Technical Note 003

Configurazione LDAP in AVEVA Edge

Rev. 2

12/08/2020

Technical Services

Contents

Introduzione

Questa TN descrive la configurazione di un server LDAP e della configurazione di un progetto sviluppato con InTouch Edge HMI utilizzando la sicurezza LDAP ed integra la precedente revisione 1 del 6 Aprile 2020 sostituendola.

Versioni

Quanto descritto in questa TN si applica ai prodotti InTouch Machine Edition (dalla versione 8.0 fino alla 8.1 SP2), InTouch Edge HMI (dalla versione 8.1 SP3 in poi) e Indusoft Web Studio (dalla versione 8.0). Da qui in avanti InTouch Machine Edition sarà sostituito con ITME, InTouch Edge HMI con ITEH e Indusoft Web Studio con IWS.

Requisiti

Per seguire la TN è necessario avere:

- Una macchina Windows Server based
- InTouch Edge HMI o InTouch Machine Edition dalla v8.0 o Indusoft Web Studio dalla v8.0

Sistema testato

Quanto descritto è stato testato con:

- Macchina Windows Server 2012 R2 per la parte server LDAP
- InTouch Machine Edition v8.0 SP2 su Windows 10 1511
- InTouch Edge HMI v8.1 SP5 su Windows 10 1809 (ha bisogno di un Hotfix per funzionare)
- AVEVA Edge 2020 su Windows 10 2004

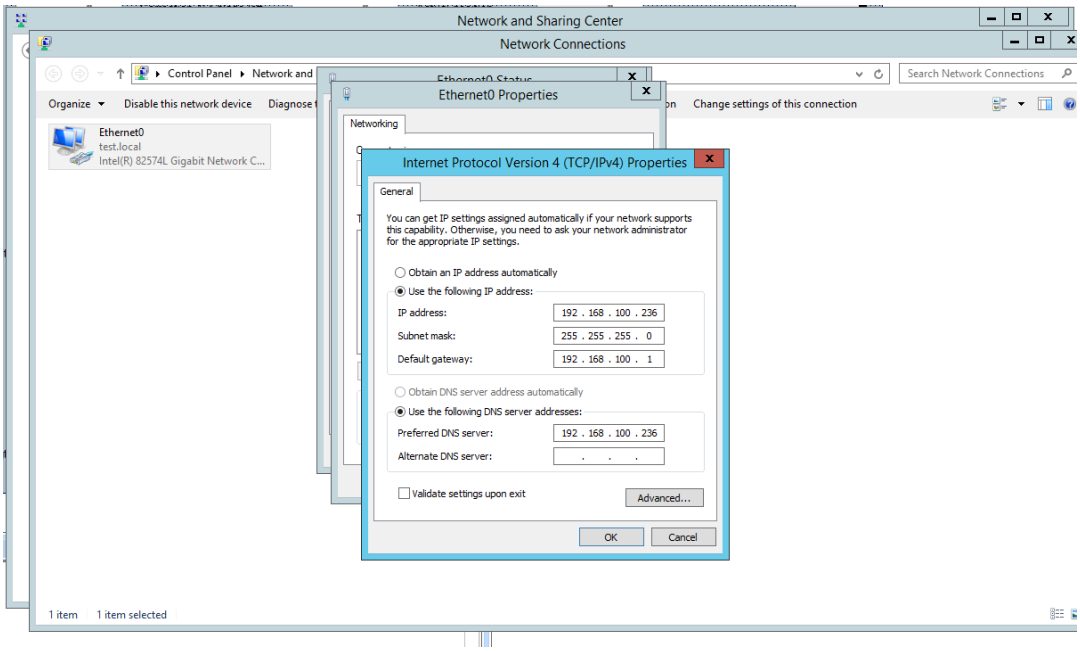
Come creare un server LDAP

Per creare un server LDAP si faccia riferimento alla guida Microsoft disponibile al seguente link (si segua dal punto 2):
https://blogs.msdn.microsoft.com/microsoftrservertigerteam/2017/04/10/step-by-step-guide-to-setup-ldaps-on-windows-server/
REMINDER: Bisogna settare il server LDAP come DNS

Come configurare il server LDAP come DNS

Per configurare il server LDAP come DNS occorre:

1. Aprire il **Control Panel**
2. Cliccare su **Network and Sharing Center**
3. Cliccare su **Change adapter setting**
4. Doppio click sulla scheda di rete scelta per la gestione della comunicazione tra clients e server LDAP
5. Cliccare su **Properties**
6. Disabilitare **Internet Protocol Version 6 (TCP/IPv6)**
7. Doppio click su **Internet Protocol Version 4 (TCP/IPv4)**
8. Selezionare **Use the following IP address** e inserire un indirizzo IP, la Subnet mask e il Default gateway
9. Selezionare **Use the following DNS server addresses** ed inserire l'indirizzo IP del server LDAP all'interno di Preferred DNS server come si vede dalla seguente immagine



Come configurare il server LDAP per la connessione SSL

Per configurare il server LDAP per utilizzare la connessione SSL occorre:

1. **Loggarsi** nel server LDAP utilizzando l'utente **Administrator**
2. Dal menu **Start**, cliccare su **Administrative Tools -> Server Manager**
3. Cliccare su **Manager -> Add Roles and Features**
4. Cliccare **Next** al primo tab
5. Selezionare l'opzione **Role-based or Feature-based installation** nella tab **Installation Type**. Cliccare **Next**
6. Selezionare l'opzione **Select a server from the server pool** nella tab **Server Selection**. Cliccare **Next**.
7. Nella tab **Server Roles** selezionare **Active Directory Certificate Services**. Cliccare **Next due volte**
8. Selezionare **Certification Authority**. Cliccare **Next**.
9. Nella pagina **Specify Setup Type**, cliccare **Enterprise**. Cliccare **Next**
10. Nella pagina **Specify CA Type**, selezionare **Root CA**. Cliccare **Next**
11. Nella pagina **Set Up Private Key**, selezionare **Create a new private key**. Cliccare **Next**
12. Nella pagina **Set Up Private Key - Cryptography**, **lasciare tutto di default**. Cliccare **Next**
13. Nella pagina **Set Up Private Key - CA name**, nella textbox **Common name for this CA**, indicare il Common Name del CA. Cliccare **Next**
14. Nella pagina **Set Up Private Key – Validity Period**, indicare il periodo di validità del certificato. Cliccare **Next**.
15. Nella pagina **Set Up Cetificate Period**, accettare i valori di default o specificare una cartella per il database dei certificati e dei loro log. Cliccare **Next**.
16. Dopo aver verificato tutte le informazioni nella pagina **Confirm Installation Selections**, cliccare **Next**.
17. Finita l'installazione, aprire il menu **Start - > Run -> gpupdate /force**.

Come esportare i certificati dal server LDAP

Per esportare i certificati dal server LDAP, per poi utilizzarli in client che non si trovano nello stesso dominio del server, occorre:

1. Dal menu **Start -> Run**
2. Scrivere **mmc** e cliccare **OK**
3. Cliccare su **File -> Add/Remove Snap-in…**
4. Doppio click su **Certificates**
5. Selezionare l'opzione **Computer Account**. Cliccare **Next**

6. Lasciare l'opzione **Local Computer** selezionata e cliccare su **Finish**. Cliccare **OK**
7. Doppio click su **Certificates -> Trusted Root Certification Authorities**.
8. Selezionare **ogni certificato con il nome della macchina server LDAP di dominio** e **tasto destro -> All Tasks -> Export…**
9. Nel **Certificate Export Wizard**, cliccare **Next**
10. Selezionare l'opzione **No, do not export the private key**. Cliccare **Next**
11. Selezionare l'opzione **DER encoded binary X.509 (.CER)**. Cliccare **Next**
12. Salvare dove è più comodo i certificati
13. Cliccare su **Finish** per terminare l'export del certificato.
14. Ripetere gli **step 8-13 per ogni certificato avente il nome della macchina server LDAP**
15. Copiare i file .cer su ogni macchina client.

Come importare i certificati sui client

Per importare i certificati Sui client che non si trovano nello stesso dominio del server LDAP occorre:

1. Dal menu **Start -> Run**
2. Scrivere **mmc** e cliccare **OK**
3. Cliccare su **File -> Add/Remove Snap-in…**
4. Doppio click su **Certificates**
5. Selezionare l'opzione **Computer Account**. Cliccare **Next**
6. Lasciare l'opzione **Local Computer** selezionata e cliccare su **Finish**. Cliccare **OK**
7. Doppio click su **Certificates -> Trusted Root Certification Authorities -> All Tasks - > Import**.
8. Nel **Certificate Import Wizard**, cliccare **Next**
9. Cliccare **Browse** per cercare i file .cer. Cliccare **Open** e poi **Next**
10. Selezionare l'opzione **Place all certificates in the following store**. Cliccare **Next**
11. Cliccare su **Finish** per terminare l'import del certificato.
12. Ripetere gli **step 7-11 per ogni file .cer**
13. Chiudere la mmc console. Non c'è bisogno di salvare

Editare il file di hosts

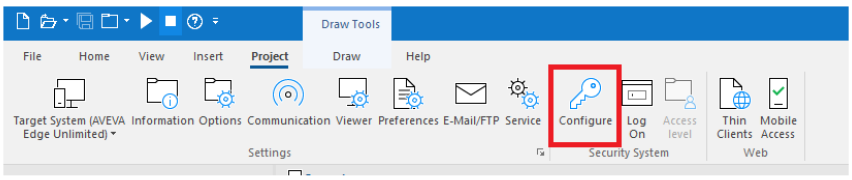
Per editare il file di hosts occorre:

1. Aprire con **privilegi di Amministratore** l'applicazione **Notepad**
2. Cliccare su **File -> Open** e cercare il file **hosts** al percorso **C:\Windows\System 32\drivers\etc** dopo aver selezionato **All Files** nella combobox vicino la textbox File Name
3. Editare il file di **hosts** indicando **indirizzo IP e nome macchina di tutte le macchine del sistema** seguendo l'esempio riportato nel file. **Il file deve essere lo stesso su server e macchine client.**

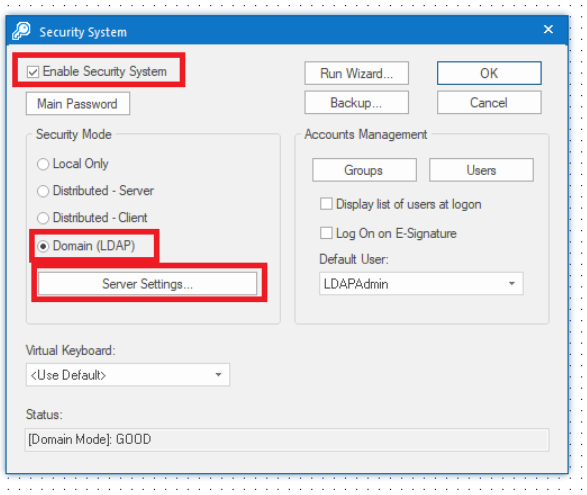
Come configurare la sicurezza LDAP in ITEH/ITME/IWS (no SSL)

Dopo aver installato e aperto il software:

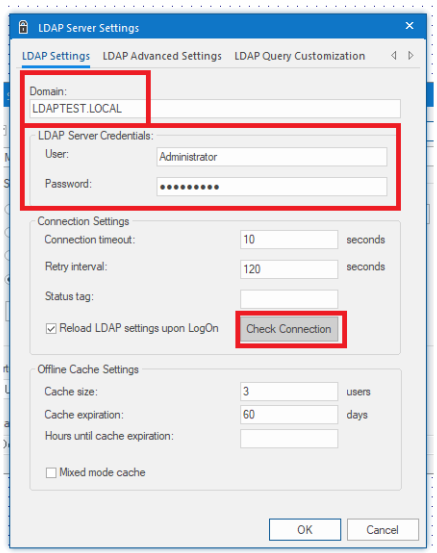
1. Cliccare sulla tab **Project** e su **Configure**



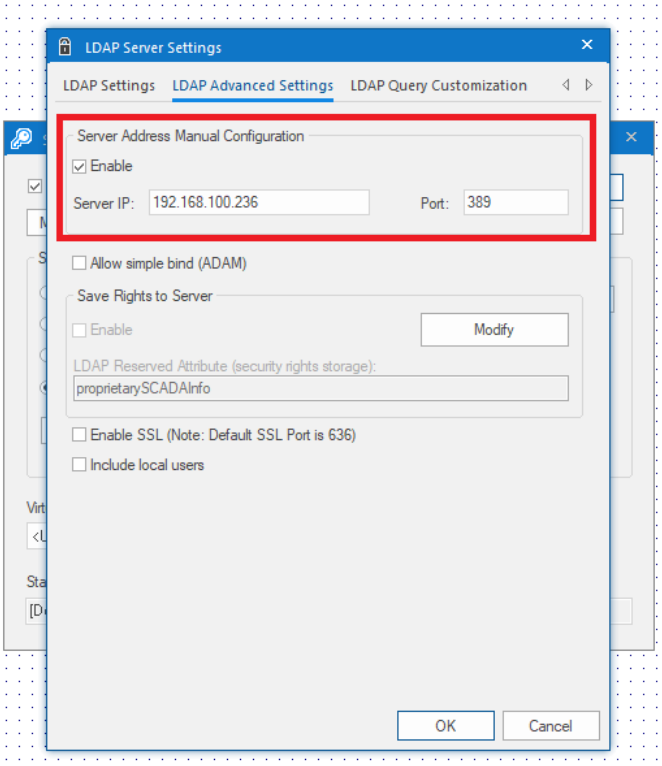
2. Spuntare **Enable Security System** e selezionare **Domain (LDAP)**
3. Cliccare su **Server Settings**



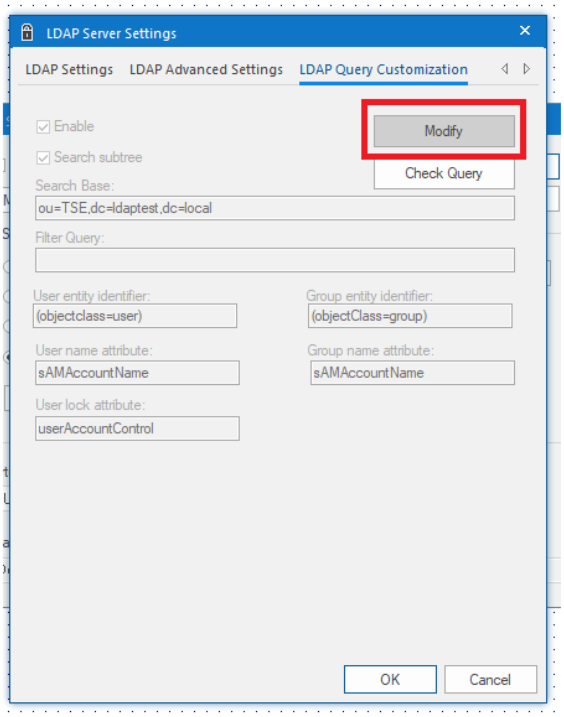
4. Appare il panel **LDAP Server Settings**
5. Nel tab **LDAP Settings**, inserire il nome del dominio (per esempio: ldaptest.local) nella textbox **Domain**
6. Inserire le **Credenziali LDAP Server** in **User** e **Password**
7. **[Opzionale]** Configurare **Connection Settings** e **Offline Cache Settings** come meglio si crede
8. Cliccare su **Check Connection** per verificare la connessione con il server



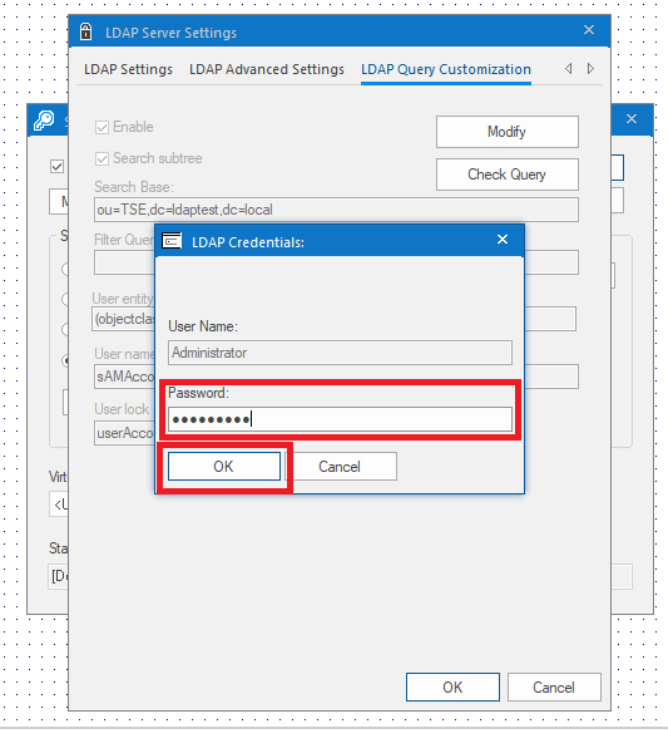
9. Cliccare sulla tab **LDAP Advanced Settings** e spuntare **Enable** sotto **Server Address Manual Configuration**
10. In **Server IP** inserire l'indirizzo IP del server LDAP e in **Port** digitare il numero della porta usata per la connessione con il server LDAP *(389 è il numero di porta di default)*



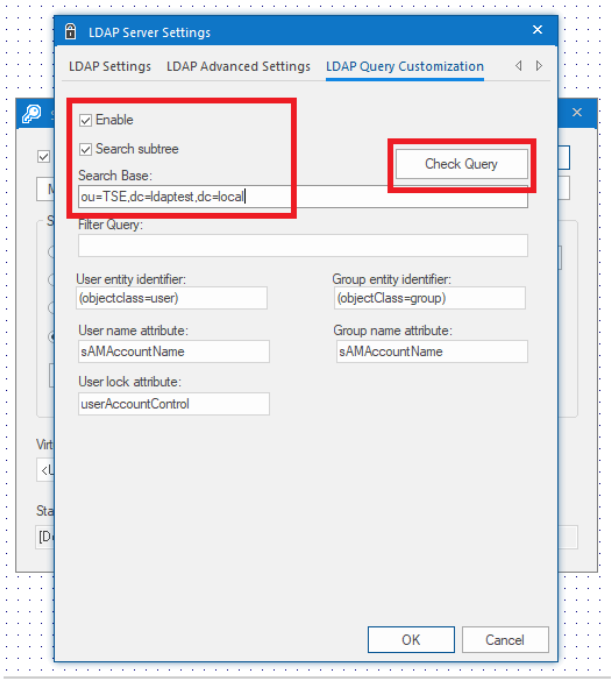
11. Click on **LDAP Advanced Settings** tab
12. Cliccare sul bottone **Modify**

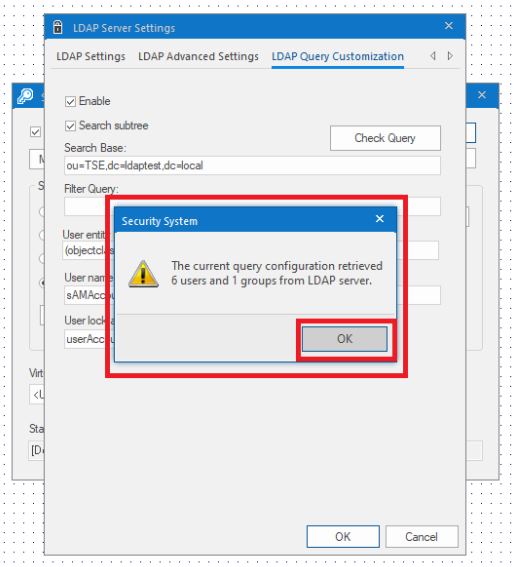


13. Inserire la password

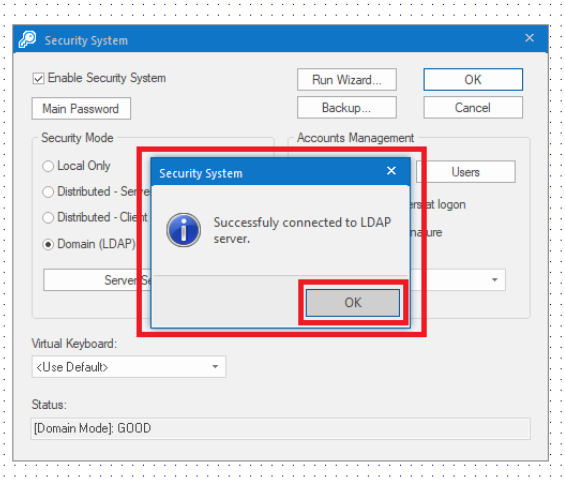


14. Spuntare **Enable** e **Search Subtree**
15. Inserire la **Search Base** *(per esempio ou=TSE,dc=ldaptest,dc=local)*
16. Inserire la query LDAP nella textbox **Filter Query**
17. Cliccare sul bottone **Check Query** per verificare la query

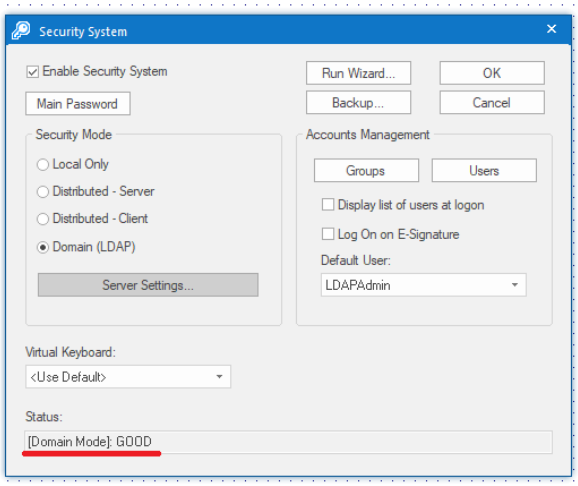




18. Cliccare **Ok**



19. Cliccare **Ok**



Hai settato correttamente il tuo Dominio LDAP nel tuo progetto.

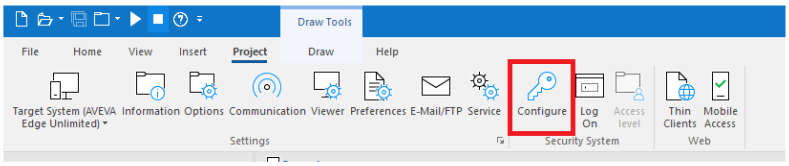
REMINDER: qualora fossero presenti delle policies nel Dominio, per esempio un utente viene bloccato quando inserisce 3 volte la password sbagliata, si deve sbloccare l'utente

nella parte Active Directory su Windows e, dopo ciò, l'utente si può nuovamente loggare al progetto con le credenziali dell'utente sbloccato.

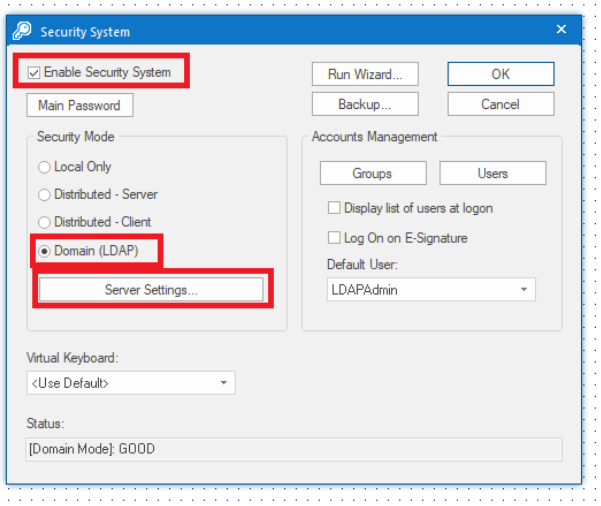
Come configurare la sicurezza LDAP in ITEH/ITME/IWS (con SSL)

Dopo aver installato e aperto il software:

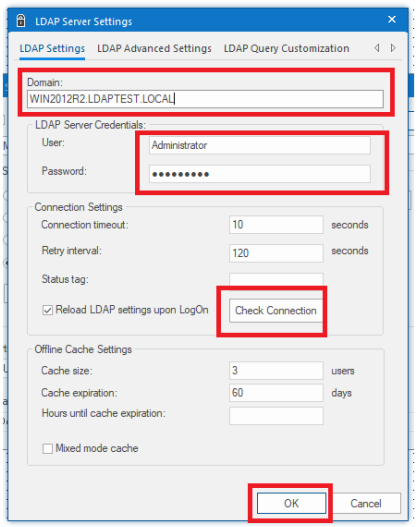
1. Cliccare sulla tab **Project** e su **Configure**



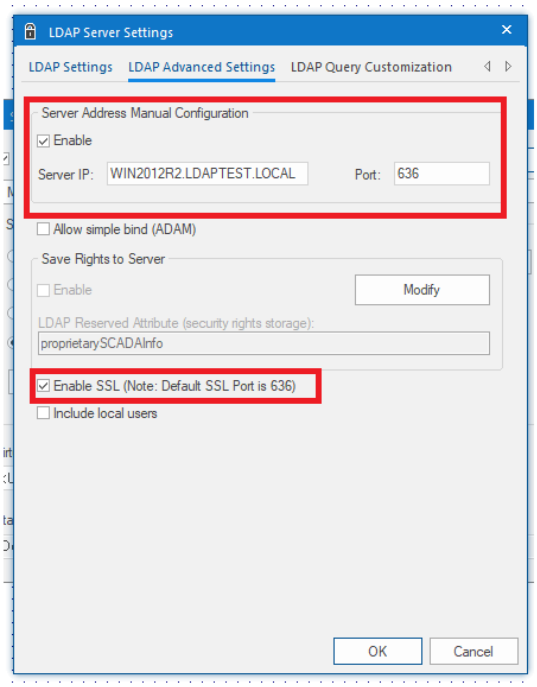
2. Spuntare **Enable Security System** e selezionare **Domain (LDAP)**
3. Cliccare su **Server Settings**



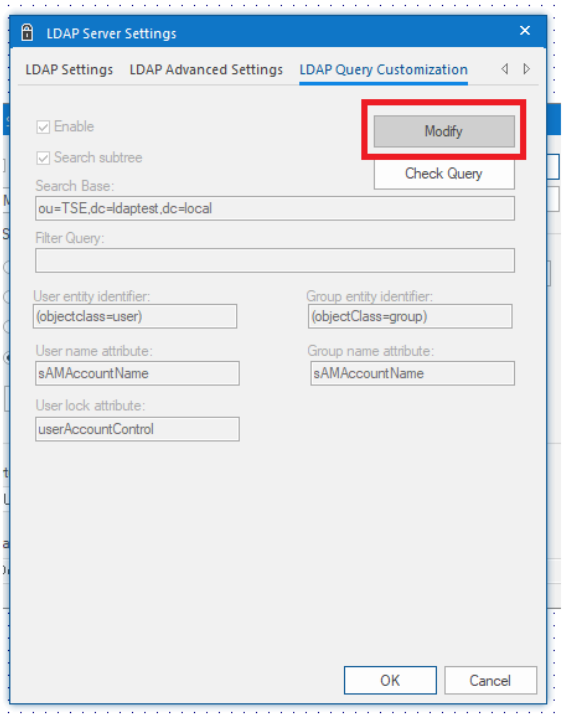
4. Appare il panel **LDAP Server Settings**
5. Nel tab **LDAP Settings**, inserire il nome del dominio utilizzando la stringa HostName.DomainName *(per esempio: WIN2012R2.LDAPTEST.LOCAL)* nella textbox **Domain**
6. Inserire le **Credenziali LDAP Server** in **User** e **Password**
7. **[Opzionale]** Configurare **Connection Settings** e **Offline Cache Settings** come meglio si crede
8. Cliccare su **Check Connection** per verificare la connessione con il server



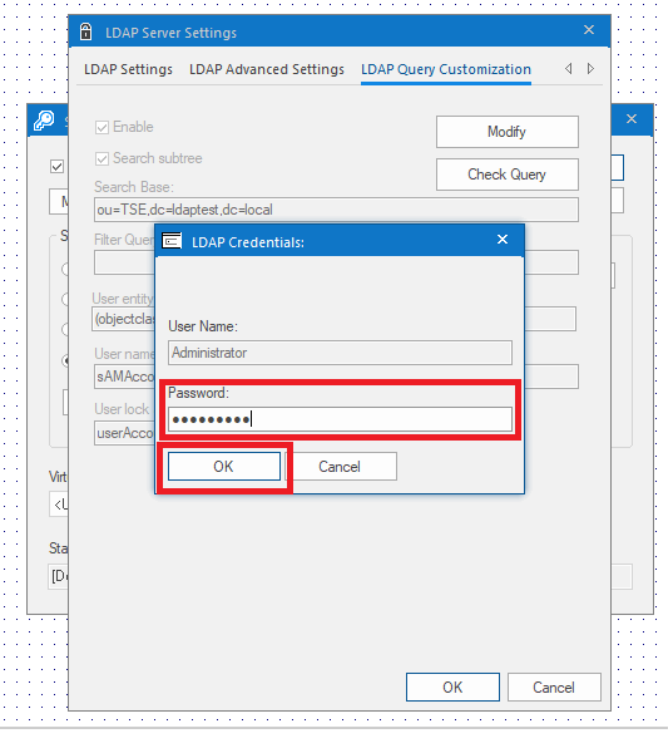
9. Cliccare sulla tab **LDAP Advanced Settings** e spuntare **Enable** sotto **Server Address Manual Configuration**
10. In **Server IP** inserire la stringa HostName.DomainName e in **Port** digitare il numero della porta usata per la connessione con il server LDAP *(636 è il numero di porta di default quando si utilizza la connessione SSL)*



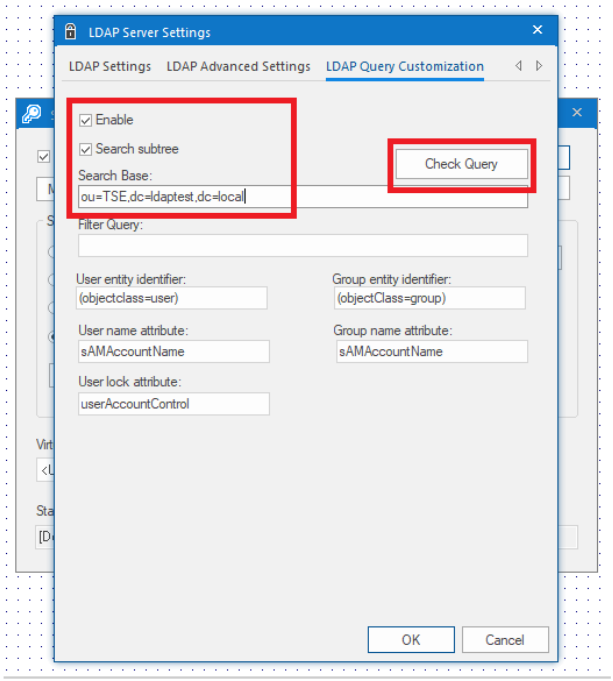
11. Click on **LDAP Advanced Settings** tab
12. Cliccare sul bottone **Modify**

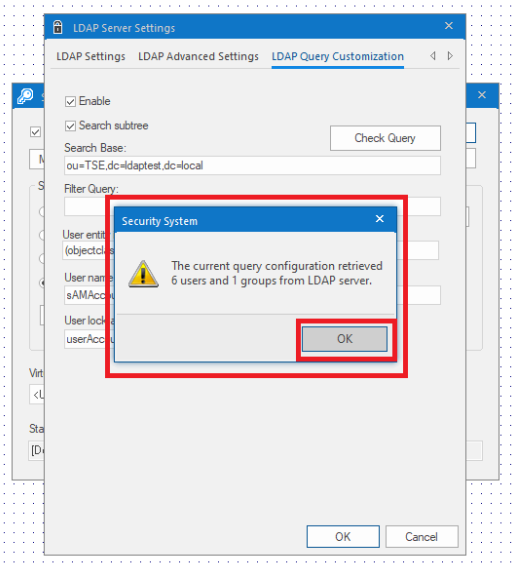


13. Inserire la password

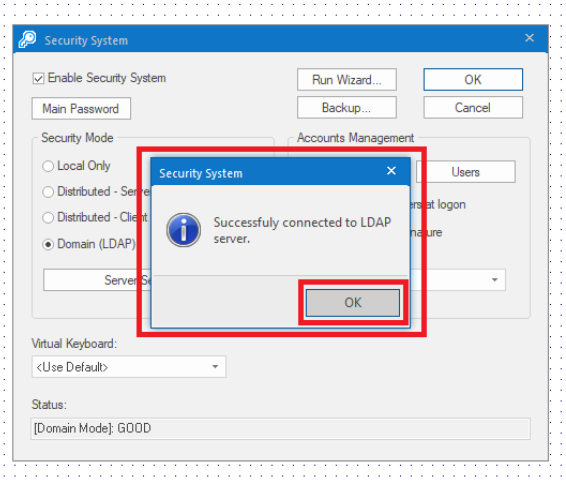


14. Spuntare **Enable** e **Search Subtree**
15. Inserire la **Search Base** *(per esempio ou=TSE,dc=ldaptest,dc=local)*
16. Inserire la query LDAP nella textbox **Filter Query**
17. Cliccare sul bottone **Check Query** per verificare la query

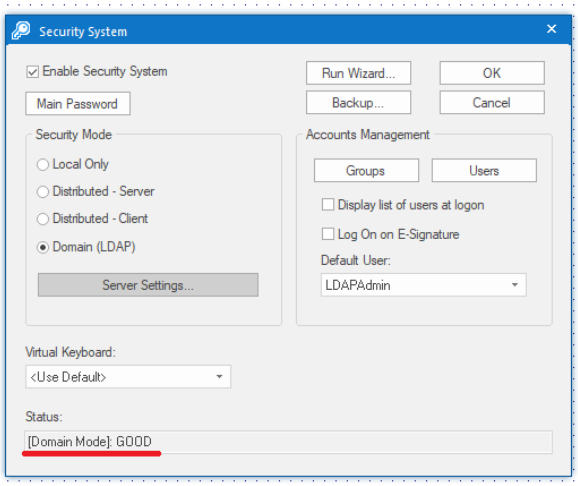




18. Cliccare **Ok**



19. Cliccare **Ok**



Hai settato correttamente il tuo Dominio LDAP nel tuo progetto.

REMINDER: qualora fossero presenti delle policies nel Dominio, per esempio un utente viene bloccato quando inserisce 3 volte la password sbagliata, si deve sbloccare l'utente

nella parte Active Directory su Windows e, dopo ciò, l'utente si può nuovamente loggare al progetto con le credenziali dell'utente sbloccato.

Esempi di query LDAP

Si possono trovare informazioni e alcuni esempi di query LDAP visitando i seguenti siti:

- https://ldapwiki.com/wiki/Main
- https://ldapwiki.com/wiki/LDAP%20Query%20Examples

Per esempio si possono trovare query come:

- ou=TSC,dc=test,dc=local
  Returns all members and groups of ou named TSC
- cn=Users,dc=test,dc=local
  Returns all members and groups of cn named Users
- (|(CN=BOLLINI)(CN=MANUTENTORI)(|(memberOf=CN=BOLLINI,OU=TSC,DC=test,DC=local)(memberOf=CN=MANUTENTORI,OU=TSC1,DC=test,DC=local)))
  Returns all members of cns named BOLLINI and MANUTENTORI

Per browsare un LDAP server si consiglia il seguente software:

https://www.ldapadministrator.com/download.htm

Referenze

- Microsoft web page: https://blogs.msdn.microsoft.com/microsoftrservertigerteam/2017/04/10/step-by-step-guide-to-setup-ldaps-on-windows-server/
- LDAP Wiki web page: https://ldapwiki.com/wiki/Main
- LDAP Wiki web page: https://ldapwiki.com/wiki/LDAP%20Query%20Examples
- Youtube video: https://www.youtube.com/watch?v=at6d-6EWr7k
- Youtube video: https://www.youtube.com/watch?v=JFPa_uY8NhY
- Softerra LDAP Administrator download page: https://www.ldapadministrator.com/download.htm
- Technote Indusoft "Configuring SSL on LDAP Server and Client"

Autore: Francesco Pastore