Policy Elements

This chapter provides information about the policy elements in Cisco ISE and Cisco Secure ACS.

Cisco ISE and Cisco Secure ACS Parity

Cisco ISE introduces the following features to achieve parity with Cisco Secure ACS.

- Disable user account if the configured date exceeds a specific period for individual users
- Disable user account if the configured date exceeds a specific period for all the users globally
- Disable user accounts after n days of configuration globally
- Disable user accounts after n days of inactivity
- Support for IP address range in all the octets for the network device
- Configuration of network device with IPv4 or IPv6 address
- Configuration of external proxy servers with IPv4 or IPv6 address
- Support for maximum length of Network Device Group (NDG) name
- Support for time and date conditions
- Support for service selection rules, authentication rules, and authorization (standard and exception) rules with compound conditions having AND and OR operators
- MAR configuration in Active Directory
- Authorization profile configured with dynamic attribute
- Two new values for the service-type RADIUS attribute
- Increased internal user support for 300,000 users
- Internal users authorization cache
- Authenticate internal users against external identity store password

- Use of length included flag while performing EAP-TLS authentication against a Terminal Wireless Local Area Network Unit (TWLU) client
- Common Name and Distinguished Name support for Group Name attribute for LDAP Identity Store

For more information on Cisco ISE and Cisco Secure ACS parity features, see Cisco Identity Services Engine 2.1 Administration Guide

Policy Models

Cisco Secure ACS and Cisco ISE have both simple and rule-based authentication paradigms, but Cisco Secure ACS and Cisco ISE are based on different policy models, which makes migrating policies from Cisco Secure ACS 5.5 or above to Cisco ISE a bit complex.

Cisco Secure ACS policy hierarchy starts with the Service selection rule that redirects the authentication requests to the access services. The access services consist of identity and authorization policies that authenticate the user against internal or external identity stores and authorize the users based on the conditions defined.

Authentication and authorization polices are migrated from Cisco Secure ACS, Release 5.5 or above to Cisco ISE, Release 2.02.4. Cisco ISE Release 2.0, supports the new policy model called Policy Set, which is similar to the Service Selection Policy (SSP) in Cisco Secure ACS, Release 5.5/5.6.

Cisco Secure ACS Service Selection Policy and Cisco ISE Policy Set

Cisco Secure ACS, Release 5.5/5.6 Service Selection Policy (SSP) distributes requests to the appropriate services based on SSP rules whereas Cisco ISE policy set holds a rule, which contains entry criteria to the policy set. The order of the policy set is in the same order as the entry rules, which is similar to the order of the SSP rules.

Several SSP rules may request the same service or reuse of service in Cisco Secure ACS. However, each policy set carries its own entry condition, therefore, you cannot reuse the policy set in Cisco ISE. If you want to migrate a single service that is requested by several SSP rules, you must create multiple policy sets that are copies of that service, which means that you must create a policy set in Cisco ISE for each SSP rule that requests the same service in Cisco Secure ACS.

You can define SSP rules as disabled or monitored in Cisco Secure ACS, and the equivalent entry rules of a policy set are always enabled in Cisco ISE. If SSP rules are disabled or monitored in Cisco Secure ACS, the policy services that are requested by SSP rules cannot be migrated to Cisco ISE.

Cisco Secure ACS Policy Access Service and Cisco ISE Policy Set

You can define a policy service without requesting that service, which means that you can define a policy service inactive by a rule in the SSP in Cisco Secure ACS. Cisco Secure ACS, Release 5.5 or above has an out-of-the-box DenyAccess service, which has neither policies nor allowed protocols for the default SSP rule in Cisco Secure ACS, which automatically denies all requests. There is no equivalent policy set for Cisco ISE. But, you cannot have a policy set without an entry rule, which refers to the policy set in Cisco ISE.

Allowed protocols are attached to the entire service (not a specific policy) that is not conditioned (except the condition in the SSP that points to the entire service) in Cisco Secure ACS, Release 5.5 or above. Allowed protocols refers only to the authentication policies as a result of a conditioned outer rule in Cisco ISE.

Identity policy is a flat list of rules that results in identity source (identity source and identity store sequence) in Cisco Secure ACS, Release 5.5 or above. An authentication policy holds two levels of rules—outer policy rules and inner policy rules. The outer policy rules result in allowed protocols, and are the entry criteria to the set of inner policy rules. The inner policy rules result in identity source.

Both Cisco Secure ACS, Release 5.5 or above and Cisco ISE, Release 2.02.4, include an optional exception policy attached to each authorization policy. Cisco ISE, Release 2.02.4 provides an optional Global Exception Policy in addition to the exception policy that affects all authorization policies. There is no equivalent policy to that of Global Exception Policy in Cisco Secure ACS, Release 5.5 or above. The local exception policy is processed first followed by the Global Exception Policy and authorization policy for authorization.

FIPS Support for ISE 802.1X Services

The Cisco ISE FIPS mode should not be enabled before the migration process is complete.

To support Federal Information Processing Standard (FIPS), the migration tool migrates the default network device keywrap data.

FIPS-compliant and supported protocols:

- Process Host Lookup
- Extensible Authentication Protocol-Translation Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP)
- EAP-Flexible Authentication via Secure Tunneling (FAST)

FIPS-noncompliant and unsupported protocols:

- EAP-Message Digest 5 (MD5)
- Password Authentication Protocol and ASCII
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)
- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)
- Lightweight Extensible Authentication Protocol (LEAP)