий входа и выхода
Не настроено
Аудит специального входа
Не настроено



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

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

1. Создайте учетную запись пользователя на контроллере домена:
   - Перейдите в меню **Пуск → Диспетчер серверов → Средства → Active Directory — пользователи и компьютеры** .
   - В соответствующем Подразделении (OU) создайте **Нового пользователя** для UserID.
2. Настройте членство в группах для новой учетной записи пользователя:
   - Нажмите правой кнопкой мыши на новой учетной записи пользователя UserID и выберите **Свойства**.
   - Перейдите на вкладку **Членство в группах**.
   - Нажмите **Добавить → Дополнительно → Поиск**.
   - Выберите следующие группы:
     - **Пользователи DCOM**;
     - **Пользователи журналов производительности**;
     - **Пользователи удаленного рабочего стола**;
     - **Читатели журнала событий**.
   - Нажмите **OK**.
3. Назначьте права Distributed Component Object Model (DCOM):
   - Перейдите в меню Windows **Пуск → Администрирование → Службы компонентов**. Откроется окно **Службы компонентов**.
   - Раскройте **Службы компонентов → Компьютеры → Мой компьютер**.
   - Нажмите правой кнопкой мыши на **Мой компьютер** и выберите **Свойства**. Откроется окно **Свойства: Мой компьютер**.
   - Перейдите на вкладку **Безопасность COM**.
   - В области **Права доступа** нажмите **Изменить ограничения.**

- Убедитесь, что для **Пользователи DCOM** выбрано: **Локальный доступ** и **Удаленный доступ**.
- Нажмите **OK**, чтобы сохранить параметры.
- В окне **Свойства: Мой компьютер** нажмите в разделе **Разрешения на запуск и активацию** на **Изменить ограничения.**
- Убедитесь, что для **Пользователи DCOM** выбрано: **Локальный запуск**, **Удаленный запуск**, **Локальная активация** и **Удаленная активация**.
- Нажмите **OK**, чтобы сохранить настройки; еще раз нажмите **OK**, чтобы закрыть окно **Свойства: Мой компьютер**.
- Выберите **Файл → Выход**, чтобы закрыть окно **Службы компонентов**.

4. Настройте назначения защиты пространства имен WMI:

- Перейдите в меню **Пуск → Выполнить**.
- Введите wmimgmt.msc и нажмите **OK**.
- Нажмите правой кнопкой мыши на **Элемент управления WMI (локальный)** и выберите **Свойства**.
- Перейдите на вкладку **Безопасность**.
- Нажмите **Безопасность → Добавить → Дополнительно → Поиск**.
- Выберите новую учетную запись пользователя, нажмите **OK**, пока вы не вернетесь в окно **Безопасность** для Root.
- Нажмите **Дополнительно** и выберите добавленную учетную запись пользователя.
- Нажмите **Изменить**.
- В меню **Применяется к:** выберите **Данное пространство и подпространство имен**.
- Убедитесь, что выбрано **Выполнение методов**, **Включить учетную запись**, **Включить удаленно** и **Прочесть безопасность**.
- Нажмите **OK,** пока вы не вернетесь в окно wmimgmt.
- Выберите **Файл → Выход**, чтобы закрыть окно wmimgmt.

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 UserGate SWG в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора: **Microsoft Active Directory**. Укажите следующие параметры:

- **Включено** — включение и 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 кеш-памяти на UserGate SWG. Значение по умолчанию - 2700 секунд (45 минут).

Syslog

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

1. Настройте источник событий.

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

   Параметры сервера syslog на UserGate SWG можно посмотреть или изменить в общих параметрах UserID-агента.

2. Разрешите сбор информации с удаленных устройств по протоколу syslog.

   В параметрах контроля доступа зоны, в которой находится отправитель syslog, разрешите сервис **UserID syslog коллектор**.

3. Настройте параметры коннектора UserID-агента для отправителя syslog.

   В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора **Отправитель syslog**. Далее укажите следующие данные:

   - **Включено** — включение или отключение получения журналов с источника.
   - **Название** — название источника.
   - **Описание** — описание источника (опционально).

- **Адрес сервера** — адрес хоста, с которого UserGate SWG 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. При использовании UserID-агента для AD/WEC в syslog-коннекторе всегда должно быть время в UTC независимо от настроек времени на контроллере домена.
- **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 кеша на UserGate SWG. 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 — в разделе «Syslog фильтры UserID-агента».

RADIUS accounting

В случае, если источником информации выступают сообщения RADIUS accounting:

1. Настройте источник событий.

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

2. Разрешите получение запросов RADIUS accounting от удаленных устройств.

В параметрах контроля доступа зон, в которых находятся NAS-серверы, разрешите сервис **Агент аутентификации**.

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

В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора: **RADIUS-сервер**. Укажите следующие данные:

- **Включено** — включение и 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 кеш-памяти. 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**. Нажмите **Редактировать** на панели инструментов.

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

- **Интервал опроса WMI** — период опроса серверов Active Directory. Значение по умолчанию: 120 секунд.
- **Интервал опроса syslog** — период опроса базы данных для поиска событий начала и завершения сеанса пользователей syslog-источников. Значение по умолчанию: 60 секунд.
- **Интервал опроса RADIUS** — период опроса базы данных для поиска событий начала и завершения сеанса пользователей по RADIUS-журналу. Значение по умолчанию: 120 секунд.

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

Для протокола TCP:

- **Включено** — включение и отключение протокола TCP для приема журналов syslog.
- **Порт** — номер порта, используемого для сбора syslog-событий. По умолчанию: порт 514.
- **Максимальное количество сессий** — максимальное количество устройств, подключенных одновременно с целью отправки сообщений.
- **Безопасное соединение** — включение и 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 и отключение протокола UDP для приема 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 (нажмите **Создать и добавить новый объект**). Подробнее о создании и настройке списков IP-адресов — в разделе «IP-адреса».

Этот параметр является глобальным 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.

Этот параметр является глобальным и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID.

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

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

Журналирование

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

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

В веб-консоли UserGate SWG журналы доступны 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. Посмотр журнала доступен в том же разделе: **Журналы и отчеты → Журналы → Агент UserID**.

О журналах источников данных и UserID-агента — в разделе « Агент UserID» документации.

Описание форматов экспорта журналов UserID доступно в Приложении в разделе « Описание форматов журналов».

Radius accounting

Version: 7.5.x
Product: SWG

UserGate SWG может прозрачно аутентифицировать пользователей, уже прошедших аутентификацию на внешнем сервере RADIUS. UserGate SWG не взаимодействует с сервером RADIUS, а только отслеживает информацию RADIUS accounting, перенаправленную от RADIUS-клиента. RADIUS accounting содержит информацию об имени и IP-адресе пользователя.

Для функции выполните следующие шаги:

1. Создайте необходимых локальных пользователей в UserGate SWG. Подробнее о создании пользователей — в разделе « Пользователи».

2. В разделе **Настройки → Сеть → Зоны** выберите зону, которой принадлежит интерфейс, на которой будут приходить сообщения RADIUS accounting. В свойствах контроля доступа зоны разрешите сервис **Агент авторизации**.

3. Установите пароль агентов терминального сервиса. В разделе **Настройки → UserGate → Настройки → Модули** в строке **Пароль агентов терминального сервиса** нажмите **Настроить** и укажите пароль агента терминального сервиса. Этот пароль будет использоваться в качестве RADIUS secret при настройке сервера RADIUS.

4. Добавьте источник RADIUS accounting в веб-консоли UserGate SWG. В разделе **Настройки → Пользователи и устройства → Терминальные серверы** добавьте источник информации RADIUS accounting, указав имя и IP-адрес узла.

5. Настройте отсылку информации RADIUS accounting на узел UserGate SWG, указав в качестве IP-адреса сервера IP-адрес UserGate SWG, порт UDP 1813. Укажите RADIUS secret, совпадающий с паролем агента для терминального сервера, добавленный на шаге 3.

Имя пользователя необходимо передавать в атрибуте RADIUS User-Name (type=1), IP-адрес пользователя — в атрибуте RADIUS Framed-IP-Address (type=8), а IP-адрес сервера RADIUS — в атрибуте RADIUS NAS_IP_Address (type=4).

Подробнее о настройке сервера RADIUS смотрите в руководстве на используемый вами сервер RADIUS и RADIUS-клиент.

Важно! Период обновления информации RADIUS accounting должен быть не более 120 секунд.

После выполнения настройки UserGate SWG будет сопоставлять имя пользователя и присылаемый RADIUS-сервером IP-адрес пользователя. В зависимости от полученной информации UserGate SWG будет работать следующим образом:

Событие	**Ответ UserGate SWG**
От RADIUS-сервера получено имя пользователя, который не создан на UserGate SWG	На сообщение Accounting request UserGate SWG отправит сообщение Accounting reject. Данные о пользователях не изменятся
От RADIUS-сервера получено имя существующего пользователя и указан тип Acct-Status-Type = Start или Interim-Update	Указанному пользователю присвоится полученный IP-адрес. • Имя пользователя начнет отображаться в журналах для этого IP-адреса. Пользовательские правила начнут применяться для трафика с этого IP-адреса. • Если у пользователя уже был IP-адрес, отличный от полученного, пользователю будет присвоен дополнительный IP-адрес. • Если пользователю уже присвоен этот IP-адрес, никаких изменений не произойдет. • Если этот IP-адрес присвоен другому пользователю, он будет удален у другого пользователя и будет присвоен пользователю, указанному в запросе
От RADIUS-сервера получено имя существующего пользователя и указан тип Acct-Status-Type = Stop	У пользователя удалится полученный IP-адрес. Имя пользователя перестанет отображаться в журналах для этого IP адреса. Пользовательские правила перестанут применяться для трафика с этого IP-адреса.

UserID-агент для серверов AD, WEC

Technology: Identification and Authentication
Version: 7.5.x
Product: SWG

UserID-агент для AD- и WEC-серверов — это программный компонент, который устанавливается на сервере-контроллере домена или на сервере 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 устройствах UserGate Log Analyzer или UserGate SWG.

Основные функции UserID-агента для AD- и WEC-серверов:

- Работа в качестве сервиса.
- Настройка параметров работы через файл конфигурации.
- Чтение журналов безопасности Windows и отправка событий на UserID-коллектор через syslog.
- Ведение файла журнала и его ротация. Возможность включить режим отладки журналирования.

Для работы агента в качестве источника данных в сценарии аутентификации с помощью UserID необходимо:

1. Установить и настроить UserID-агент для AD- и WEC-серверов.
2. Настроить сбор информации об аутентификации пользователей на UserGate Log Analyser или на UserGate SWG в зависимости от варианта интеграции.
3. Настроить работу функции UserID на UserGate Log Analyzer или на UserGate SWG.

Установка и настройка агента

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

Для установки агента:

1. Скачайте последнюю версию 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).

Удалить агент можно через панель управления:

1. Нажмите комбинацию клавиш Win + R и выполните команду control.
2. В панели управления перейдите в раздел **Программы → Программы и компоненты**.
3. Найдите в списке нужное приложение и нажмите **Удалить**.

Настройка

Чтобы настроить агент, отредактируйте его конфигурационный файл. Вы можете изменить или добавить следующие параметры:

- 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 (узлы UserGate Log Analyzer, UserGate SWG), 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]
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.

Интеграция с UserGate SWG

Для получения информации об аутентификации пользователей выполните настройку следующих параметров на UserGate SWG:

1. Активируйте сервис UserID syslog collector в параметрах контроля доступа зоны, в которой находится UserID агент для AD- и WEC-серверов. Подробнее о настройке зон — в разделе «Настройка зон».

2. Настройте параметры аутентификации для UserID-агента в домене для получения информации о группах, в которых зарегистрирован найденный в журналах syslog пользователь:

- Создайте сервер аутентификации на основе LDAP-коннектора для UserID-агента. Подробнее о создании и настройке серверов аутентификации — в разделе «Серверы аутентификации».
- Создайте профиль аутентификации для UserID-агента. Подробнее о создании и настройке профилей аутентификации — в разделе « Профили аутентификации».

3. Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.

Коннектор UserID-агента в веб-консоли UserGate SWG создается в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** . Нажмите **Добавить** и выберите тип создаваемого коннектора: **Отправитель syslog**. Укажите параметры коннектора:

- На вкладке **Общие**:
  - **Включено** — включение или отключение получения журналов от источника данных.
  - **Название** — название источника данных.
  - **Описание** — описание источника данных.
  - **Адрес сервера** — адрес узла, с которого UserGate SWG 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. При работе с AD- и WEC-серверами через UserID-агент в syslog-коннекторе всегда используется часовой пояс UTC. Этот параметр не зависит от настроек часового пояса на контроллере домена.
  - **Профиль аутентификации** — профиль аутентификации, с помощью которого UserID-агент обращается к контроллеру домена по LDAP-протоколу для получения информации о группах, в которых зарегистрирован найденный в журналах syslog пользователь.
  - **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеш-памяти на UserGate SWG. Значение по умолчанию: 2700 секунд (45 минут).
- На вкладке **Фильтры** выберите фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Настройки → Библиотеки → Syslog фильтры UserID-агента**. Подробнее — в разделе « Syslog фильтры UserID-агента ».

Параметры сервера syslog на UserGate SWG можно посмотреть или изменить в разделе **Настройки → Пользователи и устройства → Свойства агента UserID**.

О настройке функции UserID на UserGate SWG — в разделе « UserID».

Интеграция с UserGate Log Analyzer

Благодаря интеграции источника данных об аутентификации пользователей с UserGate Log Analyzer функцию UserID можно масштабировать на другие устройства сети. Принцип работы UserID на устройстве UserGate Log Analyzer аналогичен принципу работы на UserGate SWG. Найденные в собранных данных события отправляются на другие UserGate SWG в соответствии с политикой UserID Sharing на основании настроенных профилей редистрибуции. На UserGate

SWG отправляются только GUID пользователя, его IP-адрес и список идентификаторов групп, участником которых он является. Такая архитектура позволяет использовать один или несколько серверов UserGate Log Analyzer для централизованного сбора информации о пользователях с различных источников и далее централизованно и избирательно распространять эту информацию на узлы UserGate SWG в корпоративной сети.

Для получения информации об аутентификации пользователей выполните настройку следующих параметров на на UserGate Log Analyzer:

1. Активируйте сервис Сборщик логов в параметрах контроля доступа зоны, в которой находится UserID агент для AD- и WEC-серверов. Подробнее о настройке зон — в разделе «Настройка зон».

2. Создайте каталог пользователей для организации доступа UserGate LogAn к серверу AD. Доступ к AD позволяет при необходимости обновлять информацию об имени пользователя в журналах, импортированных из различных сенсоров. Подробнее о создании и настройке серверов аутентификации — в разделе «Каталоги пользователей».

3. Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.

Коннектор UserID-агента в веб-консоли UserGate Log Analyzer создается в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы**. Нажмите **Добавить** и выберите тип создаваемого коннектора: **Отправитель syslog**. Укажите параметры коннектора:

- На вкладке **Общие**:
  - **Включено** — включение или отключение получения журналов от источника данных.
  - **Название** — название источника данных.
  - **Описание** — описание источника данных.
  - **Адрес сервера** — адрес узла, с которого UserGate Log Analyzer 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. При использовании UserID-агента для AD- и WEC-серверов в syslog-коннекторе всегда должно быть время в часовом поясе UTC независимо от настроек времени на контроллере домена.
  - **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеш-памяти на UserGate SWG. Значение по умолчанию: 2700 секунд (45 минут).
  - **Профиль редистрибуции UserID** — профиль для определения круга устройств UserGate SWG, на которые отправляется информация о найденных UserID-агентом пользователях.
- На вкладке **Фильтры** выберите фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Настройки → Библиотеки → Syslog фильтры UserID-агента**. Подробнее — в разделе « Syslog фильтры UserID-агента».
- На вкладке **Каталоги пользователей** выбираются каталоги, в которых происходит поиск пользователя, найденного в логах syslog.

Общие настройки syslog-сервера на UserGate Log Analyzer можно посмотреть или изменить в разделе **Настройки → Сборщик логов → Syslog** .

О настройке функции UserID на UserGate Log Analyzer — в разделе « UserID».

Работа с доверенными браузерами

Version: 7.5.x
Product: SWG

В архитектуре zero trust network access важным требованием является проверка соответствия конечных устройств установленным политикам безопасности перед предоставлением доступа к ресурсам. Так как веб-браузер является основным инструментом доступа пользователей к корпоративным и интернет-ресурсам, система должна обеспечивать его контроль.

Идентификация браузера по заголовку User-Agent не обеспечивает достаточного уровня доверия, поскольку этот параметр может быть изменен. Система централизованного управления корпоративными браузерами не гарантирует, что пользователь будет работать именно через управляемый браузер. Для обеспечения безопасного доступа должны использоваться дополнительные механизмы доверенной идентификации и проверки браузера.

В UserGate SWG реализован механизм проверки подлинности браузера, который может выступать в качестве одного из условий в политиках доступа к ресурсам. В качестве доверенного браузера используется версия «Яндекс Браузера» для организаций.

Архитектура решения

Архитектура решения предполагает развертывание в корпоративной сети организации сервера регистрации (enrollment host), на котором будет храниться база данных зарегистрированных браузеров и выполняться генерация криптографических ключей, используемых для проверки подлинности браузеров. При проверке используются методы семейства стандартов JOSE (JSON Object Signing and Encryption).

«Яндекс Браузер» регистрируется на сервере регистрации и регулярно запрашивает у него актуальный JWT (JSON Web Token). Этот JWT включается во все HTTPS-сообщения в специальный заголовок и служит для проверки подлинности браузера на UserGate SWG.

HTTP-заголовки, добавляемые «Яндекс Браузером»:

- X-Ybe-Authorization: Bearer <JWT string> — токен авторизации (JWT);
- X-Ybe-DeviceId: <DeviceId> — идентификатор устройства, по которому можно идентифицировать инсталляцию браузера в системе управления «Яндекс Браузера»;
- X-Ybe-Id: <SessionId> — идентификатор сессии.

UserGate SWG периодически обращается к серверу регистрации для получения набора открытых ключей в формате JWKS (JSON Web Key Set). При обработке сообщений, содержащих токены авторизации от доверенного браузера, и при наличии политик, включающих проверку подлинности браузера в качестве условия доступа, UserGate SWG проверяет подпись токена с помощью открытого ключа и принимает решение о предоставлении или отказе в доступе. Для предотвращения попадания токена авторизации за контур защиты, UserGate SWG удаляет из сообщения служебные заголовки, добавленные «Яндекс Браузером», если сработало правило, в котором есть условие проверки подлинности браузера.

Настройка работы с доверенными браузерами

Для работы с доверенными браузерами выполните следующие шаги:

1. Разверните систему управления корпоративными браузерами и настройте политику безопасности браузеров. Установите корпоративные браузеры на устройствах пользователей. Документация по настройке и развертыванию корпоративных браузеров предоставляется компанией «Яндекс».

2. Разверните в корпоративной сети и настройте сервер регистрации (enrollment host). Инсталляционные файлы и документация по настройке предоставляется компанией «Яндекс».

3. Настройте подключение UserGate SWG к серверу регистрации.

4. Предоставьте пользователям доступ к ресурсам через доверенный браузер на UserGate SWG с помощью правил фильтрации контента или правил reverse-прокси.

Подключение к серверу регистрации

Для подключения UserGate SWG к серверу регистрации доверенных браузеров перейдите в раздел **Настройки → Пользователи и устройства → Доверенные браузеры**, нажмите **Добавить** и укажите параметры подключения.

Параметр	Описание
Название	Название подключения
Описание	Произвольное описание подключения

Параметр	Описание
URL сервиса Enrollment Host	URL сервера регистрации доверенных браузеров, развернутого в компании. Пример значения параметра: http://<enrollment_host>/corp/enrollment-host/jwks Где <enrollment_host> — доменное имя сервера регистрации
Issuer в стандарте JWT	Параметр задается администратором в переменных среды сервера регистрации «Яндекс Браузера» <URL_IDP> и передается в составе токена JWT. Используется для идентификации сервера регистрации, выдавшего JWT, если в сети имеется нескольких таких серверов
Порт	Порт подключения к серверу регистрации доверенных браузеров. По умолчанию: 8080
Bearer-токен	Ключ доступа к серверу регистрации доверенных браузеров. Определяется администратором сервиса регистрации

Состояние подключения к серверу регистрации доверенных браузеров отображается в колонке «Статус» списка подключений веб-интерфейса.

Предоставление доступа к ресурсам через доверенный браузер

В зависимости от сценария применения UserGate SWG может использовать проверку подлинности браузера в качестве одного из условий для предоставления доступа к ресурсам в правилах фильтрации контента или в правилах reverse-прокси:

- Чтобы разрешить доступ к интернет-ресурсам только через доверенный браузер, применяйте правила фильтрации контента.
- Чтобы разрешить доступ к корпоративным ресурсам только через доверенный браузер, используйте правила reverse-прокси.

ПримечаниеУбедитесь, что пользовательские устройства имеют сетевой доступ к серверу регистрации доверенных браузеров. Это необходимо для получения браузером веб-токенов (JWT).

Настройка доступа к интернет-ресурсам через доверенный браузер

Для предоставления доступа к веб-ресурсам через доверенный браузер:

1. На UserGate SWG заранее настройте правила SSL-инспектирования и аутентификации пользователей (если пользователи или группы пользователей будут использоваться в качестве условий предоставления доступа). Подробнее о правилах инспектирования SSL — в разделе «Инспектирование SSL»; о методах аутентификации — в разделе «Пользователи и группы».

2. Создайте правило фильтрации контента, в котором проверка подлинности браузера используется в качестве дополнительного условия.

В разделе **Настройки → Политики безопасности → Фильтрация контента** нажмите **Добавить** и укажите обязательные параметры правила:

- На вкладке **Общие**:
  - Установите флажок включения правила.
  - Укажите название правила.
  - В поле **Действие** выберите **Разрешить**.
- На вкладке **Доверенные браузеры** выберите созданное ранее подключение к серверу регистрации доверенных браузеров.
- Укажите дополнительные условия фильтрации трафика (например, разрешенные категории URL, списки URL, типы контента, группы пользователей).

Подробнее о создании правил фильтрации контента — в разделе « Фильтрация контента».

3. Так как встроенное правило фильтрации контента Default allow разрешает любой доступ, для блокировки использования недоверенных браузеров создайте запрещающее правило с инверсным условием идентификации доверенного браузера.

Вы также можете создать дополнительное правило фильтрации контента, чтобы сформировать предупреждения пользователям, использующим недоверенный браузер, с указанием ссылки на ресурс для скачивания доверенного браузера на странице блокировки. Для этого:

1. В разделе **Настройки → Политики безопасности → Фильтрация контента** нажмите **Добавить** и укажите обязательные параметры правила:

- На вкладке **Общие**:
  - Установите флажок включения правила.
  - Укажите название правила.
  - В поле **Действие** выберите **Запретить**.
  - Выберите настроенную заранее страницу блокировки со ссылкой на скачивание доверенного «Яндекс Браузера».
- На вкладке **Доверенные браузеры** выберите созданное ранее подключение к серверу регистрации доверенных браузеров и включите **Инвертировать** внизу окна.

Подробнее о создании правил фильтрации контента — в разделе « Фильтрация контента»; о шаблонах страниц — в разделе « Шаблоны страниц».

2. Чтобы пользователи могли загрузить доверенный браузер, создайте разрешающее правило для доступа к указанному ресурсу и разместите его выше запрещающего правила.

Настройка доступа к корпоративным ресурсам через доверенный браузер

Для предоставления доступа к корпоративным ресурсам через доверенный браузер выполните следующие шаги:

1. Для обмена трафиком с публикуемыми ресурсами по защищенному соединению создайте на UserGate SWG профиль SSL, содержащий нужные

криптографические протоколы, и импортируйте сертификат публикуемого ресурса.

Подробнее о профилях SSL — в разделе « Профили SSL »; о сертификатах — в разделе « Управление сертификатами».

2. Создайте правило reverse-прокси, в котором проверка подлинности браузера используется в качестве дополнительного условия.

В разделе **Настройки → Глобальный портал → Правила reverse-прокси** нажмите **Добавить** и укажите обязательные параметры правила:

- На вкладке **Общие**:
    - Установите флажок включения правила.
    - Укажите название правила.
    - Выберите сервер или балансировщик reverse-прокси, которому UserGate SWG будет пересылать запросы.
    - Укажите порты, на которых UserGate SWG будет слушать входящие запросы.
    - Выберите заранее созданный профиль SSL и сертификат публикуемого сервера.
- На вкладке **Источник** выберите минимум одну зону источника трафика, а также, если необходимо, добавьте списки IP-адресов, доменных имен или GeoIP-адреса, для которых будет разрешен обмен трафиком с веб-серверами.
- На вкладке **Подмена путей** настройте переопределение путей URL.
- На вкладке **Доверенные браузеры** выберите созданное ранее подключение к серверу регистрации доверенных браузеров.

Укажите дополнительные условия предоставления доступа (например, группы пользователей).

Подробнее о создании правил reverse-прокси — в разделе « Публикация ресурсов с помощью reverse-прокси ».

Вы также можете создать правило reverse-прокси с перенаправлением аутентифицированных пользователей, пытающихся подключиться к корпоративному ресурсу с недоверенного браузера, на страницу для скачивания.

Для этого в разделе **Настройки → Глобальный портал → Правила reverse-прокси** нажмите **Добавить** и укажите обязательные параметры правила:

- На вкладке **Общие**:
    - Установите флажок включения правила.
    - Укажите название правила.
    - Выберите сервер или балансировщик reverse-прокси, которому UserGate SWG будет пересылать запросы.
    - Укажите порты, на которых UserGate SWG будет слушать входящие запросы.
    - Выберите заранее созданный профиль SSL и сертификат публикуемого сервера.
    - Включите авторизацию пользователей, выбрав в поле **Авторизовать по сертификату** значение **PKI**, и затем укажите предварительно созданный профиль клиентских сертификатов. Подробнее о профилях — в разделе «Профили клиентских сертификатов».
- На вкладке **Источник** выберите минимум одну зону источника трафика, а также, если необходимо, добавьте списки IP-адресов, доменных имен или GeoIP-адреса, для которых будет разрешен обмен трафиком с веб-серверами.
- На вкладке **Пользователи** выберите пользователей или группы пользователей, для которых будет разрешено скачать дистрибутив доверенного браузера.
- На вкладке **Подмена путей** настройте переопределение на страницу для скачивания дистрибутива Яндекс Браузера.
- На вкладке **Доверенные браузеры** выберите созданное ранее подключение к серверу регистрации доверенных браузеров и включите **Инвертировать** внизу окна.

Разместите это правило выше правила, разрешающего доступ к корпоративным ресурсам через доверенный браузер.

Подробнее о создании правил reverse-прокси — в разделе « Публикация ресурсов с помощью reverse-прокси ».