Contents

Introduction

Machine Access Restriction (MAR) was a feature introduced into ISE and ACS as a way to verify a successful machine authentication. This feature allows the creation of policies which can authorize a user based on a previous machine authentication.

The behavior below is seen in Access Control Server (ACS) versions 4.x and 5.x as well as all versions of the Identity Services Engine (ISE).

Q. What configuration is required to add an endpoint into the Machine Access Restriction (MAR) cache?

A.

Password Based

If the machine authenticates against Active Directory (AD) using the machine password(MSCHAPv2), no additional configuration is needed as the endpoint will be added to the MAR Cache.

Certificate Based

If the machine authenticates against Active Directory (AD) using the machine certificate (EAP-TLS), you must configure Binary Comparison in order for the host to be cached in MAR. When Binary Comparison is enabled, ISE/ACS will check the hash of the machine certificate and compare it to the published certificate hash associated to the machine object stored in AD. Without Binary Comparison checked, the machine authentication request cannot be validated against AD. As a result, the machine authentication would not be added to the MAR Cache.

References

[Machine Access Restriction Pros and Cons](#)