Troubleshoot Backup Operations in UCS Manager

Contents

Introduction

This document describes how to resolve common backup failure scenarios for the UCS system.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document covers UCS Manager and Cisco Intersight. The document covers UCS regardless of the specific Fabric Interconnect model.

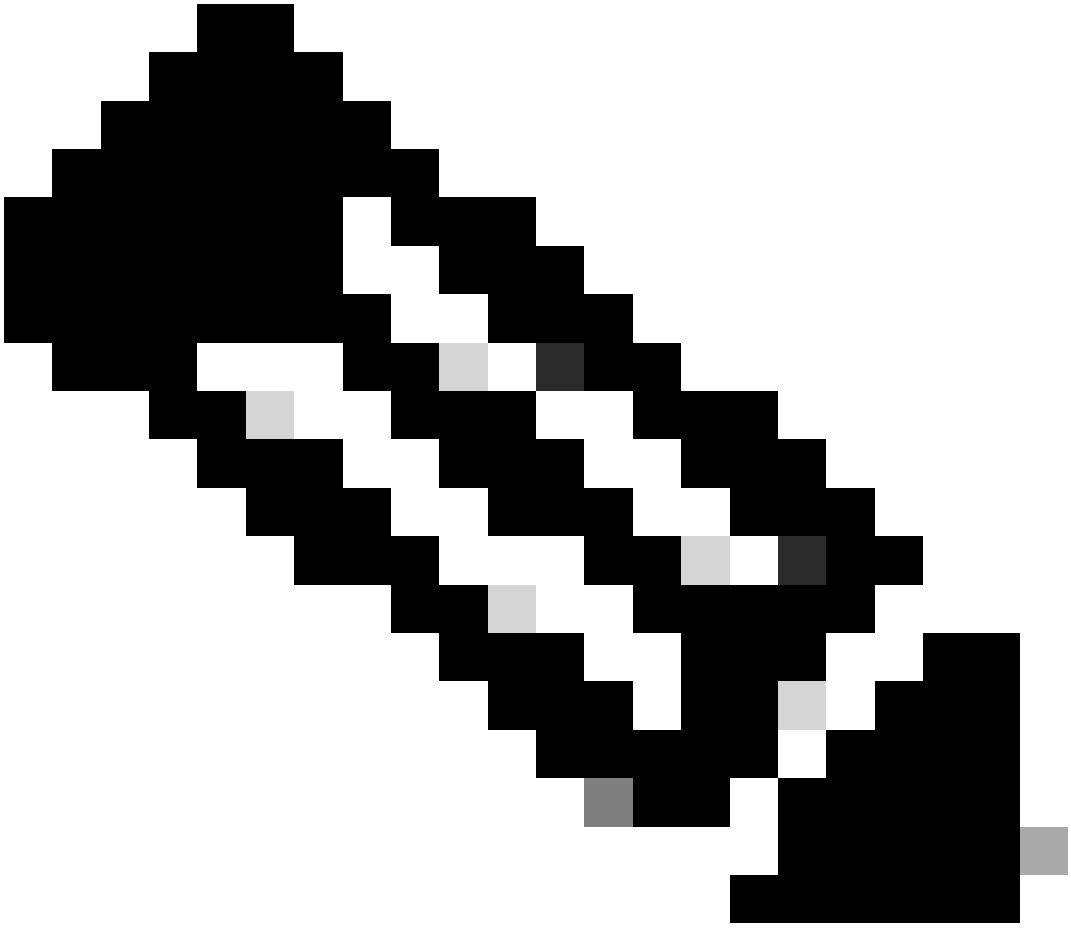
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Performing a backup operation for a UCS Domain allows for a snapshot of all or a partial system configuration in order to be able to recover the UCS environment after a catastrophic failure.

There are several backup options available depending on which configurations are deemed necessary for a timely recovery of the UCS system configuration.

Full State - A binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. This file can restore or rebuild the configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import.



Note: You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported. It is also important that the bundles from which the backup was taken remain present in the Cisco UCS Manager and cannot be deleted.

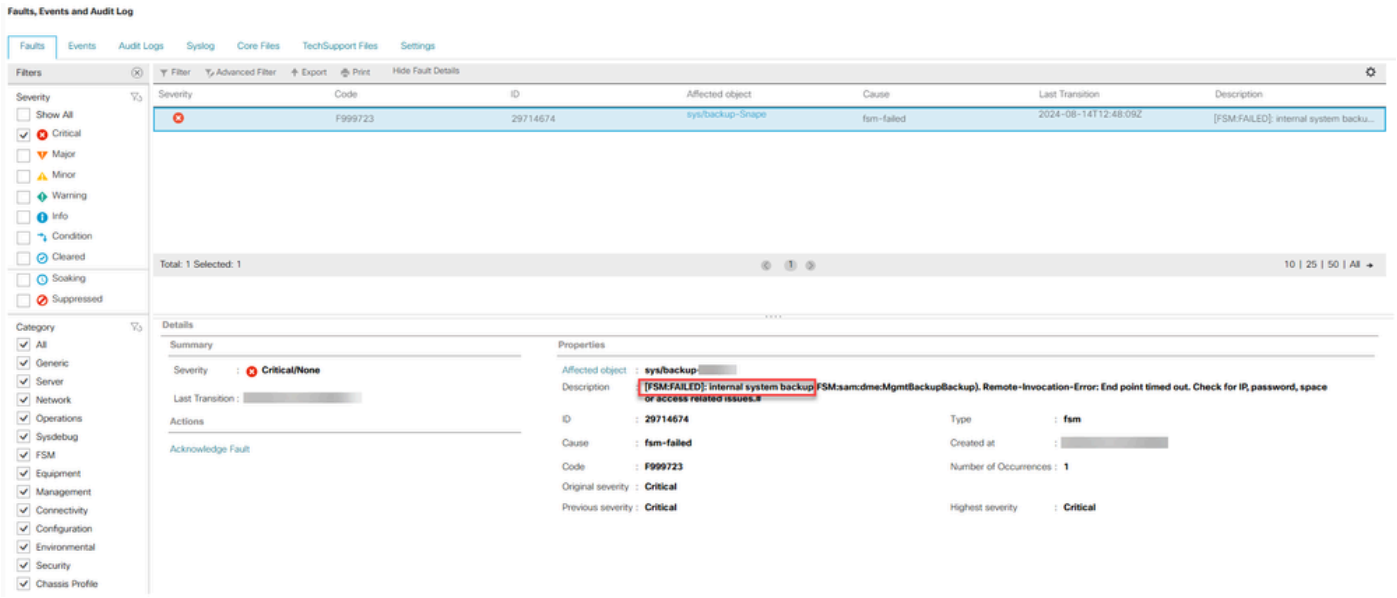
All configuration - An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. This file does not include passwords for locally authenticated users.

System configuration - An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Logical configuration - An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Solution to Common Scenarios

[FSM:FAILED]: Internal System Backup

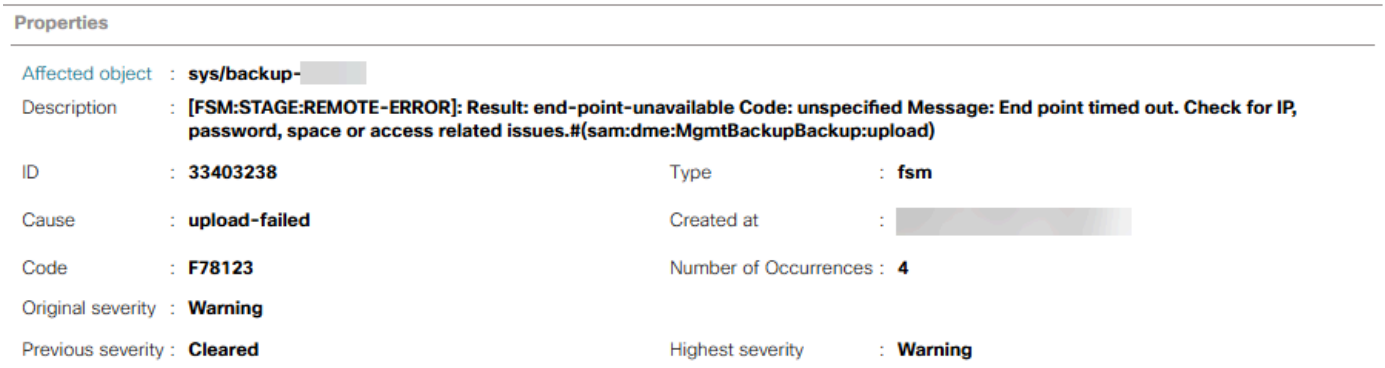


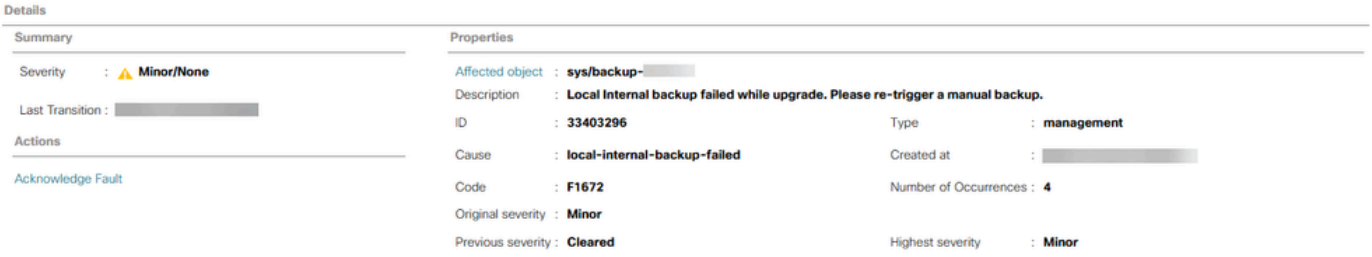
This fault can arise if there is a communication error between the Primary and Secondary Fabric Interconnect.

The exact cause can vary as this fault can arise due to the most common causes but not limited to:

Cause	**Solution**
Inoperable Fabric Interconnect	If the error is not due to a scheduled power or maintenance related event, please engage Cisco Support Services
Failed Firmware Upgrade Operation	If the Firmware Upgrade Operation has been resolved, the fault can be cleared by implementing these Steps
SSH Key Mismatch	If you are receiving this error as a result of a recent upgrade to UCSM 4.0 or 4.1, please refer to these Steps

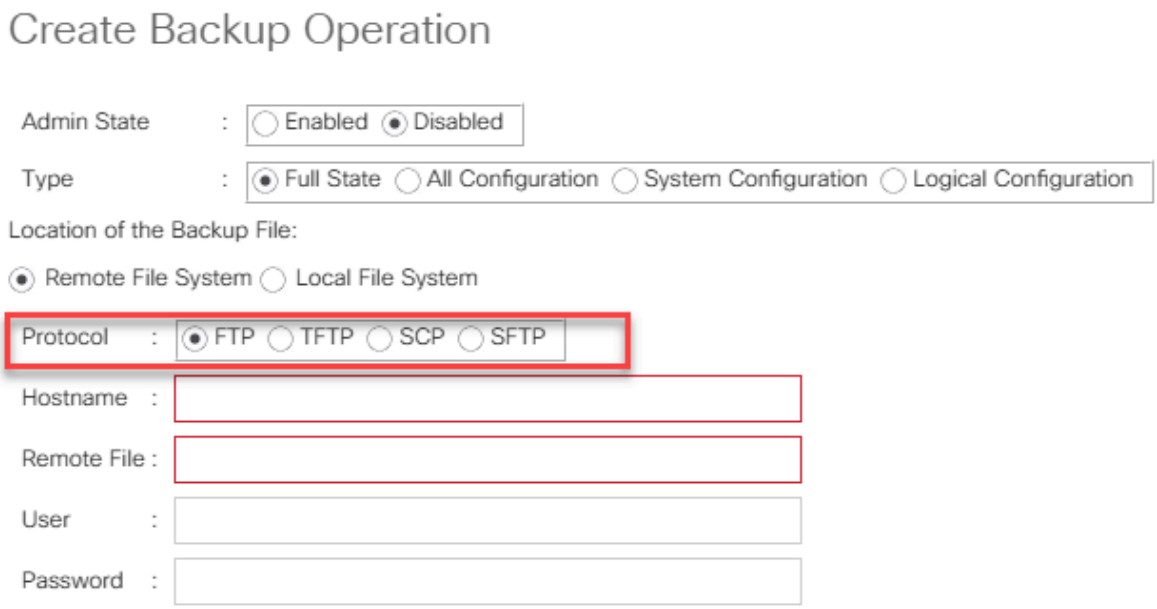
End Point Timed Out: Check for IP, Password, Space or Access Related Issues





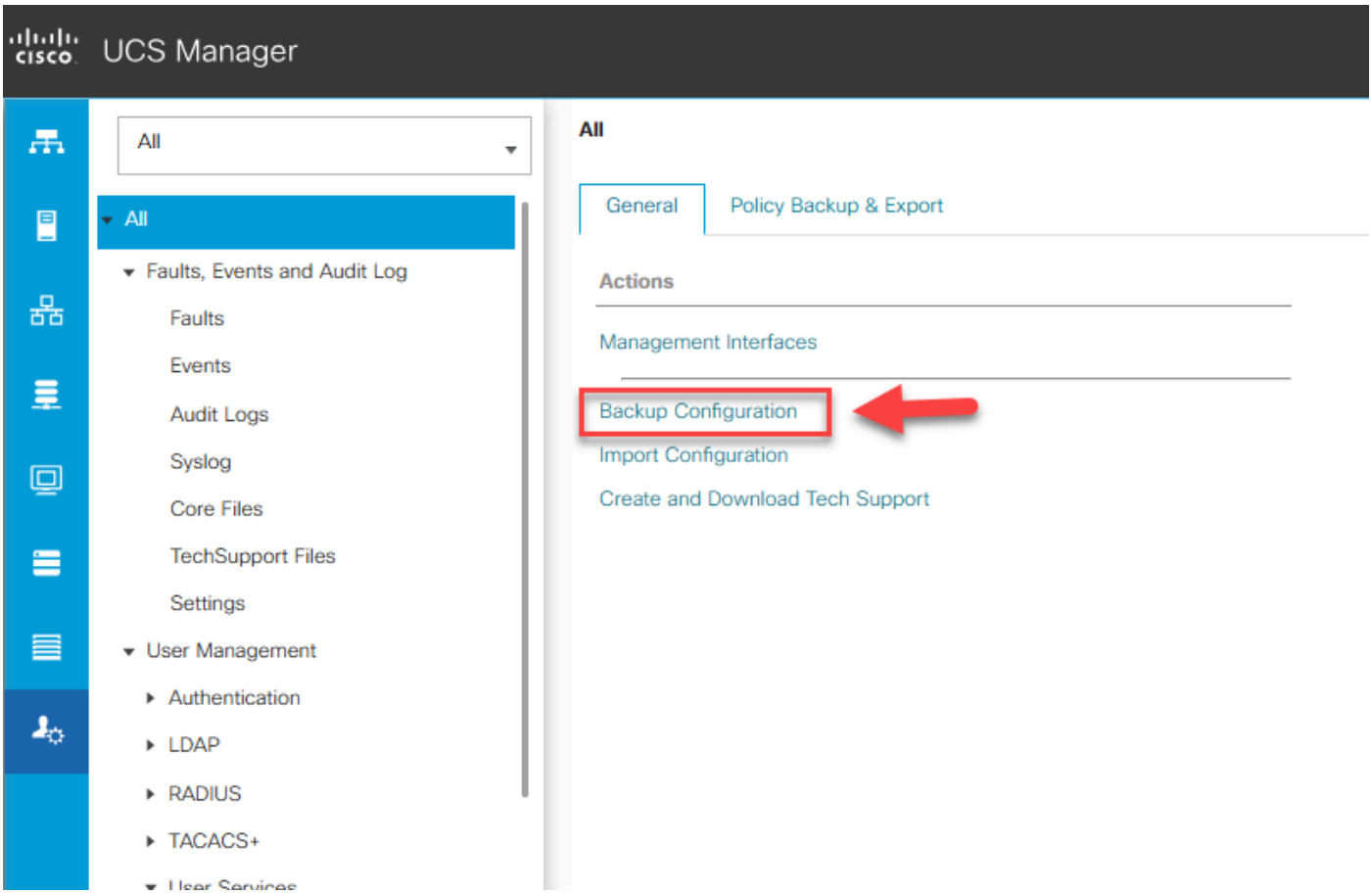
This fault indicates that the UCS Domain was unable to successfully connect and transfer the backup file to the configured destination server.

The remote file transfer protocols either manually or automatically transfer the UCS backup file:



If there is a network communication issue during the time of the backup file transfer, a fault indicating that the endpoint (remote server) has timed out or was unreachable appears.

Manually create a backup operation as a first step in order to verify whether there is a persistent network communication issue between the UCS Domain and the remote file server. If successful, this indicates that there is possibly an intermittent network communication issue between the UCS Domain and the remote file server during the specific window where a backup is generated and remotely transferred.

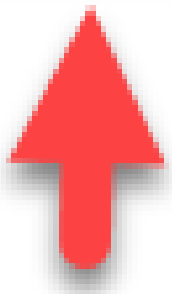

UCS Manager
All
All
Faults, Events and Audit Log
Faults
Events
Audit Logs
Syslog
Core Files
TechSupport Files
Settings
User Management
Authentication
LDAP
RADIUS
TACACS+
All
General
Policy Backup & Export
Actions
Management Interfaces
Backup Configuration
Import Configuration
Create and Download Tech Support

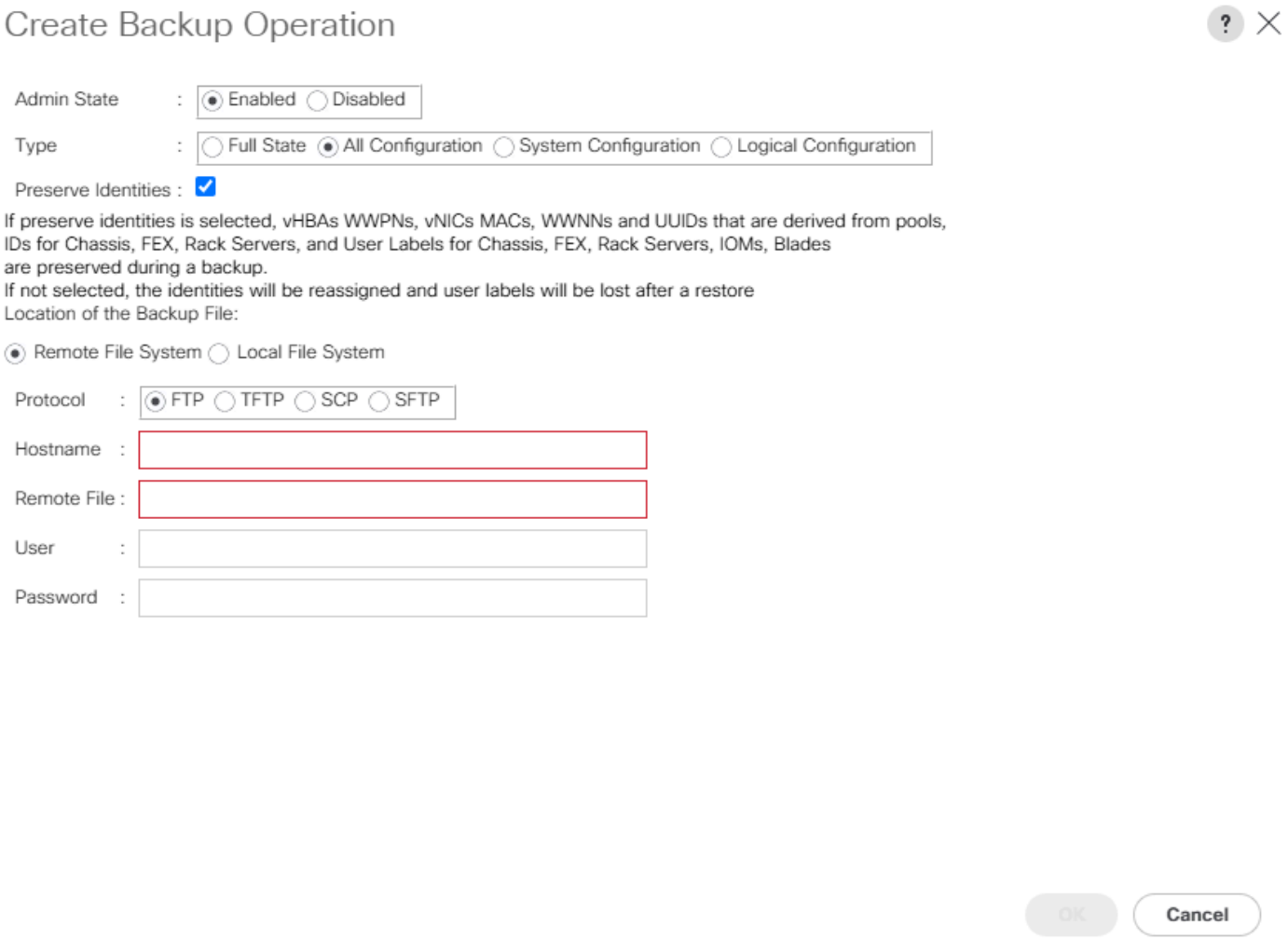
Backup Configuration

General

Actions

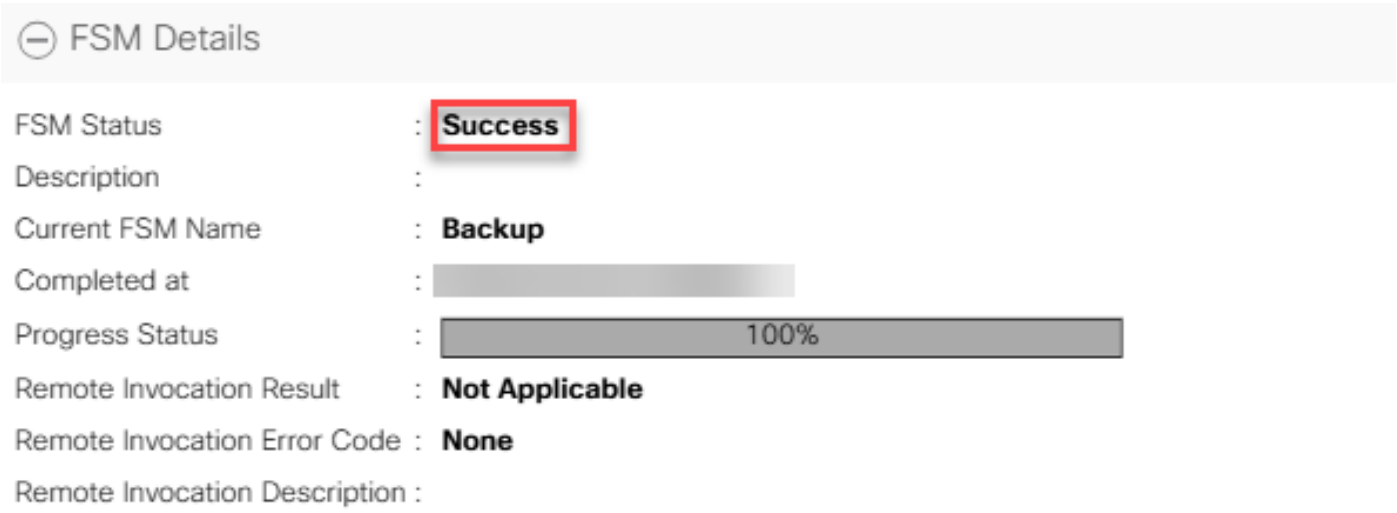
Create Backup Operation





Select the **Admin State** as **Enabled** and then select all applicable options such as **Type, Protocol, Hostname, Remote File name** and **Username/Password**, if applicable.

Once complete, click **Ok**.



If you do not receive a Success state, then it would imply that there is a communication error between the UCS Domain and the Remote File Server.

There must be open communication between the UCS Management Network and the Remote File Server location. The Protocol used requires traffic to be allowed between both Source and Destination.

SSH into the Virtual IP Address of your UCS Cluster. Connect to the local management shell and then run the command **show open-network-ports** to validate.

```
# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

(local-mgmt)#
(local-mgmt)# show open-network-ports
Name        Description                    Port  Protocol
----------- ------------------------------ ----- --------
http        HTTP Service                     80 tcp
https       Secure HTTP Service             443 tcp
snmp        SNMP Service                    161 tcp
snmp        SNMP Service                    161 udp
ssh         Secure Shell Server              22 tcp
telnet      Telnet Server                    23 tcp
xmlPolicy   XML client connection policy    843 tcp
```

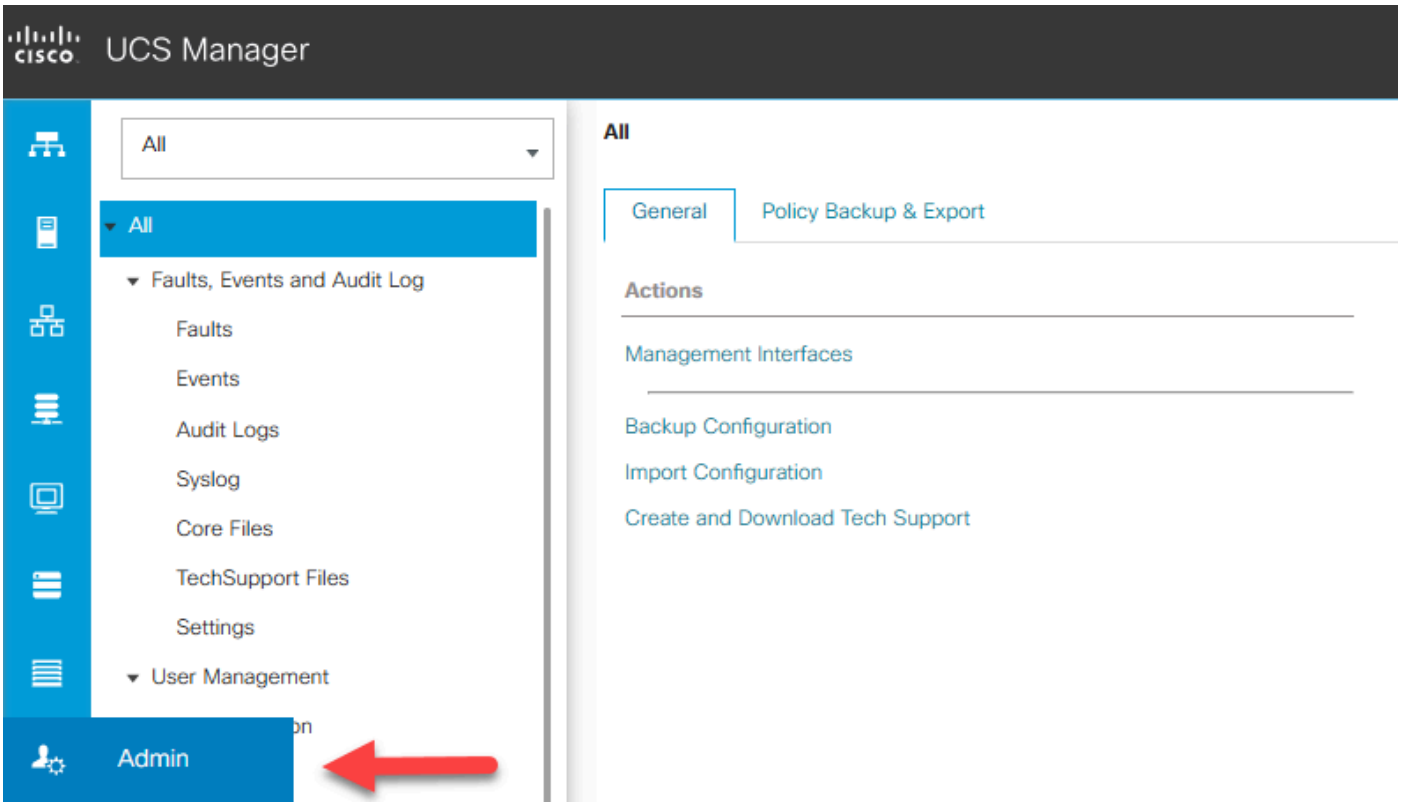
The Password Encryption Key has not Been Set

Beginning with release 4.2(3d), Cisco UCS Manager introduces Password Encryption Key to enhance security for backup configuration files. Password Encryption Key, by default, is not set once you upgrade to release 4.2(3d). For more information about how to set the Password Encryption Key

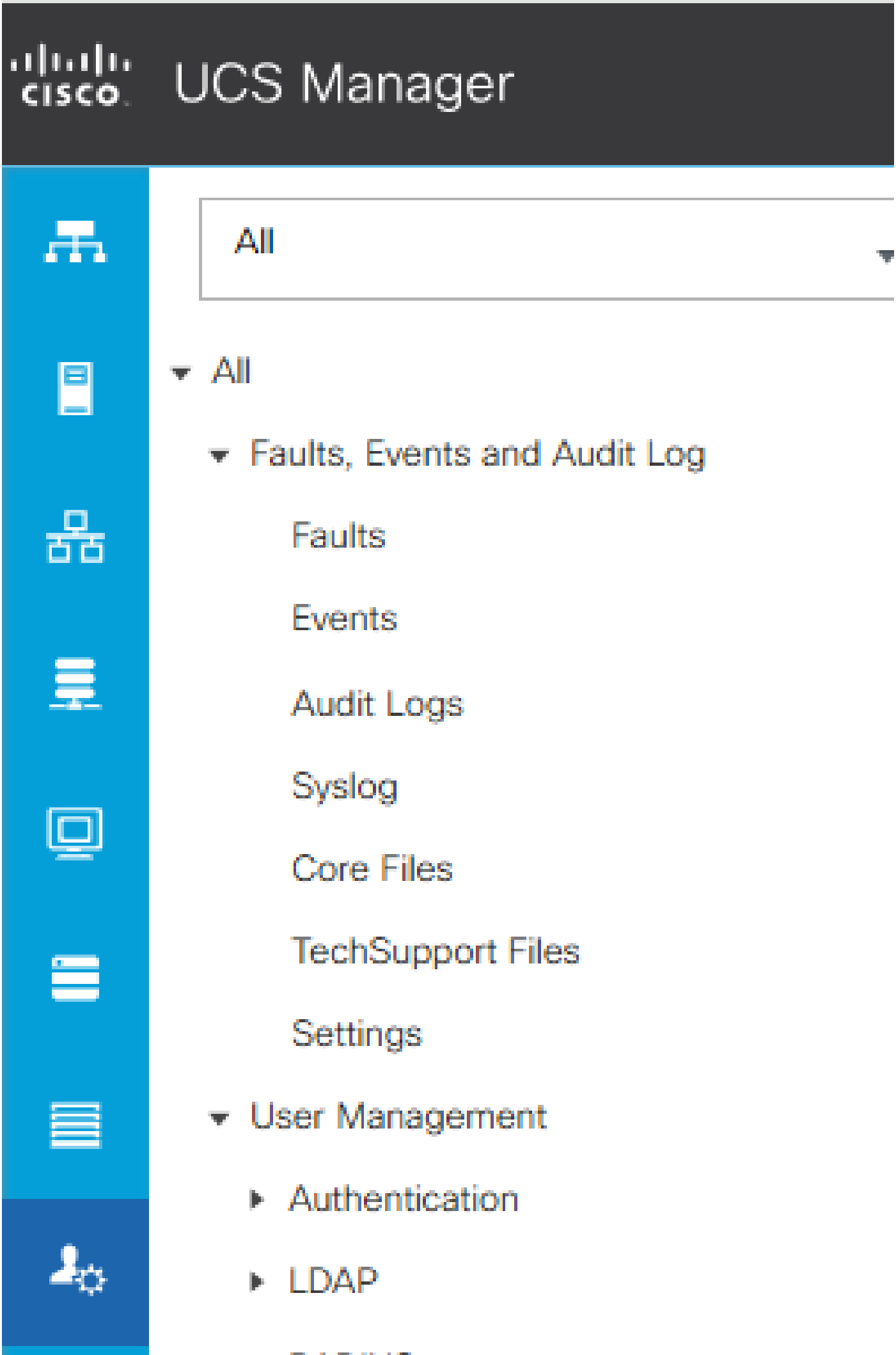
This procedure outlines how to set the password encryption key and clear the fault. If you do not see these GUI options, please try a different browser or clear your browser cache/cookies.

Procedure:

Step 1: In the Navigation pane, click **Admin**.



Step 2: **Expand All > User Management > User Services > Locally Authenticated Users**.


cisco
UCS Manager
All
All
Faults, Events and Audit Log
Faults
Events
Audit Logs
Syslog
Core Files
TechSupport Files
Settings
User Management
Authentication
LDAP