

INCIDENT RESOLUTION: MISSING TENANT-ID

1. Betroffene Umgebungen

- SEPPmail Appliance mit Exchange Online Kunden
- SEPPmail.cloud mit Exchange Online Kunden

2. Problembeschreibung

Bis vor kurzem hat SEPPmail die Tenant-ID eines Exchange-Online Tenants benutzt, um in der Managed Domain Konfiguration nur Mails von Systemen anzunehmen, die von diesem Tenant kommen.

Die Tenant-ID musste dazu in der Managed Domain-Konfiguration eingetragen werden.

Diese Information wird nun in vielen Tenants nicht mehr mitgeschickt. Microsoft rollt diese Änderung schrittweise in ihrer Cloud aus.

Dies hat zur Folge, dass ab dem 31.8.2022 die SEPPmail Appliance und die SEPPmail.Cloud manche E-Mails mit dem Fehler:

Could not find a 'X-MS-Exchange-CrossTenant-id' header, mail will be rejected

abweist.

3. Auswirkung und Workaround

3.1. SEPPmail Appliance Kunden

Da diese Änderung in den oben genannten Umgebungen zu einer Beeinträchtigung der Mailkommunikation geführt hat, haben wir ad-hoc einen Workaround angeboten. Die Microsoft Mail-Systeme wurden als Relay-Server eingetragen und die Tenant-ID Prüfung abgeschaltet. Damit konnte der Mailfluss wieder aktiviert werden.

3.2. SEPPmail.Cloud Kunden

Ein zentraler Workaround wurde eingespielt.

4. Lösung

Da nach internen Quellen Microsoft die Tenant-ID nicht mehr in ihren E-Mails mitsenden wird, wird ab der Version 12.1.16 der SEPPmail-Appliance und ab 8.September 2022 08:00 in der SEPPmail.cloud die Prüfung anhand eines anderen X-Headers durchgeführt. Der X-Header

X-OriginatorOrg

liefert die Maildomäne der **sendenden Domäne** mit jeder E-Mail mit.

Die Versionen von SEPPmail ab 12.1.16 können nun diesen X-Header prüfen und mit der SEPPmail Managed Domain vergleichen. **In der SEPPmail Appliance muss in der Exchange Online Integration dieser Wert konfiguriert werden**, weitere Alias-Domains können alternativ manuell gepflegt werden. Beispiele sind unten in der Schritt-für-Schritt Anleitung inklusive Screenshots aufgeführt.

ACHTUNG! Falls der Wert "Originator Organizations" in der Appliance leer ist und E-Mails von Microsoft IP's kommen, werden diese E-Mails abgelehnt. (Gleiches Verhalten wie mit der früheren Tenant-ID).

Die Tenant-ID kann aus Referenz und für Dokumentationszwecken immer noch immer eingetragen werden, hat aber keine Funktion mehr im Regelwerk.

5. Anwendung der Änderung

5.1. SEPPmail Appliance Kunden

SEPPmail wird die HotFix-Version 12.1.16 am Tagesende des 7. September 2022 zum Download zur Verfügung stellen.

Die Anleitung ist für MSP's und Endkunden identisch.

- 1.) Systembackup und weitere Fallback Mechanismen gemäß Handbuch.
- 2.) Update der SEPPmail Appliance auf Version 12.1.16
- 3.) Rückstellen des Workarounds
 - a. In Mail-System setzen (reaktivieren) der Checkbox „Exchange Online-Integration“

MAIL SYSTEM ➔ EXCHANGE ONLINE RELAYING

Exchange Online Relaying																																												
Enable relay integration	<input checked="" type="checkbox"/> Allow relaying for Exchange Online servers (remember to also set correct originator organisations for each managed domain)																																											
Currently registered MTAs	<table border="1"> <tbody> <tr> <td>IPv4:</td> <td>40 . 92 . 0 . 0</td> <td>15 ▼</td> </tr> <tr> <td>IPv4:</td> <td>40 . 107 . 0 . 0</td> <td>16 ▼</td> </tr> <tr> <td>IPv4:</td> <td>52 . 100 . 0 . 0</td> <td>14 ▼</td> </tr> <tr> <td>IPv4:</td> <td>104 . 47 . 0 . 0</td> <td>17 ▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:111:f400::</td> <td>48 ▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:111:f403::</td> <td>48 ▼</td> </tr> <tr> <td>IPv4:</td> <td>51 . 4 . 72 . 0</td> <td>24 ▼</td> </tr> <tr> <td>IPv4:</td> <td>51 . 4 . 80 . 0</td> <td>27 ▼</td> </tr> <tr> <td>IPv4:</td> <td>51 . 5 . 72 . 0</td> <td>24 ▼</td> </tr> <tr> <td>IPv4:</td> <td>51 . 5 . 80 . 0</td> <td>27 ▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:4180:4050:400::</td> <td>64 ▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:4180:4050:800::</td> <td>64 ▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:4180:4051:400::</td> <td>64 ▼</td> </tr> <tr> <td>IPv6:</td> <td>2a01:4180:4051:800::</td> <td>64 ▼</td> </tr> </tbody> </table>		IPv4:	40 . 92 . 0 . 0	15 ▼	IPv4:	40 . 107 . 0 . 0	16 ▼	IPv4:	52 . 100 . 0 . 0	14 ▼	IPv4:	104 . 47 . 0 . 0	17 ▼	IPv6:	2a01:111:f400::	48 ▼	IPv6:	2a01:111:f403::	48 ▼	IPv4:	51 . 4 . 72 . 0	24 ▼	IPv4:	51 . 4 . 80 . 0	27 ▼	IPv4:	51 . 5 . 72 . 0	24 ▼	IPv4:	51 . 5 . 80 . 0	27 ▼	IPv6:	2a01:4180:4050:400::	64 ▼	IPv6:	2a01:4180:4050:800::	64 ▼	IPv6:	2a01:4180:4051:400::	64 ▼	IPv6:	2a01:4180:4051:800::	64 ▼
IPv4:	40 . 92 . 0 . 0	15 ▼																																										
IPv4:	40 . 107 . 0 . 0	16 ▼																																										
IPv4:	52 . 100 . 0 . 0	14 ▼																																										
IPv4:	104 . 47 . 0 . 0	17 ▼																																										
IPv6:	2a01:111:f400::	48 ▼																																										
IPv6:	2a01:111:f403::	48 ▼																																										
IPv4:	51 . 4 . 72 . 0	24 ▼																																										
IPv4:	51 . 4 . 80 . 0	27 ▼																																										
IPv4:	51 . 5 . 72 . 0	24 ▼																																										
IPv4:	51 . 5 . 80 . 0	27 ▼																																										
IPv6:	2a01:4180:4050:400::	64 ▼																																										
IPv6:	2a01:4180:4050:800::	64 ▼																																										
IPv6:	2a01:4180:4051:400::	64 ▼																																										
IPv6:	2a01:4180:4051:800::	64 ▼																																										

- b. Ggf. Entfernen der Exchange Online IP-Adressen aus der Managed Domain Liste „Allowed sending servers for this domain“.

MAILSYSTEM ➔ <MANAGEDDOMAIN> ➔ ALLOWED SENDING SERVERS FOR THIS DOMAIN

Allowed sending servers for this domain		
<p>Allowed sending servers for this domain (leave empty to allow all relaying networks). Note: Entering an address here does not automatically allow relaying</p>	Add allowed network:	<div>IPv4: <input type="text"/> . <input type="text"/> . <input type="text"/> 32 ▼</div> <div>IPv6: <input type="text"/> 128 ▼</div>

- c. Ggf. den Header für den „Header check“ für die zusätzliche Validierung des Tenants entfernen.

MAILSYSTEM → MANAGEDDOMAIN → HEADER CHECK

Header check	Mails from this domain must have a header <input type="text"/> with the following value: <input type="text"/>
--------------	---

4.) Neue Konfiguration einstellen

- a. Manuelles Eintragen der Managed Domains in den Exchange-Online Settings wie oben.

MAIL SYSTEM → <MANAGED DOMAIN> → MAIL SYSTEM SETTINGS

Die Liste an Domains wird mit Kommas getrennt (keine Leerzeichen).

Beispiel: contoso.eu

Exchange Online Integration	List of allowed exchange online originator organisations (comma seperated list) <input type="text" value="contoso.eu"/>
-----------------------------	---

Beispiel für contoso.eu und die Alias-Domains contoso.eu.onmicrosoft.com

Exchange Online Integration	List of allowed exchange online originator organisations (comma seperated list) <input type="text" value="contoso.eu,contoso.eu.onmicrosoft.com"/>
	Exchange online tenant ID (informational only): <input type="text" value="9fb3-4031-cd9f9c"/>

5.) Test Mailflow

Es sind keine Änderungen in Exchange Online notwendig und es ist auch kein neues Setup der Integration mittels PowerShell notwendig. Falls Sie im Zuge der Support-Bearbeitung Transportregeln für den Workaround hinzugefügt haben, können Sie diese aus Exchange-Online entfernen.

5.2. SEPPmail Cloud Kunden

Die Änderung wird im Hintergrund automatisch eingespielt und ist am 8. September 2022 um 08:00 aktiv.

Die Originator Organizations werden seitens SEPPmail automatisch konfiguriert.

6. Support

Falls Fragen auftauchen, erstellen Sie bitte ein Ticket per E-Mail an support@seppmail.ch mit dem Titel „ExO Patch 12.1.16“

ENDE DES DOKUMENTES