

Reset ISE Configuration to Factory Defaults

Contents

Issue

You need to reset the configuration of a Cisco Identity Services Engine (ISE) node to factory defaults.

Environment

- Cisco ISE version: version 3.1 and later
- Deployment type: Distributed
- Policy Administration Node (PAN)
- Monitoring Node (MNT)
- Policy Service Node (PSN)
- Network Access Device (NAD), for example, a switch or wireless controller

Resolution

Impact Assessment

- If you reset the Primary PAN, promote a Secondary PAN to Primary first.
 - A Primary PAN must always exist on your deployment.
- If you reset a PSN:
 - Ensure that a remaining PSN is available.
 - Ensure that NADs are configured in order to direct the RADIUS and TACACS+ authentications

to remaining PSNs.

- Test authentication with remaining PSNs.
- If you reset an MNT:
 - Ensure that a remaining Monitoring node is available.
- Verify that no sync operations are in progress on remaining nodes.

Before You Reset the Configuration

You must document the target node configuration before you reset the configuration, if you intend to rebuild and/or reregister the factory default target node later.



Note: Resetting an ISE node to factory defaults causes the node to restart.

Configuration Reset Steps

1.- Use Secure Shell (SSH) in order to log into the target node.

2.- At the ISE CLI prompt, enter:

```
application reset-config ise
```



Note: This command resets application-level settings, including all user-defined policies, users, and logs, and retains only the default system entries.

3.- ISE prompts:

```
Initialize your Application configuration to factory defaults? (y/n):
```

4.- Enter: **y**

5.- ISE then prompts:

Retain existing Application server certificates? (y/n):

6.- Choose one of the options outlined in the next sections.

Option A - Retain Existing Server Certificates

ISE saves the server certificates locally before wiping the configuration, then imports them after the reset.

Enter: **y**



Note: The option to retain certificates is **not a substitute for exporting certificates manually**. In particular, **Internal CA private keys are not included when you use the option to retain certificates**.

Option B - Delete Existing Certificates and Use Self-Signed Certificates

ISE deletes the existing server certificates and creates new self-signed certificates.

Enter: **n**



Note: Use this option only if:

7.- ISE stops services, clears and re-creates the ISE databases, primes the database, and restarts application services.

Wait for the confirmation:

application reset-config is success



Note: Do not interrupt or reboot the node while this process runs.

8.- Validate the ISE application service runs after you initialize it with this command:

```
show application status ise
```

Cause

This process can be required for:

- Decommissioning or rebuilding ISE nodes.
- Hardware replacement.
- Topology changes.
- Resolution of persistent synchronization / replication failures.

Related Content

- [Export Configuration and Operation Data Backup from ISE](#)
- [Cisco Identity Services Engine CLI Reference Guide](#)