

## Scope of Work - PR9233260: MRU-CISCO Identity Services Engine (ISE)

### **CISCO ISE-QTY 3**

This device should be consolidated policy-base access control system capable of these functions:

- Combines authentication, authorization, accounting (AAA), posture, and profiler into one appliance
- Provides for comprehensive guest access management for the Cisco ISE administrator, sanctioned sponsor administrators, or both
- Enforces endpoint compliance by providing comprehensive client provisioning measures and assessing device posture for all endpoints that access the network, including 802.1X environments
- Provides support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network
- Enables consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed
- Employs advanced enforcement capabilities including security group access (SGA) through the use of security group tags (SGTs) and security group access control lists (SGACLs)
- Supports scalability to support a number of deployment scenarios from small office to large enterprise environments

This device should provide identities-base functions such as:

- The system should determine whether users are accessing the network on an authorized, policy-compliant device.
- The system should establish user identity, location, and access history, which can be used for compliance and reporting.
- The system should assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).
- The system should grants authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.