

Руководство по администрированию

WM42

Москва 2024

Содержание:

Использование Embedded Web Server	3
Сброс пароля при помощи sec jumper	5
Подготовка к настройке принтера в беспроводной сети	6
Установка сертификата, цепочки сертификатов	8
Ограничение доступа к порту	8
Сброс всех настроек	9
Настройки сканирования SMTP	11
Поддержка алгоритмов шифрования	13

Использование Embedded Web Server

Примечание: Эта функция доступна только для сетевых принтеров или для принтеров, подключенных к серверам печати.

Если принтер установлен в сетевом окружении, Embedded Web Server можно использовать для выполнения следующих функций:

- Просмотр виртуального изображения панели управления принтера;
- Проверка состояния расходных материалов принтера;
- Настройка уведомлений о расходных материалах;
- Настройка параметров принтера;
- Настройка сетевых параметров;
- Просмотр отчетов.

Для доступа принтера к веб-серверу Embedded Web Server:

1) Получите IP-адрес принтера.

- В разделе «TCP/IP» меню «Сеть/порты»
- Путем печати страницы настройки сети или параметров меню и поиска раздела «TCP/IP»

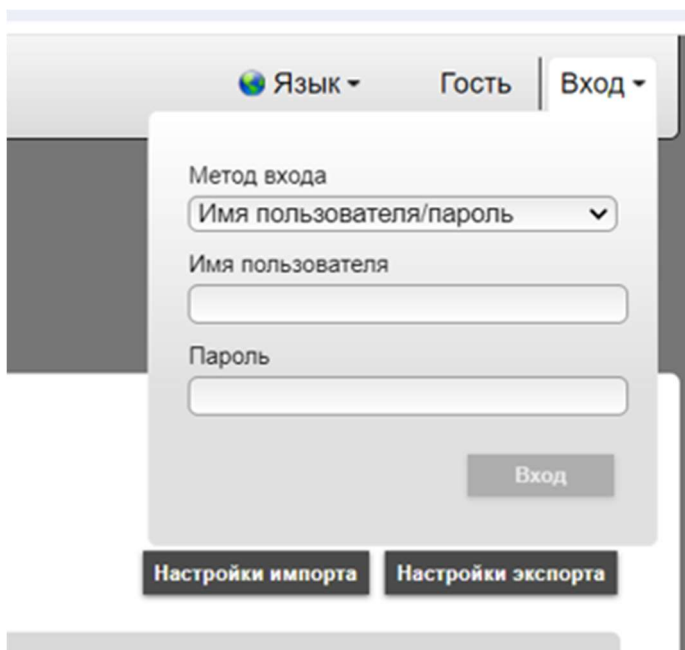
Примечание: IP-адрес отображается в виде четырех наборов цифр, разделенных точками, например 123.123.123.123. Если используется прокси-сервер, временно отключите его, чтобы обеспечить правильную загрузку веб-страницы.

- 2) Откройте веб-обозреватель и в поле адреса введите IP-адрес принтера.
- 3) Нажмите клавишу Enter. Откроется страница Embedded Web Server.

Создание пароля на вход в веб интерфейс устройства

На главной странице веб интерфейса в окне входа указываются пароль, логин и пароль либо ПИН-код для входа в веб интерфейс. Для этого требуется выбрать метод входа.

Пример:

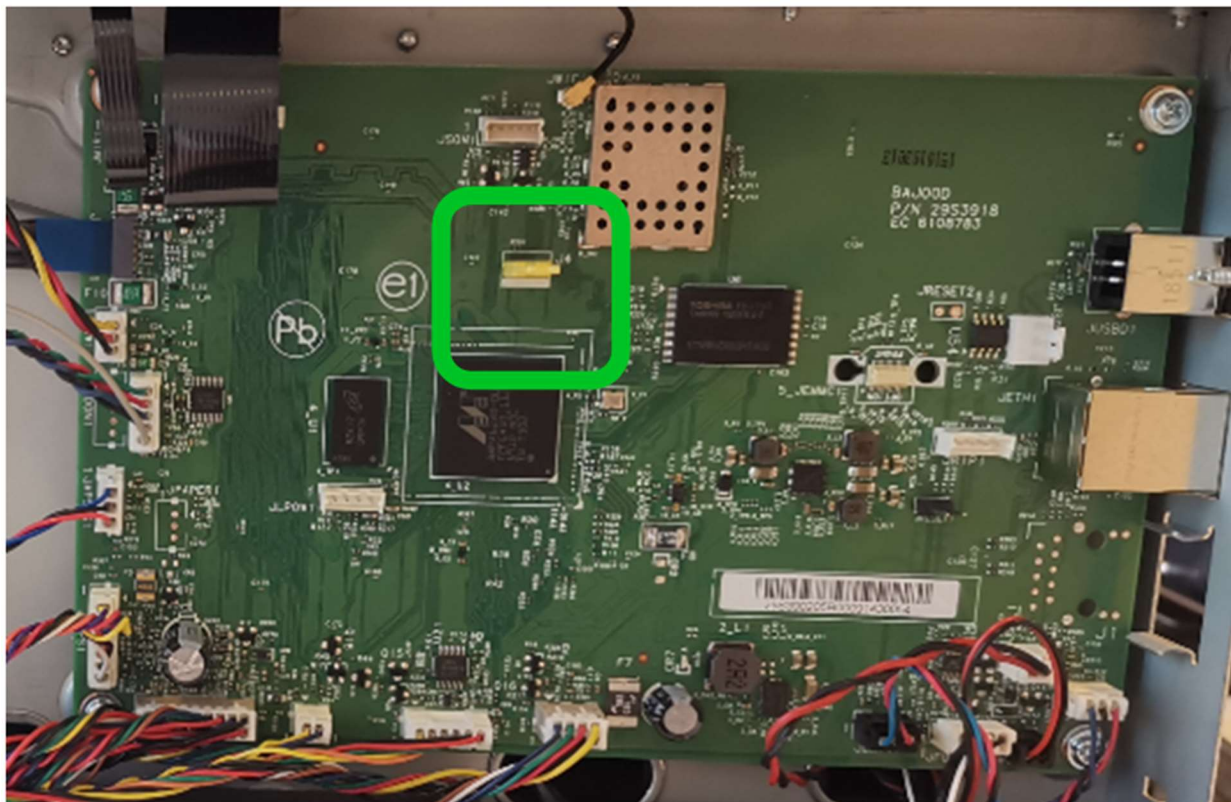


В зависимости от выбранного метода входа изменится приглашение для входа.

Внимание! При утере пароля допускается сброс пароля на главной плате устройства. При помощи `sec/jumper`.

Сброс пароля при помощи sec jumper

Главная плата устройства содержит единственный Jumper для сброса пароля:



Сброс административного пароля:

- 1) Выключите принтер.
- 2) Откройте доступ к системной плате устройства.
- 3) Найдите жёлтую перемычку.
- 4) Переставьте перемычку в соседнюю позицию. Начальная позиция значения не имеет.
- 5) Включите питание. Сброс пароля должен состояться. Возвращать перемычку в первоначальное положение не обязательно.

Подготовка к настройке принтера в беспроводной сети

Примечания:

- Убедитесь в том, что адаптер беспроводной сети установлен в принтер и работает нормально. Для получения дополнительных сведений см. инструкции, прилагаемые к адаптеру беспроводной сети.
- Убедитесь в том, что точка доступа (беспроводной маршрутизатор) включена и работает.

Перед настройкой принтера в беспроводной сети убедитесь в наличии следующих данных:

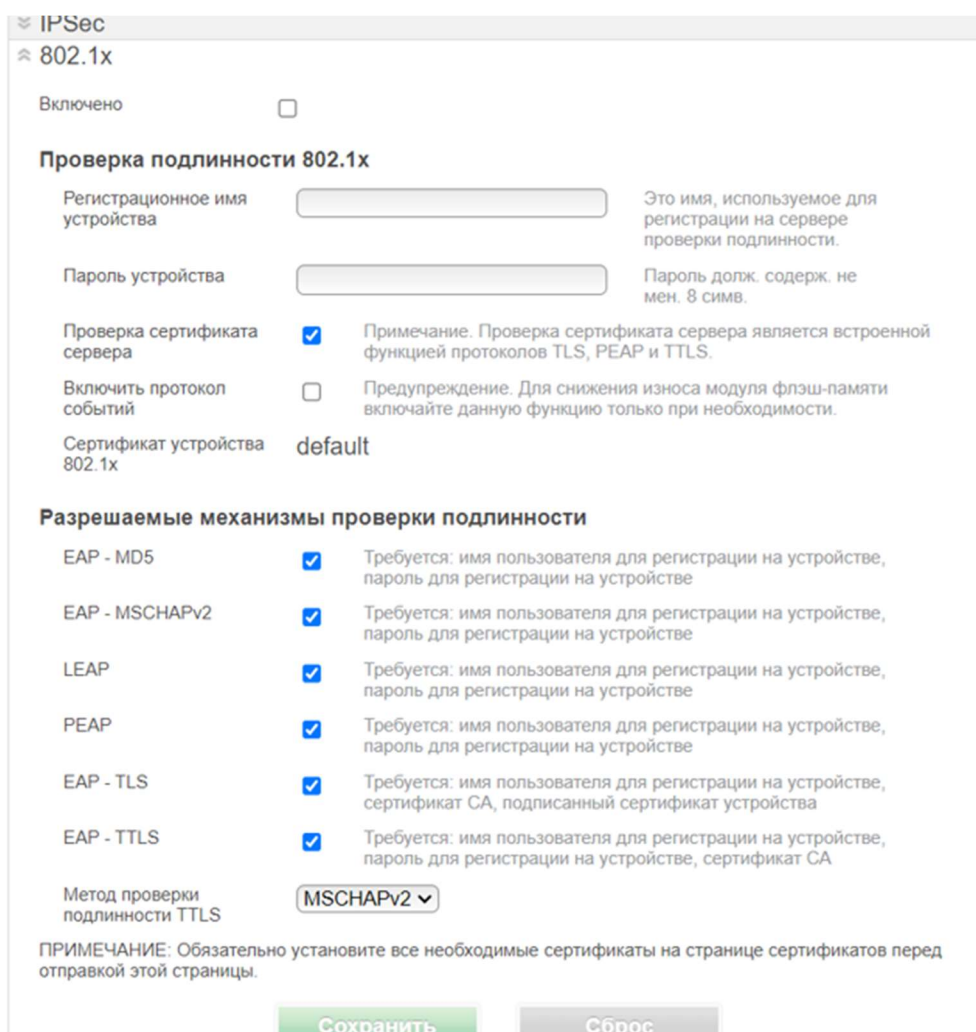
- SSID. SSID также называют именем сети.
- Беспроводной режим (или режим сети) - это может быть либо одноранговый режим, либо режим инфраструктуры.
- Канал (для одноранговых сетей). Для сетей в режиме инфраструктуры по умолчанию канал выбирается автоматически. В некоторых одноранговых сетях также необходимо использовать параметр автоматического выбора. Если вы сомневаетесь, какой канал следует выбрать, обратитесь к специалисту службы поддержки.
- Способ защиты. Существует четыре базовых варианта «Способа защиты»:
 - ключ WEP. Если в беспроводной сети используется несколько ключей WEP, введите до четырех ключей в имеющихся полях. Выберите ключ, который в настоящее время используется в сети. Для этого выберите параметр «Ключ передачи WEP по умолчанию»;
 - предварительный ключ или фраза доступа WPA или WPA2. В WPA используется шифрование в качестве дополнительного уровня безопасности. Возможные варианты: AES и TKIP. Необходимо выбрать один и тот же тип шифрования на маршрутизаторе и принтер. В противном случае обмен данными по сети будет невозможен для принтера.
 - 802.1X–RADIUS. В случае установки принтера в сети 802.1X может потребоваться следующая информация:
 - Тип проверки подлинности;
 - Тип внутренней проверки подлинности;
 - Имя пользователя и пароль 802.1X;
 - Сертификаты.
 - Защита отсутствует.

Если в беспроводной сети не используется защита, никакие данные безопасности не потребуются.

Внимание! Не рекомендуется использовать беспроводные сети без защиты.

Примечания:

- Если имя SSID сети, к которой подключен компьютер, неизвестно, запустите программу настройки беспроводного соединения сетевого адаптера компьютера, чтобы узнать имя сети.
- Если не удастся найти имя SSID или сведения по безопасности для сети, обратитесь к документации, прилагаемой к беспроводной точке доступа, или к специалисту по поддержке системы.
- Чтобы найти предварительный ключ/фразу доступа WPA/WPA2 или фразу доступа для беспроводной сети, обратитесь к документации, прилагаемой к беспроводной точке доступа (беспроводному маршрутизатору), перейдите на встроенный сервер Embedded Web Server соответствующей точки доступа, или обратитесь к представителю службы поддержки.



IPSec

802.1x

Включено

Проверка подлинности 802.1x

Регистрационное имя устройства Это имя, используемое для регистрации на сервере проверки подлинности.

Пароль устройства Пароль долж. содерж. не мен. 8 симв.

Проверка сертификата сервера Примечание. Проверка сертификата сервера является встроенной функцией протоколов TLS, PEAP и TTLS.

Включить протокол событий Предупреждение. Для снижения износа модуля флэш-памяти включайте данную функцию только при необходимости.

Сертификат устройства 802.1x default

Разрешаемые механизмы проверки подлинности

EAP - MD5 Требуется: имя пользователя для регистрации на устройстве, пароль для регистрации на устройстве

EAP - MSCHAPv2 Требуется: имя пользователя для регистрации на устройстве, пароль для регистрации на устройстве

LEAP Требуется: имя пользователя для регистрации на устройстве, пароль для регистрации на устройстве

PEAP Требуется: имя пользователя для регистрации на устройстве, пароль для регистрации на устройстве

EAP - TLS Требуется: имя пользователя для регистрации на устройстве, сертификат CA, подписанный сертификат устройства

EAP - TTLS Требуется: имя пользователя для регистрации на устройстве, пароль для регистрации на устройстве, сертификат CA

Метод проверки подлинности TTLS MSCHAPv2

ПРИМЕЧАНИЕ: Обязательно установите все необходимые сертификаты на странице сертификатов перед отправкой этой страницы.

Сохранить Сброс

Примечание: Длина пароля ограничена 32 символами. Допускается использование спецсимволов: (!?@#\$\$%^&* _).

Установка сертификата, цепочки сертификатов

На веб интерфейсе устройства в разделе «Безопасность»:

⌵ Управление сертификатами

[Настройка сертификатов по умолчанию](#)

Сертификаты устройства

Создать
Импорт
Удалить

<input type="checkbox"/>	Понятное имя	Общепринятое название	Общее имя поставщика	Действ. с	Действ. до	Подпи
Нет сертификатов						

Управление сертификатами ЦС

Загрузка ЦС
Удалить

<input type="checkbox"/>	Общее имя ЦС	Действ. с	Действ. до
Нет сертификатов ЦС			

Внимание! Доступ открыт только при наличии SSL соединения с устройством.

В адресной строке требуется указание IP address устройства с «https://», о чем будет выведена соответствующая подсказка. Клавиша импорт позволяет импортировать сертификаты. Сертификаты должны быть импортированы с использованием форматов .cer и pcks-12. Импортированные сертификаты будут храниться в защищенном хранилище в энергонезависимой памяти.

Ограничение доступа к порту

Активация порта USB На начальном экране выберите Параметры > Сеть/Порты > USB > Включить порт USB

В случае необходимости ограничения доступа к сетевым портам в разделе Параметры > Сеть/Порты > выбрать доступ к порты TCP/IP

Пример:

Доступ к порту TCP/IP

TCP 21 (FTP)	<input checked="" type="checkbox"/>	Открытый
UDP 69 (TFTP)	<input checked="" type="checkbox"/>	Открытый
TCP 80 (HTTP)	<input checked="" type="checkbox"/>	Открытый
TCP 443 (HTTPS)	<input checked="" type="checkbox"/>	Открытый
UDP 137 (WINS)	<input checked="" type="checkbox"/>	Открытый
UDP 161 (SNMP)	<input checked="" type="checkbox"/>	Открытый
UDP 162 (Ловушки SNMP)	<input checked="" type="checkbox"/>	Открытый
TCP 515 (LPR/LPD)	<input checked="" type="checkbox"/>	Открытый
TCP 631 (IPP)	<input checked="" type="checkbox"/>	Открытый
TCP 5001 (IPDS)	<input checked="" type="checkbox"/>	Открытый
UDP 5353 (mDNS)	<input checked="" type="checkbox"/>	Открытый
TCP 9100 (Raw Print)	<input checked="" type="checkbox"/>	Открытый
UDP 9200 (Поиск устройств)	<input checked="" type="checkbox"/>	Открытый
UDP 9300 UDP 9301 UDP 9302 (NPAP)	<input checked="" type="checkbox"/>	Открытый
TCP 9400 (Улучшенный порт печати)	<input checked="" type="checkbox"/>	Открытый
TCP 9500 TCP 9501 (NPAP)	<input checked="" type="checkbox"/>	Открытый
TCP 9600	<input checked="" type="checkbox"/>	Открытый
ThinPrint	<input checked="" type="checkbox"/>	Открытый

Сброс всех настроек

Очистка памяти принтера

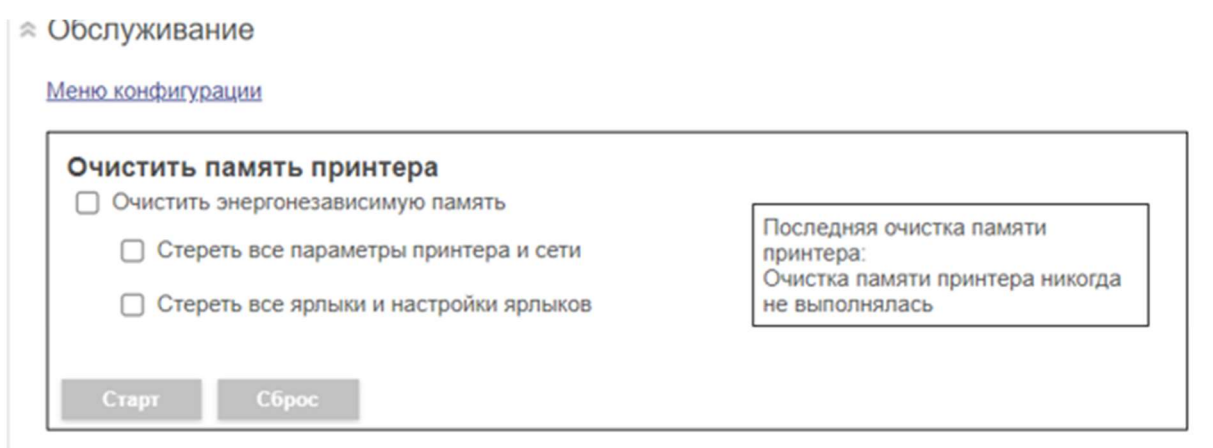
Внимание! Устройство не содержит дисков или ссд накопителей.

Некоторые пароли и ссылки на сетевые ресурсы могут быть сохранены в энергонезависимой памяти.

Чтобы очистить энергонезависимую память или буферизованные данные принтера, выключите принтер.

Чтобы очистить энергонезависимую память или удалить отдельные параметры, параметры устройства и сети, параметры безопасности и встроенных решений, выполните следующие действия:

- 1) На начальном экране выберите Параметры > Устройство > Обслуживание > Очистка при простое.
- 2) Поставьте флажок «Очистить энергонезависимую память» и нажмите ОК.
- 3) Выберите либо «Запуск первоначальной установки», либо «Оставить принтер в автономном режиме», а затем нажмите ОК.



Внимание! Большая часть параметров продублированы на панели устройства. И могут быть выполнены с панели оператора.

Настройки сканирования SMTP

Настройте параметры протокола SMTP (Simple Mail Transfer Protocol) для передачи отсканированного документа по электронной почте. Настройки зависят от поставщика услуг электронной почты. Для получения дополнительных сведений см. раздел поставщиков услуг электронной почты.

Прежде чем начать, убедитесь, что принтер подключен к сети и что сеть подключена к Интернету.

Использование Embedded Web Server

1) Откройте веб-браузер и в поле адреса введите IP-адрес принтера.

Примечания:

- IP-адрес принтера указан на начальном экране принтера. IP-адрес отображается в виде четырех наборов цифр, разделенных точками, например, 123.123.123.123.
- Если используется прокси-сервер, временно отключите его, чтобы обеспечить правильную загрузку веб-страницы.

2) Нажмите Параметры>Электронная почта.

3) Настройте параметры в разделе «Настройка электронной почты».

Примечания:

- Для получения дополнительной информации о пароле см. список поставщиков услуг электронной почты.
- Если требуемого поставщика услуг электронной почты нет в списке, обратитесь к нему для получения информации о настройках.

4) Нажмите «Сохранить».

Параметры > Электронная почта

Электронная почта

⌵ Настройка эл. почты

Первичный шлюз SMTP	<input type="text"/>	Требуется.
Порт первичного шлюза SMTP	<input type="text"/>	Диапазон: 1-65535. По умолчанию = 25.
Вторичный шлюз SMTP	<input type="text"/>	
Порт вторичного шлюза SMTP	<input type="text"/>	Диапазон: 1-65535. По умолчанию = 25.
Время ожидания SMTP	<input type="text"/>	Диапазон: 5-30 сек.
Адрес для ответа	<input type="text"/>	
Всегда использовать адрес SMTP для ответа	<input checked="" type="checkbox"/>	
Использовать SSL/TLS	<input type="text" value="Согласование"/>	
Требуется доверенный сертификат	<input type="checkbox"/>	
Проверка подлинности сервера SMTP	<input type="text" value="Проверка подлинности не требует"/>	
Эл. сообщение от устройства	<input type="text" value="Нет"/>	Электронные уведомления, отправка факсов и т.д.
Имя польз. устройства	<input type="text"/>	
Пароль устройства	<input type="text"/>	
Домен NTLM	<input type="text"/>	Требуется для проверки подлинности NTLM.
Отключить ошибку "Не настроен сервер SMTP"	<input checked="" type="checkbox"/>	

Сохранить

Сброс

⌵ Параметры по умолчанию для эл. почты

Правила длины пароля и содержания спец символов аналогично другим параметрам сетевых конфигураций.

Поддержка алгоритмов шифрования

Список поддерживаемых алгоритмов:

DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA

Протокол TLS

Включить TLSv1.0

Вкл.*

Выкл.

Включение протокола TLSv1.0.

Включить TLSv1.1

Вкл.*

Выкл.

Включение протокола TLSv1.1.

Список поддерживаемых протоколов на веб интерфейсе TLS:

MTU	<input type="text" value="1500"/>
Порт печати Raw	<input type="text" value="9100"/>
Максимальная скорость передачи данных для исходящего трафика	<input type="checkbox"/>
<input type="text" value="100000"/>	Кбит/с (диапазон: 10
Включить TLSv1.0	<input checked="" type="checkbox"/>
Включить TLSv1.1	<input checked="" type="checkbox"/>
Сп. ал. шиф. SSL	<input type="text" value="DHE-RSA
SHA384:D
GCM-SHA"/>

SNMP

Использование меню принтера. Пункт меню «Описание»:

SNMP версий 1 и 2с

Включено

Выкл

Вкл.*

Разрешить управление по SNMP

Выкл

Вкл.*

Включить PPM MIB

Выкл

Вкл.*

Сообщество SNMP

Настройка простого протокола сетевого администрирования (SNMP) версий 1 и 2с для установки драйверов печати и приложений.

Примечание: (*) - заводские настройки по умолчанию.

802.1x

Использование меню принтера. Пункт меню «Описание»:

Активный

Выкл.*

Вкл.

Позволяет устанавливать соединение принтера с сетями, требующими аутентификации для разрешения доступа.

Примечание: (*) - заводские настройки по умолчанию.