Troubleshoot Email Threat Defense Remediation Errors

Contents

Introduction

This document describes how to troubleshoot Remediation Errors on Cisco Secure Email Threat Defense.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Email Threat Defense
- Microsoft O365 Suites (Exchange Online, Entra, or Azure AD)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Email Threat Defense
- Microsoft Exchange Online
- Microsoft Entra ID (formerly known as Azure AD)

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

Email Threat Defense uses the Microsoft Graph API to communicate with Microsoft 365, enabling very fast detection and remediation such as Move to Trash, Move to Junk, Move to Quarantine.

Problem

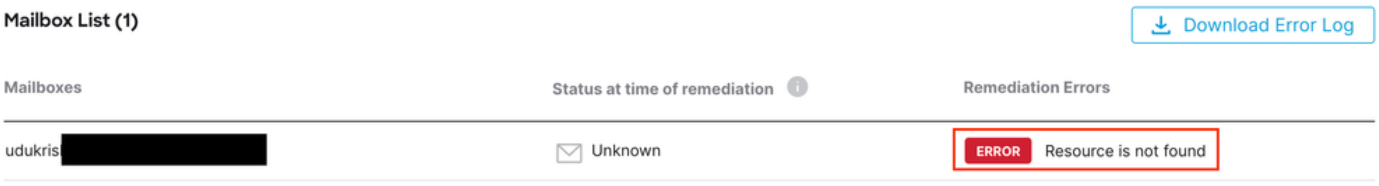
In some cases, Secure Email Threat Defense remediation fails to move or quarantine emails from end user mailboxes with different reasons.

Solution

Remediation fails under different conditions as described.

Scenario 1: Resource is Not Found

Email Threat Defense remediation fails with "Resource is Not Found".



Mailbox List (1)

Mailboxes	Status at time of remediation	Remediation Errors
udukris[redacted]	Unknown	ERROR Resource is not found

Error Resource is Not found

Cause

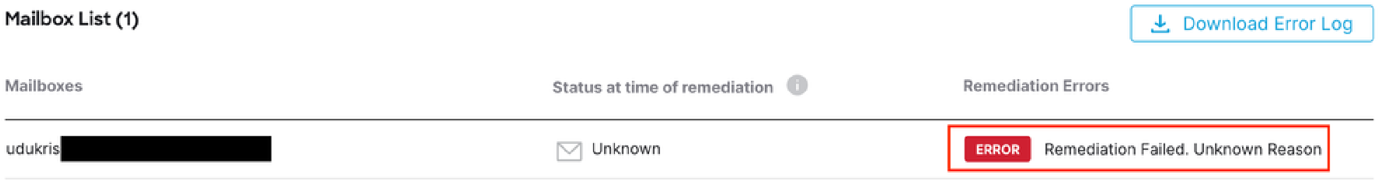
1. Email is deleted or moved to a different folder by the Mailbox Owner.

2. An account is created on Microsoft O365 Admin Center, but it has not been allocated a license, nor has the mailbox been set up.

Verify subscription status of the user on Microsoft O365 Admin Center. Assign correct Exchange Online license to auto create mailbox for the affected user.

Scenario 2: Remediation Failed - Unknown Reason

Email Threat Defense remediation fails with "Remediation Failed - Unknown Reason".



Mailbox List (1)

Mailboxes	Status at time of remediation	Remediation Errors
udukris[redacted]	Unknown	ERROR Remediation Failed. Unknown Reason

Error Remediation Failed - Unknown Reason

Cause

Incorrect or missing permissions on Microsoft Entra ID for the registered Secure Email Threat Defense Application.

1. Log in to Microsoft 365 Admin Center as at least a Cloud Application Administrator. In the left-hand menu, expand **Admin Centers** and click **Identity**.

2. Navigate to **Identity** > **Applications** > **Enterprise Applications** and click registered **Secure Email Threat Defense Application**. Navigate to **Permissions**.

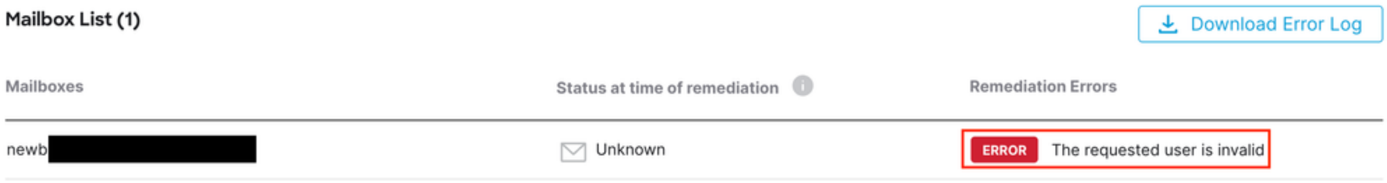
3. Verify that the application has correct Microsoft Graph API permissions with type **Application**.

- Mail.ReadWrite
- Organization.Read.All

If there are any missing permissions, click **Grant Admin Consent for <Tenant-ID>**. Log in with a Cloud Admin account and click **Accept**.

Scenario 3: The Requested User is Invalid

Email Threat Defense remediation fails with "The Requested User is Invalid".



Mailbox List (1)

Mailboxes	Status at time of remediation	Remediation Errors
newb[redacted]	Unknown	ERROR The requested user is invalid

Error Requested User is Invalid

Cause

1. Mailbox or User Account is invalid or does not exist in the Microsoft O365 organization directory.

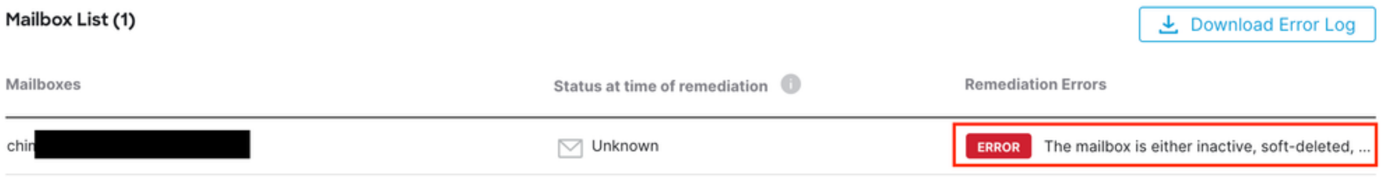
2. Secure Email Threat Defense is integrated with Multiple Tenants or Domains. However, the registered application on Entra ID (Azure AD) has access to a Single Tenant.

Verify that the User Account or Mailbox is valid and exists on Microsoft O365.

In a multi-tenant environment, ensure the registered Secure Email Threat Defense Application has permissions to access accounts in any organizational directory.

Scenario 4: The Mailbox is either Inactive, Soft-Deleted, or is Hosted On-Premise

Email Threat Defense remediation fails with "The Mailbox is either Inactive, Soft-Deleted, or is Hosted On-Premise".



Mailbox List (1)

Mailboxes	Status at time of remediation	Remediation Errors
chi[redacted]	Unknown	ERROR The mailbox is either inactive, soft-deleted, ...

Error Mailbox is Inactive or Soft-Deleted

Cause

1. An account has been set up on Microsoft Entra Identity (formerly Azure AD) but lacks an assigned valid M365 or Exchange Online license.

2. A hybrid setup with Microsoft O365 and an on-premises Exchange, with the user account solely existing on the Microsoft on-premises server.

Verify subscription status of the user on Microsoft O365 Admin Center. Assign correct Exchange Online license to auto create mailbox for the affected user.

Related Information

- Cisco Secure Email Threat Defense User Guide
- Cisco Technical Support & Downloads