# Creating Tenants for Exchange 2010 SP2 Multi Tenant

Submitted by jdixon on Tue, 01/03/2012 - 8:04pm
Exchange 2010

Exchange 2010 SP2 has been released! Sucks for some of us using /hosting since there isn't really a good migration path other than doing a forest migration. Anyways, SP2 has been released and we get the EMC back, and also some more roles such as the unified messaging role!

Most automation software [as of 1/2/2012] do not support SP2 yet. Some that currently do are ExtendASP, and I believe Machsol will in a couple of weeks. Personally I have not used either.

Anyways you can still separate your tenants manually without using a automation software but it is more complex and requires more steps than Exchange /hosting did. You will have to create multiple address lists and also use custom attributes. You can read the documentation at Download: Exchange 2010 SP2 Multi-Tenant Scale Guidance … [1]

Note: Lync is supposed to be coming out with a hosting pack and requires a specific active directory organizational unit structure to work. I do not have this information so you may want to wait if you plan on deploying Lync Hoster pack with Exchange 2010 SP2.

Here are some things you will need to create:

- A tenant organizational unit
- Accept SMTP domain
- Global Address List
- Address List for "All Rooms", "All Users", "All Contacts" and "All Groups"
- Offline Address Book
- Address Book Policy

I am currently working on a powershell script to automate this process and will post it once I finish. Below are the commands to create what you need. Just replace some of the things such as the name of the tenant I used along with the domain names. Also I used CustomAttribute1 but you can of course use any of the custom attributes [1-15].

Create an OU for the tenant. I placed mine under a OU called 'Tenants'

Notes:

- I used the parent OU as 'Tenants'. Lync has certain requirements for the hoster pack that I haven't read yet.
- Be sure to change the domain to your local domain name
- Each user must have the address book policy assigned to the user for that specific Tenant
- Each user must also have the CustomAttribute1 set to the Tenant name
- Each user must have the UPN suffix set for that specific Tenant

**Import-Module ActiveDirectory**
**$connect = "LDAP://<domain controller>/OU=Tenants,DC=cloud,DC=local"**
**$ad = [ADSI]$connect**
**$ou = $ad.Create("OrganizationalUnit", "ou=New Tenant 1")**
**$ou.SetInfo()**

Now you must create the UPN:

**Set-ADForest -Identity cloud.local -UPNSuffixes @{Add="newtenant1.com"}**

Create Accepted Domain

***New-AcceptedDomain -Name "New Tenant 1" -DomainName newtenant1.com -DomainType:Authoritative***

Create Global Address List

***New-GlobalAddressList -Name "New Tenant 1 - GAL" -ConditionalCustomAttribute1 "New Tenant 1" -IncludedRecipients MailboxUsers -RecipientContainer "cloud.local/Tenants/New Tenant 1"***

Create All Rooms Address List

***New-AddressList -Name "New Tenant 1 - All Rooms" -RecipientFilter "(CustomAttribute1 -eq 'New Tenant 1') -and (RecipientDisplayType -eq 'ConferenceRoomMailbox')" -RecipientContainer "cloud.local/Tenants/New Tenant 1"***

Create All Users Address List

***New-AddressList -Name "New Tenant 1 - All Users" -RecipientFilter "(CustomAttribute1 -eq 'New Tenant 1') -and (ObjectClass -eq 'User')" -RecipientContainer "cloud.local/Tenants/New Tenant 1"***

Create All Contacts Address List

***New-AddressList -Name "New Tenant 1 - All Contacts" -RecipientFilter "(CustomAttribute1 -eq 'New Tenant 1') -and (ObjectClass -eq 'Contact')" -RecipientContainer "cloud.local/Tenants/New Tenant 1"***

Create All Groups Address List

***New-AddressList -Name "New Tenant 1 - All Groups" -RecipientFilter "(CustomAttribute1 -eq 'New Tenant 1') -and (ObjectClass -eq 'Group')" -RecipientContainer "cloud.local/Tenants/New Tenant 1"***

Create the Offline Address Book

***New-OfflineAddressBook -Name "New Tenant 1" -AddressLists "New Tenant 1 - GAL"***

Create the Email Address Policy

**New-EmailAddressPolicy -Name "New Tenant 1 - EAP" -RecipientContainer "cloud.local/Tenants/New Tenant 1" -IncludedRecipients "AllRecipients" -ConditionalCustomAttribute1 "New Tenant 1" -EnabledEmailAddressTemplates "SMTP:%m@newtenant1.com","smtp:%g.%s@newtenant1.com"**

Create the Address Book Policy

***New-AddressBookPolicy -Name "New Tenant 1" -AddressLists "New Tenant 1 - All Users", "New Tenant 1 - All Contacts", "New Tenant 1 - All Groups" -GlobalAddressList "New Tenant 1 - GAL" -OfflineAddressBook "New Tenant 1" -RoomList "New Tenant 1 - All Rooms"***

Create the First User

**$c = Get-Credential**
**$u = New-Mailbox -Name 'Tenant 1 User 1' -Alias 'tenant1user2' -OrganizationalUnit 'cloud.local/Tenants/New Tenant 1' -UserPrincipalName 'tenant1user2@newtenant1.com' -SamAccountName 'tenant1user2' -FirstName 'Test' -Initials '1' -LastName 'User 2' -Password $c.password -ResetPasswordOnNextLogon $false -AddressBookPolicy 'New Tenant 1'**

**Set-Mailbox $u -CustomAttribute1 "New Tenant 1"**

Be sure to run ***Update-OfflineAddressBook*** after creating everything. Also when creating mailbox users you must put the tenant's name in the mailbox CustomAttribute1.

Keep in mind there can be other settings that need to be set to make sure your users do not have access to other tenants. This is where the automation software comes in with creating group policies that make sure some users (like RDP users) cannot access or see the other tenants, not to mention the fact that it would just make your life easier.

**********

***UPDATED* 3/17/2012**

**Below are the changes:**

- **Fixed error that was caused by entering the display name as 'Lastname, First'. It will now set the Name to 'Firstname Lastname' and set the DisplayName to what you specify, even if it is with a comma.**

***UPDATED* 3/16/2012**

**Below are the changes:**

- **New powershell script to secure the root OAB container (Secure-DefaultOAB)**
- **Modified New-Tenant script to put 'Username_Domain.ext' for the samAccountName. So if I created a domain called itswapshop.com and a user called Jacob Dixon then it will set the samAccountName to: jdixon_itswapshopcom (20 characters max... if over then it will trim it automatically)**
- **Modified New-Tenant script to no longer include an email address policy. Instead when creating a tenant the administraotr mailbox primary smtp address is set to administrator@domain.com[2].**
- **Modified New-User script with the same samAccountName changes as well not using an email address policy. Instead it will put the primary smtp address to <first initial><last name>@<domain>.<ext>. Example:jdixon@itswapshop.com[3]**
- **Modified New-Tenant to grant the ALL USERS group for that tenant to be able to download the OAB for that specific tenant.**
- **Modified New-Tenant to specify the OAB when creating the user**
- **Modified New-User to specify the OAB when creating the user**

**Notes:**

1. **IF you used the previous script then it did not secure the OAB. You must do this manually. Remove the 'MS-EXCH-DOWNLOAD-OAB' extended right from the Authenticated Users group on the root container and all OABs. Then you must grant the specific All Users group for that tenant the extended right 'MS-EXCH-DOWNLOAD-OAB' for that tenants OAB.**
2. **The newest ZIP file is at the bottom of this article. It is labeled with todays date (3/16/2012). If you have any problems feel free to email me @jacobdixon@live.com [4] or post a comment here. Thanks!**

***UPDATED* 3/3/2012**

**I have replaced the orginial New-Tenant powershell script and added one for removing tenants and adding new users.**

**Some of the changes I have done is changed the OU in the script to "Hosting" for the parent OU. In each script I wrote examples of how to use it. Also it now creates two security groups. One is "Organization Management" and the other is "All Users" under each tenant. When you use the script to create a new user it automatically adds it to the All Users group and grants ORganization Management security group full access to that user. From there you can write your own web interface so the Administrator user can make changes to people in the "All Users" group. You WILL NOT be able to use OWA/ECP online to make these changes. Exchange 2010 SP2 is not setup this way and is why you need a control panel.**

**If you have any problems please let us know! You will find the new scripts in a ZIP file at the bottom of the article**

***UPDATED* 2/29/2012**

**I left out some important steps when I posted this article. I have updated the article and it now does not show the other address lists to the other users in Outlook.**

**I have also uploaded a powershell script I created. Keep in mind it doesn't do any error checking. It will create all the address lists, GAL, address book policies, and the administrator mailbox for you.**

**Be sure to run it rom the Exchange Shell and enter the commands before you run it:**
**Import-Module ActiveDirectory**
**Set-ExecutionPolicy RemoteSigned**

**File attachments:**
Exchange 2010 SP2 Powershell Scripts.zip[5]
Exchange 2010 SP2 PS 3-16-2012.zip[6]
Exchange 2010 SP2 PS 3-17-2012.zip[7]
.



---



**Links:**
[1] http://www.microsoft.com/download/en/details.aspx?id=28565
[2] mailto:administrator@domain.com
[3] mailto:jdixon@itswapshop.com
[4] mailto:jacobdixon@live.com
[5] http://itswapshop.com/sites/default/files/Exchange%202010%20SP2%20Powershell%20Scripts.zip
[6] http://itswapshop.com/sites/default/files/Exchange%202010%20SP2%20PS%203-16-2012.zip
[7] http://itswapshop.com/sites/default/files/Exchange%202010%20SP2%20PS%203-17-2012.zip