Introduction

This document details the necessary tasks to be applied in the UDS Enterprise environment to perform a correct integration with an “Active Directory” server with LDAPS (LDAP over SSL) communication enabled.

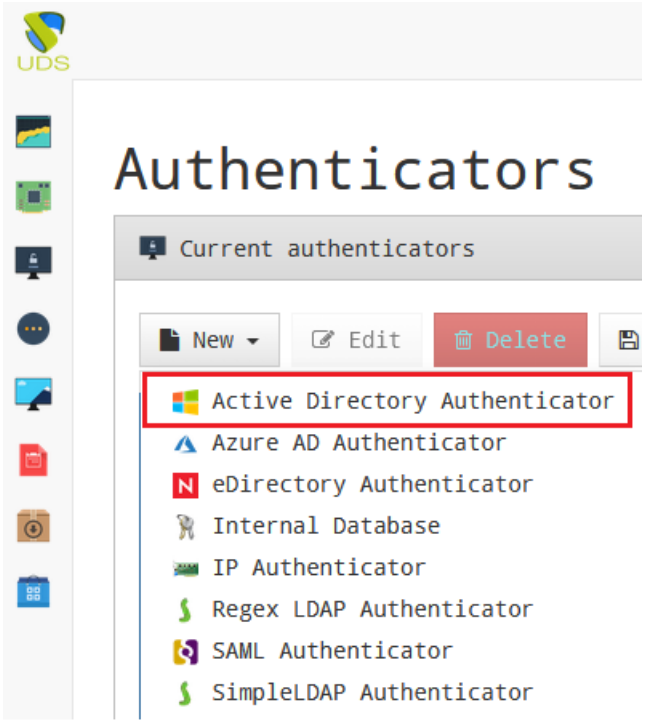
Once “Secure LDAP” (LDAPS) is enabled on the “Active Directory” server or servers, it will be necessary to modify two UDS components for complete the integration:

- **Authenticator “Active Directory”:** In the UDS dashboard we will have to enable the SSL communication.
- **OS Manager for Windows Domain:** A patch must be applied to allow machines registered in the Domain Controller to be automatically deleted and to allow machines to be assigned to a specific group.

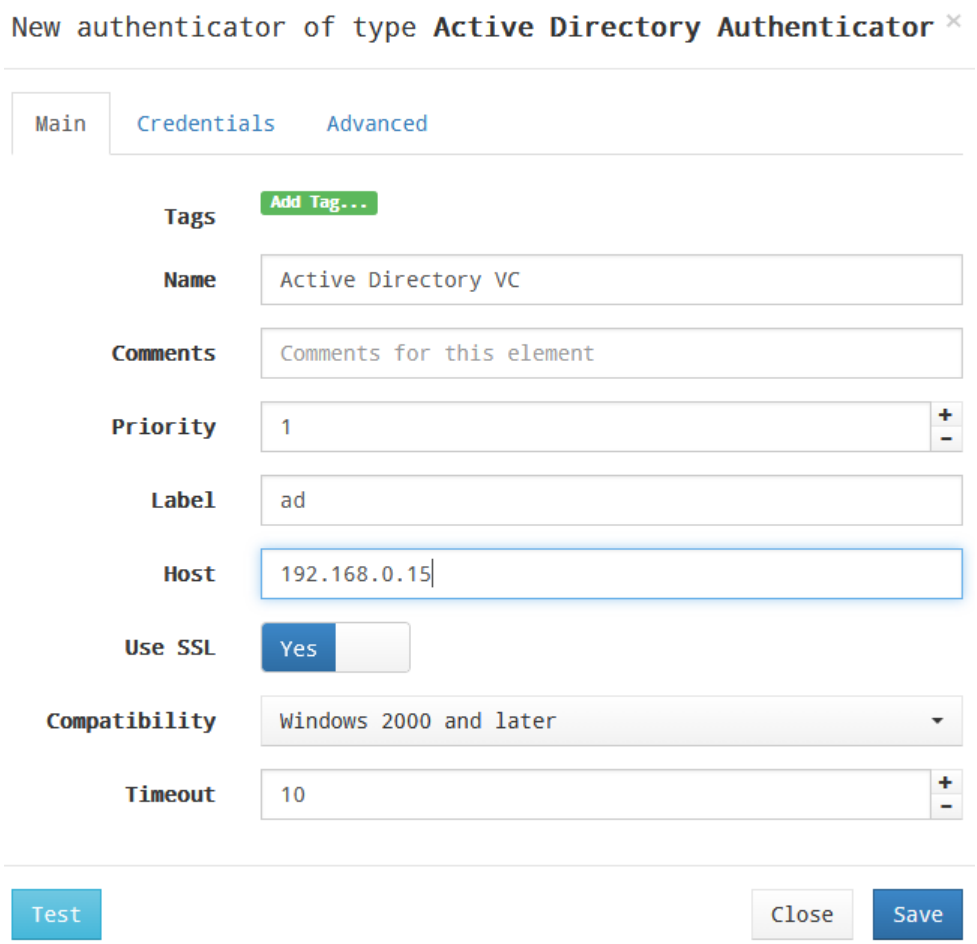
Configuring “Active Directory” authenticator

UDS Enterprise allows an integration with the authentication system “Active Directory”, thus allowing the validation of users of this authenticator in the UDS login portal.

To perform this integration, you will need to access the UDS dashboard, go to the section “**Authenticators**”, click on “**New**” and select “**Active Directory Authenticator**”:



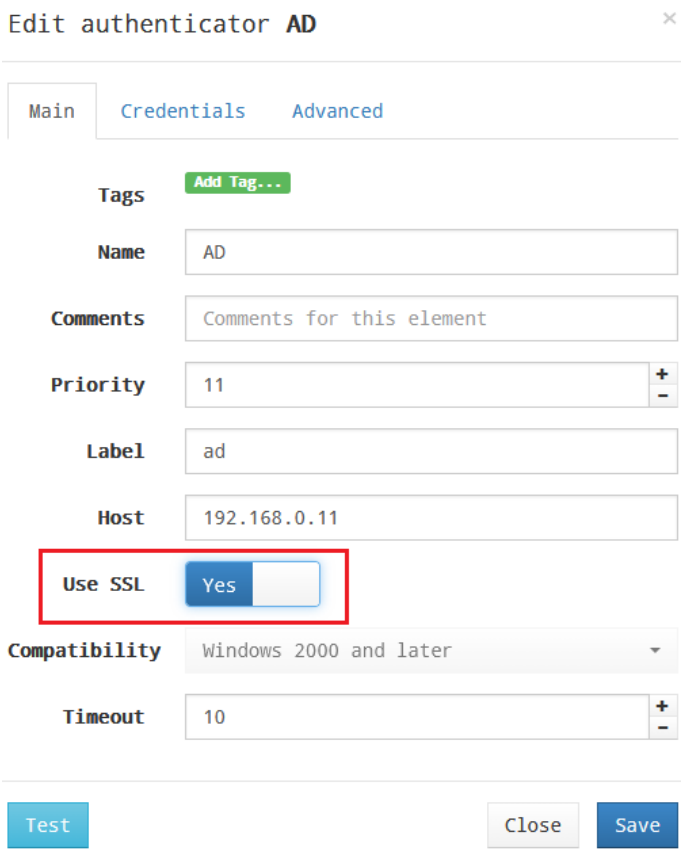
We must indicate a name for the authenticator, the IP address or server name “Active Directory” and the credentials of a user with at least read permissions:



In order for UDS to carry out an LDAPS communication, we must ensure **that the “Use SSL” option is enabled** (“**Yes**”).

Once all the necessary data has been indicated and the “**Use SSL**” option is with “**Yes**”, we must execute a “Test” connection to verify that the provided data are correct.

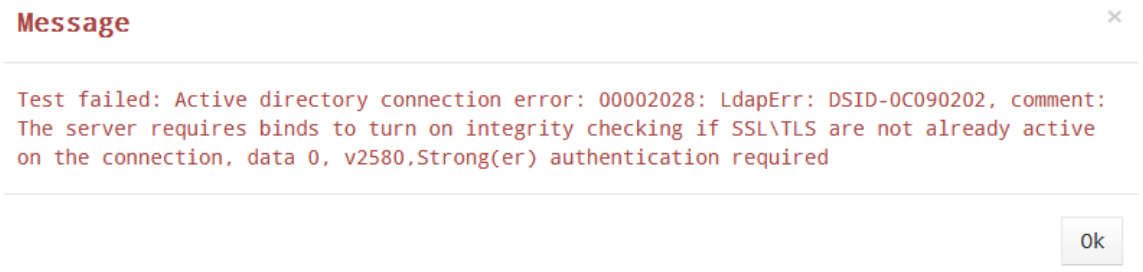
If we already have an “Active Directory” authenticator integrated with UDS Enterprise but we need to enable the LDAPS connection, we will simply have to select it, click on “**Edit**” and modify the “**Use SSL**” option to “**Yes**”:



Note: For the connection to be performed successfully, the "Active Directory" server or servers will need to have LDAPS communication enabled. You can confirm this communication using the "ldap.exe" tool. For more information, you can consult the following article:

https://blogs.msdn.microsoft.com/microsoftrservertigerteam/2017/04/10/step-by-step-guide-to-setup-ldaps-on-windows-server/

Note2: If we initially had a communication with "Active Directory" without using SSL and after the update of the Windows O.S. hosting the "Active Directory" the service has stopped working, obtaining the following error (when running the UDS connection test):

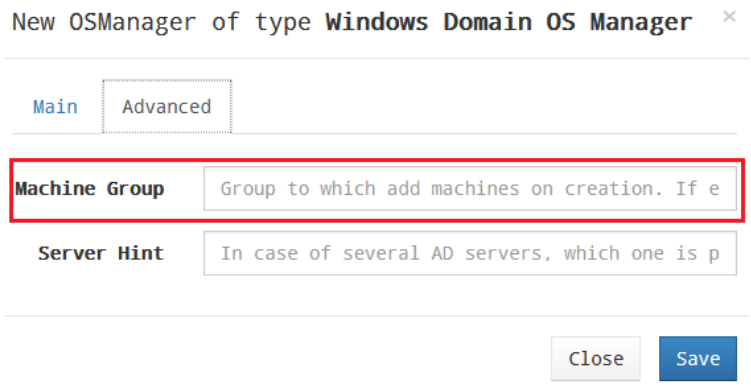


This error may be because Microsoft, through an update, will only allow the connection via LDAPS.

Apply patch for “Windows Domain OS Manager”

If we are using an “**OS Manager**” like “**Windows Domain OS Manager**” in UDS Enterprise, and if communication with the Active Directory server is only allowed via LDAPS, we will need to apply a patch to the “**UDS Server**” component to:

- Allow UDS to delete virtual desktops (previously registered) in an Organizational Unit (OU) of the “Active Directory”. If this patch is not applied, UDS will automatically register the desktops in the specified OU, but when those desktops are destroyed (either by non-persistent service configuration or by an administrator’s manual action), they will not be automatically deleted.
- Allow UDS to automatically add virtual desktops to a specific group. This configuration is available within “**Windows Domain OS Manager**”, tab “**Advanced**”, section “**Machine Group**”.



To apply the patch to the UDS Server, we must perform the following tasks:

1. Download the file “**WinDomainOsManager.py**” from the following repository:

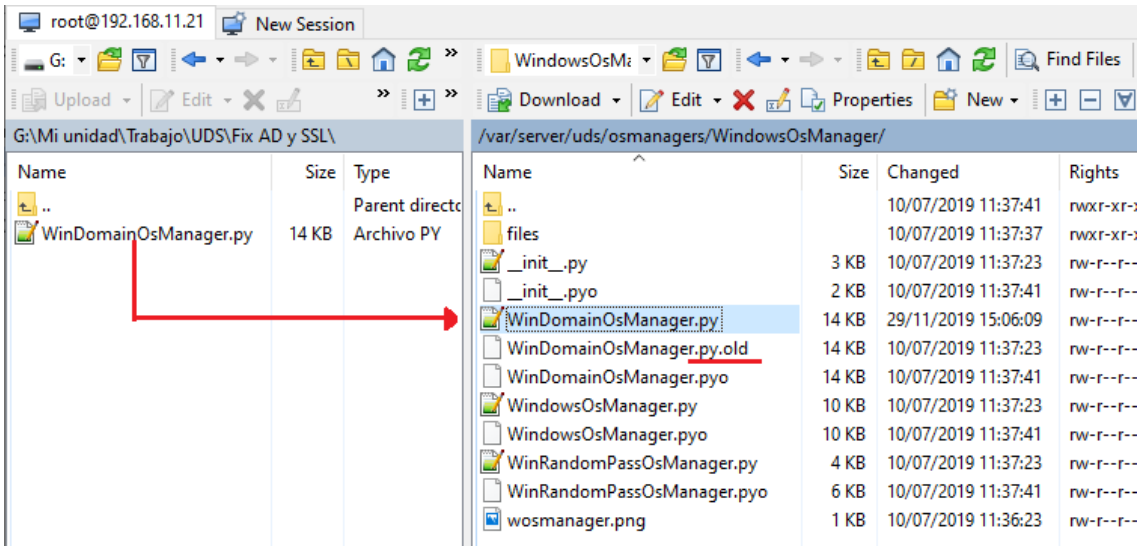
http://images.udsenterprise.com/files/UDS%20Patchs/UDS%202.2.1/OSManager_WinDomain_SSL/

2. Copy the “**WinDomainOsManager.py**” file to the “UDS Server” machine (if you have several UDS Servers, it will be necessary to copy the file to all) in the path:

   /var/server/uds/osmanagers/WindowsOsManager/

NOTE: To copy the file to the UDS Server, we can use third-party tools such as WinSCP.

NOTE2: It is recommended to make a copy of the original “**WinDomainOsManager.py**” file in case its restoration is necessary.



3. Restart de “UDS Server” machine to apply the patch (if we have several UDS Servers, it will be necessary to restart all of them).

About VirtualCable

VirtualCable develops, supports and markets UDS Enterprise through a subscription model based on the number of users, including product support and updates.

Additionally, VirtualCable offers professional services to install and configure UDS Enterprise.

For further information visit www.udsenterprise.com or email us at info@udsenterprise.com