Содержание

Введение

Ограничение доступа машины (MAR) было функцией, введенной в ISE и ACS как способ проверить успешную аутентификацию компьютера. Эта функция позволяет создание политики, которая может авторизовать пользователя на основе предыдущей аутентификации компьютера.

Поведение ниже замечено в версиях 4.x и 5.x Access Control Server (ACS), а также всех версиях платформы Identity Services Engine (ISE).

Вопрос. Какая конфигурация требуется, чтобы добавлять оконечную точку в кэш Ограничения доступа машины (MAR)?

О.

Базирующийся пароль

Если машина аутентифицируется против Active Directory (AD) с помощью пароля (MSCHAPv2) машины, никакая дополнительная настройка не необходима, поскольку оконечная точка будет добавлена к Кэшу MAR.

Базирующийся сертификат

Если машина аутентифицируется против Active Directory (AD) с помощью сертификата компьютера (EAP-TLS), необходимо настроить двоичное сравнение для хоста, который будет кэшироваться в MAR. Когда двоичное сравнение будет включено, ISE/ACS проверит хэш сертификата компьютера и сравнит его с публикованным хэшем сертификата, привязанным к объекту машины, хранившему в AD. Без проверенного двоичного сравнения запрос аутентификации компьютера не может быть проверен против AD. В результате аутентификация компьютера не была бы добавлена к Кэшу MAR.

Ссылки

[За и против ограничения доступа машины](#)