

ВЕРСИЯ 1.0
ОКТАБРЬ 2024
702P09325

Trellix[®] Embedded Control и Trellix[®] ePO

Руководство по конфигурации

©2024 Xerox Corporation. All rights reserved. Unpublished rights reserved under the copyright laws of the United States. Contents of this publication may not be reproduced in any form without permission of Xerox Corporation.

Copyright protection claimed includes all forms of matters of copyrightable materials and information now allowed by statutory or judicial law or hereinafter granted, including without limitation, material generated from the software programs which are displayed on the screen such as styles, templates, icons, screen displays, looks, and so on.

Xerox® and CentreWare® are trademarks of Xerox Corporation in the United States and/or other countries.

Microsoft® is a trademark of Microsoft group of companies.

Trellix, ePolicy Orchestrator, and ePO are trademarks Musarubra US LLC.

Содержание

Trellix Embedded Control	5
Обзор Trellix Embedded Control	6
Установка уровня безопасности	7
Настройка параметров уведомлений	8
Конфигурация уведомлений о событиях безопасности Trellix ePO	9
Обзор процесса	10
Настройка уведомлений о событиях безопасности в Trellix ePO	10
Загрузка и установка расширений Xerox для Trellix ePO	12
Предоставление лицензионных ключей в Trellix ePO	13
Изменение порта связи для выхода агента из режима ожидания в Trellix ePO	14
Изменение ограничения на максимальный размер загружаемых файлов на сервере Trellix ePO	15
Создание и назначение политики в Trellix ePO	16
Настройка автоматического реагирования в Trellix ePO	17
Настройка параметров сервера Trellix ePolicy Orchestrator	18
Назначение принтеров в качестве суперузлов	19
Добавление записей DNS к одному или нескольким существующим доменам	19
Добавление записей DNS в один новый домен	19
Обеспечение управления устройством в Trellix	21
Настройка прокси-сервера Trellix ePO	23
Настройка прокси-сервера Trellix ePO	24
Удаление и повторная установка расширений Trellix ePO	25
Удаление и повторная установка расширений Trellix ePO	26

Trellix Embedded Control

Содержание этой главы:

Обзор Trellix Embedded Control	6
Установка уровня безопасности	7
Настройка параметров уведомлений	8



Примечание. Trellix®, ранее известная как McAfee®.

Обзор Trellix Embedded Control

Если на вашем сервере установлен Trellix® ePolicy Orchestrator (ePO), используйте данное руководство для интеграции многофункциональных принтеров Xerox, оснащенных функцией безопасности Trellix Embedded Control.

Решение Trellix Embedded Control включает в себя две функции защиты:

- Функция «Дополнительная защита» обеспечивает целостность программы принтера, контролируя системные файлы и предупреждая пользователя в случае их несанкционированного изменения.
- Контроль целостности представляет собой программный модуль, обладающий помимо функций дополнительной защиты способностью контролировать и предотвращать запуск несанкционированных исполняемых файлов. Для включения данной опции требуется предоставить ключ для установки функции на странице «Установка функции». Для получения Ключа установки функции обратитесь в местное представительство Xerox.

На принтере можно настроить отправку уведомлений по электронной почте о событиях, связанных с безопасностью. Доступно несколько методов отправки уведомлений.

Уведомления по электронной почте могут быть отправлены непосредственно вам или в приложение для централизованного управления, например:

- Trellix® ePolicy Orchestrator (ePO)
- Xerox® CentreWare® Web
- Xerox® Device Manager


Подробные сведения о Trellix ePO и Trellix Embedded Control см. на сайте www.trellix.com.

Установка уровня безопасности


Если вы не приобрели Trellix Integrity Control, компания Xerox рекомендует сохранить уровень безопасности, установленный по умолчанию, – Дополнительная защита.

Решение Trellix Embedded Control включает в себя два уровня безопасности:

- Дополнительная защита
- Контроль целостности

 **Примечание.** Устанавливайте уровень безопасности только в случае необходимости. В стандартной комплектации принтер поставляется с уровнем «Дополнительная защита», который во многих случаях является достаточным.

1. В приложении Embedded Web Server многофункционального принтера нажмите **Свойства > Безопасность**.
2. Выберите **Trellix Embedded Control**.
3. Для включения функций Trellix Embedded Control и настройки параметров в разделе Методы передачи тревожных сигналов нажмите кнопку **Редактировать**.
4. Для установки Уровня безопасности в поле «Уровень безопасности» выберите **Дополнительная защита** или **Контроль целостности**.
5. Если в качестве уровня безопасности выбрана Дополнительная защита, нажмите **Сохранить**.
6. Если в качестве уровня безопасности выбран Контроль целостности, нажмите **Далее**, введите Ключ установки функции программного обеспечения, затем нажмите **Применить**.

 **Примечание.** Если настройка уровня защиты изменяется, принтер перезапускается. Процесс может занять несколько минут.

Настройка параметров уведомлений

Можно настроить на принтере уведомление пользователя о событиях, связанных с безопасностью.

Для настройки параметров уведомлений:

1. В приложении Embedded Web Server многофункционального принтера нажмите **Свойства > Безопасность**.
2. Выберите **Trellix Embedded Control**.
3. Для того чтобы настроить параметры в разделе Методы передачи тревожных сигналов, нажмите кнопку **Редактировать**.
4. Для того чтобы настроить принтер на отправку уведомлений по электронной почте:
 - a. В разделе «Локально на устройстве» выберите **Предупреждения по электронной почте**, затем нажмите **Сохранить**.
 - b. Рядом с полем Предупреждения по электронной почте в разделе Действие, нажмите кнопку **Редактировать**.
 - c. В разделе Адреса группы получателей введите действительные адреса электронной почты для каждой соответствующей группы 1, 2 или 3.
 - d. Для каждой группы с адресами электронной почты выберите **Включить группу**.
 - e. В разделе Предпочтения группы получателей для Trellix Embedded Control выберите каждую группу, которая будет получать уведомления: **Группа 1, Группа 2 и Группа 3**.
 - f. Нажмите кнопку **Применить**.
 - g. При появлении запроса нажмите кнопку **ОК**.
5. Настройте метод передачи тревожных сигналов.
 - Для того чтобы настроить принтер на отправку уведомлений на сервер Trellix ePolicy Orchestrator, в разделе «Решения Trellix для удаленной защиты» выберите **Сервер Trellix ePolicy Orchestrator**.
 - Если вы используете Xerox® CentreWare® Web для управления принтерами, настройте оповещения о безопасности в Xerox® CentreWare® Web.
 - Если управление принтерами осуществляет компания Xerox, используйте Xerox® Device Manager для отправки уведомлений о безопасности с зарегистрированных принтеров.



Примечание. Когда включены функции Trellix Embedded Control, принтер также регистрирует события безопасности в журнале аудита.

Конфигурация уведомлений о событиях безопасности Trellix ePO

Содержание этой главы:



Обзор процесса	10
Загрузка и установка расширений Xerox для Trellix ePO	12
Предоставление лицензионных ключей в Trellix ePO	13
Изменение порта связи для выхода агента из режима ожидания в Trellix ePO	14
Изменение ограничения на максимальный размер загружаемых файлов на сервере Trellix ePO	15
Создание и назначение политики в Trellix ePO	16
Настройка автоматического реагирования в Trellix ePO	17
Настройка параметров сервера Trellix ePolicy Orchestrator	18
Назначение принтеров в качестве суперузлов	19
Обеспечение управления устройством в Trellix	21

Обзор процесса

В данном обзоре представлены процедуры, необходимые для настройки в определенном порядке уведомлений о безопасности в Trellix ePO.

НАСТРОЙКА УВЕДОМЛЕНИЙ О СОБЫТИЯХ БЕЗОПАСНОСТИ В TRELIX EPO


Для того чтобы настроить уведомления о безопасности в Trellix ePO, выполните каждую процедуру в указанном порядке:

1. Приобретите и установите серверное программное обеспечение Trellix ePO. Для получения подробной информации обратитесь к представителю компании Trellix или посетите сайт www.trellix.com.
2. Расширения Xerox® для Trellix ePO требуют наличия Microsoft .NET Framework. Загрузите и установите Microsoft .NET Framework, версию 4.0 или более позднюю. Подробности см. на сайте www.microsoft.com.
 Примечание. Необходимая версия .NET зависит от SQL-сервера, используемого в вашем сервере ePO.
 Примечание. Если вы не выполните эту процедуру, то при открытии расширения Xerox MFP появится сообщение Ошибка-2.
3. Загрузите и установите расширения Xerox® для Trellix ePO. Подробности см. в разделе [Загрузка и установка расширений Xerox для Trellix ePO](#).
4. Предоставьте лицензионные ключи в Trellix ePO. Подробности см. в разделе [Предоставление лицензионных ключей в Trellix ePO](#).
5. Для того чтобы убедиться, что принтер может взаимодействовать с сервером Trellix ePO, измените порт связи для выхода агента из режима ожидания по умолчанию в Trellix ePO. Подробности см. в разделе [Изменение порта связи для выхода агента из режима ожидания в Trellix ePO](#).
6. Для того чтобы разрешить обновление программного обеспечения принтера, измените ограничение на максимальный размер загружаемых файлов на сервере Trellix ePO. Максимальный размер загружаемого файла должен быть больше размера файла обновления программного обеспечения принтера Xerox®. Подробности см. в разделе [Изменение ограничения на максимальный размер загружаемых файлов на сервере Trellix ePO](#).
7. Убедитесь, что уведомления о событиях безопасности отправляются в момент их возникновения, а не через регулярные промежутки времени. Создайте политику безопасности, а затем свяжите ее с принтерами Xerox® в Trellix ePO. Подробности см. в разделе [Создание и назначение политики в Trellix ePO](#).
8. Для того чтобы обеспечить автоматическое получение электронных писем в случае уведомления о безопасности, настройте Автоматическое реагирование в Trellix ePO. Подробности см. в разделе [Настройка автоматического реагирования в Trellix ePO](#).
9. В приложении Embedded Web Server многофункционального принтера на странице Trellix Embedded Control укажите сведения о сервере Trellix ePO. Подробности см. в разделе [Настройка параметров сервера Trellix ePolicy Orchestrator](#).


10. Назначьте принтеры в качестве суперузлов в вашей сети. Подробности см. в разделе [Назначение принтеров в качестве суперузлов](#).
11. Обеспечьте управление устройством в Trellix ePO. Подробности см. в разделе [Обеспечение управления устройством в Trellix ePO](#).
12. Настройте прокси-сервер Trellix ePO. Подробности см. в разделе [Настройка прокси-сервера Trellix ePO](#).

Загрузка и установка расширений Xerox для Trellix ePO

1. Найдите и загрузите расширения Xerox®. Расширения содержатся в файле .zip.
 - a. Для того чтобы перейти на веб-сайт технической поддержки Xerox®, откройте веб-браузер и введите www.xerox.com/office/support.
 - b. Для того чтобы перейти на страницу технической поддержки для конкретного устройства, в поле Поиск введите модель устройства и нажмите **Enter**.
 - c. В появившемся списке результатов для вашего устройства выберите **Драйверы и загрузка**.
 - d. В выпадающем меню Операционная система выберите операционную систему для вашего сервера.

 Примечание. Необходимо убедиться в выборе операционной системы для своего сервера, а не операционной системы своего компьютера.

 - e. В поле Утилиты и приложения выберите **Расширение Xerox для Trellix ePolicy Orchestrator (ePO)**.
 - f. Прочтите Лицензионное соглашение для конечного пользователя и нажмите **Принимаю**.
2. Откройте файл .zip, а затем переместите два сжатых файла расширения во временную папку. Не открывайте файлы расширения .zip.
3. В Trellix ePO установите файлы расширения .zip.
 - a. Откройте веб-интерфейс Trellix ePO по адресу <https://servername.domain:8443>.
 - b. Перейдите в раздел **Меню > Программное обеспечение > Расширения**.
 - c. В левом верхнем углу нажмите **Установить расширение**.
 - d. Перейдите во временную папку, выберите и откройте файл расширения .zip.
 - e. Нажмите **ОК**.

 Примечание. Если во время установки появляется сообщение о том, что расширение Solidcore уже установлено, удалите существующее расширение Solidcore. После завершения установки переустановите программное обеспечение, предоставленное компанией Xerox, и обновите расширение Solidcore. Подробности см. в разделе [Удаление и повторная установка расширений Trellix ePO](#).

 - f. Установите другой файл расширения .zip.
4. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу «Предоставление лицензионных ключей в Trellix ePO».

Предоставление лицензионных ключей в Trellix ePO

1. Откройте веб-интерфейс Trellix ePO по адресу <https://servername.domain:8443>.
2. Перейдите в раздел **Меню > Конфигурация > Настройки сервера**.
3. Нажмите **Solidcore**.
4. В правом нижнем углу нажмите **Изменить**.
5. Введите следующие лицензионные ключи:
 - Контроль изменений: XL17-ZCWK-K7E2-9PZY-OT6V
 - Контроль приложений: ZM7H-FX52-3SFL-TR5Z-MAG3
 - Контроль целостности: K5DA-AG51-5AR3-OB99-WTDG
6. Нажмите **Сохранить**.
7. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу **Изменение порта связи для выхода агента из режима ожидания в Trellix ePO**.

Изменение порта связи для выхода агента из режима ожидания в Trellix ePO

1. Откройте веб-интерфейс Trellix ePO по адресу <https://servername.domain:8443>.
2. Перейдите в раздел **Меню > Конфигурация > Настройки сервера**.
3. Нажмите **Порты**.
4. В правом нижнем углу нажмите **Изменить**.
5. Введите 8083 рядом с портом связи для выхода агента из режима ожидания или любой другой неиспользуемый порт, кроме 8081, установленного по умолчанию.
6. Нажмите **Сохранить**.
7. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу [Изменение ограничения на максимальный размер загружаемых файлов на сервере Trellix ePO](#).

Изменение ограничения на максимальный размер загружаемых файлов на сервере Trellix ePO

1. Зайдите на сервер Trellix ePO, а затем перейдите в `C:\Program Files (x86)\Trellix\ePolicy Orchestrator\Server\conf\orion`.
2. С помощью приложения текстового редактора откройте файл **orion.properties**.
3. Измените текст `orion.upload.max.size=900000000` на `orion.upload.max.size=500000000`.
4. Сохраните текстовый файл.
5. Перезапустите сервер ePO.
6. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу [Создание и назначение политики в Trellix ePO](#).

Создание и назначение политики в Trellix ePO

1. Откройте веб-интерфейс Trellix ePO по адресу <https://servername.domain:8443>.
2. Перейдите в раздел **Меню > Политика > Каталог политик**.
3. Рядом с полем Продукт выберите **Агент Trellix**.
4. Рядом с полем Категория выберите **Общие**.
5. Для того чтобы создать политику, рядом с полем Мои значения по умолчанию в столбце Действия нажмите на **Дублировать**.
 - a. Рядом с полем Имя введите **Агент MFP**.
 - b. Рядом с полем Примечания введите **Для конечных точек Xerox**.
 - c. Нажмите **ОК**.
6. Для того чтобы отредактировать политику, в поле Имя выберите **Агент MFP**.
7. Перейдите на вкладку **События**.
 - a. Если ранее не было выбрано, выберите **Включить приоритетную пересылку событий**.
 - b. Рядом с полем Пересылать события с равным или большим приоритетом выберите **Информационный**.
 - c. Рядом с полем Интервал между загрузками введите **1**.
 - d. Рядом с полем Максимальное количество событий за одну загрузку введите **20**.
 - e. Нажмите **Сохранить**.
8. Перейдите в раздел **Меню > Политика > Правила назначения политик**.
9. Нажмите кнопку **Новое правило назначения**.
 - a. Рядом с полем Имя введите **Агент MFP**.
 - b. Нажмите **Далее**.
 - c. Нажмите **Добавить политику**.
 - d. В поле Продукт выберите **Агент Trellix**, в поле Категория выберите **Общие**, а затем в поле Политика выберите новую политику **Агент MFP**.
 - e. Нажмите **Далее**.
 - f. В поле Доступные свойства выберите **Тег**.
 - g. В поле Сравнение выберите **Имеет тег**.
 - h. В поле Значение выберите **Xerox MFP**.
 - i. Нажмите **ОК**.
 - j. Нажмите **Далее**.
10. Нажмите **Сохранить**.
11. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу **Настройка автоматического реагирования в Trellix ePO**.

Настройка автоматического реагирования в Trellix ePO

Для того чтобы предоставить администраторам безопасности возможность получать автоматические уведомления по электронной почте, установите функцию Автоматическое реагирование. Эти уведомления отправляются каждый раз, когда Trellix Embedded Control обнаруживает событие безопасности на аппарате Xerox. После установки эта система реагирования применяется ко всем устройствам, которые в настоящее время предоставляются сервером ePO. Событиями, вызывающими Автоматическое реагирование уведомлений Xerox MFP являются Запрет на чтение файлов, Запрет на запись файлов или Запрет на выполнение.

По умолчанию опция Автоматическое реагирование отключена. Для того чтобы включить ее, администратор безопасности должен указать действительный адрес электронной почты.

Для того чтобы добавить адрес электронной почты и включить реагирование:

1. В поле Trellix ePO выберите **Меню > Автоматизация > Автоматическое реагирование**.
2. Нажмите **Новое реагирование**.
 - a. Рядом с полем Имя введите **Уведомления Xerox MFP**.
 - b. Рядом с полем Описание введите **Опасные события**.
 - c. Для Группы событий выберите **События Solidcore**.
 - d. Для Типа событий выберите **События клиента**.
 - e. В качестве Статуса выберите **Включено**.
 - f. Нажмите **Далее**.
3. Нажмите **Событие**.
 - a. В поле Значение выберите **Файл создан, Файл удален, Файл изменен, Запрет на выполнение и Запрет на чтение файлов**, а затем нажмите значок плюса (+), чтобы создать строку.
 - b. В поле Получатели введите адреса электронной почты.
 - c. Нажмите кнопку **Далее**, а затем **Сохранить**.
4. В поле Совокупность для параметра Дросселирование выберите **Запустить это реагирование, если каждый 1 час происходят несколько событий**.
5. На вкладке Действия выберите **Отправить электронное письмо**.
6. Нажмите кнопку **Далее**, а затем **Сохранить**.
7. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу **Настройка параметров сервера Trellix ePolicy Orchestrator**.

Настройка параметров сервера Trellix ePolicy Orchestrator

1. В приложении Embedded Web Server многофункционального принтера нажмите **Свойства > Безопасность**.
2. Выберите **Trellix Embedded Control**.
3. На странице Trellix Embedded Control рядом с полем Уровни защиты устройства нажмите **Изменить**.
4. Выберите **Сервер Trellix ePolicy Orchestrator**, затем нажмите **Сохранить**.
5. Выберите **Сервер Trellix ePolicy Orchestrator**, затем нажмите **Изменить**.
6. Выберите тип адреса. Введите адрес или имя хоста своего сервера в нужном формате и измените номер порта по умолчанию, если это требуется.
7. В поле Имя пользователя введите имя для доступа принтера к приложению сервера Trellix ePO.
8. Введите пароль, затем подтвердите его.
9. Нажмите кнопку **Сохранить**.
10. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу **Назначение принтеров в качестве суперузлов**.

Назначение принтеров в качестве суперузлов

Расширение Xerox® для Trellix ePO использует до трех принтеров Xerox® в качестве суперузлов для связи с другими принтерами Xerox®, которые оно контролирует. Компания Xerox рекомендует назначать более одного принтера Xerox® в качестве суперузла. Если один суперузел не работает или находится в автономном режиме, Trellix ePO может использовать другие суперузлы для связи с другими принтерами. Вы назначаете принтеры в качестве суперузлов, добавляя определенные записи в свой сервер DNS.



Примечание.

- Принтеры Xerox® и сервер Trellix ePO должны использовать один и тот же сервер DNS.
- Выполните следующие процедуры на сервере DNS, а не на сервере Trellix ePO.

Чтобы добавить запись DNS, выполните одно из следующих действий:

ДОБАВЛЕНИЕ ЗАПИСЕЙ DNS К ОДНОМУ ИЛИ НЕСКОЛЬКИМ СУЩЕСТВУЮЩИМ ДОМЕНАМ

Если в вашей сети небольшое количество доменов, используйте этот метод для добавления записей DNS в каждый домен.

1. На сервере DNS найдите домен каждого принтера, который вы хотите назначить суперузлом.
2. Для каждого домена добавьте записи для всех суперузлов и назначьте им имена:
 - XeroxDiscoverySuperNode1
 - XeroxDiscoverySuperNode2
 - XeroxDiscoverySuperNode3



Примечание. Записи для всех суперузлов не чувствительны к регистру.

3. Если в сети используется более одного сервера DNS, повторите предыдущий шаг для всех остальных серверов DNS.
4. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу [Обеспечение управления устройством в Trellix ePO](#).

ДОБАВЛЕНИЕ ЗАПИСЕЙ DNS В ОДИН НОВЫЙ ДОМЕН

Если в вашей сети большое количество доменов, используйте этот метод для добавления записей DNS в один домен.

1. На своем сервере DNS создайте домен с именем Xerox.local. Расширение Xerox для Trellix ePO осуществляет поиск домена с таким именем.
2. Для домена Xerox.local добавьте записи для каждого суперузла и назначьте им имена:
 - XeroxDiscoverySuperNode1
 - XeroxDiscoverySuperNode2
 - XeroxDiscoverySuperNode3

3. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу [Обеспечение управления устройством в Trellix ePO](#).

Обеспечение управления устройством в Trellix

1. В Trellix ePO выберите **Дерево системы**.
2. Нажмите **Находки**.
3. В поле «Предустановки» выберите **Эта группа и все подгруппы**.
4. Убедитесь, что отображается аппарат Xerox.
5. Убедитесь, что аппарат Xerox отображается как Управляемый в поле Состояние управления.
6. В окне Trellix ePO в разделе Меню выберите **Сторонние услуги**, а затем расширение **Xerox MFP**.
7. Для того чтобы получить удобный доступ к Trellix ePO, перетащите значок расширения **Xerox MFP** вверх.
8. Для того чтобы продолжить настройку уведомлений безопасности, перейдите к разделу **Настройка прокси-сервера Trellix ePO**.

Настройка прокси-сервера Trellix ePO

Содержание этой главы:

Настройка прокси-сервера Trellix ePO.....	24
---	----

Настройка прокси-сервера Trellix ePO

При использовании прокси-сервера необходимо выполнить его настройку в Trellix ePO.

1. В разделе Trellix ePO в поле Меню выберите **Конфигурация**.
2. Выберите **Настройки сервера**.
3. Выберите **Настройки прокси-сервера**.
4. В правом нижнем углу нажмите **Изменить**.
5. В поле Тип выберите **Настроить параметры прокси-сервера вручную**.
6. В поле Настройки прокси-сервера настройте вручную уникальные параметры для вашего сайта.
7. Нажмите **Сохранить**.
8. Перезапустите сервер ePO.



Примечание. Если вы не выполните эту процедуру, то при открытии расширения Xerox MFP появится сообщение «Ошибка-2».

Удаление и повторная установка расширений Trellix ePO

Содержание этой главы:

Удаление и повторная установка расширений Trellix ePO	26
---	----

Удаление и повторная установка расширений Trellix ePO

Если во время установки появляется сообщение о том, что расширение Solidcore уже установлено, удалите существующее расширение Solidcore. После завершения установки переустановите программное обеспечение, предоставленное компанией Xerox, и обновите расширение Solidcore. Выполнение этих двух шагов создает необходимую основу для обновления программного обеспечения до более новой версии.

1. Удалите текущее программное обеспечение.
2. Установите программное обеспечение, предоставленное компанией Xerox.
3. Выполните всю процедуру настройки, используя только что установленную версию программного обеспечения.
4. Если есть возможность, обновите программное обеспечение до более актуальной версии.

