Create service account

A service account must be created for the sync client. This is a domain user that can be created using the built in tools of Windows Server, such as Active Directory Users and Computers.

The service account needs:

- A password that generally shouldn't expire
- A mailbox – This is for reviewer rights to be granted to the service account A mailbox is not required for running impersonation
- Local "run as a service" privileges if the sync service itself is to run in context of this account
- Privileges on contact calendars, either through impersonation or folder rights

Privileges can either be granted through impersonation or by giving the service account folder rights on the users calendars. In general there is slightly more administration when using folder rights as privileges must be set on individual mailboxes. This is also the most secure since impersonation rights are very powerful. Refer to the relevant chapters below based on the approach taken.

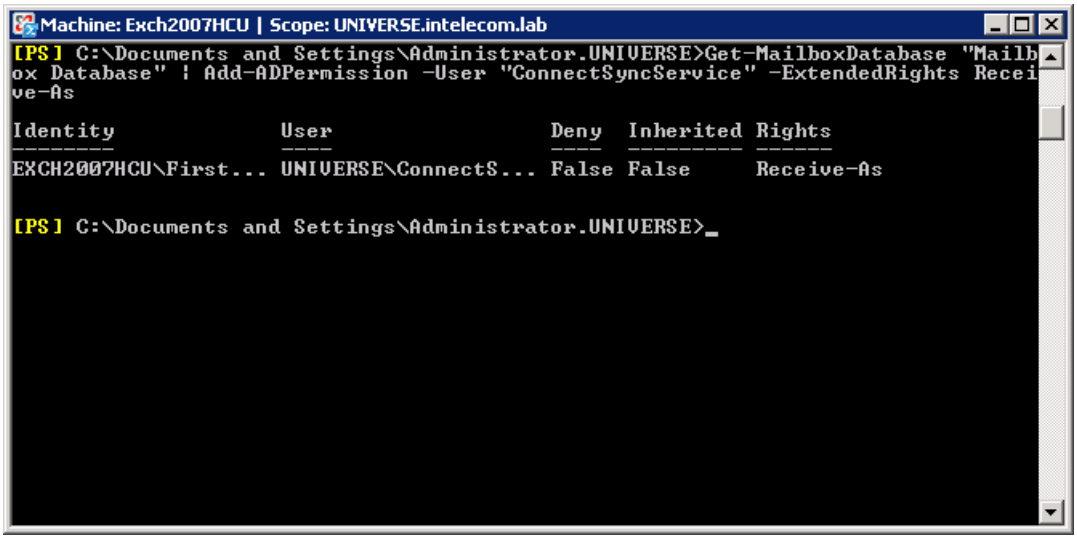
Option 1: Impersonation

To use impersonation the service account needs both Receive As and Impersonation permissions.

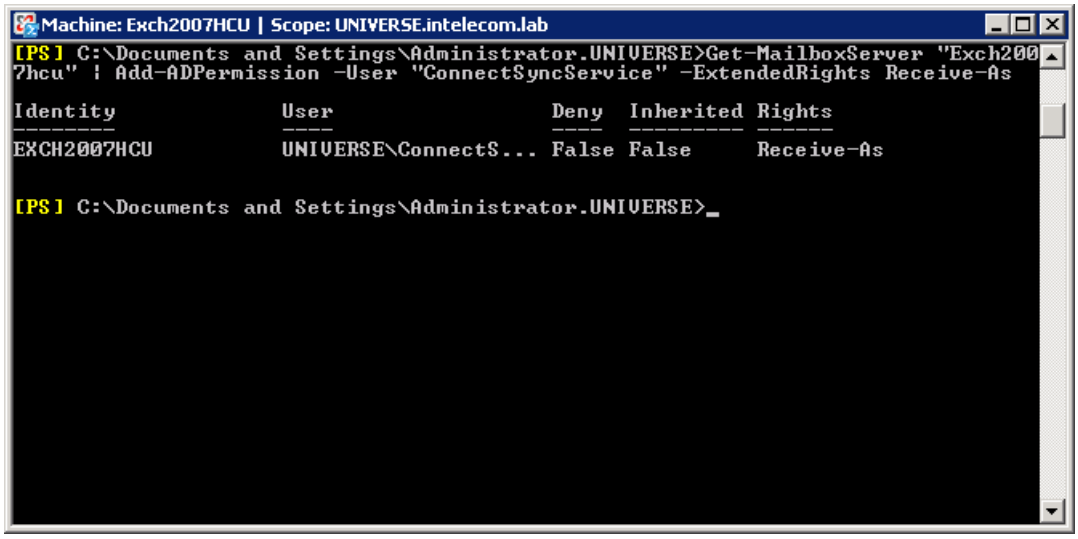
Receive As

To assign "receive as" permissions to a given user, run the following command for each database

Get-MailboxDatabase "Mailbox Database" | Add-ADPermission –User "Username" –ExtendedRights Receive-As

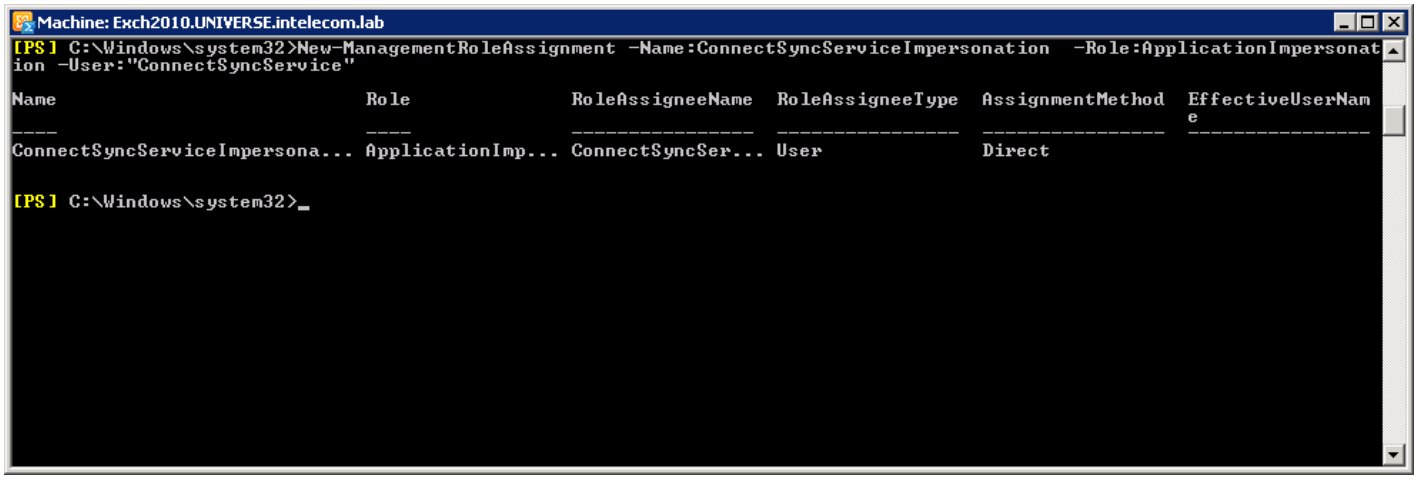


"Mailbox Database" is the database that the rights will be assigned on. Alternatively, assign the rights on all databases hosted on a given server:
Get-MailboxServer "Servername" | Add-ADPermission –User "Username" –ExtendedRights Receive-As



Impersonation

To set up impersonation, run the following command:
New-ManagementRoleAssignment -Name:"ImpersonationName" -Role:ApplicationImpersonation -User:"Username"



"ImpersonationName" must be a unique name that serves as the ID for this aassignment.

Option 2: Folder rights

The sync client will attempt to retrieve calendars without impersonation if "use impersonation" is not checked for the provider. Folder rights must be granted for the service account on every calendar that is to be synced. The following privileges are required per mailbox:

Object	Priviledge
"Top of information store" (Mailbox root)	Reviewer
Calendar	Reviewer

This will grant read access to these objects. The reason why the sync client requires reviewer rights on mailbox root is that it initially traverses the structure of each mailbox to find the ID of the calendar folder. Reviewer rights on the root will not grant read access to any subfolders.
Folder rights can be set using the "Add-MailboxFolderPermission" cmdlet.

An example of how to set these permissions for mailbox root and calendar per mailbox is provided below.

```
$serviceAccount = "serviceaccount@domain.topdomain"
$mailboxes = Get-Mailbox
Write-Host "Adding reviewer rights for mailboxes to" $serviceAccount
foreach ($mailbox in $mailboxes)
{
  Write-Host "Updating privileges for" $mailbox
  If ((Get-MailboxFolderPermission -Identity ${mailbox} -User $serviceAccount -EA    SilentlyContinue).AccessRights -notlike "Reviewer")
  {
     Write-Host "... Service account is not a reviewer on mailbox root. Adding privileges"
     Add-MailboxFolderPermission -Identity ${mailbox} -User $serviceAccount -AccessRights   Reviewer
  }
  Else
  {
     Write-Host "... Service account is allready a reviewer on mailbox root"
  }


  If ((Get-MailboxFolderPermission -Identity ${mailbox}:\Calendar -User $serviceAccount -EA SilentlyContinue).AccessRights -notlike "Reviewer")
  {
Write-Host "... Service account is not a reviever on calendar. Adding privileges"
     Add-MailboxFolderPermission -Identity ${mailbox}:\Calendar -User $serviceAccount - AccessRights Reviewer
  }
  Else
  {
     Write-Host "... Service account is allready a reviewer on calendar"
  }
}
```

This example and an example for removing the same privileges is also installed together with the sync client in the “Scripts” folder. These are named AddPrivileges.ps1 and RemovePrivileges.ps1.

It is likely that the script will have to be adapted before it can be used in different environments as different logic may apply for selecting appropriate mailboxes to add privileges on. In order for privileges to be set on new mailboxes this script should either be run when a new mailbox have been created or at some interval. Powershell scripts can be scheduled by using the Windows Task Scheduler.
To use folder rights the sync service account must have a mailbox in the Exchange organization.

