

# Extranet Auth Installation Guide

This document shall serve as the installation guide to Active Directory Lightweight Directory Services.

The goal of this guide will be to provide the foundation for the engineering, installation, and maintenance of an authentication system that is flexible, secure, and made easily accessible to outside sources.

This document will begin with a brief overview of the current functionality, following with detailed steps of installation, and ending with thoughts on future migration paths and redundancy.

## Overview of Active Directory Lightweight Directory Services

Active Directory Lightweight Directory Services (here forth known simply as LDS) is a basic stripped down version of Active Directory Directory Services. The databases, storage mechanisms, and much of the code is similar (if not the same) as to its bigger brother Directory Services.

Our test environments allowed us to go into more depth without risking any damage to our current infrastructure and through this we were able to gain insight on several potentially crippling areas, that if done incorrectly could possibly adversely affected our DC's and the information they contain.

LDS operates using many of the same tools that AD DS uses or has the ability to use. Some of these tools can be used interchangeably with AD DS and LDS. Tools like ADSI Edit, LDP, etc. However there is one such tool that is unique crucial to the successful operation of LDS is one called **adamsync**<sup>1</sup>. LDS was previously referred to as ADAM (Active Directory Application Mode) and was renamed to LDS in 2008.

Adamsync allows data to be extracted from an LDAP source and then synced into the LDS data stores. The sync not only contains the ability to synchronize the data, but to also modify the data in the objects that it imports. We will see how this is done in the installation guide.

Once the data is brought into the LDS data stores, the information is no longer synchronized, unless it has reached its aging value, and then the information will simply be refreshed. We will not be using aging, and will be simply letting it do differential updates, where only information that has changed will be modified after the initial full sync.

Synchronizations will need to be setup on a scheduled task to synchronize LDS every X amount of minutes.

### Contents

- Scope of Document
- Overview- Extranet Auth
- Gotcha's
- Prepping for LDS
- Installation of the LDS Role
- Setting Up An Initial Instance
- Configuring the LDS Extranet Instance
- Adamsync Setup and Initialization
- Installing the Adamsync XML
- Removing LDS Instances

---

<sup>1</sup> Adamsync is a utility that provides object synchronization to Active Directory LDS from AD DS. Object synchronization rules are defined in a specific XML file.

# Extranet Auth Installation Guide

---

## Before We Begin... Gotcha's.

1. AD LDS servers MUST be member servers of the domain \*IF\* they are doing any reverse proxying of authentication (which is our goal).
2. AD LDS must be sysprep'ed if using a clone or copy of an already existing installation. Despite Microsoft alluding to sysprep being no longer needed when deploying new server instances (virtual or otherwise), this is most definitely not the case, especially when using LDS.

Many odd behaviors were noticed, very few of them generated any descript error messages pointing to this being the issue. Long story short, this is required.

3. If using any service account other than the default Network Service account, there will be errors generated in the event logs that make it appear that the service was unable to connect to the domain.

This is not the case, however best practices have proven out to be that there are too many limitations with LDS to easily use any other service account and keep the setup as easily replicable as possible.

4. When applying the certificate for LDAPS, the service account must be explicitly allowed read access to the cert.
5. Setup and application of the NLB must be done as the final last step to the overall setup.

---

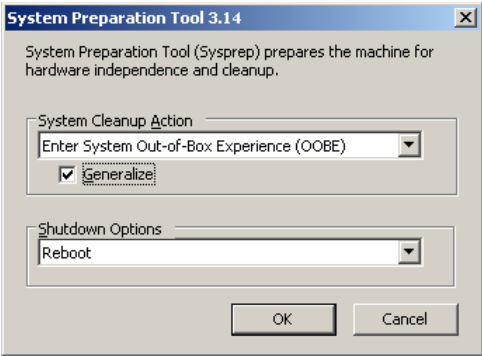
Notes:


# Extranet Auth Installation Guide

---

## In Preparation of LDS

1. Create a new Active Directory group called **LDS Admins** and add the group to your user account.
2. If you have already logged into the servers that will run our LDS instance, please log out of the server and log back in so that the group parameters get successfully attached to the user.
3. If the server that will be running LDS has not been sysprep'ed yet please do so now.
  - a. **Open** a new command prompt with the **Run-As Administrator**.
  - b. **Change directory** to `C:\windows\system32\sysprep`
  - c. Type **sysprep** and press **Enter**
  - d. **Select** "Generalize" and click **Ok**



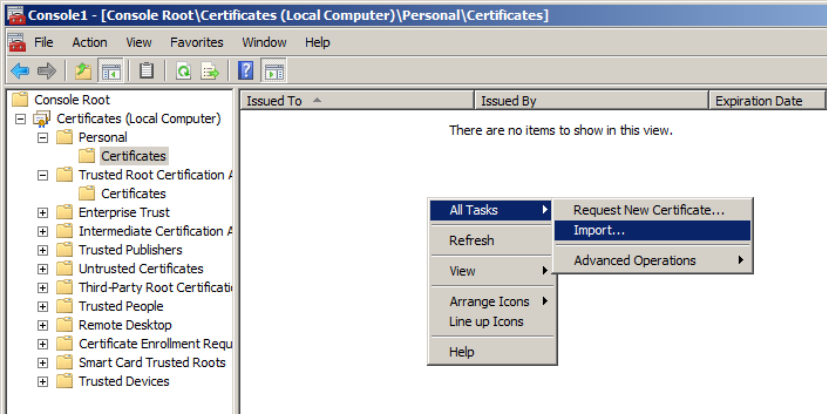
- e. After the system goes through the process, it will reboot, and the system will be refreshed with new information unique to that server.

---

Notes:


# Extranet Auth Installation Guide

- 4. After the machine comes back up from the reboot we will want to install our certificates that will be used for secure communications.
  - a. **Open** a new mmc instance by going to **Start > Run >** and in the *Search Programs and Files* type **mmc**.
  - b. Once you see mmc come up in the list above the “Start Menu”, **right click** mmc and choose “*Run as administrator*”.
  - c. If a UAC notification pops-up choose **Ok**.
  - d. In the mmc application click on **File > Add/Remove Snapins**.
  - e. In the left side, “Available snap-ins:” column, **double click** on *Certificates*.
  - f. Under “This snap in will always manage certificates for:” **Select** the radio button next to **Computer Account** and press **Finish**.
  - g. Expand out the Personal Certificates in the certificates tree, and right click in the right frame. Choose All Tasks > and click Import...




Notes:


# Extranet Auth Installation Guide

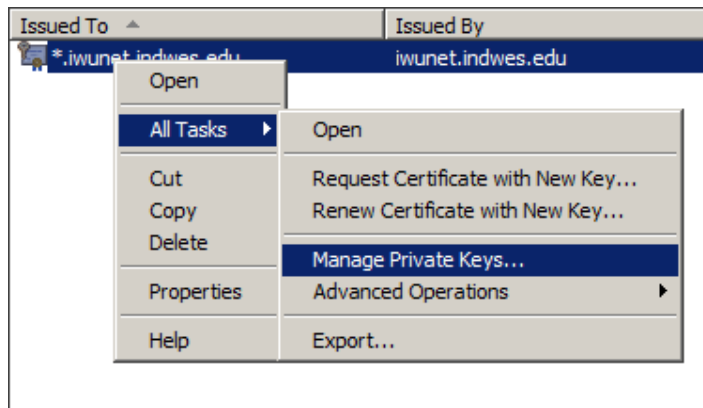
---

- h. The **Welcome to the Certificate Import Wizard** opens. Click **Next**.
- i. Choose the filename of the certificate that you wish to import. Click **Next**.



If the location of this file is not known contact the security administrators for a valid certificate.

- j. Type the password for the certificate (if any). Click **Next**.
- k. Place all certificates in the **Personal** store (default). Click **Next**.
- l. Click **Finish**.
- m. **Right click** the newly installed cert, and **All Tasks > Manage Private Keys**.



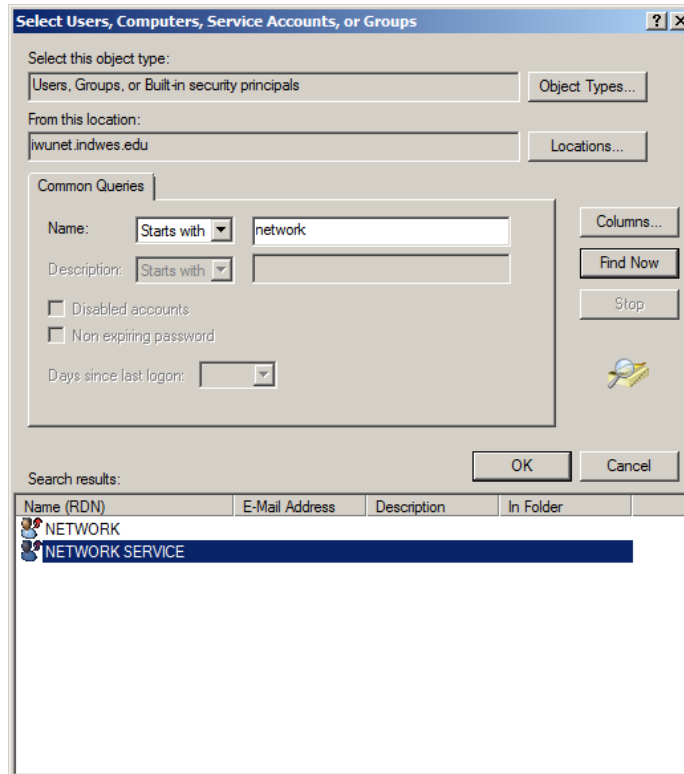
---

Notes:


# Extranet Auth Installation Guide

---

- n. We will need to add the **Network Service** account to have permissions to use this certificate.



- o. Choose the account to have **Read** permissions. Click **Next**.

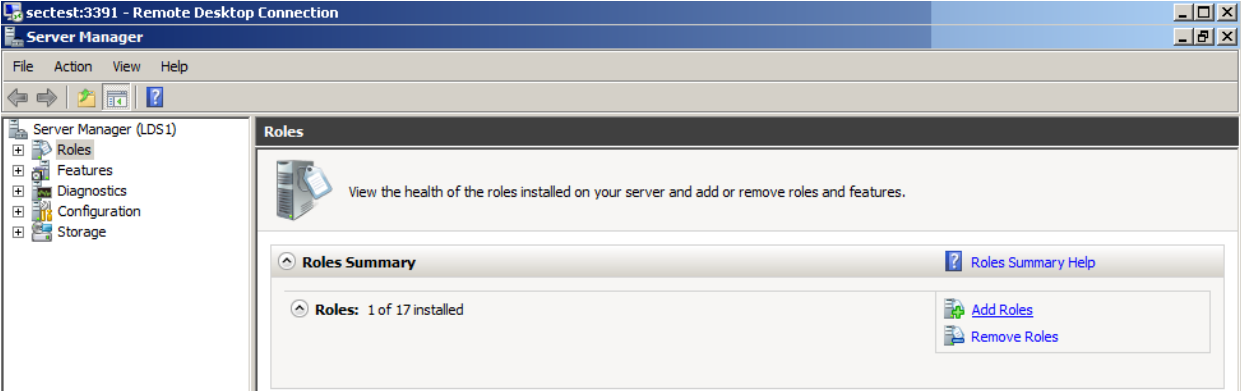
---

Notes:


# Extranet Auth Installation Guide

## Installation of the LDS Role

1. Begin by adding the LDS role in the server manager console. **Click** on **Roles** in the left column under Server Manager and **Add Roles** along the right edge of the server manager console.



2. The next window that opens will be the welcome page to the **Add Roles Wizard**. **Click Next**.
3. Underneath the “Select one or more roles to install on this server.” **Select Active Directory Lightweight Directory Services** and **Click Next**.
4. Continue to follow any additional prompts for installation. There should be no further prompts but if there are use the default options. Once the installation has completed, you may be prompted to reboot. Please do so.

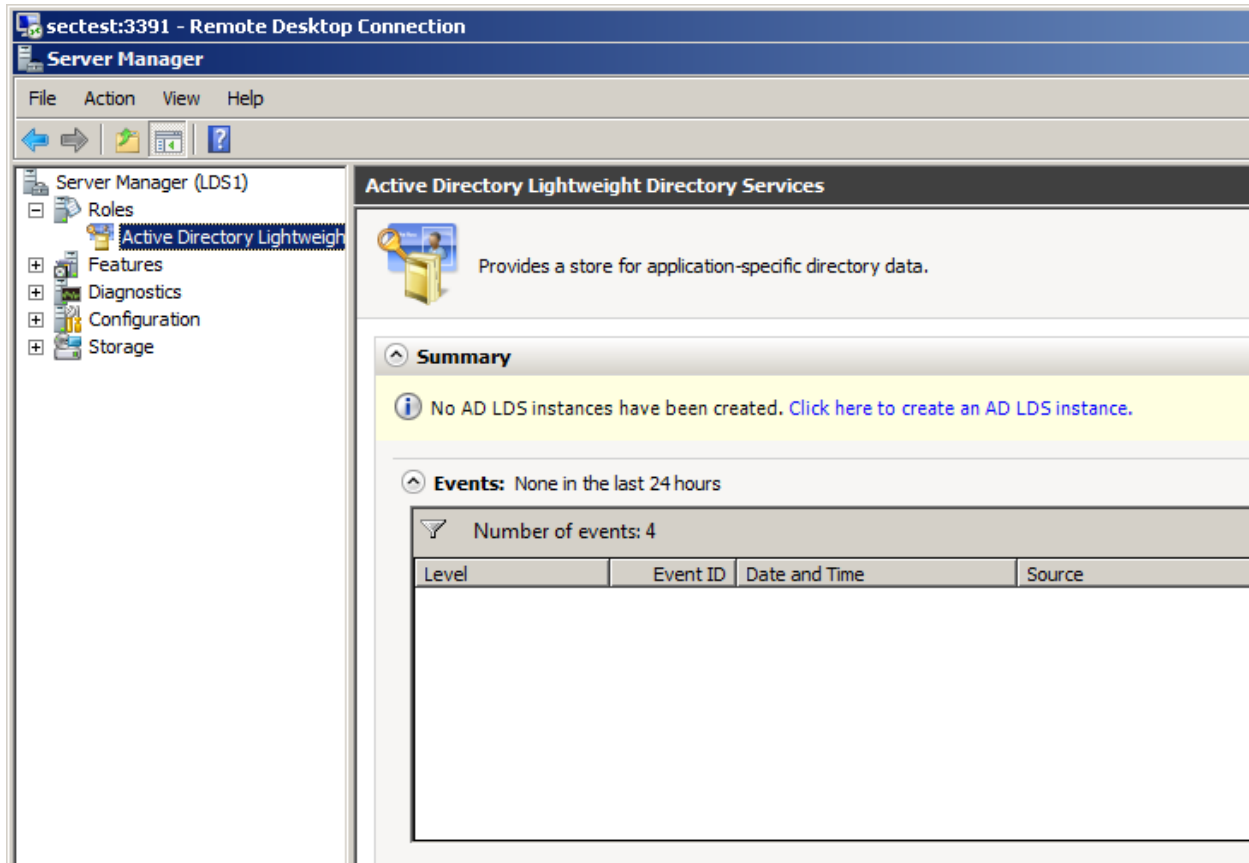
Notes:


# Extranet Auth Installation Guide

---

## Setting Up An Initial LDS Instance

1. In the Server Manager console, underneath roles, click on Active Directory Lightweight Directory Services.



2. **Click** the “[Click here to create an AD LDS instance](#)” in the right frame underneath **Summary**.

---

Notes:





# Extranet Auth Installation Guide

---

3. A new window will appear that will look like the following:



4. Click **Next** to begin our installation.



The next screen(s) which open will be **Setup Options**. LDS can run many different instances, each of which can be a completely unique schema. You also have the option (if setting up a secondary LDS server) to create a replica of an instance.

---

Notes:


# Extranet Auth Installation Guide

---

*Setup Options*

- 5. For the instance installation type, choose (default) “**a unique instance**” and click **Next**.

*Instance Name*

- 6. For instance name, name the LDS instance something that pertains to what its information will represent. For our testing and setup I chose:

**Extranet-Authentication**

The name must be alpha-numeric only and without any spaces. Hyphens are permitted. The description can be left the default; it will only be used as a descriptor in the **Services** section of the control panel as a descriptor of the above named instance. Click **Next** after everything is how it should look.

*Ports*

- 7. The default port settings of 389 and 636 are the optimal for what we will be doing. Make sure that information is correct and click **Next**.

*Application Directory Partition*

- 8. This section we will be deviating somewhat from the defaults. Select, “**Yes, create an application directory partition**”.

For the partition name:  
DC=iwunet,DC=indwes,DC=edu and click **Next**.



*Basically what we are doing here is setting up an application partition that is closest to that of our own structure in our AD DS.*

---

Notes:


# Extranet Auth Installation Guide

---

*File Locations*

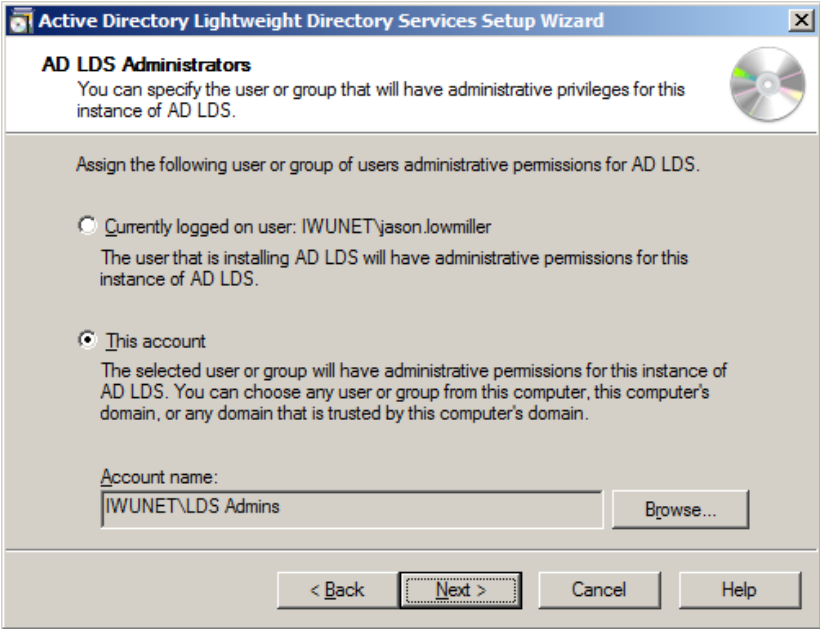
- 9. The default file locations for installation of the service are fine to use, please use the default and click **Next** to continue.

*Service Account Selection*

- 10. The (default) **network service account** will be used to run this system.

*AD LDS Administrators*

- 11. Please choose the group that you will want to allow Administration of the LDS instances, if using any other groups other than the one we created.



---

Notes:


# Extranet Auth Installation Guide

---

## *Importing LDIF Files*

12. Choose the following LDIF Files for import:

MS-AdamSyncMetadata.ldf  
MS-ADLDS-DisplaySpecifiers.ldf  
MS-InetOrgPerson.ldf  
MS-User.ldf  
MS-UserProxy.ldf  
MS-UserProxyFull.ldf

... and click **Next**.

## *Ready to Install*

13. Verify that all looks appear to be correct. Click **Next**.

## **Quick Test the Initial LDS Instance**

1. Click the start menu and in the Search Programs and Files box type **LDP** and press enter.
2. In the LDP program, under the **Connection** menu click **Connect**. The server should be typed as **localhost**, port should be **636** and select the box that says **SSL**.

---


Notes:


# Extranet Auth Installation Guide

---

3. You should get output that looks a bit like this:

- `ld = ldap_sslinit("localhost", 636, 1);`
- `Error 0 = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3);`
- `Error 0 = ldap_connect(hLdap, NULL);`
- `Error 0 = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)&lv);`
- `Host supports SSL, SSL cipher strength = 128 bits`
- **Established connection to localhost.**
- `Retrieving base DSA information...`
- `Getting 1 entries:`
- `Dn: (RootDSE)`
- `configurationNamingContext: CN=Configuration,CN={98F208B7-E7E7-4405-AoF6-418EE2377059};`
- `currentTime: 5/2/2012 11:19:02 AM Eastern Daylight Time;`
- `dnsHostName: lds1.iwunet.indwes.edu;`
- `domainControllerFunctionality: 4 = ( WIN2008R2 );`
- `dsServiceName: CN=NTDS Settings,CN=LDS1$Extranet-Authentication,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,CN={98F208B7-E7E7-4405-AoF6-418EE2377059};`
- `forestFunctionality: 2 = ( WIN2003 );`



Take special note to the section highlighted in Yellow. The **dsServiceName** ID string is something we will need later on when setting up adamsync. Copy this down at this time.

---

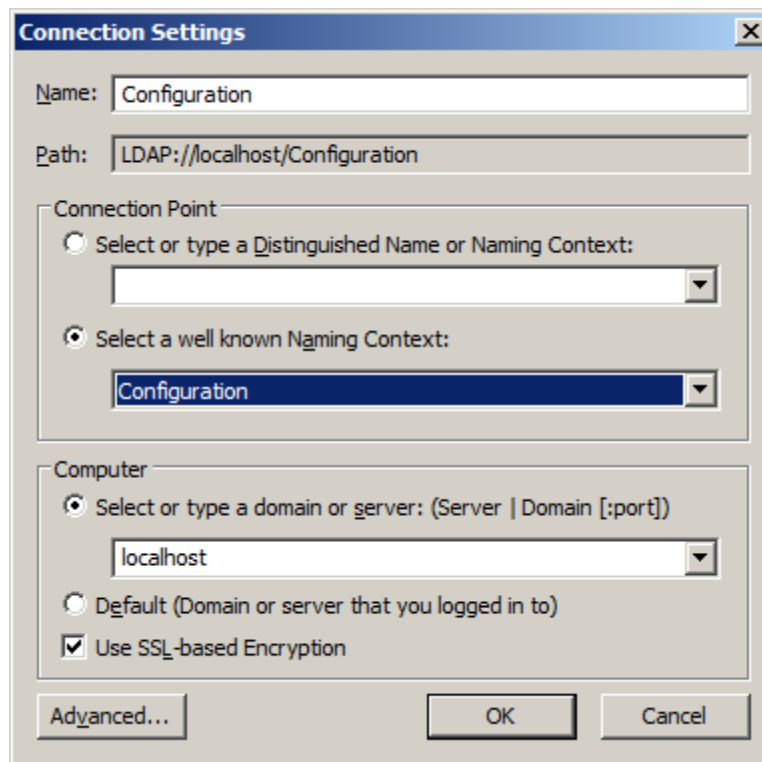
Notes:


# Extranet Auth Installation Guide

---

## Configuring the LDS Extranet Instance

1. Open the server manager console, select the AD LDS role underneath roles and scroll down to the **Advanced Tools** section in the left frame.
2. Click on **ADSI Edit**, and under the **Action** menu, click **Connect to...** and connect with the following information.



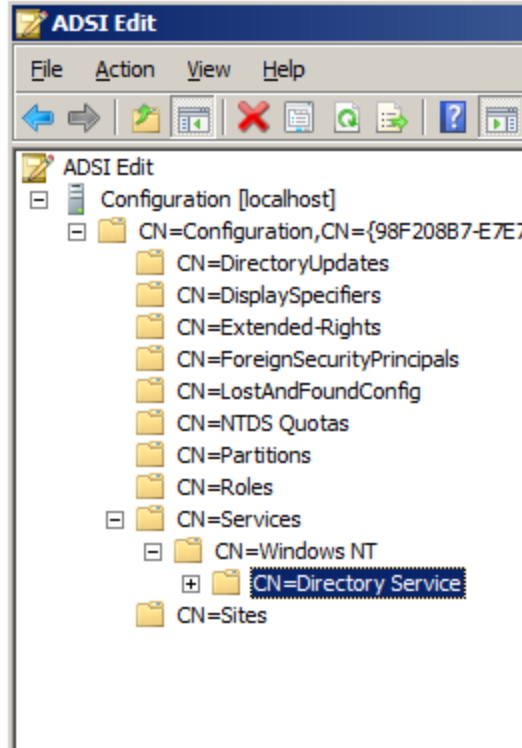
---

Notes:


# Extranet Auth Installation Guide

---

- Expand out the tree in the left frame as follows:



- With CN=Directory Service selected, right click it with the mouse, and choose **Properties**.
- You should see a new properties box appear for this object, titled **CN=Directory Service Properties**

---

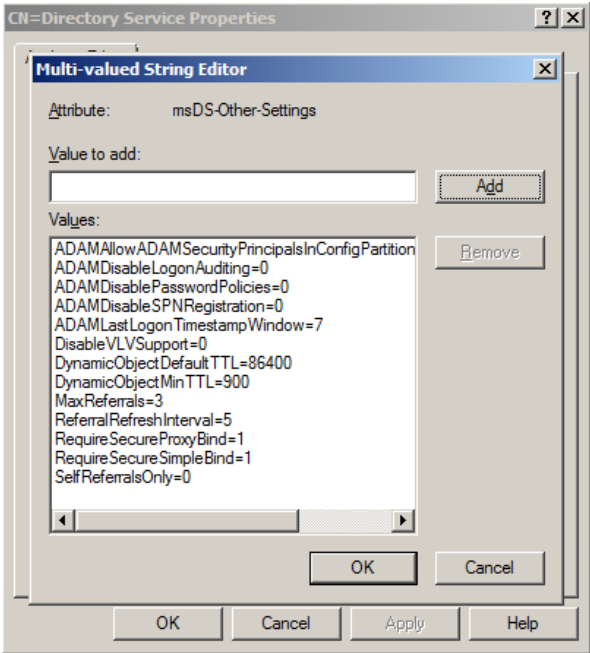
Notes:


# Extranet Auth Installation Guide

---

- 6. Scroll through the list and look for an attribute called **msDS-Other-Settings** and double click it.
- 7. We will want to change the requirement for **RequireSecureSimpleBind** (default is off for non-encrypted simple binds) to require encryption. Even though we will not be using simple binds, because we will be using an SSL cert there is not a good enough reason not to. When you highlight and click remove, it will move the line text up to the textbox, so you just have to replace the 0 with a 1. Close ADSIEdit once done.

Below is an example:



Notes:




# Extranet Auth Installation Guide

---

- 8. Go back to the **Server Manager** console application and return to the LDS role, and under **Advanced Tools** open the **ADSchemaAnalyzer.exe**

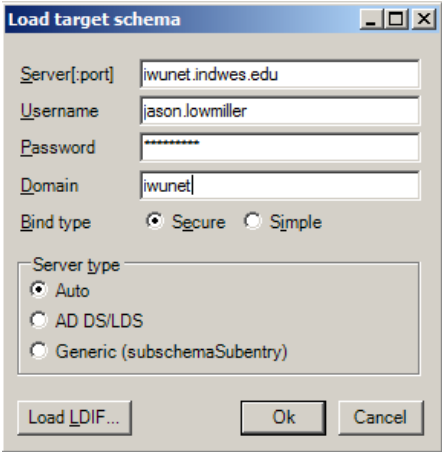


ADSchemaAnalyzer is a program that can look at two directory services (AD DS or AD LDS) and compare (and contrast) the data in both, and create files containing that differential data (if there are differences), or to backup existing data, so that it may be reimported elsewhere.

The program will open in a command prompt, but if you type ADSchemaAnalyzer in the command prompt, it will load the GUI interface to the program.

- 9. In the AD DS/LDS Schema Analyzer program, click **File> Load Target Schema**.

The target schema will be that of our production AD DS environment. Follow the example below and press **Enter**.

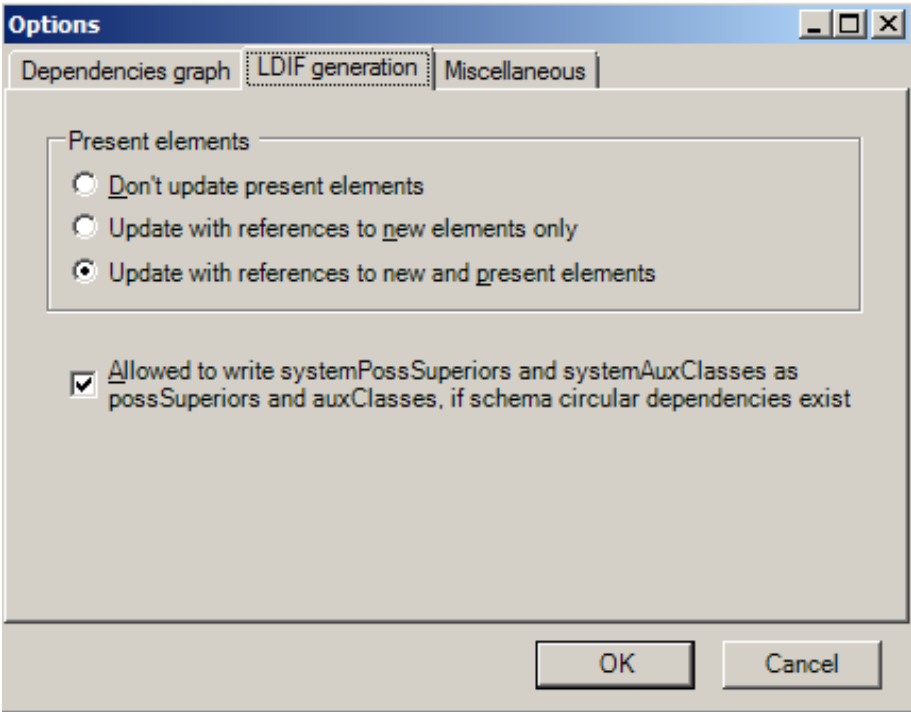


Notes:


# Extranet Auth Installation Guide

---

- 10. After the connection is made, we will want to click the **Tools > Options**, and in the options screen click on the **LDIF Generation** tab.
- 11. In this LDIF Generation tab area, we will want to change the **Present Elements** options to **Update with References to new and present elements**.



---

Notes:


# Extranet Auth Installation Guide

---

12. The next connection we will want to make is to the **base schema**, and that will be the LDS box that we are doing this operation from. So connect using information similar to that below:



Note that we are using **localhost** to help prevent confusion.

Load base schema

Server[port] localhost

Username jason.lowmiller

Password \*\*\*\*\*

Domain iwunet

Bind type  Secure  Simple

Server type

Auto

AD DS/LDS

Generic (subschemaSubentry)

Load LDIF... Ok Cancel

13. After the connection is made, you will see some data go past in the data window at bottom. When it's completed you should see something like this at the end:

Update Script  
Done comparing schemas.

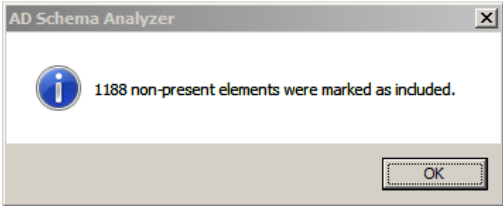
---

Notes:


# Extranet Auth Installation Guide

---

- 14. Once you see this, click the **Schema** menu and make sure that “**Show Present Elements**” is selected. Once this is selected, also select to “Mark all non-present items as included”. You should get a message box that looks a bit like the following:



In a production setting with our DC's we should expect to see a lot more data than this. Click **OK**.

- 15. Now we will save the information from the schemas into our own ldif file for importing into our LDS schema.

Click **File > Create LDIF File** and name the file something pertinent yet compact (ex: extranet.ldf); we will need to work with the file from the command line in just a bit. The file will want to save to **C:\Windows\Adam**. Please save it to this location and exit the program. (ex: c:\windows\adam\extranet.ldf)

---

Notes:


# Extranet Auth Installation Guide

---

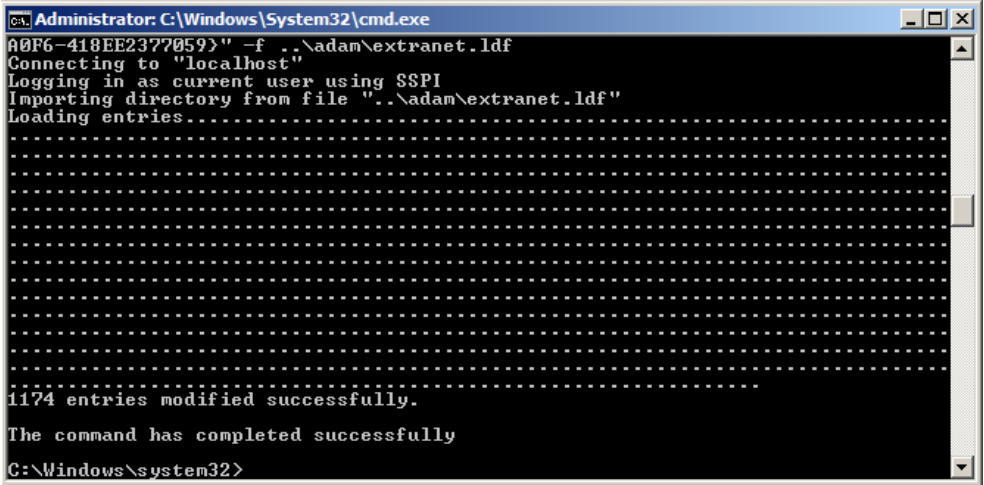
16. Return to the server manager console application, and to the LDS role and instance that we have configured. Underneath **Advanced Tools** we will want to click on **ldifde.exe**

This program will launch a command prompt, in the directory of **C:\windows\system32** which is where ldifde.exe lives. We will next need to import our saved file into our AD LDS system.

17. In the command prompt type:

```
ldifde -i -k -s localhost -c "DC=X" "CN={98F208B7-E7E7-4405-A0F6-418EE2377059}" -f ..\adam\extranet.ldf
```

18. After the above has completed executing you should see something like the following:



Notes:


# Extranet Auth Installation Guide

---

In a production AD DS environment you may expect to see a much higher “entries modified” number.

## Adamsync Setup and Initialization

Adamsync is the utility that we will use to automatically synchronize the user objects that live in AD DS into AD LDS, as well as their group membership information. Only objects that meet specific parameters (for instance either being (or not being) in a particular group, etc.) will be synchronized.

The synchronization runs by scheduled task. The first initial sync (since there were none previous) runs a full sync. Sync’s following are then done on as changed basis.

These parameters of what gets synchronized and where, lives in an XML file that is specific to the LDS partition (the DC=iwunet,DC=indwes,DC=edu) that we created when we first setup the instance. Any LDS server can have any number of LDS instances, and as such, Adamsync can contain multiple XML files in order to handle each instance.

In the setup files that I have created, the XML file is set to look for specific items, and we’ll go through the XML line by line.

## Installing the Adamsync XML File

1. Return to the server manager console, and under the roles section, select the LDS Role. Under the advanced tools, click on **Adamsync.exe**. It will load a command prompt like the other tools that we’ve used before.
2. See if there are any installed adamsync xml files already installed. At the command prompt type (and press Enter):

```
adamsync /list localhost
```

---

Notes:


# Extranet Auth Installation Guide

---

You will not get any files listed back if this is the first installation. If you do, you will need to delete them first before we install them.

- 3. To delete any previously installed adamsync files run the following command at the command prompt. You may need to adjust the context information to point to the correct partition if working with multiple instances of LDS:

```
adamsync /delete localhost "DC=iwunet,DC=indwes,DC=edu"
```

- 4. The XML file is shown on the last page, parts of it have been removed that contain no changed data for sake of brevity:

- 5. What it all means:
  - a. **Lines 1 through 10** basically setup very typical information, the security mode has two options, the one we are using (object) is for read only operation to the DC's. The other mode (partition) would allow for the possibility of LDS to make changes to the DC's.

The source information that is being spoken of refers to the name of the AD DS member server we want to grab data from. So we can pull information from either server, we choose the round robin DNS name of iwunet.indwes.edu. In the event that either server is unreachable, the theory is that it will try until a successful connection is made.

Therefore the source partition information should be in our case:  
DC=iwunet,DC=indwes,DC=edu

The target information spoken of in the XML refers to LDS, in this perspective. Because we want to mimic our DN, we chose the same values

---

Notes:


# Extranet Auth Installation Guide

---

(even though we wouldn't have needed to, for complexity sake, we used the same DN structure)

- b. **Lines 11-22** refer to AD DS, and the constraints for what DN we are pulling information from (line 12). LDS is flexible enough to adjust the scope to include as many (or as few) objects as possible, and their structure.

**Line 13** determines on what objects get synchronized. We are only after user objects (or objects that are specified by that class), but we also want their group membership information. While we are at it, we also only want to synchronize objects that are not disabled, and we have added a group called "ProxyAccess". If a user is not in this group, their "user object" will not be brought over into LDS.

**Lines 15-19** contain the actual specific data that we are bringing over into LDS. We don't want (or need) all of the specific users object data.

**Lines 24-25** specifies that when user objects are brought in, they are modified to no longer be considered to be defined by the User class, but by the userProxy class. The userProxy class specifies how the authentication is handled (by a Microsoft API that passes the credentials to the DC's)

**Line 29** sets the frequency with which each objects data is checked for consistency on sync's. 0 would mean that there would be no checks. (An objects aging TTL would max out at 1 day, and then object would be removed, but this seems not idea). A 1 would mean that at every sync each object would be checked for consistency. A 2 would mean that every other sync (and on from there).

---

Notes:




# Extranet Auth Installation Guide

---

## extranet.xml

1. <?xml version="1.0"?>
2. <doc>
3. <configuration>
4. <description>IWU Adamsync File</description>
5. <security-mode>object</security-mode>
6. <source-ad-name></source-ad-name>
7. <source-ad-partition>dc=iwunet,dc=indwes,dc=edu</source-ad-partition>
8. <source-ad-account></source-ad-account>
9. <account-domain></account-domain>
10. <target-dn>dc=iwunet,dc=indwes,dc=edu</target-dn>
11. <query>
12. <base-dn>dc=iwunet,dc=indwes,dc=edu</base-dn>
13. <object-filter>(|  
(&!(objectClass=user)(objectCategory=person)(!userAccountControl:1.2.840.113556.1.4.803:  
=2)(!memberOf=CN=ProxyDeny,CN=Users,DC=iwunet,DC=indwes,DC=edu))(objectClass=grou  
p))</object-filter><attributes>
14. <include>objectSID</include>
15. <include>sourceObjectGuid</include>
16. <include>member</include>
17. <include>userPrincipalName</include>
18. <include>uid</include>
19. <exclude></exclude>
20. </attributes>
21. </query>
22. <user-proxy>
23. <source-object-class>user</source-object-class>
24. <target-object-class>userProxy</target-object-class>
25. </user-proxy>
26. <schedule>
27. <aging>
28. <frequency>1</frequency>
29. <num-objects>0</num-objects>
30. </aging>
31. .... fields with no data removed for sake of brevity.
32. </doc>

---

Notes:


# Extranet Auth Installation Guide

---

- 6. To install our XML file (file is on next page) for adamsync, run the following command:

```
adamsync /install localhost extranet.xml
```

- 7. Run the initial synchronization:

```
adamsync /fs localhost "DC=iwunet,DC=indwes,DC=edu"
```

- 8. Additional syncs needs to be run with the following command. A scheduled task should be setup to do this procedure once every 15 minutes:

```
adamsync /sync localhost "DC=iwunet,DC=indwes,DC=edu"
```

- 9. To view data in the LDS data stores, use **ADSI Edit** and connect to it specifying the DN as "DC=iwunet,DC=indwes,DC=edu" but for server Localhost.

## Removing AD LDS Instances

- 1. AD LDS instances may be removed in the **Control Panel** like any program that has been installed, under **Programs and Features**.

---

Notes:
