Authentication

Cisco UCS Central Authentication

Cisco UCS Central supports either local or LDAP-based authentication. Other authentication types, such as TACACs+ or RADIUS, are supported in v1.4 and higher. They are not supported for earlier versions. You can use Cisco UCS Central to configure these authentication types for Cisco UCS Manager through operational administrative policies.

Note Do not use '$' as a password character when using local authentication.

In Cisco UCS Central, you can only activate one defined form of native authentication exclusively (either local or LDAP). Cisco UCS Central allows selecting from multiple authentication domains. Unlike Cisco UCS Manager, it does not currently support configuring multiple authentication realms.

Cisco UCS Central includes third-party and self-signed certificate support for LDAP integration and user authentication.

Authentication

Cisco UCS Central can globalize the configuration of the Cisco UCS Manager GUI authentication model across all registered Cisco UCS domains.

In v1.4, and higher, of Cisco UCS Central you can use RADIUS or TACACS+ as authentication realms. You cannot use them in earlier versions. Aim for simplicity and to minimize and centralize the number of authentication schemes and definitions. Similarly, if you require access to multiple authentication schemes and definitions, then aim for simplicity when constructing authentication scheme maps and definitions in Cisco UCS Central domain groups.

RBAC

RBAC (Role-Based Access Control) is typically linked to global or corporate-level authentication, such as LDAP or AD. For Cisco UCS Central, it is preferable to enforce central control for access.

If you do not currently have central authentication and role management, then the best practice dictates that administrators define role-based access within Cisco UCS Central. Define it as high up in the domain group hierarchy's operational policies as possible.