Forefront Identity Manager 2010 Installation & Configuration



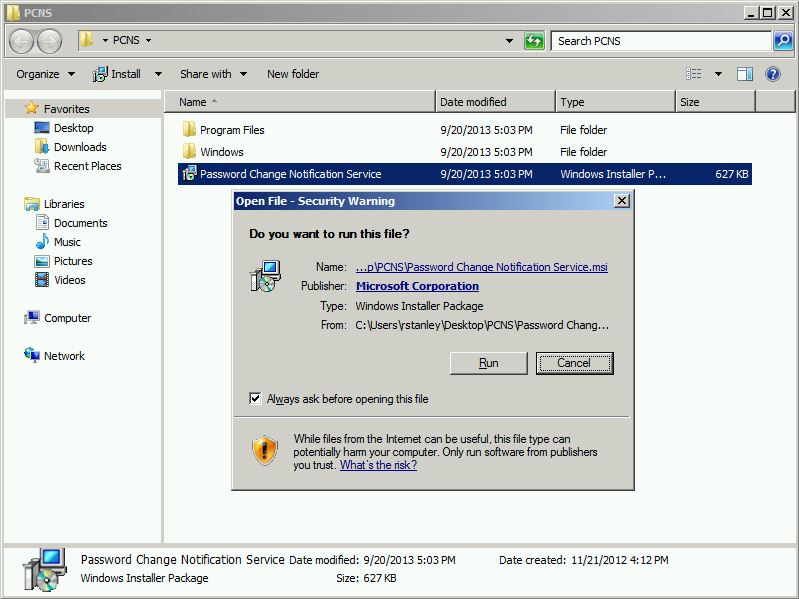
Implementing Password Synchronization with PCNS

**Anthony Marsiglia & Kristopher Tackett**

Microsoft Premier Field Engineering

Implementing Password Synchronization with PCNS

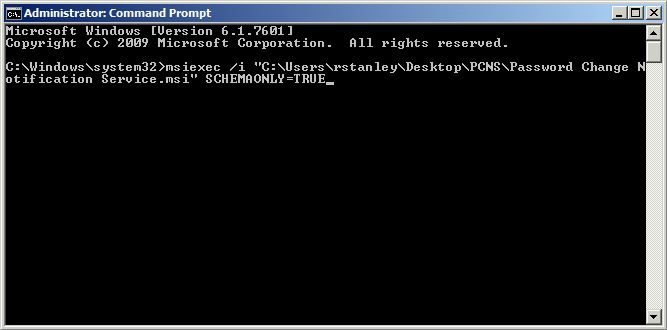
In this section we will cover the installation and configuration of the Password Change Notification Service (PCNS). To begin, navigate to a Domain Controller (DC) in the source forest. For PCNS to function, we must be able to capture the password change (whatever the mechanism) at the DC level. Therefore, the PCNS agent must be installed on each DC. After downloading the PCNS agent, double-click to open it, then select “Run”.



At this point, you may be notified that a schema extension is required.



If so, from an elevated command prompt, run the following command, as shown:

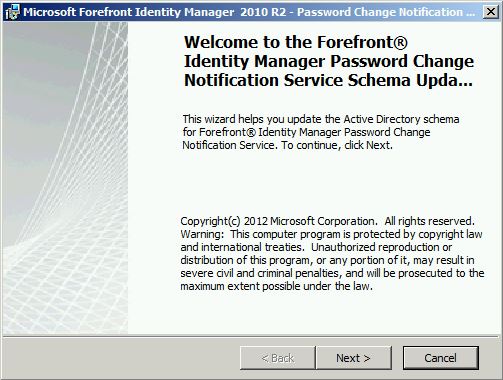


Format:

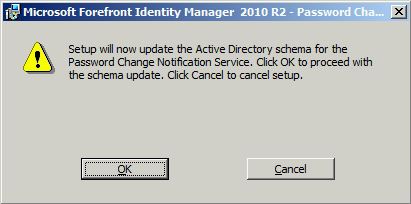
***msiexec /i <path of Password Change Notification Service.msi package> SCHEMAONLY = TRUE***

Please note that the account used needs to be a member of the “Schema Administrators” group in AD.

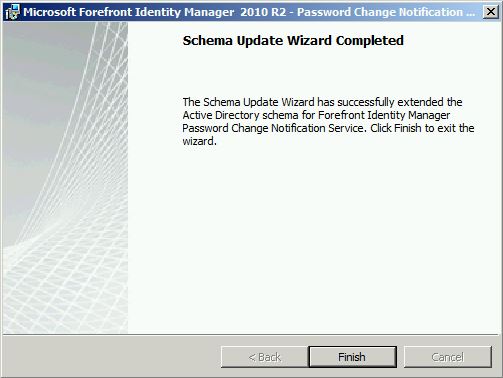
After entering the above command in an elevated command prompt, the schema update tool will open. Click “Next” to continue.



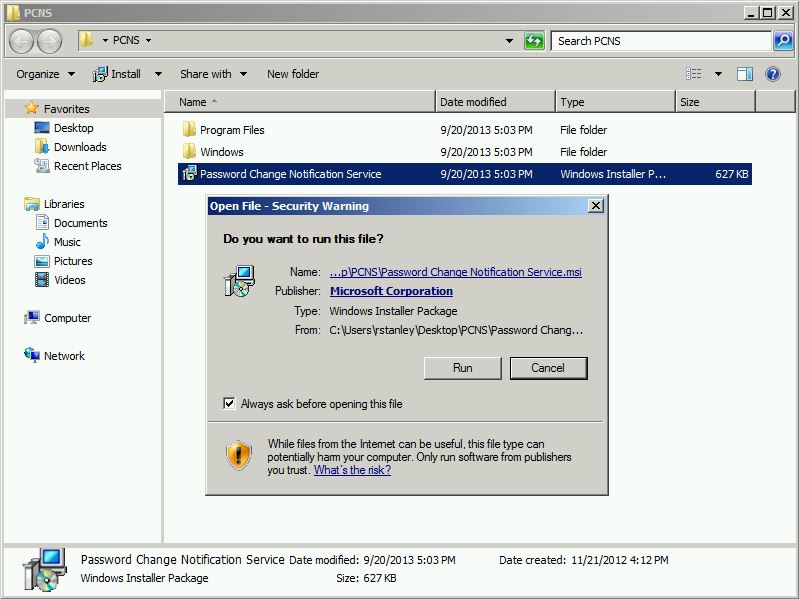
Click “OK”.



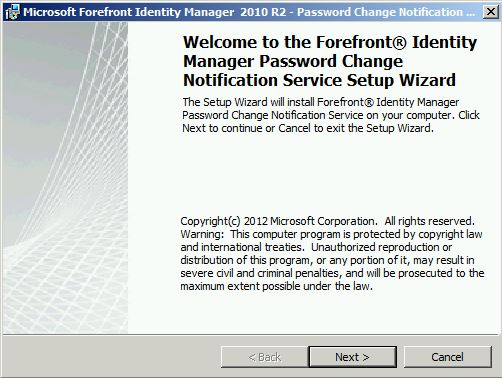
Click “Finish” to complete the schema update wizard.



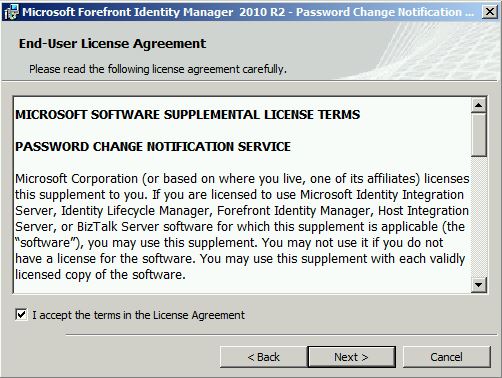
Now we will install the PCNS agent. Double click the installer again, and again click “Run”



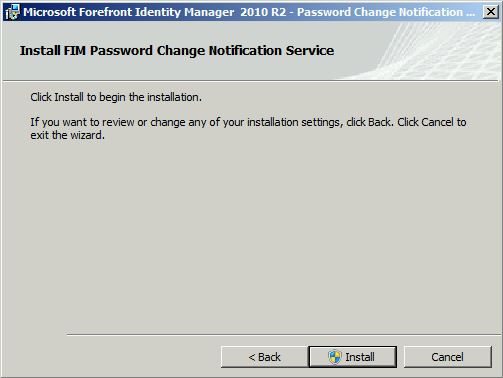
Click “Next” to continue.



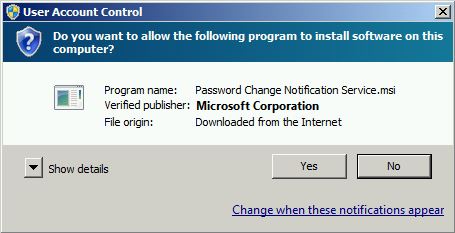
Read and accept the EULA, then click “Next”



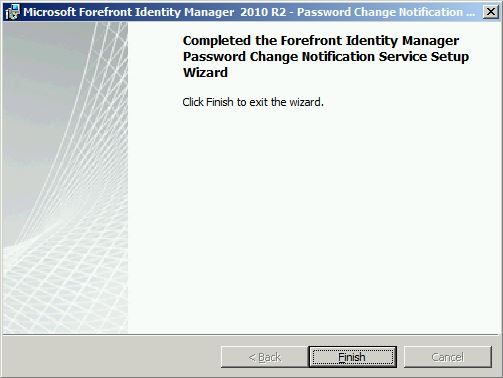
To begin the installation, click “Install”



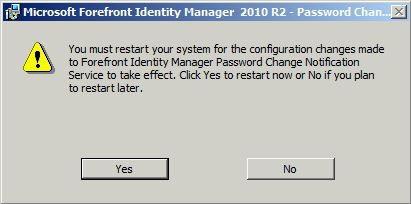
Click “Yes”



Click “Finish” to complete.

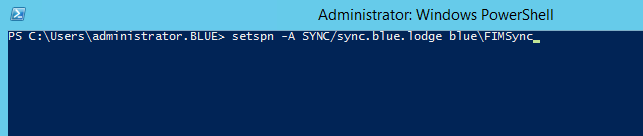


You will now be prompted to restart the machine.



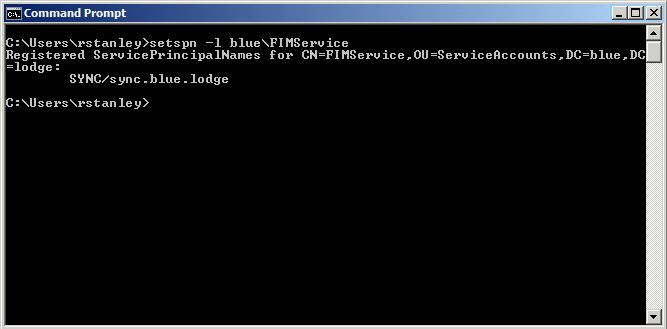
Now we must configure the Service Principal Name (SPN). The format for the SPN is as follows:

**Setspn.exe** <*user defined friendly name for FIM server*>/<*FQDN of FIM server*>\<*domain*>\<*FIM Sync account*>



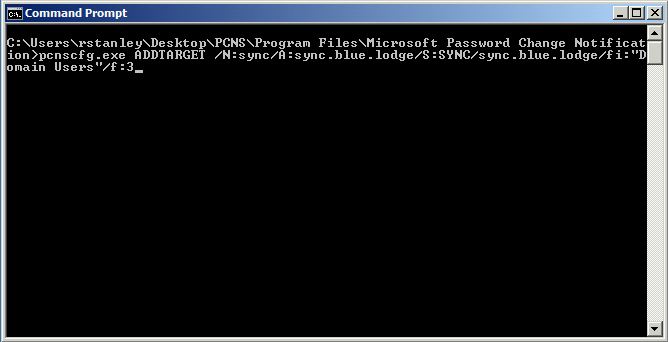
You can verify the SPN has been set correctly with:

**Setspn.exe –L**

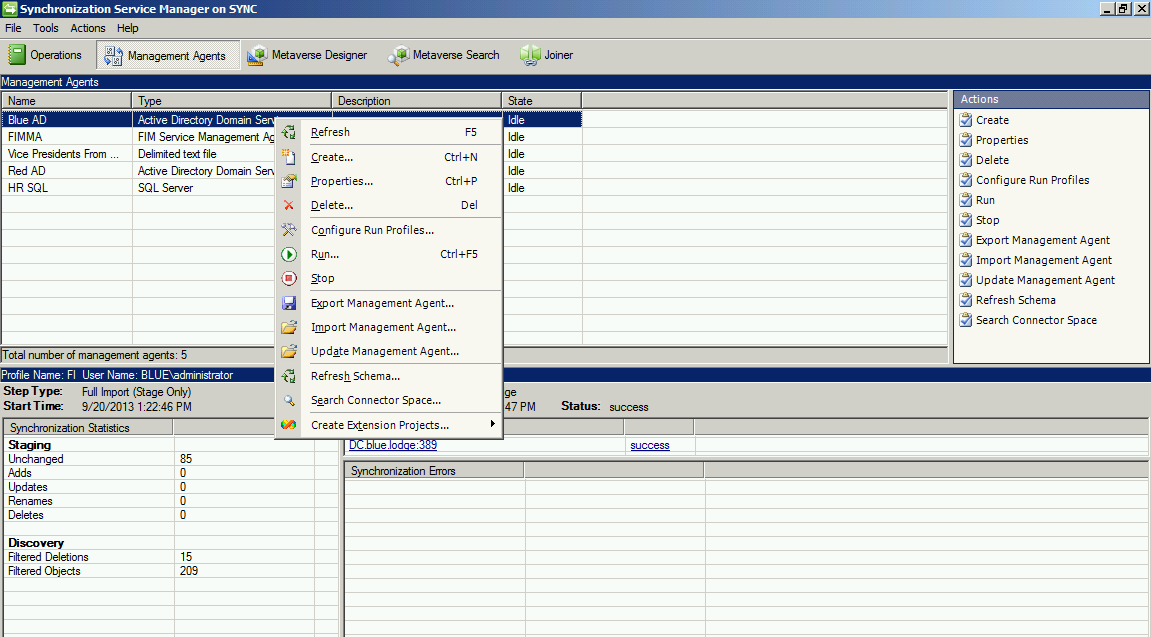


Now, we must configure the PCNS agent using PCNSCFG.exe. The command structure is as follows:

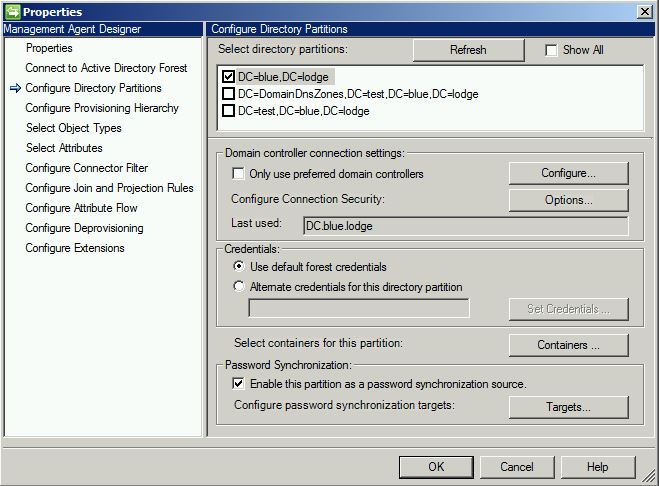
**Pcnscfg.exe addtarget** **/N:***<user define friendly name of the FIM server>***/A:***<FQDN of the FIM server>***/S:***<SPN we configured above>***/FI:***<group to include>***/F:3**



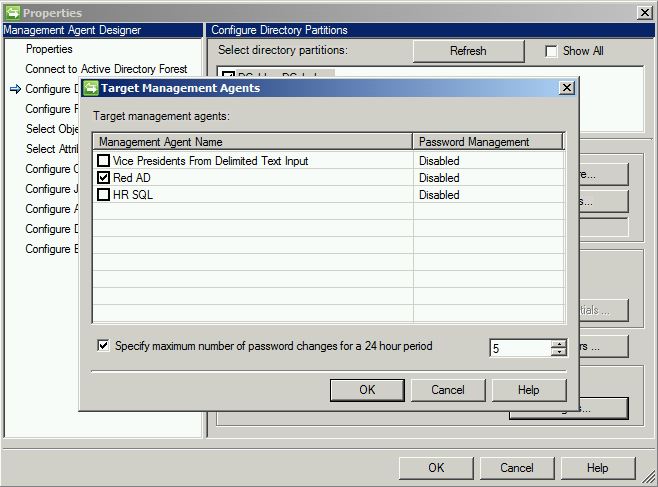
Finally, we must configure the Management Agents (MA) on the synchronization server. Start by navigating to your synchronization server, and right-click on the AD MA for the ***source*** forest, then select “Properties”.



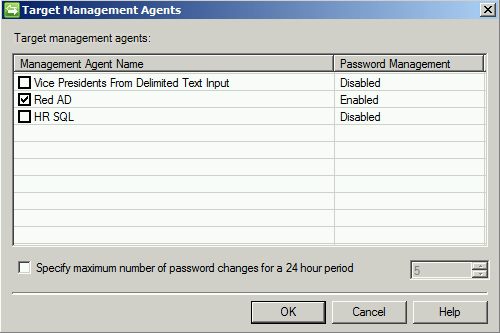
On the “Configure Directory Partitions” tab, check the box for “Enable this partition as a password synchronization source.”



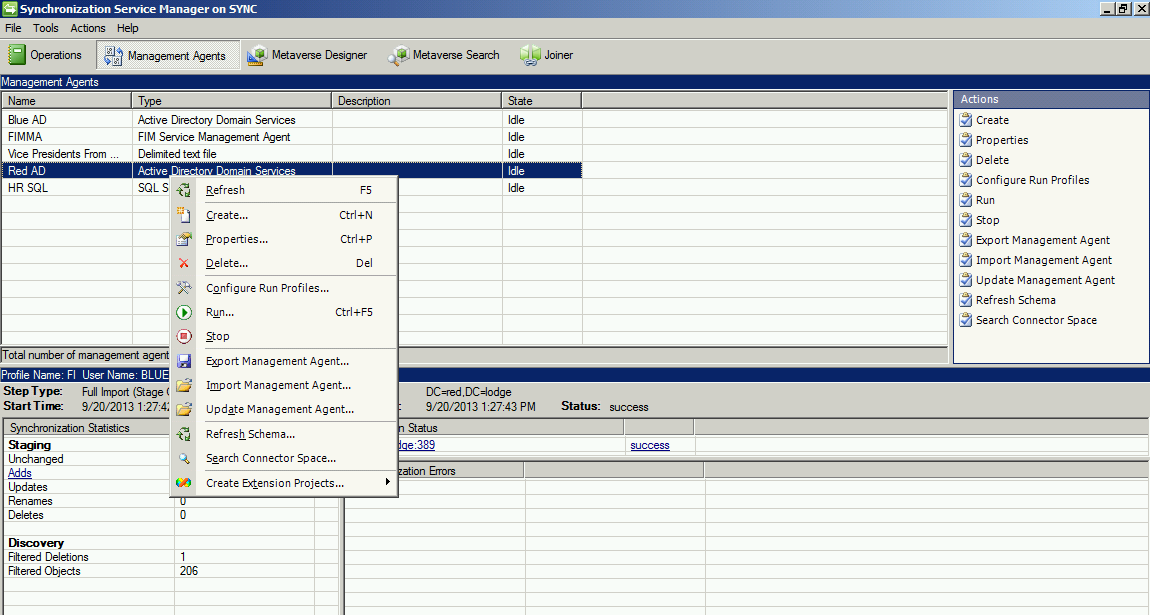
Next, click the “Target” box. From here, select the MA you wish to target to receive changed passwords.



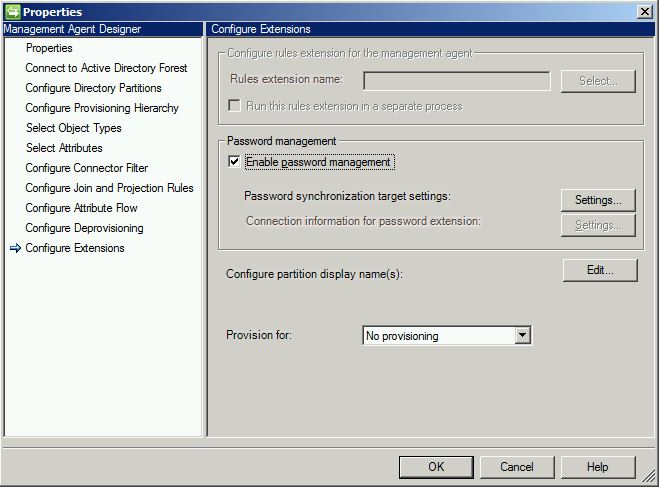
Notice that above, under “Password Management”, the target MA says “Disabled”. This is because, at this point, password synchronization is still disabled. However, once the target is selected and you click “OK”, if you re-open, you will see the value is now set to “Enabled”.



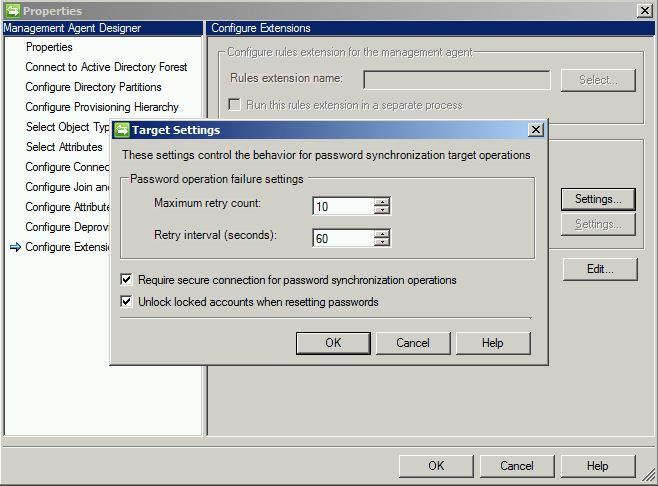
Next, right click on the ***target*** management agent and select “Properties”



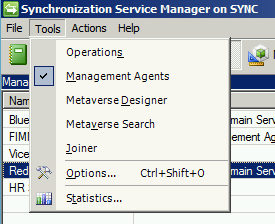
On the “Configure Extensions” tab, select “Enable password management”.



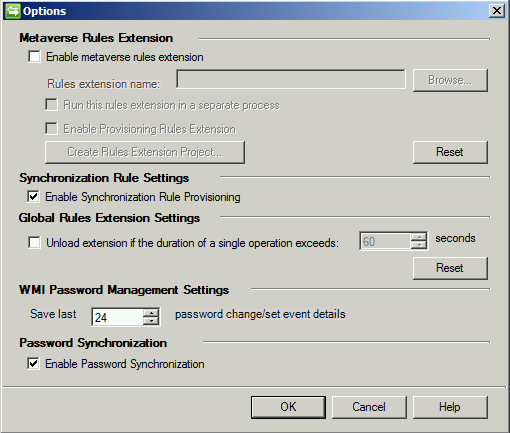
You may also click “Settings” for more granular configuration options.



From here, click on “Tools” and then “Options”.



Under “Password Synchronization”, select “Enable Password Synchronization”, then click “OK”.



At this point, you are ready to test functionality. To test, change the password of a user in the ***source*** forest, then attempt to login in with the same account and newly set password in the ***target***. If PCNS is functioning as intended, you should be able to successfully login.