Troubleshooting ISE Admin SAML Login Fails with Access Denied Due to Missing Domain Name Configuration

Contents

Issue

Identity Services Engine (ISE) admin Security Assertion Markup Language (SAML) login fails with an "Access Denied" error after a successful Azure Entra authentication. Although Azure Entra shows a successful SAML authentication, ISE denies access to the management portal. Additionally, Certificate Signing Request (CSR) generation fails with the following error:

```
cpm.admin.caservice.utils.CAUtil -::admin::addLocalCert:- Error occurred managing certificates :::-CSRF
```

ISE logs show DNS resolution failures for the node's FQDN and SSL handshake exceptions during internal HTTPS validation:

```
SSLHandshakeException: No subject alternative names matching IP address 10.X.X.X found
```

The system also displays repeated warnings about expired default self-signed certificates and RESTConf falling back to HTTP due to certificate unavailability.

Environment

- Cisco Identity Services Engine (ISE) version 3.4 Patch 3
- Azure Entra (formerly Azure AD) configured as SAML Identity Provider
- ISE management accessed via both IP address and FQDN
- Environment upgraded from ISE 3.3 to 3.4

Resolution

1. Verify the current ISE node configuration and DNS resolution by running the following commands:

```
show running-config | include domain
nslookup xxxxxxxxxx.internal
ping xxxxxxxxxx.internal
```

Note: Expected results show successful DNS resolution returning the correct IP address with no DNS errors.

---

2. Re-add the domain name to the ISE node configuration using the ISE CLI:

```
device# config t
device(config)# ip domain-name xxxxxxxxxx.internal
```

3. Navigate to **Administration** > **System** > **Certificates** > **Certificates** in the ISE GUI and regenerate the default self-signed certificate. Ensure the new certificate includes both the FQDN and IP address in the Subject Alternative Name (SAN) field.

4. Confirm that the regenerated certificate includes the node IP address in the SAN field and is properly bound to both Admin and Portal services.

5. Test the ISE admin SAML login. The authentication should now succeed without the "Access Denied" error.

Cause

This issue is caused by Cisco Bug ID CSCwm59777, which relates to IP domain-name handling during upgrades from ISE 3.3 to ISE 3.4. During the upgrade process, the node's top-level domain name configuration is removed, preventing ISE from properly resolving its own FQDN. This causes two related problems:

1. **DNS Resolution Failure**: ISE cannot resolve its own hostname, causing internal HTTPS calls to fail hostname validation during SAML authentication processing.

2. **Certificate SAN Mismatch**: The default admin certificate does not include the node IP address in the SAN field, causing SSL handshake failures when ISE attempts internal HTTPS validation using the IP address as a fallback.

The combination of these issues results in successful Azure Entra SAML authentication followed by ISE access denial due to failed internal certificate validation.

Related Content

- Cisco Bug ID CSCwm59777
- Configure ISE Admin Log in Flow via SAML SSO with Azure AD
- Cisco Technical Support & Downloads