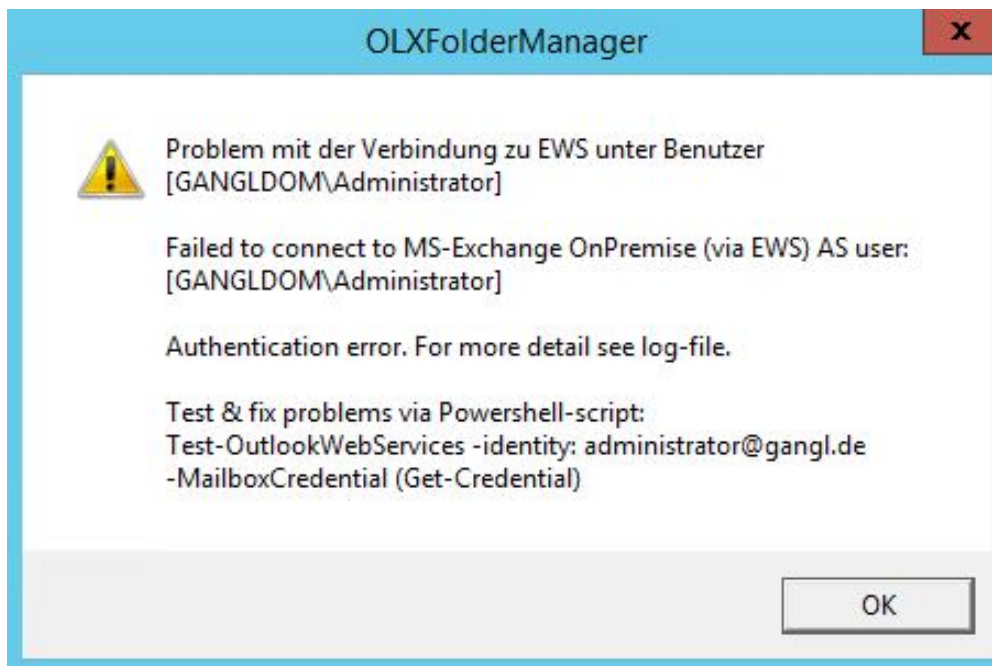
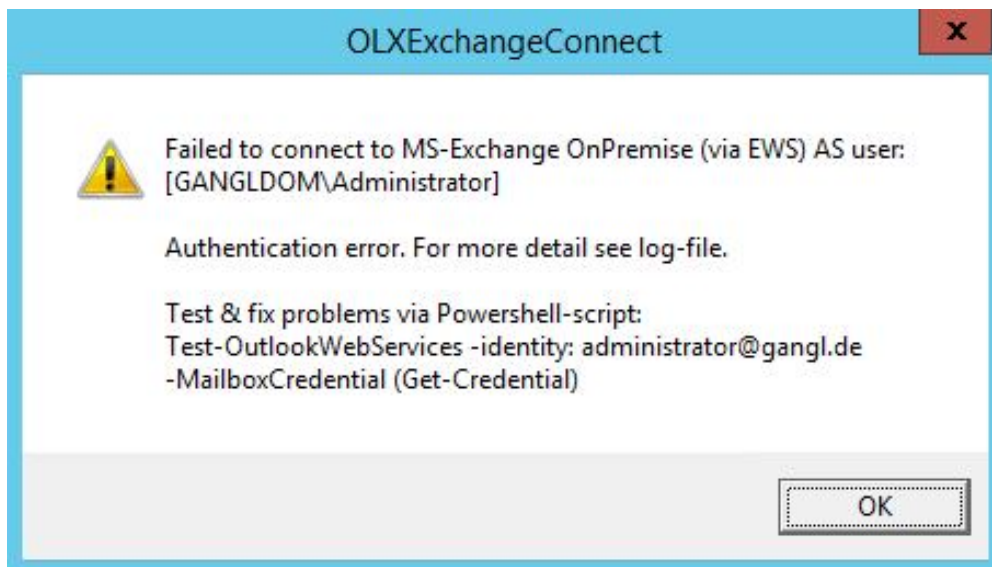


Was tun bei Authentication error?



Ursache

CVE-2019-0586 | Microsoft Exchange Memory Corruption Vulnerability

CVE-2019-0588 | Microsoft Exchange Information Disclosure Vulnerability

CVE-2018-8581 | Microsoft Exchange Server Elevation of Privilege Vulnerability

Exchange 2013 CU 22 (und folgende)

Exchange 2016 CU 12 (und folgende)

Exchange 2019 CU 1 (und folgende)

Registrykey: DisableLoopBackCheck

Hinweis

Es handelt sich hierbei grundsätzlich um fehlschlagendes AutoDiscover!

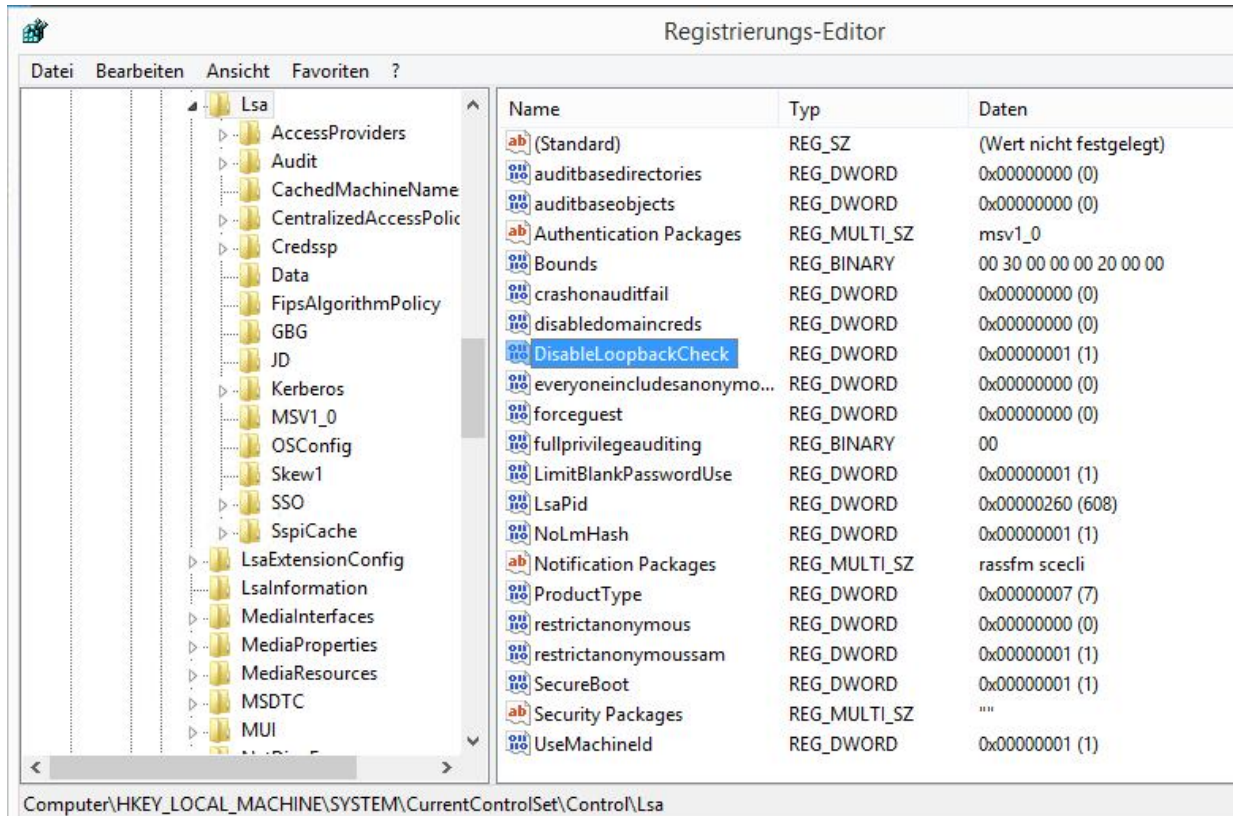
Das Problem existiert NUR direkt auf dem Exchange!

Alternativ könnten Sie den OLXAgent auch auf einem anderen Computer installieren und betreiben denn dann existiert dies MS-Problem nicht.

Nachstehende Schritte sind somit nur dann durchzuführen wenn der OLXAgent DIREKT auf dem Exchange betrieben wird

Schritt 1

Nachstehender Registrykey wird von obigen neuen Exchange-Versionen automatisch entfernt:



-> Ohne diesen Registrykey schlägt jegliches Autodiscover fehl

-> 401 Unauthorized wird erscheinen

Schritt 2 Exchange-ManagementShell

Prüfen ob Autodiscover (direkt auf dem Server) ohne Fehler klappt:

Test-OutlookWebServices -identity: xxx@mydomain.com -MailboxCredential (Get-Credential)

Source	ServiceEndpoint	Scenario	Result	Latency (MS)
EX2013.gangldom.intern	XXX	AutoErmittlung: Outlook-Anb...	Failure	44
EX2013.gangldom.intern		Exchange-Webdienste	Skipped	0
EX2013.gangldom.intern		Verfügbarkeitsdienst	Skipped	0
EX2013.gangldom.intern		Offlineadressbuch	Skipped	0

Wenn bei Autodiscover **Failure** erscheint:

Test-OutlookWebServices -identity: xxx@mydomain.com -MailboxCredential (Get-Credential) | fl

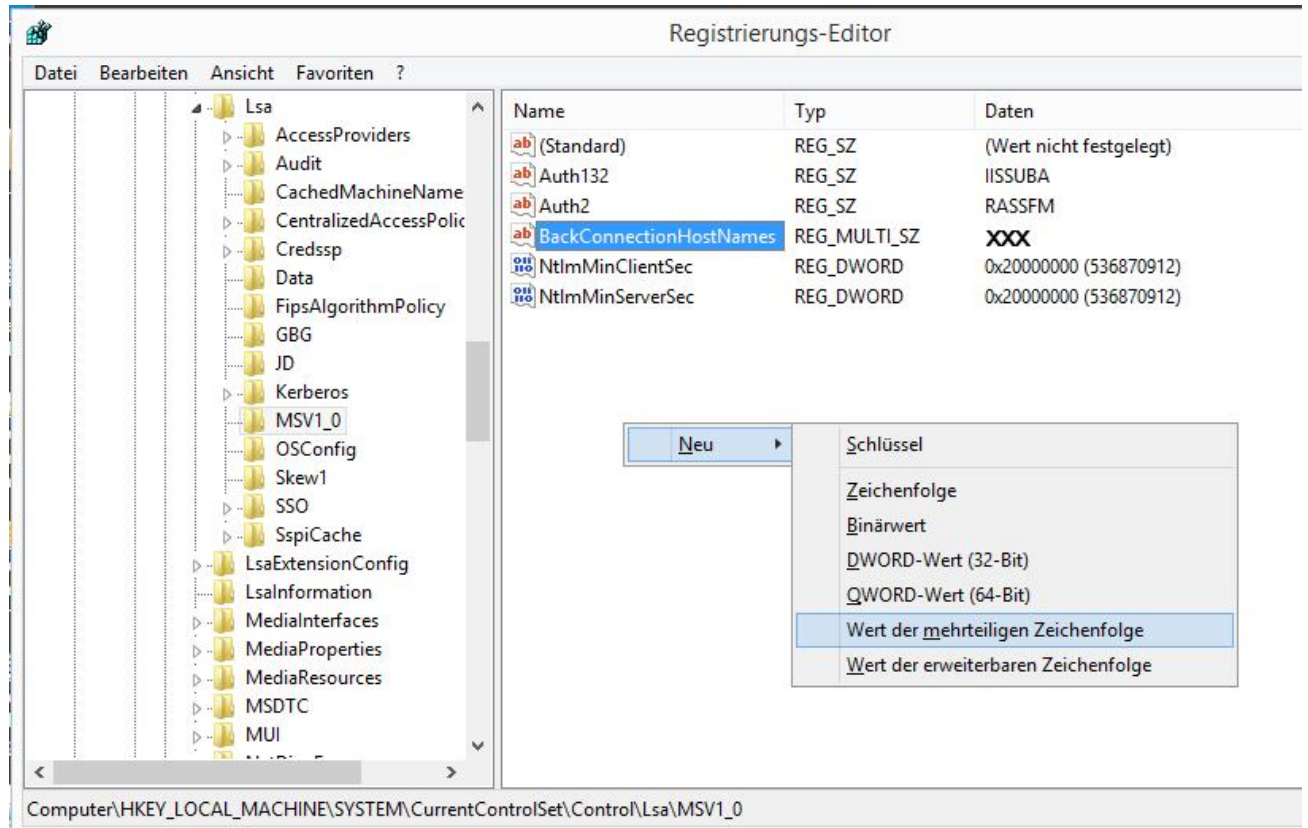
Im Output diesen Eintrag suchen:

```
</Autodiscover>
[2019-03-14 06:02:14Z] Antwort von AutoErmittlung:
request-id: e6292b6e-d4e4-4390-882b-bf165bf9903b
Server: Microsoft-IIS/8.5
WWW-Authenticate: NTLM,Negotiate,Basic realm="XXX"
X-Powered-By: ASP.NET
X-FEServer: EX2013
Date: Thu, 14 Mar 2019 06:02:14 GMT
Content-Length: 0
[2019-03-14 06:02:14Z] Antwort von AutoErmittlung:
System.Net.WebException: Der Remoteserver hat einen Fehler zurückgegeben: (401) Nicht
autorisiert.
    bei System.Net.HttpWebRequest.GetResponse()
    bei
Microsoft.Exchange.Management.SystemConfigurationTasks.ServiceValidatorBase.InternalInvoke()
    bei Microsoft.Exchange.Management.SystemConfigurationTasks.ServiceValidatorBase.Invoke()
```

Dieser Wert (XXX) muss für den nachfolgenden neuen Registrykey verwendet werden!

Schritt 3 Regedit

Diesen Registrykey neu erstellen:



<https://support.microsoft.com/en-ca/help/896861/you-receive-error-401-1-when-you-browse-a-web-site-that-uses-integrate>

Schritt 4 IIS

Gegebenenfalls den IIS restarten. Allerdings war dies in unseren Tests nicht einmal nötig.

Schritt 5 Exchange-ManagementShell

Erneut prüfen ob Autodiscover (direkt auf dem Server) ohne Fehler klappt:

Test-OutlookWebServices -identity: xxx@mydomain.com -MailboxCredential (Get-Credential)

Source	ServiceEndpoint	Scenario	Result	Latency (MS)
EX2013.gangldom.intern	XXX	AutoErmittlung: Outlook-Anb...	Success	44
EX2013.gangldom.intern		Exchange-Webdienste	Success	0
EX2013.gangldom.intern		Verfügbarkeitsdienst	Success	0
EX2013.gangldom.intern		Offlineadressbuch	Success	0

BINGO!

Schritt 6 Exchange-ManagementShell

Vulnerability prüfen!

HealthChecker.ps1

<https://gallery.technet.microsoft.com/office/Exchange-2013-Performance-23bcca58>

```
Hotfix Check:
KB3041832 is Installed

Exchange Web App Pools - GC Server Mode Enabled | Status:
MSExchangeOWAAppPool: false | Started
MSExchangeRpcProxyAppPool: false | Started
MSExchangeMapiAddressBookAppPool: false | Started
MSExchangeRpcProxyFrontEndAppPool: | Started
MSExchangePowerShellAppPool: false | Started
MSExchangePowerShellFrontEndAppPool: false | Started
MSExchangeMapiFrontEndAppPool: false | Started
MSExchangeMapiMailboxAppPool: false | Started
MSExchangeOABAppPool: false | Started
MSExchangePushNotificationsAppPool: false | Started
MSExchangeOWACalendarAppPool: false | Started
MSExchangeAutodiscoverAppPool: false | Started
MSExchangeECPAppPool: false | Started
MSExchangeSyncAppPool: false | Started
MSExchangeServicesAppPool: false | Started

Vulnerability Check:
All known security issues in this version of the script passed.
```

OLXAgents

Microsoft Outlook®
Microsoft Exchange®
aus der Reihe **Solutions** 
„Praxisorientierte Tools“ für

MS-Outlook

und

MS-ExchangeServer

Copyright by

GANGL
DIENSTLEISTUNGEN

Nelkenstrasse 16
73540 Heubach-Lautern
Tel: +49 (7173) 92 90 53
E-Mail: info@gangl.de
Internet: <https://www.gangl.de>