

Troubleshooting ISE SSH Public Key Import Failure Error "Unable to update authorized key file"

Contents

Issue

When attempting to configure SSH public key authentication on a Cisco ISE node, the SSH key import process fails with the error:

Unable to update authorized key file

Environment

- Cisco Identity Services Engine (ISE) version 3.1 and above
- ISE SSH public and private key generated

Resolution



Warning: This process deletes all authorized keys for the logged-in user and causes subsequent key-based SSH logins to fail. Complete the key import process before closing the current session to re-enable key-pair authentication.

1. Login to the ISE node CLI with an account with Admin privileges.
2. Delete the existing corrupted or problematic authorization keys from the ISE node using this command.

```
crypto key delete authorized_keys
```

3. Import the new SSH public key.

```
crypto key import <public key file Name> repository <repository Name>
```

For example,

```
crypto key import mypubkey repository MyRepo
```

4. Verify that the key is added to the authorized key list using this command.

```
show crypto authorized_keys
```

5. Verify the SSH access with an SSH client mapped with the private key.

Cause

The SSH public key import failure resulted from corrupted or improperly formatted authorization keys on the ISE node. The "Unable to update authorized key file" error indicated that the existing authorized key file reached an inconsistent state, which prevented new key imports.

Related Content

- [Configure Private Key Authentication with ISE](#)
- [Reset ISE SSH keys for Cisco ISE Deployed in Azure](#)