Содержание

Введение

Этот документ описывает различные уровни административного доступа или предопределенные роли пользователя, которые доступны на Email Security Appliance (ESA).

Что уровни административного доступа доступны на ESA?

При создании учетной записи нового пользователя вы назначаете пользователя на предопределенный или пользовательскую роль пользователя. Каждая роль пользователя содержит разные уровни привилегий в ОС и доступе устройства, следующим образом:

Администраторы	Учетные записи пользователя с Ролью Администратор имеют полный доступ ко всем параметрам конфигурации системы. Однако только у пользователя с правами администратора есть доступ к **resetconfig** и **командам revert**.
Операторы	Учетные записи пользователя с ролью Оператора ограничены от: • Создание или редактирование учетных записей пользователя. • Выдача **resetconfig** команды. • Обновление устройства. • Выдача **systemsetup** команды или выполнение Системного Мастера настройки. • Выдача **adminaccessconfig** команды. • Выполнение некоторых карантинных функций (включая создание, редактирование, удаление и централизацию карантина). • Если LDAP включен для внешней проверки подлинности, изменение Серве LDAP представляет параметры настройки кроме имени пользователя и пароля. В противном случае у них есть те же привилегии как Роль Администратор.
Операторы только для чтения	Учетные записи пользователя с ролью Оператора Только для чтения имеют доступ для просмотра сведений о конфигурации. Пользователи с ролью Оператора Только для чтения могут сделать и отправить изменения, чтобы видеть, как настроить функцию, но они не могут передать их. Если доступ включен в карантине, пользователи с этой ролью могут управлять сообщениями в карантине. Пользователи с этой ролью не могут обратиться к придерживающемуся: • Файловая система, FTP или SCP. • Параметры настройки для создания, редактирования, удаления или централизации карантина.
Гости	Пользовательские учетные записи с Ролью guest могут только просмотреть сведения о статусе. Если доступ включен в карантине, пользователи с Ролью guest могут также управлять сообщениями в карантине. Пользователи с Ролью guest не могут обратиться к Отслеживанию сообщений.
Технический	Учетные записи пользователя с ролью Технического специалиста могут

специалист	выполнить обновления системы, перезагрузить устройство и управлять характерными чертами. Технические специалисты могут также выполнить следующие действия для обновления устройства: • Приостановите почтовую доставку и получение. • Обзорный статус workqueue и слушателей. • Сохраните и пошлите по электронной почте файлы конфигурации. • Безопасные списки резервного копирования и черные списки. Технические специалисты не могут восстановить эти списки. • Разъедините устройство от кластера. • Включите или отключите удаленный сервисный доступ для службы технической поддержки Cisco. • Повысьте запрос поддержки.
Пользователи справочного стола	Учетные записи пользователя с Ролью пользователя Справочного стола ограничены: • Отслеживание сообщений. • Управление сообщениями в карантине. Пользователи с этой ролью не могут обратиться к остатку системы, включая CL Необходимо включить доступ в каждом карантине, прежде чем пользователь с этой ролью сможет управлять ими.
Пользовательская роль пользователя	Учетные записи пользователя с пользовательской ролью пользователя могут только получить доступ к функциям безопасности электронной почты, назначенным на роль. Этими функциями может быть любая комбинация политики DLP, почтовой политики, отчётов, карантина, отслеживания локальног сообщения, профилей шифрования и средства отладки Трассировки. Пользователи не могут функции конфигурации системы доступа. Только администраторы могут определить пользовательские роли пользователя.

Примечание: Пользователи, назначенные на настраиваемые роли, не могу обратиться к CLI.

Учетная запись пользователя по умолчанию на систему, admin, имеет все административные привилегии. Учетная запись пользователя с правами администратора не может быть удалена, но можно изменить пароль и блокировать учетную запись.

Несмотря на то, что нет никакого предела количеству учетных записей пользователя, которые можно создать на устройстве, вы не можете создать учетные записи пользователя с названиями, которые зарезервированы системой. Например, вы не можете создать учетные записи пользователя, названные "оператором" или "root".

Все роли, определенные на вышеупомянутое , могут обратиться и к GUI и к CLI, кроме Роли пользователя Справочного стола и пользовательских ролей пользователя, которые могут только обратиться к GUI.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Cisco Systems – техническая поддержка и документация