# Exchange 2010 Permissions Debugging Protocol

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 | Full access | It's basically a migration in reverse, so you use the same permissions as a migration, UNLESS the user account is already disabled. In that case, you need full access |

| | | |
|---|---|---|
| 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
```

## Full Access, Send-as, Receive-as

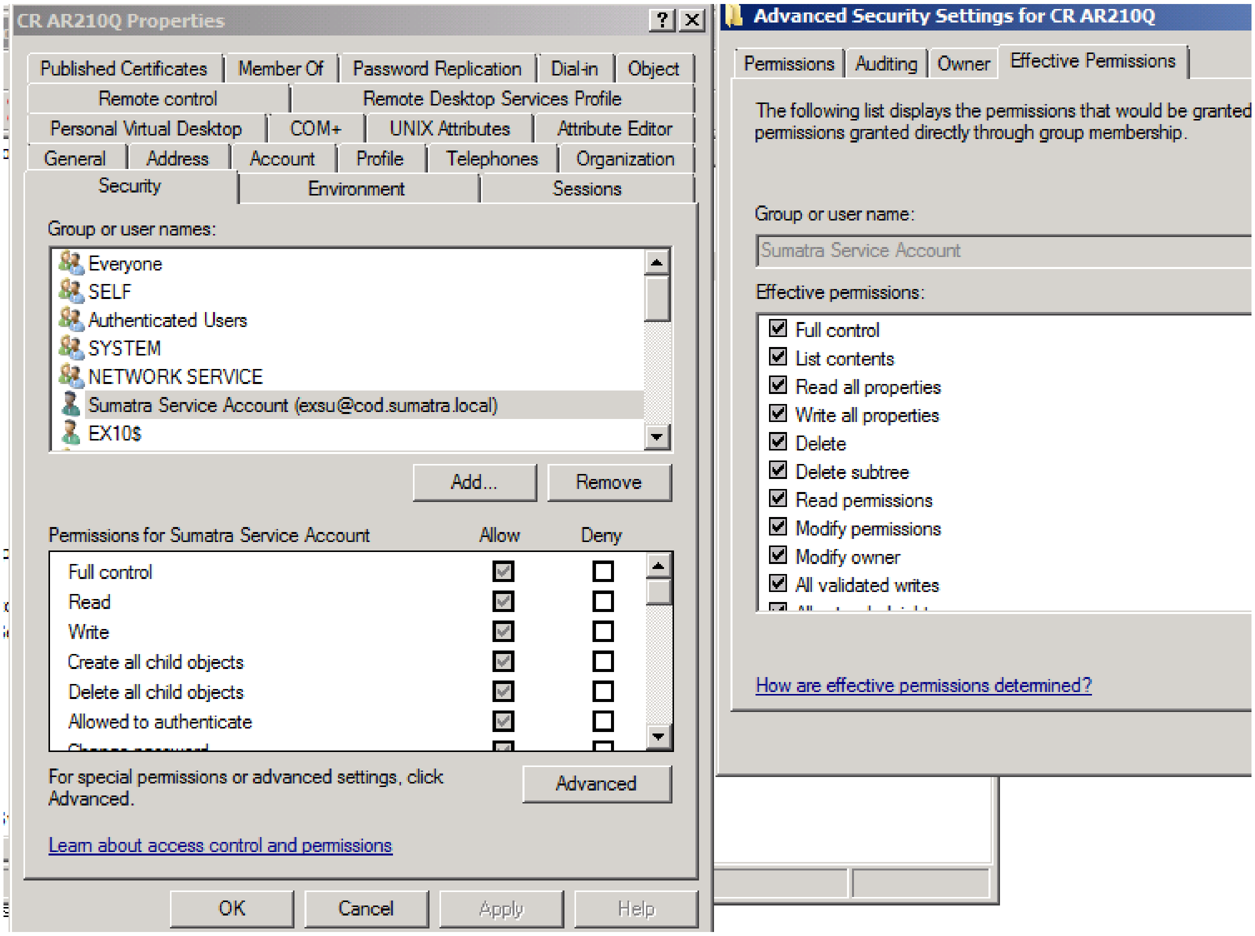
Full Access grants the service account permission to access the user account. Full access allows you to read from and write to folders in both enabled and disabled accounts. If you are just cancelling meetings from the conference room, full access is sufficient. If you want to send mail on behalf of 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!



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.

Learn about access control and permissions

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

How are effective permissions determined?

## Add Send-as, Receive-as

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

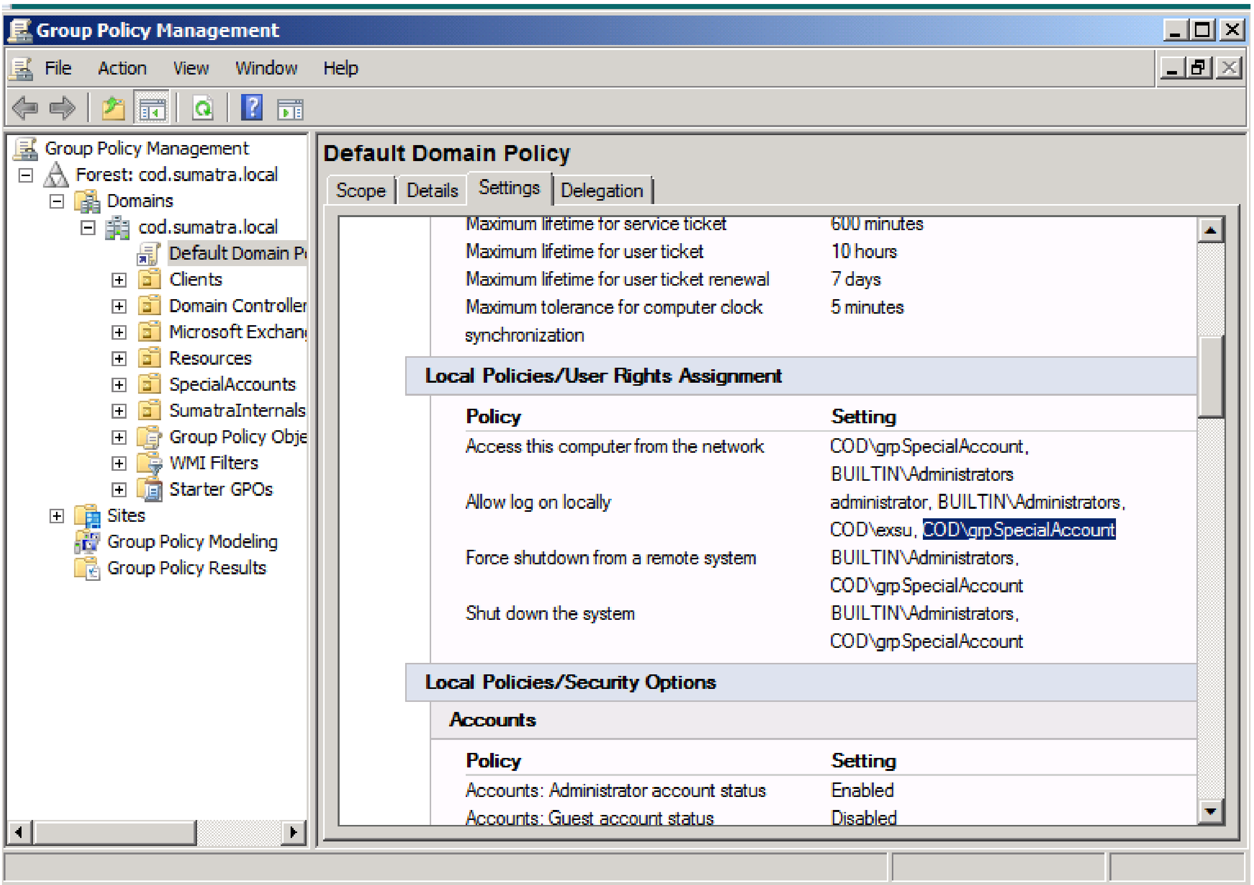
```
Add-ADPermission
   “CR 101B”
   -user: exsu
   -AccessRights:  genericall
   -ExtendedRights: "receive as","send as",
                    "ms-exch-epi-may-impersonate","ms-exch-epi-impersonation"
   -InheritanceType: All
```

## 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

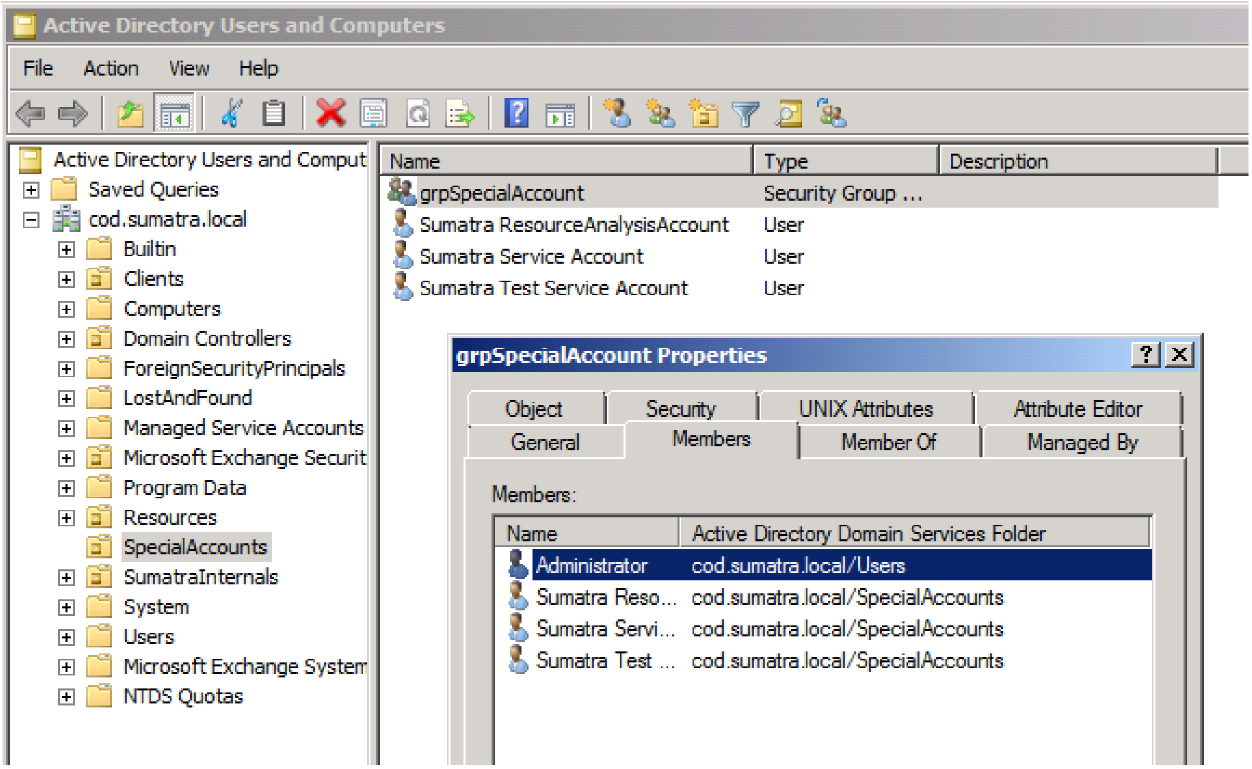
| Policy | Setting |
|---|---|
| Access this computer from the network | COD\grpSpecialAccount, BUILTIN\Administrators |
| Allow log on locally | administrator, BUILTIN\Administrators, COD\exsu, COD\grpSpecialAccount |
| Force shutdown from a remote system | BUILTIN\Administrators, COD\grpSpecialAccount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



Active Directory Users and Comput
- Saved Queries
- cod.sumatra.local
  - Builtin
  - Clients
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - Managed Service Accounts
  - Microsoft Exchange Securit
  - Program Data
  - Resources
  - SpecialAccounts
  - SumatraInternals
  - System
  - Users
  - Microsoft Exchange System
  - NTDS Quotas

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

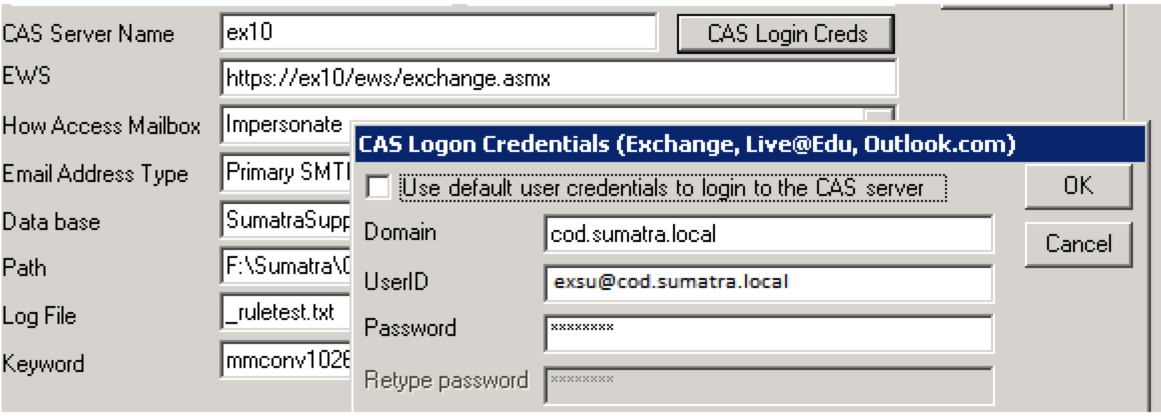
grpSpecialAccount Properties

Members:

| 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.



| | |
|---|---|
| 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@cod.sumatra.local |
| Password | ********* |
| Retype password | ********* |

## STILL having a 401 error?

If you are using Windows Server 2008 on your client – this could be due to changes in the default .NET crypto library.

In this case you need to log in to the service account using your Default User Credentials

**To DO this:**

1. Log into the term server/client box using the Sumatra Service Account
2. Launch SuExchange.
    a. Open the CAS Logon Creds,
        i. Ensure the Domain and Userid are set to your service account,
        ii. CLEAR the password box. (Repeat: Make sure the Password box is BLANK so it does not get saved!)
    b. THEN check the "Use default user credentials… " box.
    c. Click OK.
    d. SAVE your configuration.
3. Exit SuExchange
4. Re-launch SuExchange.

## Exchange 2010: 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 | PowerShell | For applications like the cmdlet always run Windows PowerShell in the "Run as Administrator" mode. |
| | Service account not allowed 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. |
| | Windows  authentication is not enabled for the EWS virtual directory in IIS<br>--or--<br>suExchange is using Basic authentication | Set Windows authentication in IIS; remember to restart IIS.<br>Edit _config_SuExchange.xml. Set "HTTPAuthType" to Negotiate. Exit suExchange and re-test. |
| | The "Service Account" cannot login to that domain (often because its primary SMTP is different…) | If you have multiple domains, and the service account's primary SMTP account is on a different domain, use that domain and SMTP account, not the domain you are targeting for insertion. Do you have multiple domains? See below. |
| | 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 credentials to ensure the password is correct. Paste the "EWS url" into a browser. Enter the service account credentials, when prompted. Do you see a EWS WSDL page? (Note: this could show up as a 500 error in some instances.) |

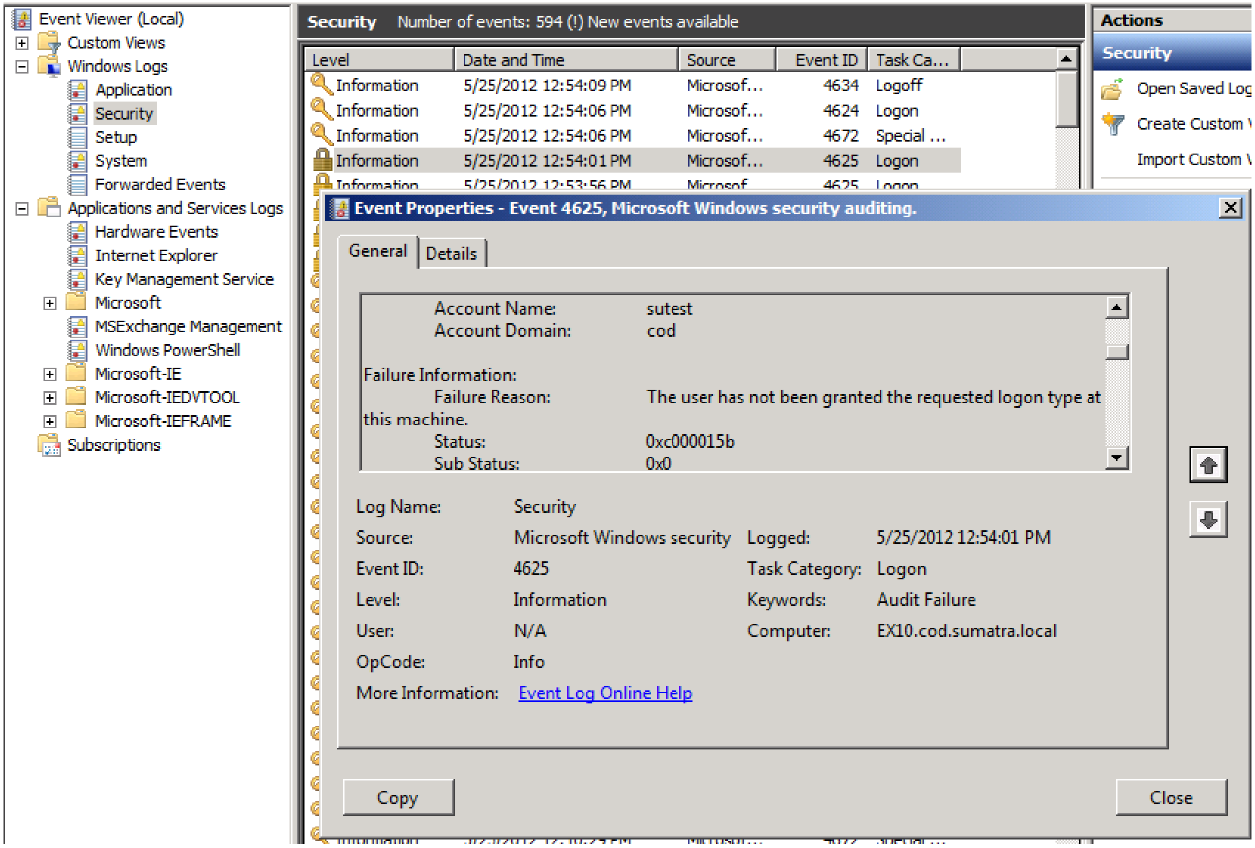
| | | |
|---|---|---|
| | All above checks and you still get a 401 error. | Log in with the service account.<br>Use OWA to access to a known valid user account.<br>IF THIS WORKS: then the service account credentials are valid and it is an issue passing to Exchange.<br>So use the full DOMAIN\service account format when logging in. |
| 500 | The "test user" does not exist in Exchange<br>or<br>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. |
| | SOAP Request rejected | If your logs tell you the SOAP request has been rejected with a 500 error, try the SMTP address, not the UPN.  Why? Because MS Exchange Web Services requires a primary SMTP address to be used for “impersonation”.  This usually happens in cases with multiple domains, see below. |

## Basic debugging protocol – 401 error

Open a browser window, and try to open your 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://ex10/ews/exchange.asmx](http://ex10/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

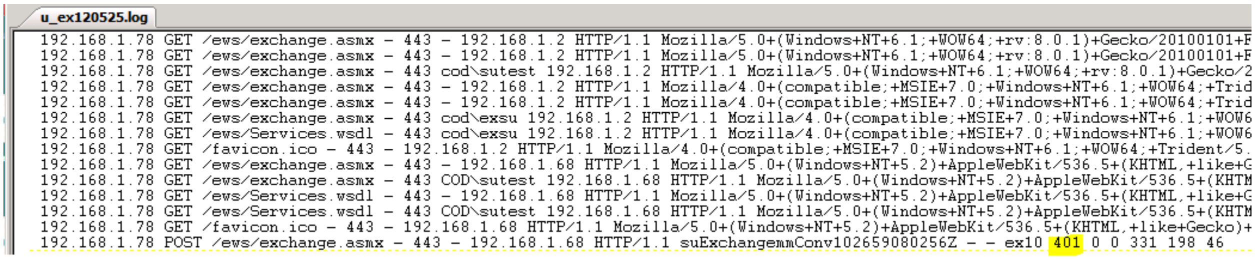
## Issue: EWS Virtual Directory Authentication

**The HTTP Authentication method set in IIS and SuExchange MUST agree** 401 errors usually result when each is set for a different HTTP Authentication method.

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 between IIS and SuExchange.

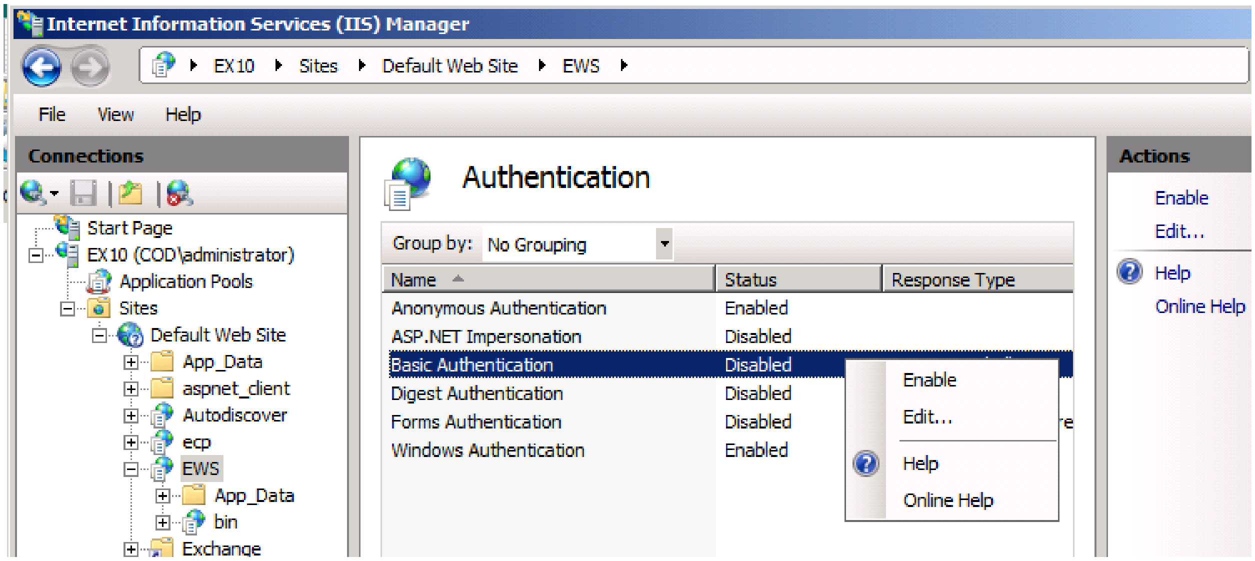
If you are getting a 401 error, either ensure the IIS virtual directory includes Basic authentication[1], or change the Sumatra tool to use "Negotiate" authentication.

If you change the EWS virtual directory to enable Basic authentication, 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
```

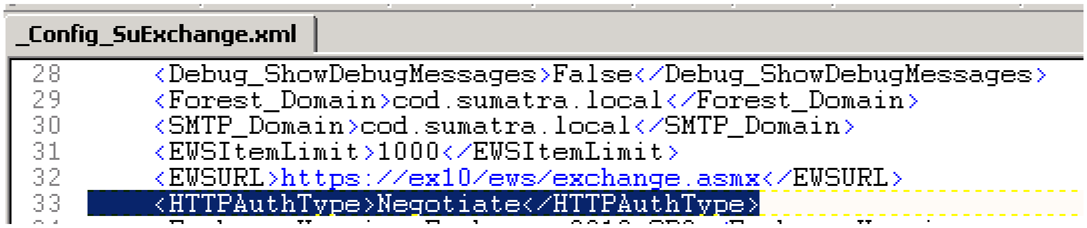


| Name | Status | Response Type |
|---|---|---|
| Anonymous Authentication | Enabled | |
| ASP.NET Impersonation | Disabled | |
| Basic Authentication | Disabled | |
| Digest Authentication | Disabled | |
| Forms Authentication | Disabled | |
| Windows Authentication | Enabled | |

[1] Microsoft changed the default authentication methods for the EWS virtual directory in Exchange 2010 Sp1+. Basic Authentication is no longer the default setting for the EWS directory. See: http://technet.microsoft.com/en-us/library/gg247612.aspx

Changing HTTP Authentication for EWS Virtual Directory Authentication in the SuExchange XML Configuration.

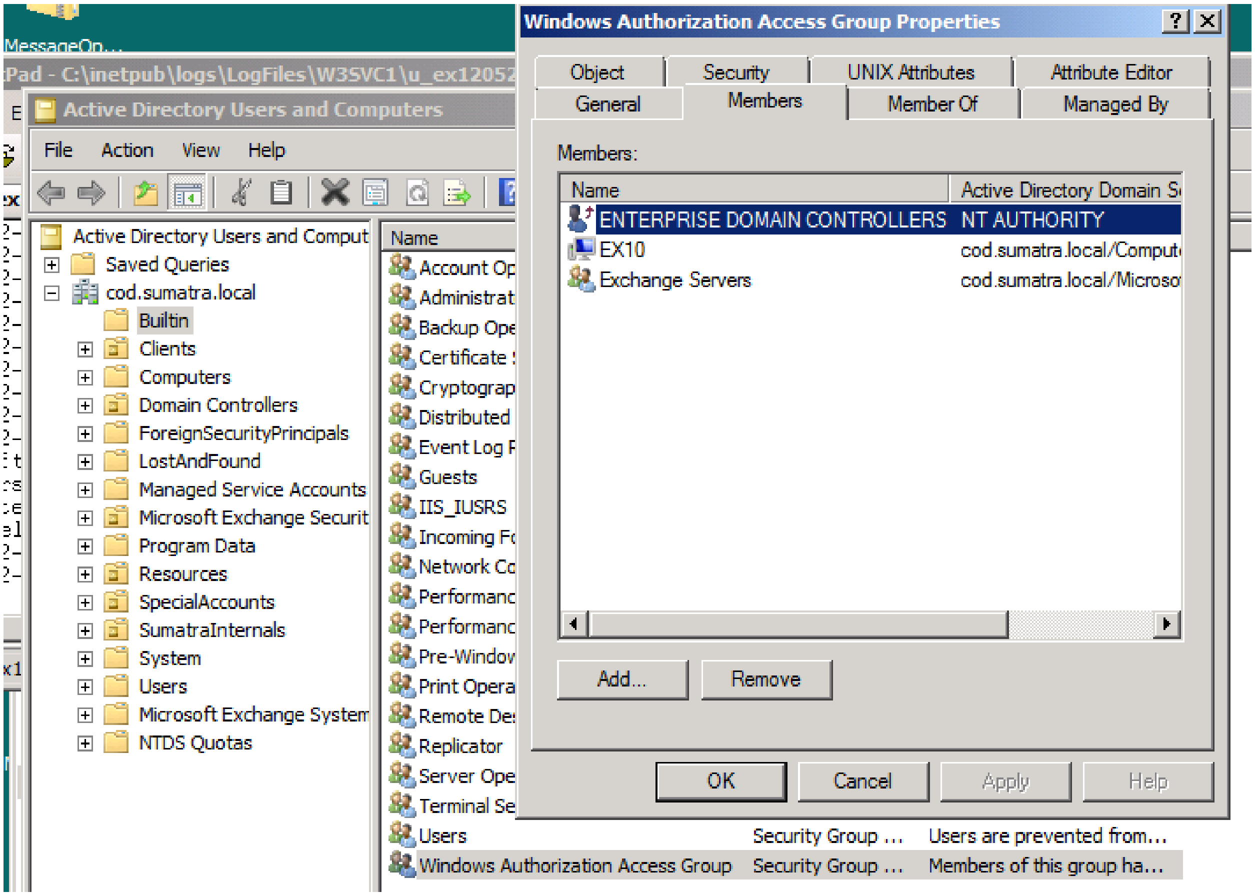
If you want to change SuExchange to match IIS, edit the _config.xml file, and ensure “HTTPAuthType” is set to Negotiate.  (If Basic is enabled, you can set the HTTPAuthType to Basic.)  The default is now “Negotiate” in suExchange builds 3.3.19+.  (Basic was the default in prior builds.)



```
        <Debug_ShowDebugMessages>False</Debug_ShowDebugMessages>
        <Forest_Domain>cod.sumatra.local</Forest_Domain>
        <SMTP_Domain>cod.sumatra.local</SMTP_Domain>
        <EWSItemLimit>1000</EWSItemLimit>
        <EWSURL>https://ex10/ews/exchange.asmx</EWSURL>
        <HTTPAuthType>Negotiate</HTTPAuthType>
```

## 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.



Windows Authorization Access Group Properties

Members:

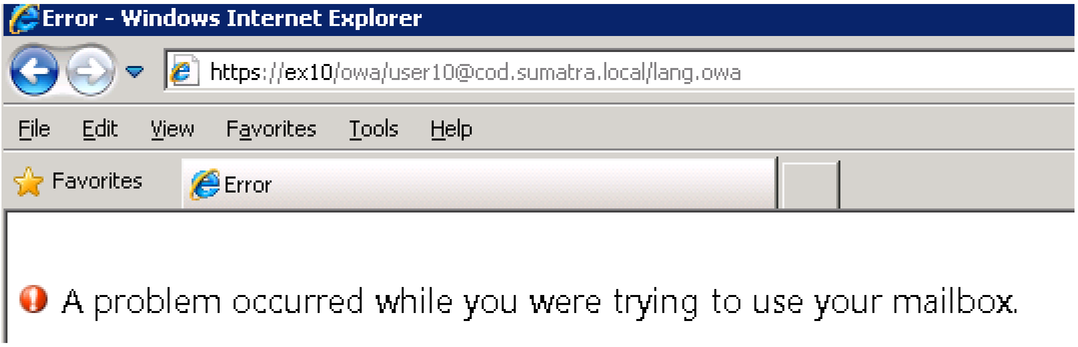
| Name | Active Directory Domain S |
|---|---|
| ENTERPRISE DOMAIN CONTROLLERS | NT AUTHORITY |
| EX10 | cod.sumatra.local/Comput |
| Exchange Servers | cod.sumatra.local/Microso |

| Name | | |
|---|---|---|
| Account Op | | |
| Administrat | | |
| Backup Ope | | |
| Certificate : | | |
| Cryptograp | | |
| Distributed | | |
| Event Log F | | |
| Guests | | |
| IIS_IUSRS | | |
| Incoming Fo | | |
| Network Co | | |
| Performanc | | |
| Performanc | | |
| Pre-Window | | |
| Print Opera | | |
| Remote Des | | |
| Replicator | | |
| Server Ope | | |
| Terminal Se | | |
| 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

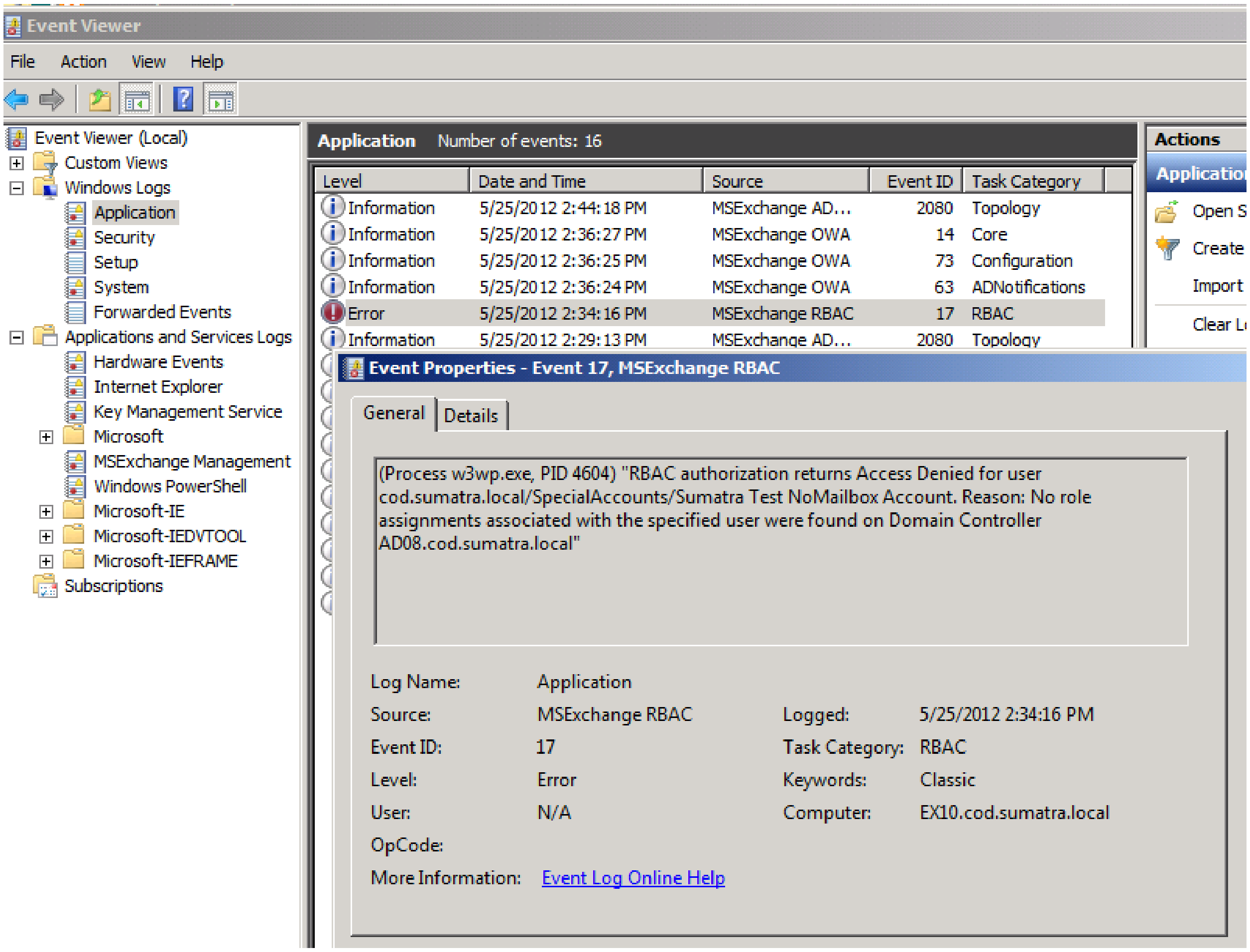
If you are still getting a 500 error, try logging into an active end user's mailbox via OWA (like your own!) using the service account credentials.  If you see an error in OWA:



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 |

(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.)