Exchange 2016 / Office 365: Permissions Debugging Protocol

Permissions are your most likely issue in a calendar migration or working server-side with calendars with Sumatra technology. This guide (which should also work for Exchange 2013) will help you diagnose any issues.

In general, start with our blog post: **The Cookbook Version of Exchange 2013 Migration Rights**.

There are four permissions your service account must have to function successfully:

1. Impersonation
2. Full access
3. Read access to the GC
4. Other details: Allow Log On Locally

In which situations are these permissions used?

This summarizes the types of permissions you must use when using Sumatra calendar technology.

Situation	Use Permission	Notes
Migrating Calendar Data into Exchange	Impersonation	Resource mailboxes are Disabled accounts by default, so in a full-state calendar migration they are ENABLED temporarily so that the Sumatra process can populate data correctly.
"Faster simpler" ICS calendar migration to Exchange	Impersonation	
Using the SuHoliday cmdlet or the Sumatra Pump on users	Impersonation	Putting holidays into user calendars requires only impersonation
Using the SuHoliday cmdlet or Sumatra Pump on resources	Full access	Why Full access in this case? Impersonation will not work unless you enable the accounts. In a migration there are many reasons for doing this, but for holidays that is a wasteful extra step. Use Full access.
Terminating an Existing User	Impersonation	It's basically a migration in reverse, so you use the same permissions as a migration
Removing broken meetings from resource or user calendars	Full access	Don't mess around in this case. You're trying to scrub out bad data, don't let low permissions get in the way of a fast job.

Impersonation

Impersonation grants the service account permission to ‘send-as’, and ‘receive-as’ the user account. Note, however, that impersonation works only when the account is enabled. For disabled accounts you will need full access.

To impersonate in Exchange 2010, create a new ManagementRoleAssignment (called “_suImp8”) for your service account (called “exsu”.)

```
new-ManagementRoleAssignment
  -Name:_suImp8
  -Role:ApplicationImpersonation
  -User:exsu@cod.sumatra.local
```

SPECIAL NOTE ON THE SERVICE ACCOUNT:

> **Make sure you are using the full, correct, SMTP address for your service account.**

Full Access, Send-as, Receive-as

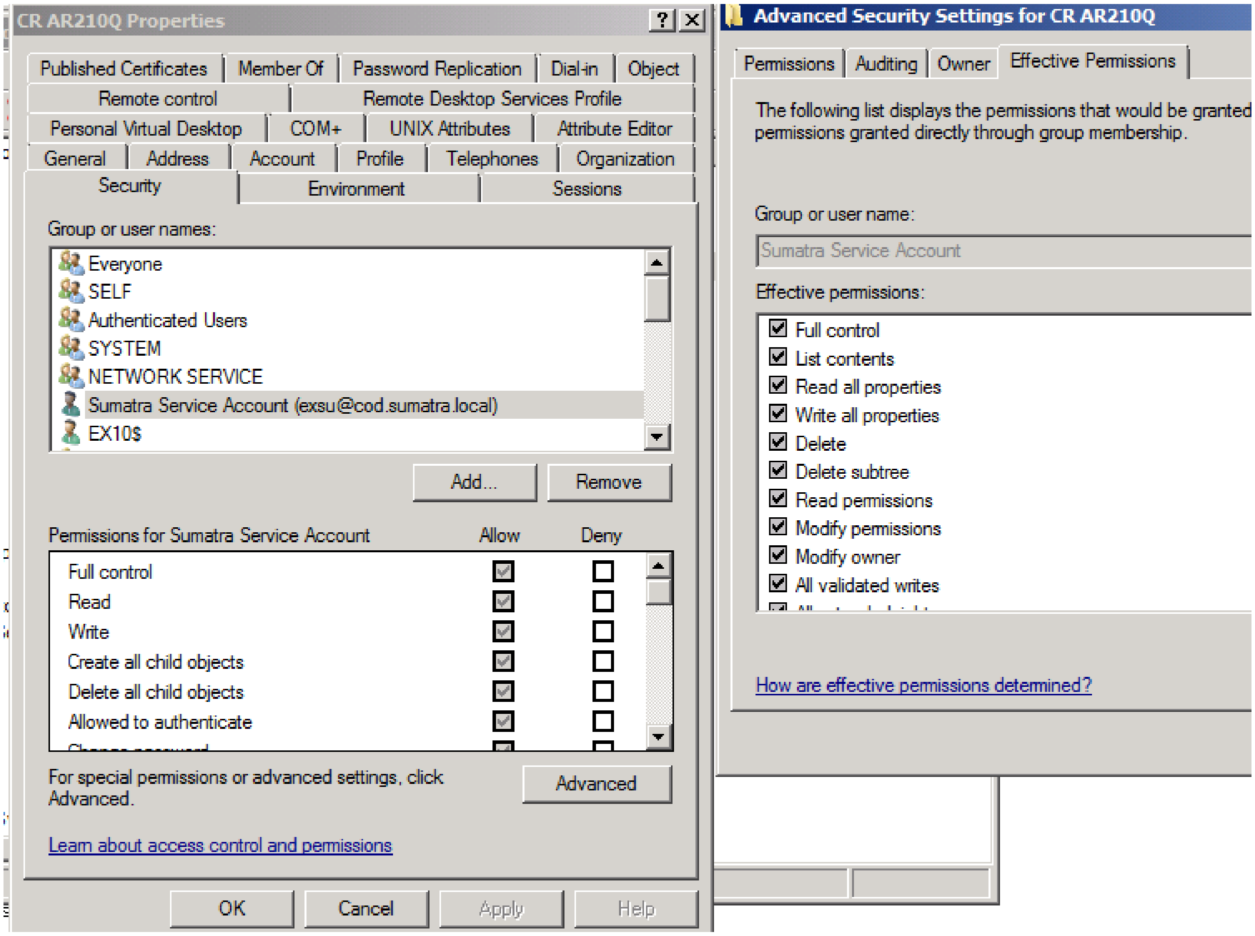
Full Access grants the service account permission to access the user account. Full access allows you to read from and write to folders in both enabled and disabled accounts. If you are just cancelling meetings from the conference room, full access is sufficient. If you want to send mail on behalf of a disabled user/room, you will also have to grant send-as receive-as (see the next section)

To grant your service account (called “exsu”,) full access for a room (“crar210q”), use the add-mailboxpermission cmdlet.

```
Add-MailboxPermission
   -Identity: crar210q
   -User: exsu@cod.sumatra.local
   -AccessRights: FullAccess
   -InheritanceType: All
```

See our blog: (http://calendarservermigration.blogspot.com/2009/10/fullaccess-fails-with-error-specified.html)

Note that group policies sometimes prevent permissions from being inherited. Please use Active Directory Users and Computers (ADUC) to ensure the permissions were set! Find the account (crar210q) and right-hand click to obtain properties. Select the security tab, then advanced. (If the security tab is missing, select Advanced Features under View.) You can check the permissions, or the effective permissions. You should not see deny checked!



CR AR210Q Properties

Published Certificates | Member Of | Password Replication | Dial-in | Object
Remote control | Remote Desktop Services Profile
Personal Virtual Desktop | COM+ | UNIX Attributes | Attribute Editor
General | Address | Account | Profile | Telephones | Organization
Security | Environment | Sessions

Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- NETWORK SERVICE
- Sumatra Service Account (exsu@cod.sumatra.local)
- EX10$

Permissions for Sumatra Service Account	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□
Allowed to authenticate	☑	□

For special permissions or advanced settings, click Advanced.

Advanced Security Settings for CR AR210Q

The following list displays the permissions that would be granted permissions granted directly through group membership.

Group or user name: Sumatra Service Account

Effective permissions:

- ☑ Full control
- ☑ List contents
- ☑ Read all properties
- ☑ Write all properties
- ☑ Delete
- ☑ Delete subtree
- ☑ Read permissions
- ☑ Modify permissions
- ☑ Modify owner
- ☑ All validated writes

Add Send-as, Receive-as

If you have to add send-as receive-as, here is the commandlet

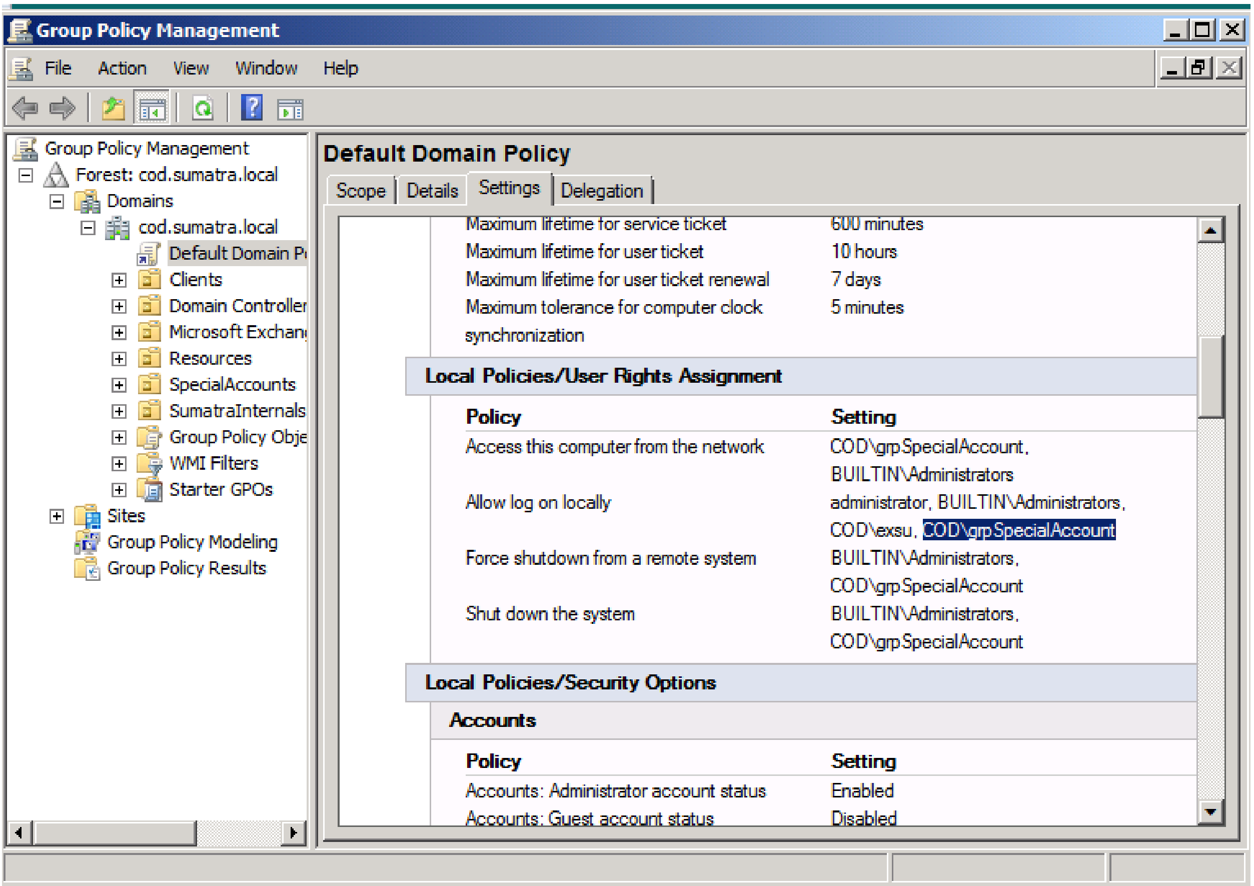
```
Add-ADPermission
   “CR 101B”
   -user: exsu
   -AccessRights:  genericall
   -ExtendedRights: "receive as","send as",
                    "ms-exch-epi-may-impersonate","ms-exch-epi-impersonation"
   -InheritanceType: All
```

Read access to the Global Catalog

Many enterprises grant access to the global catalog if the user is a member of the domain. If login is failing, anonymous access is probably disabled (since Windows 2000 DCs). Make sure you are an authenticated user.

Other Details: Allow log on locally

Make sure your service account is allowed to log on locally (as in the Local security policy, or if you have multiple machines, set via Group Management Policy, screen shot below.) Otherwise you will generate a 401 error.



Default Domain Policy

Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/User Rights Assignment

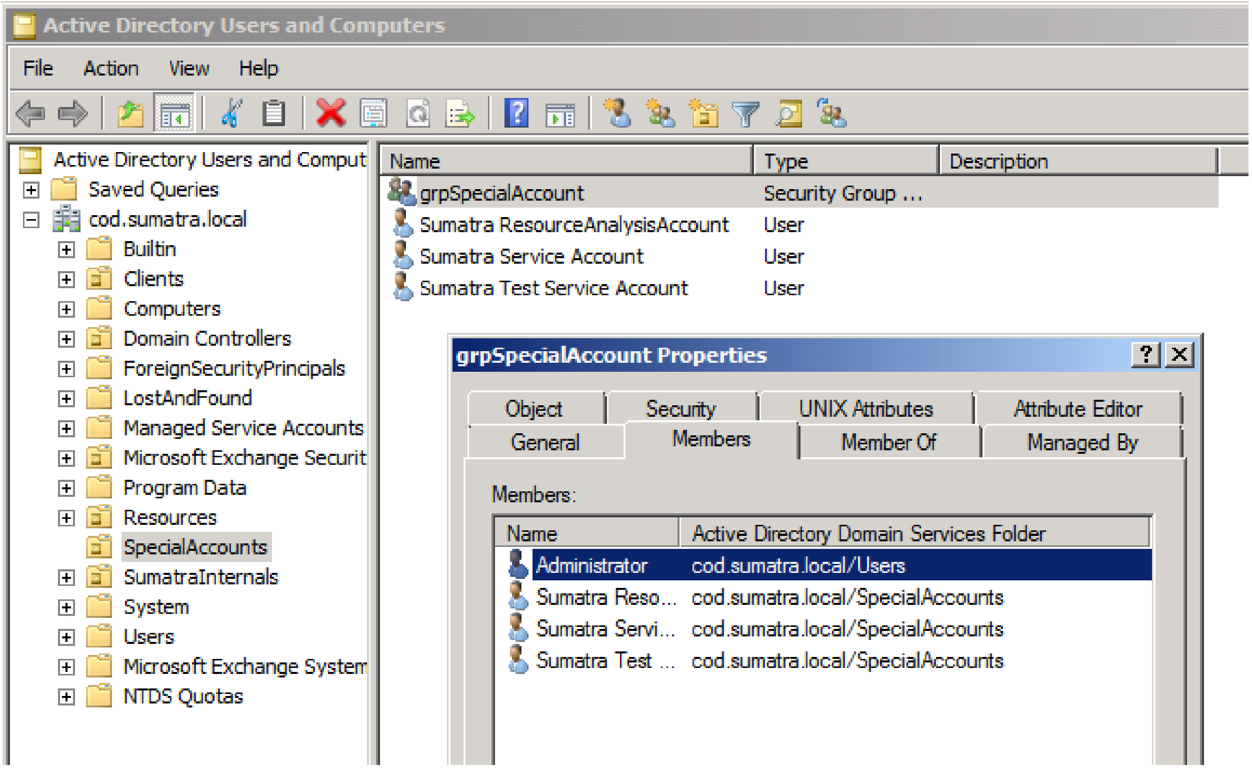
Policy	Setting
Access this computer from the network	COD\grpSpecialAccount, BUILTIN\Administrators
Allow log on locally	administrator, BUILTIN\Administrators, COD\exsu, COD\grpSpecialAccount
Force shutdown from a remote system	BUILTIN\Administrators, COD\grpSpecialAccount
Shut down the system	BUILTIN\Administrators, COD\grpSpecialAccount

Local Policies/Security Options

Accounts

Policy	Setting
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled

Note that in the example above we have both a specific service account and a Group of Service accounts. Using groups in this way is an effective means of managing several accounts if you need to segment them for Exchange data insertion.



Name	Type	Description
grpSpecialAccount	Security Group ...	
Sumatra ResourceAnalysisAccount	User	
Sumatra Service Account	User	
Sumatra Test Service Account	User	

Name	Active Directory Domain Services Folder
Administrator	cod.sumatra.local/Users
Sumatra Reso...	cod.sumatra.local/SpecialAccounts
Sumatra Servi...	cod.sumatra.local/SpecialAccounts
Sumatra Test ...	cod.sumatra.local/SpecialAccounts

Where to put your credentials

Store your credentials in the “CAS Login Creds” button next to the CAS server textbox in the user interface. The password is stored encrypted in the XML config file. It’s important you do this – signing in at the system level with the service account is not necessarily sufficient for an entire migration.

Scenario: Your admin LOGIN account differs from your IMPERSONATION account has a different SMTP address, or is from a different domain!

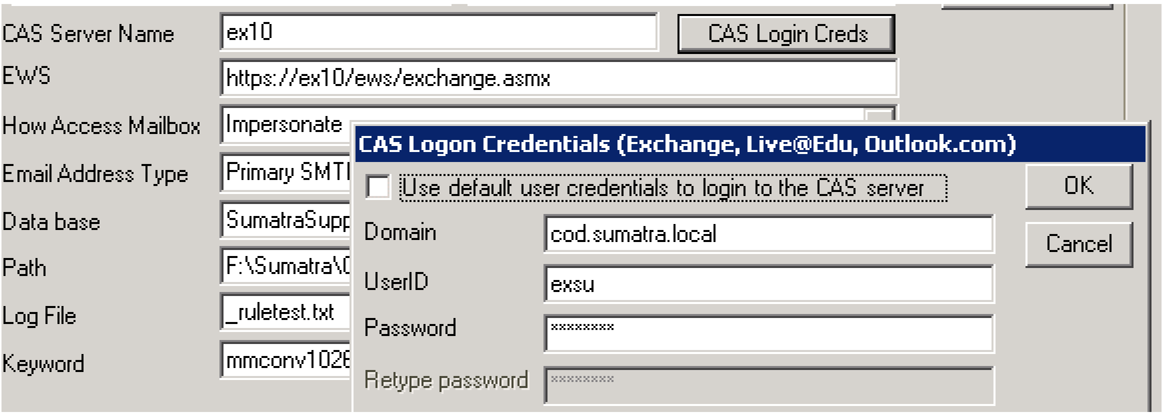
For example,

exsu-admin@internal.sumatra.local could be the account used to log in (this would be used for the CAS Server)

Your service account’s SMTP address could be:

exsu@sumatra.local

If you don’t get this correct, you’ll get a 401 error when trying to login



CAS Server Name: ex10

EWS: https://ex10/ews/exchange.asmx

How Access Mailbox: Impersonate

Email Address Type: Primary SMTI

Data base: SumatraSupp

Path: F:\Sumatra\(

Log File: _ruletest.txt

Keyword: mmconv1026

CAS Logon Credentials (Exchange, Live@Edu, Outlook.com)

□ Use default user credentials to login to the CAS server

Domain: cod.sumatra.local

UserID: exsu

Password: ********

Retype password: ********

Exchange 2016: Debugging Permissions

Setting permissions correctly is one of the largest stumbling blocks in the process.   Here is a list of the HTTP errors, and ways to debug (and fix) permissions.

HTTP Response	Most Likely Issue	Solution
401	FIRST THING TO CHECK (seriously):	Use the full, correct SMTP address for your service account in logging on. See above.
	Service account not allow to “log on locally”	Grant permission to “log on locally” via group or local security policy
	The CAS and Mailbox servers are not members of Windows Authorization Access Group.	Add all computers as members to “Windows Authorization Access Group” in ADU&C.
	BASIC authentication is not enabled for the EWS virtual directory in IIS	Set Basic authentication in IIS; remember to restart IIS
	The "SERVICE ACCOUNT" is not authorized to submit requests to the CAS Server	Create a new-ManagementRoleAssignment, and grant ApplicationImpersonation rights to the service account. Also remember to check the service account creds to ensure they password is correct. Paste the "ews url" into a browser. Enter the service account creds, when prompted. Do you see a EWS WSDL page? (Note: this could show up as a 500 error in some instances.)
500	The "test user" does not exist in Exchange or is not mailbox enabled	Verify account exists in the domain, it is enabled, a mailbox user (try to access the account in OWA using the service account credentials). If the account is disabled, did you grant “fullAccess” to the service account?

	The "SERVICE ACCOUNT" cannot impersonate the "test user"	Verity there is a management_role assignment "ApplicationImpersonation" (Exchange 2010) or ExtendedRights:"ms-Exch-EPI-Impersonation","ms-Exch-EPI-May-Impersonate" (Exchange 2007) for the SERVICE ACCOUNT that is applied to the server or the user you are attempting to test.

Start with IIS Basic authentication on the EWSvirtual directory. It’s the easiest to see / fix.

Basic debugging protocol – 401 error

Open a browser window, and try to open you EWS URL. If you typically point to the load balancer, point to one CAS server instead. Try to open the EWS URL e.g., http://YOURDOMAIN/ews/exchange.asmx. You should be prompted for credentials. Enter the service account credentials. If the credentials are rejected, your service account may not be allowed to log on locally. If you can login, try to insert a "test" appointment using suExchange. If you see a 401, it will be due to :

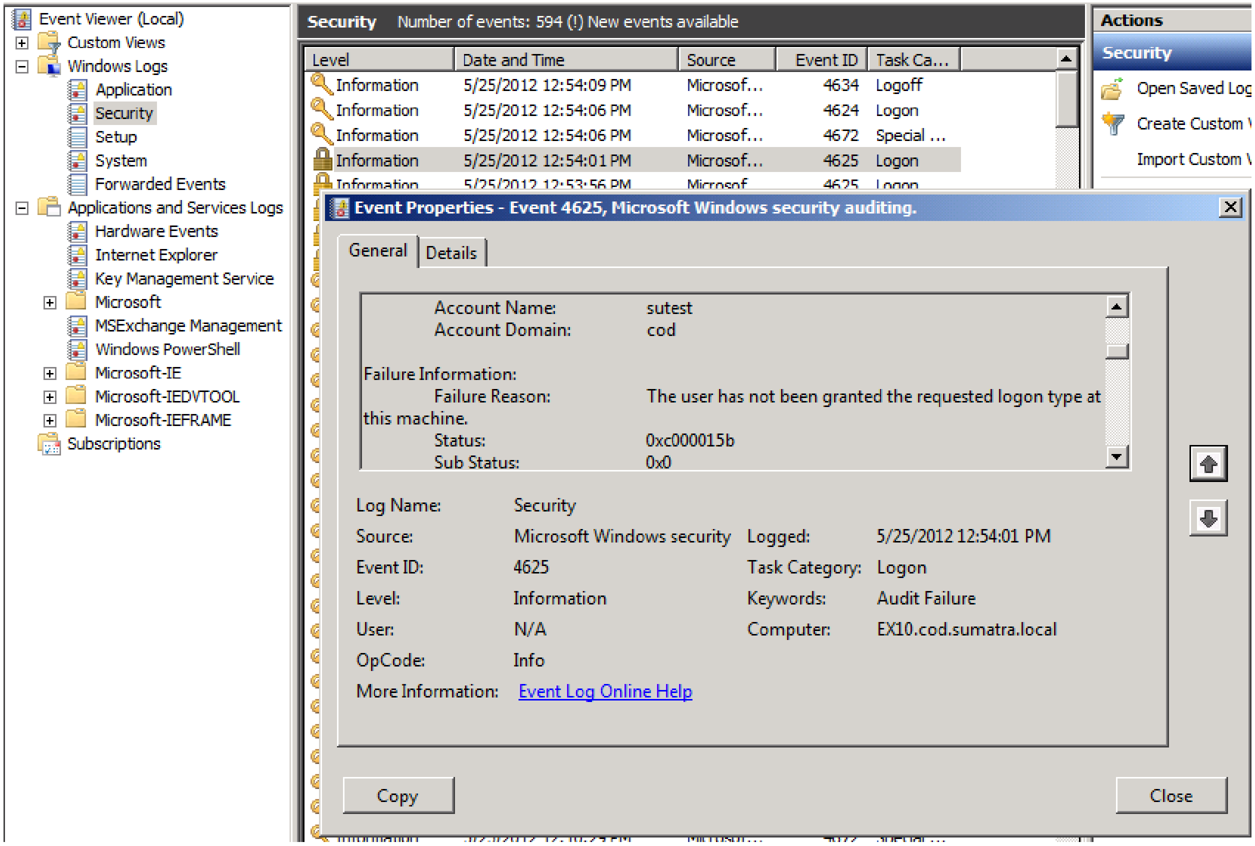
BASIC authentication not set

OR

The CAS/MBX server(s) are not members of Windows Authorization Access group.

Issue: Service account not allowed to log on locally.

Here's an easy way to confirm you cannot log on locally. Go to the CAS server you pointed to in the EWS url, and open up the Security event log. Search for event ID 4625, keyword Audit Failure. You'll know you have to grant log on locally if you see your service account, with failure information "*the user has not been grated the requested logon type at this machine*". If so, allow the service account to log on locally via a group policy or local security policy.



Security Number of events: 594 (!) New events available

Level	Date and Time	Source	Event ID	Task Ca...
Information	5/25/2012 12:54:09 PM	Microsof...	4634	Logoff
Information	5/25/2012 12:54:06 PM	Microsof...	4624	Logon
Information	5/25/2012 12:54:06 PM	Microsof...	4672	Special ...
Information	5/25/2012 12:54:01 PM	Microsof...	4625	Logon
Information	5/25/2012 12:53:56 PM	Microsof...	4625	Logon

Event Properties - Event 4625, Microsoft Windows security auditing.

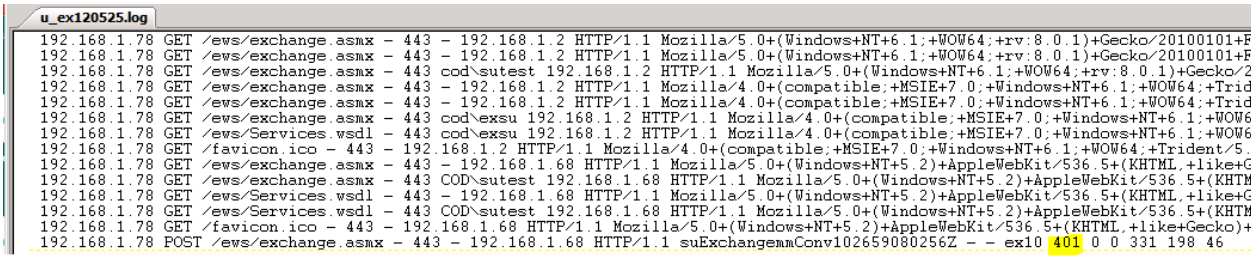
```
        Account Name:           sutest
        Account Domain:         cod

Failure Information:
        Failure Reason:         The user has not been granted the requested logon type at
this machine.
        Status:                 0xc000015b
        Sub Status:             0x0
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/25/2012 12:54:01 PM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	EX10.cod.sumatra.local
OpCode:	Info		
More Information:	Event Log Online Help		

Issue: Basic Authentication not set

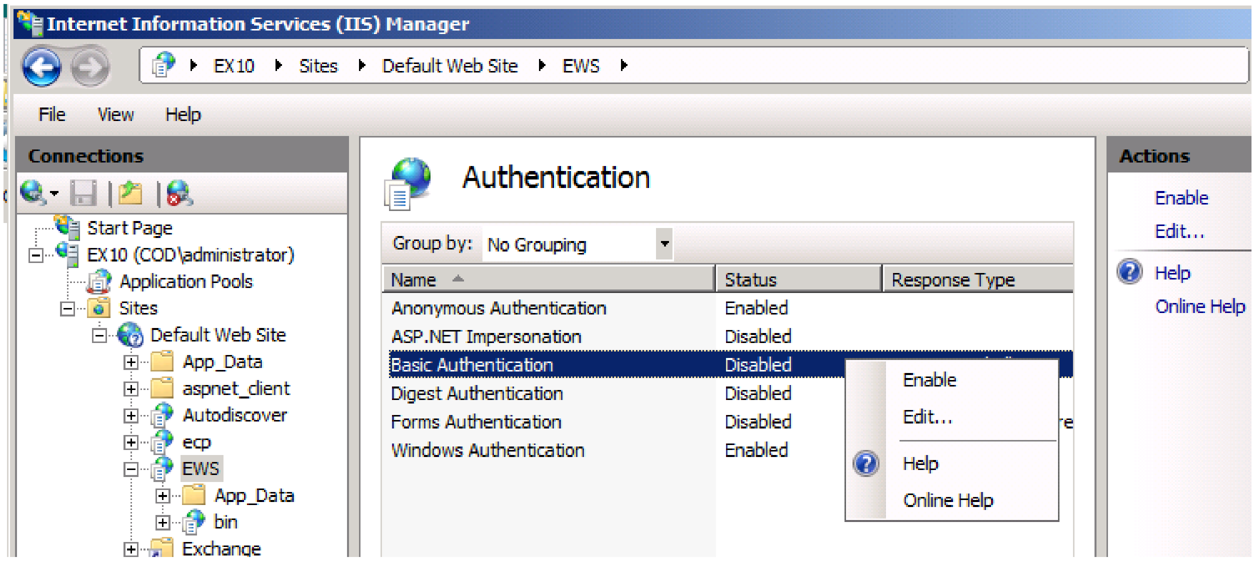
Look in the IIS logs. If you see a 401 error, check IIS. This is sometimes due to an authentication failure because of a difference of authentication protocols used. If you are getting a 401 error, you have two choices, either ensure the IIS virtual directory includes basic authentication, or change the Sumatra tool to use “BASIC” authentication (In past Exchange iterations “Negotiate” authentication was required We expect it will someday make a surprise return).

To change the EWS virtual directory to use basic authentication, check IIS to see if it is disabled. If so, enable it. Remember to cycle IIS: “iisreset /noforce.”



u_ex120525.log

```
192.168.1.78 GET /ews/exchange.asmx - 443 - 192.168.1.2 HTTP/1.1 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+rv:8.0.1)+Gecko/20100101+F
192.168.1.78 GET /ews/exchange.asmx - 443 - 192.168.1.2 HTTP/1.1 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+rv:8.0.1)+Gecko/20100101+F
192.168.1.78 GET /ews/exchange.asmx - 443 cod\sutest 192.168.1.2 HTTP/1.1 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+rv:8.0.1)+Gecko/2
192.168.1.78 GET /ews/exchange.asmx - 443 - 192.168.1.2 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trid
192.168.1.78 GET /ews/exchange.asmx - 443 - 192.168.1.2 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trid
192.168.1.78 GET /ews/exchange.asmx - 443 cod\exsu 192.168.1.2 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW6
192.168.1.78 GET /ews/Services.wsdl - 443 cod\exsu 192.168.1.2 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW6
192.168.1.78 GET /favicon.ico - 443 - 192.168.1.2 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/5.
192.168.1.78 GET /ews/exchange.asmx - 443 - 192.168.1.68 HTTP/1.1 Mozilla/5.0+(Windows+NT+5.2)+AppleWebKit/536.5+(KHTML,+like+G
192.168.1.78 GET /ews/exchange.asmx - 443 COD\sutest 192.168.1.68 HTTP/1.1 Mozilla/5.0+(Windows+NT+5.2)+AppleWebKit/536.5+(KHTM
192.168.1.78 GET /ews/Services.wsdl - 443 - 192.168.1.68 HTTP/1.1 Mozilla/5.0+(Windows+NT+5.2)+AppleWebKit/536.5+(KHTML,+like+G
192.168.1.78 GET /ews/Services.wsdl - 443 COD\sutest 192.168.1.68 HTTP/1.1 Mozilla/5.0+(Windows+NT+5.2)+AppleWebKit/536.5+(KHTM
192.168.1.78 GET /favicon.ico - 443 - 192.168.1.68 HTTP/1.1 Mozilla/5.0+(Windows+NT+5.2)+AppleWebKit/536.5+(KHTML,+like+Gecko)+
192.168.1.78 POST /ews/exchange.asmx - 443 - 192.168.1.68 HTTP/1.1 suExchangemmConv102659080256Z - - ex10 401 0 0 331 198 46
```

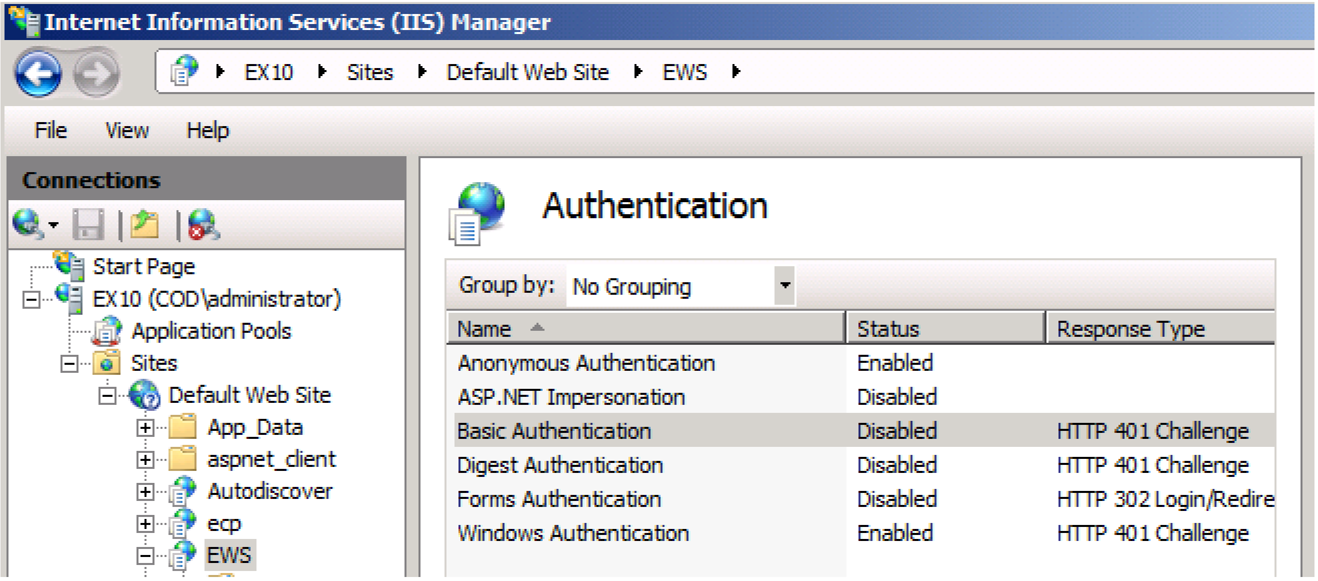


Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	
Digest Authentication	Disabled	
Forms Authentication	Disabled	
Windows Authentication	Enabled	

EWS Virtual Directory Authentication

If you get a 401 error, check IIS to see what is enabled (by default, Anonymous and Windows are enabled, and Basic is disabled.)



Authentication

Group by: No Grouping

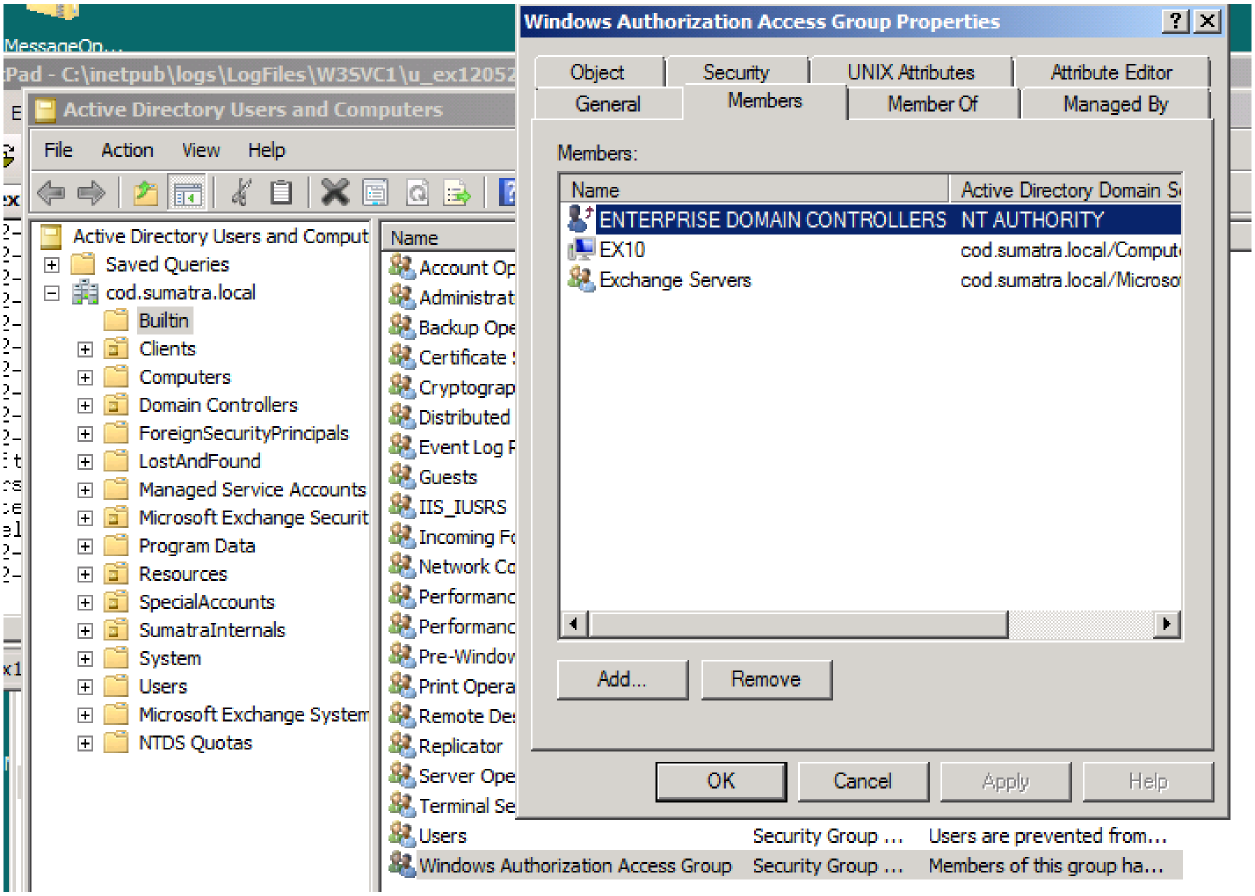
Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redire
Windows Authentication	Enabled	HTTP 401 Challenge

If so, edit the _config.xml file, and ensure "HTTPAuthType" is set to BASIC. (If Basic is enabled, you can set the HTTPAuthType to Basic.)

```
<SMTP_Domain>livetest.sumatraresourcewatch.com</SMTP_Domain>
<EWSItemLimit>1000</EWSItemLimit>
<EWSURL>https://sn1prd0202.outlook.com/EWS/Exchange.asmx</EWSURL>
<HTTPAuthType>Basic</HTTPAuthType>
<HTTPAuthPreAuthenticateRequest>True</HTTPAuthPreAuthenticateRequest>
```

Issue: Computers are not members of Windows Authorization Access Group

If you are still getting a 401 error, ensure that ALL exchange computers and domain controllers are members of windows authorization access group.



Members:

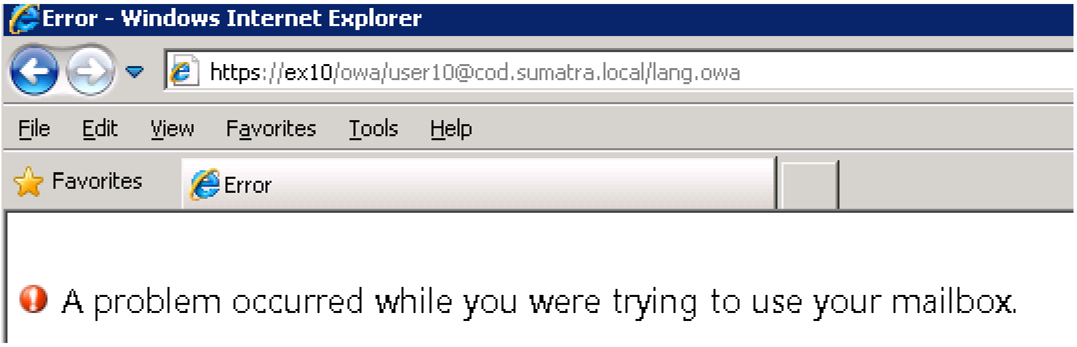
Name	Active Directory Domain S
ENTERPRISE DOMAIN CONTROLLERS	NT AUTHORITY
EX10	cod.sumatra.local/Comput
Exchange Servers	cod.sumatra.local/Microso

Users	Security Group …	Users are prevented from…
Windows Authorization Access Group	Security Group …	Members of this group ha…

Basic debugging protocol – 500 error

Issue: Service account does not have impersonation permissions or full access

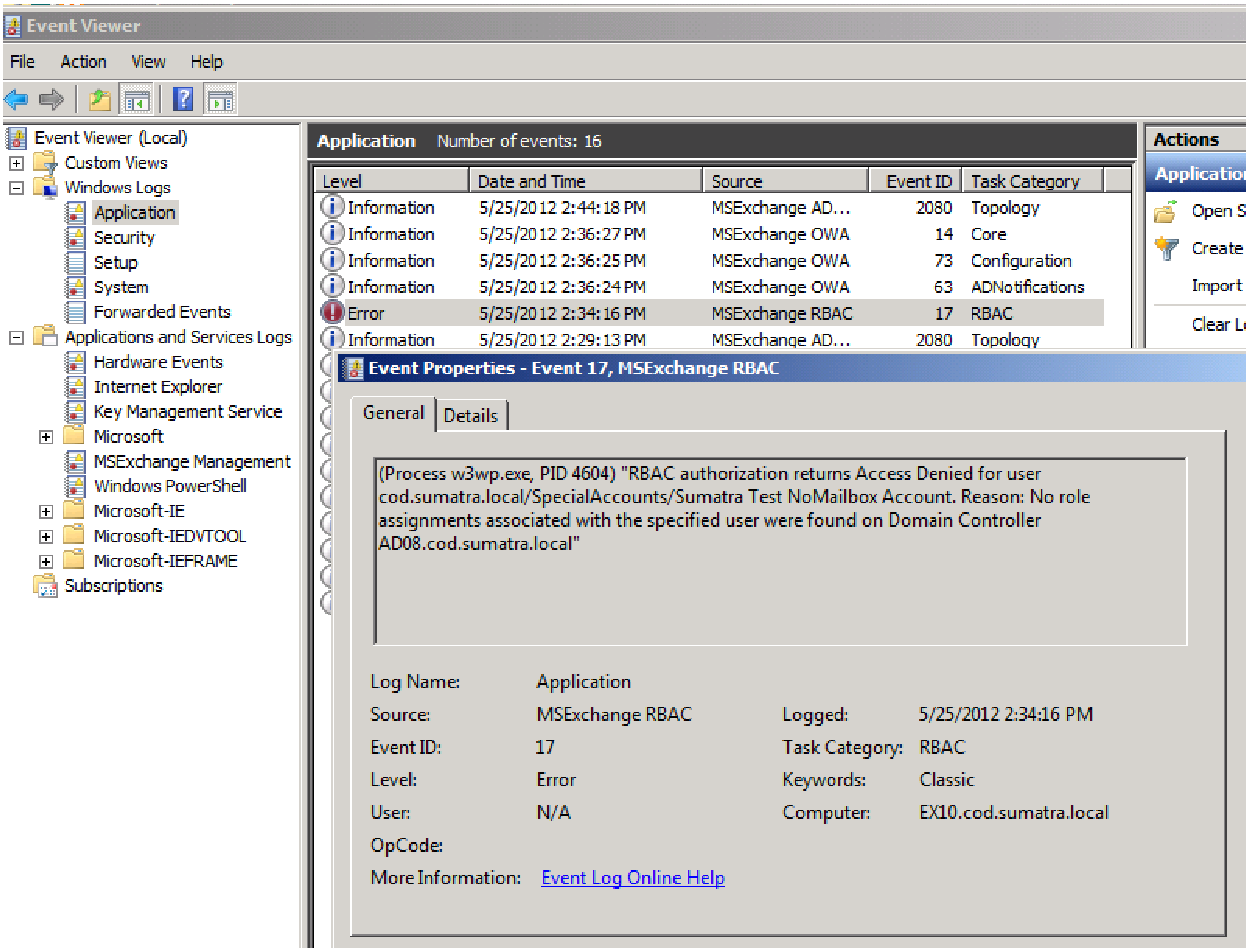
If you are still getting a 500 error, try logging into an active end user's mailbox via OWA (like your own!) using the service account credentials. If you see an error in OWA:



https://ex10/owa/user10@cod.sumatra.local/lang.owa

A problem occurred while you were trying to use your mailbox.

Check the Application event logs on the CAS server for Event ID 17. If you do, then create a "New-ManagementRoleAssignment" to grant the service account ApplicationImpersonation permissions (see "Impersonation," above.)



Application Number of events: 16

Level	Date and Time	Source	Event ID	Task Category
Information	5/25/2012 2:44:18 PM	MSExchange AD...	2080	Topology
Information	5/25/2012 2:36:27 PM	MSExchange OWA	14	Core
Information	5/25/2012 2:36:25 PM	MSExchange OWA	73	Configuration
Information	5/25/2012 2:36:24 PM	MSExchange OWA	63	ADNotifications
Error	5/25/2012 2:34:16 PM	MSExchange RBAC	17	RBAC
Information	5/25/2012 2:29:13 PM	MSExchange AD...	2080	Topology

Event Properties - Event 17, MSExchange RBAC

(Process w3wp.exe, PID 4604) "RBAC authorization returns Access Denied for user cod.sumatra.local/SpecialAccounts/Sumatra Test NoMailbox Account. Reason: No role assignments associated with the specified user were found on Domain Controller AD08.cod.sumatra.local"

Log Name:	Application		
Source:	MSExchange RBAC	Logged:	5/25/2012 2:34:16 PM
Event ID:	17	Task Category:	RBAC
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	EX10.cod.sumatra.local
OpCode:			
More Information:	Event Log Online Help		

Basic debugging protocol – multiple domains

Issue: You have domains "company.com" and "temporary.company.com"

In this case your environment is set up roughly as follows:

Company.com:
This is the current forest in use and a full open source environment but no Active Directory is in place. All clients are a member of the company.com forest and are authenticating against the directory service to get access to all resources. No resources of this forest are used in the "temporary" environment;.

Temporary.company.com:
This is a separate environment which may be your proof of concept (POC) environment or just a temporary environment for testing or security. This forest is connected to company.com but no permissions are set cross-forest, so it is only used for DNS lookups for other domains. Active Directory is used for authentication which includes the DNS service for only the temporary.company.com domain.

Users look like this in the combined environment:

> username: domain\username or UPN: username@temporary.company.com
> e-mail: firstname.lastname@company.com

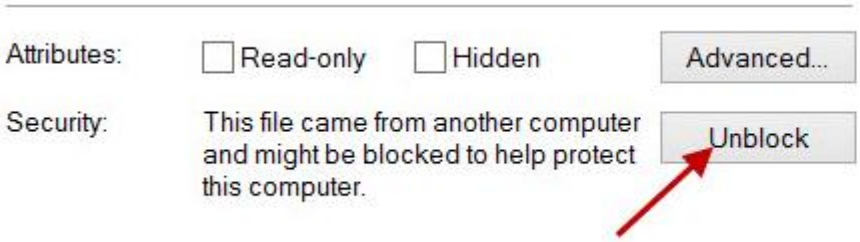
Solution:

Since there are multiple domains in the proof-of-concept environment, you have to change the way you authenticate the requests. Thus:

- For the "CAS" server credentials, you need to use:
  - The POC domain "temporary.company.com",
  - The service account's UPN, "sumatraserviceaccount@temporary.company.com", and of course the password.
- To "test" access, you'll want to use the primary SMTP address for the end user account, e.g. firstname.lastname@company.com (This will also be true for all user/resource account email addresses.)
- For the CAS server, start with the NLB (https://mail.domain.company.com/ews/exchange.asmx.) If that fails to authenticate your request, point to one of the CAS servers in the "temporary" domain.
- Finally, check the Sumatra code's _*config*_.xml file. The HTTP authenticate switch should be set to negotiate (NOT basic.)
- You may find that the soap request may get rejected (500 error). If so, try the SMTP address, not the UPN. Why? Because MS Exchange Web Services requires a primary SMTP address be used for "impersonation". (You could ensure the UPN AND the Primary SMTP addresses are the same for the service account.)

Basic debugging protocol – Sumatra holiday cmdlet

Scenario: You downloaded the cmdlet zip file from the Sumatra site, and want to run it on your Exchange server. Before you do, however, take the properties (via right-click->Properties) of the suholiday.dll file, and "unblock" the dll.



Attributes: ☐ Read-only ☐ Hidden

Security: This file came from another computer and might be blocked to help protect this computer.

‘Microsoft.ACE.OLEDB.12.0’ provider is not registered….

How to fix: 'Microsoft.ACE.OLEDB.12.0' provider is not registered on the local machine

Our full-state calendar migration executes on a 32-bit or 64-bit architecture. We default to using the JET database engine, though this can be changed in _Config_XML:

Provider=Microsoft.ACE.OLEDB.12.0;Data Source=

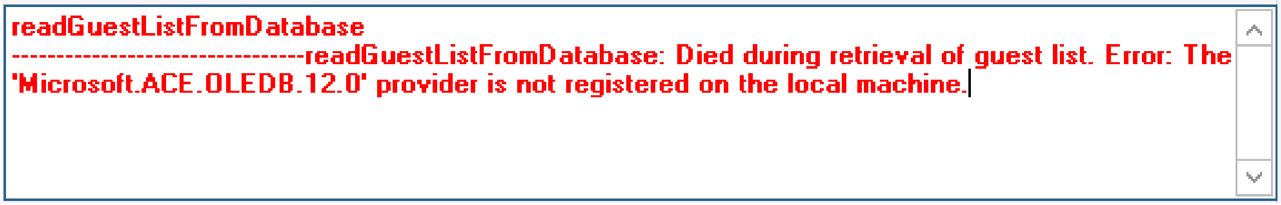
If you don't have the x64 version of MS Office 2010 installed, (or NO version of office installed) download the Microsoft Access DB Engine 2010 Redistributable (pick the x64 version!)

http://www.microsoft.com/download/en/details.aspx?id=13255 Install the x64 version via the Command Prompt with:

```
AccessDatabaseEngine_X64.exe /passive
```

Do it this way OR you'll see the error: The 'Microsoft.ACE.OLEDB.12.0' provider is not registered on the local machine.

The error will look like this in the error window of our migration tools:



```
readGuestListFromDatabase
--------------------------------readGuestListFromDatabase: Died during retrieval of guest list. Error: The 'Microsoft.ACE.OLEDB.12.0' provider is not registered on the local machine.
```

If you look in _Config_XML you will see the default (top line) as well as the other options should you need to change them.

```
Provider=Microsoft.ACE.OLEDB.12.0;Data Source=

Provider=Microsoft.ACE.OLEDB.12.0;Data Source=

PROVIDER=Microsoft.Jet.OLEDB.4.0;Data Source=
```

Slow PowerShell Response Debugging

Slow PowerShell Response to Get-Mailbox Debugging Protocol

Gentle reader of calendar migration intent,

Ms. Calendar received the following (edited slightly for clarity):

When setting up an impersonation account in our active environment the first few steps (editor's note: see The Cookbook Version of Exchange Migration Rights) go fine and then when I run this:

Get-Mailbox -resultsize unlimited | add-mailboxpermission -user OurDomainUser -accessrights: fullaccess -InheritanceType: All

It just sits there and never spits out any output. Yesterday I left it running for hours and eventually Exchange Management Shell closed itself but I still get the you don't have access to this email when trying to log in to any email accounts with the service account.

An interesting case which does occur!

There is not a lot of love across the community for Get-Mailbox performance and even less for practical actions to take. See: Performance issues with Get-Mailbox -Database PowerShell cmdlet and Count Mailboxes Per Database Faster.

It is probably a problem with "get-mailbox"

To test:

1) First try without any qualifiers:

```
 get-mailbox
```

or limit it to 100

```
 get-mailbox  -resultsize 100
```

2) Second add the resultsize qualifier

```
 Get-Mailbox -resultsize unlimited
```

Once they set a static limit instead of unlimited they were able to set impersonation on all accounts. We have seen in instances where the performance is deplorable it's usually a problem getting the "join"s to work through AD. Keep in mind we're linking two separate AD actions here, Get-Mailbox and Add-MailboxPermission.

Where is the AD server located?

on the same subnet?

Are there access issues there?

To test if it's a connectivity issue, use PortQry to check for connectivity issues. You can download it from Microsoft. Test ports 389 (LDAP) and 3268 (Global Catalog). There are other possible ports, but these are the main ones used.

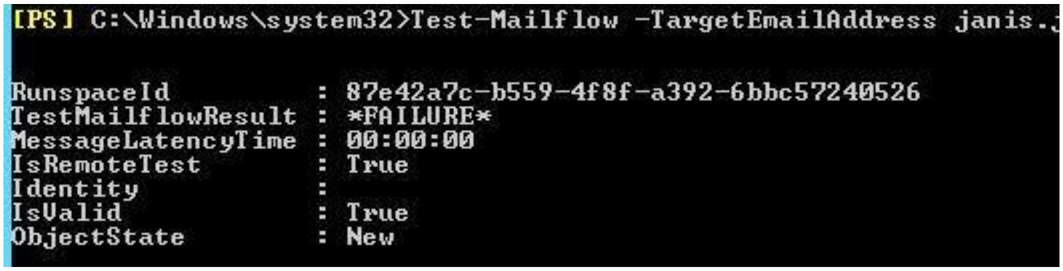
On the related issue when you have trouble with Exchange performance itself, see Troubleshooting performance issues with Exchange when RPC request spike high.

Messages Stuck in OWA DRAFTS Debugging

Messages stuck in OWA's DRAFTS folder (Post Exchange 2013 CU6 update)

If CU6 failed on the mailbox role, the solution is: remove the Discovery mailbox. Then setup successfully completes. Remember to recreate the discovery mailbox!

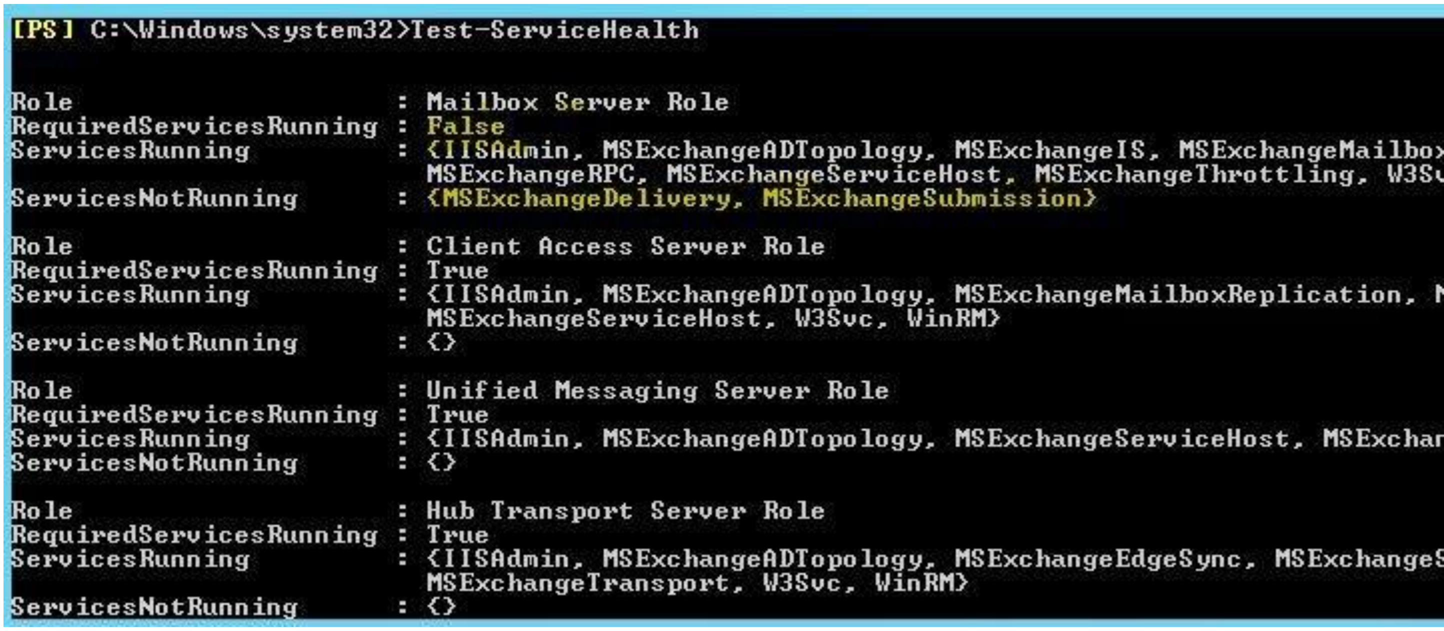
Restarting the Exchange servers, mail can be stuck in the drafts folder. I tested mailflow using the "test-mailflow" cmdlet, and saw it failed (not that stuck messages in OWA weren't enough):



```
[PS] C:\Windows\system32>Test-Mailflow -TargetEmailAddress janis.


RunspaceId            : 87e42a7c-b559-4f8f-a392-6bbc57240526
TestMailflowResult    : *FAILURE*
MessageLatencyTime    : 00:00:00
IsRemoteTest          : True
Identity              :
IsValid               : True
ObjectState           : New
```

Check for DNS or Security policy problems.

If this is not the case then check if all services are running: "Test-ServiceHealth"



```
[PS] C:\Windows\system32>Test-ServiceHealth


Role                      : Mailbox Server Role
RequiredServicesRunning   : False
ServicesRunning           : {IISAdmin, MSExchangeADTopology, MSExchangeIS, MSExchangeMailbo
                            MSExchangeRPC, MSExchangeServiceHost, MSExchangeThrottling, W3Sv
ServicesNotRunning        : {MSExchangeDelivery, MSExchangeSubmission}

Role                      : Client Access Server Role
RequiredServicesRunning   : True
ServicesRunning           : {IISAdmin, MSExchangeADTopology, MSExchangeMailboxReplication, M
                            MSExchangeServiceHost, W3Svc, WinRM}
ServicesNotRunning        : {}

Role                      : Unified Messaging Server Role
RequiredServicesRunning   : True
ServicesRunning           : {IISAdmin, MSExchangeADTopology, MSExchangeServiceHost, MSExchar
ServicesNotRunning        : {}

Role                      : Hub Transport Server Role
RequiredServicesRunning   : True
ServicesRunning           : {IISAdmin, MSExchangeADTopology, MSExchangeEdgeSync, MSExchangeS
                            MSExchangeTransport, W3Svc, WinRM}
ServicesNotRunning        : {}
```

In this case two services are disabled: MS Exchange Transport Delivery (MSExchangeDelivery) and MS Exchange Transport Submission (MSExchangeSubmission.) Restarting those services makes the mail flow once more!