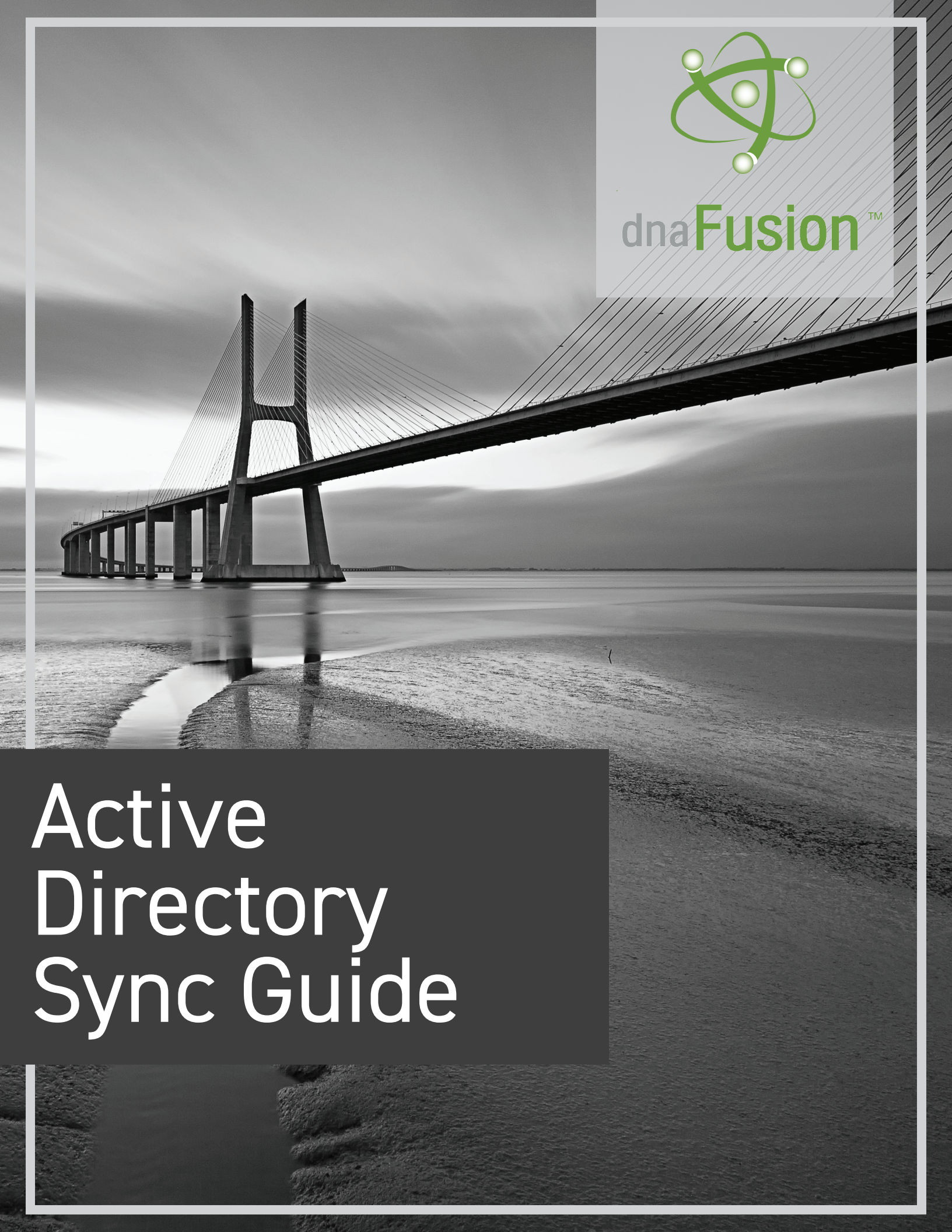


Active Directory Sync Guide

This Page Intentionally Left Blank

Active Directory (AD) Sync with DNA Fusion

Introduction

The purpose of this guide is to provide you a step-by-step method of integrating your existing Active Directory network or users into DNA Fusion for the purpose of automatically adding and deleting user rights in an access control environment based on the associated DNA Fusion Operator profile category. By doing so, you reduce the necessary workload needing to be performed by the access control administrator allowing them to focus on the proper integration and management of the overall system.

In This Guide

- DNA Fusion Operator Groups
- Integrated AD Sync Service
- Features with Plugin

Note: this feature while offered by DNA Fusion requires the purchase of a separate plug in and is offered in versions of DNA Fusion 7.X+

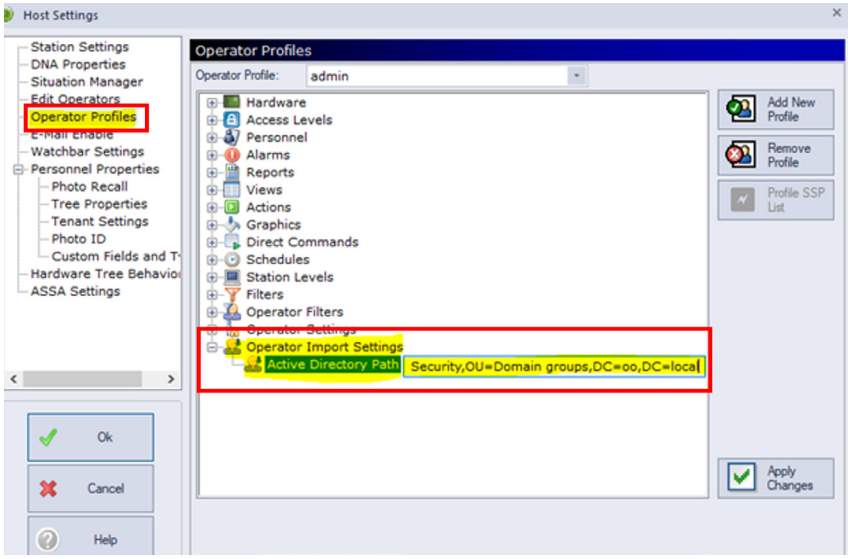
DNA Fusion Operator Groups:

DNA Fusion Operator Profiles are security profiles found within DNA Fusion allow for the assigning of specific roles based on DNA Permissions assigned to a profile when logging into DNA.

While Operator Profiles serve an essential function in only allowing users logged in to DNA to have only the privileges and rights required by each user group, with AD Sync, you can also separate AD Common Name group for each DNA Profile. While the number of groups needed for each system will differ, the most common used are:

- Admin
- Security
- Badging

The current AD group assigned to a user can be locate through the “DNA Properties” window in “Operator Profiles” as shown below:



DNA Fusion Active Directory Sync Service

The AD Sync Service is an application that must be integrated to DNA Fusion through the use of an installation file. The install file can be downloaded using the following address link shown below.

http://license.ooaccess.com/download/ADSyncService

Additionally, prior to installing the separate application as a service, any old AD installation files must be removed. To accomplish this you must:

1. **Stop** the "DNADrvr32" driver
2. **Remove** the "ADSync Folder" and its contents from the folder:

   C:\programfiles(x86)\DNAFusion\Plugins

3. **Run** the installation file and **Configure** using the installation and configuration steps mentioned previously in this guide.

Note: During the install, the configuration file:

C:\Users\Public\Documents\Open Options, Inc\DNA Plugins\Plugin.ADSync.config) will be moved to:

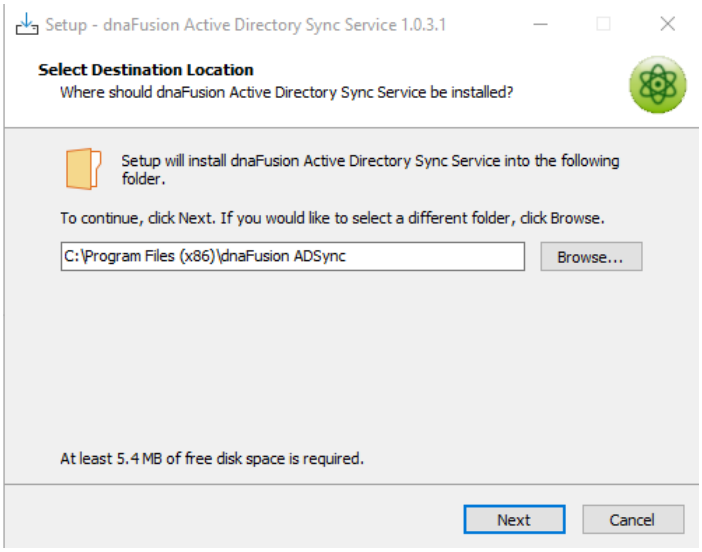
C:\Users\Public\Documents\Open Options, Inc\ADSync\ADSync.config

The log files will be stored in C:\Users\Public\Documents\Open Options, Inc\ADSync\Log Files

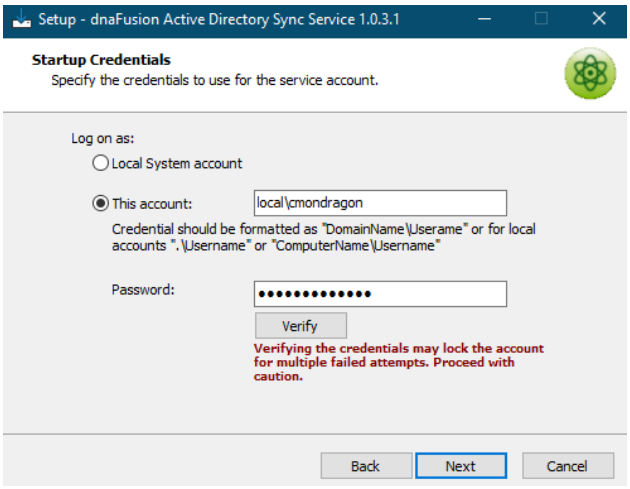
Any settings will automatically be copied over for upgrades.(including conversions from plugin to services)

Installation:

1. **Double-Click** the "ADSyncService.exe" file to begin the installation. A New Window will appear. **Confirm** the install location. The default location is the C:/ drive. **Click** "Next".

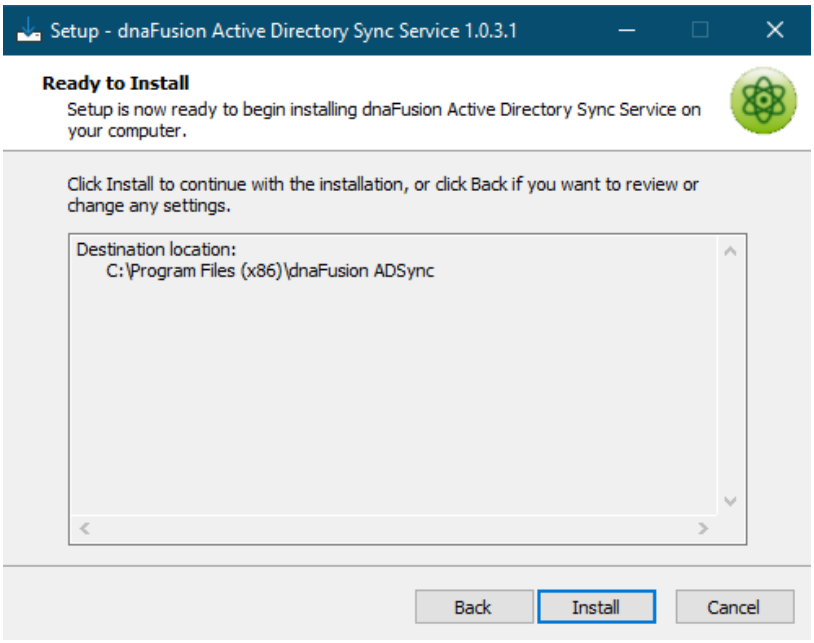


2. **Input** the "Startup Credentials" for the service account. The service account must have "Administrator" level privileges assigned for the AD groups that need to be integrated. **Click** "Next".

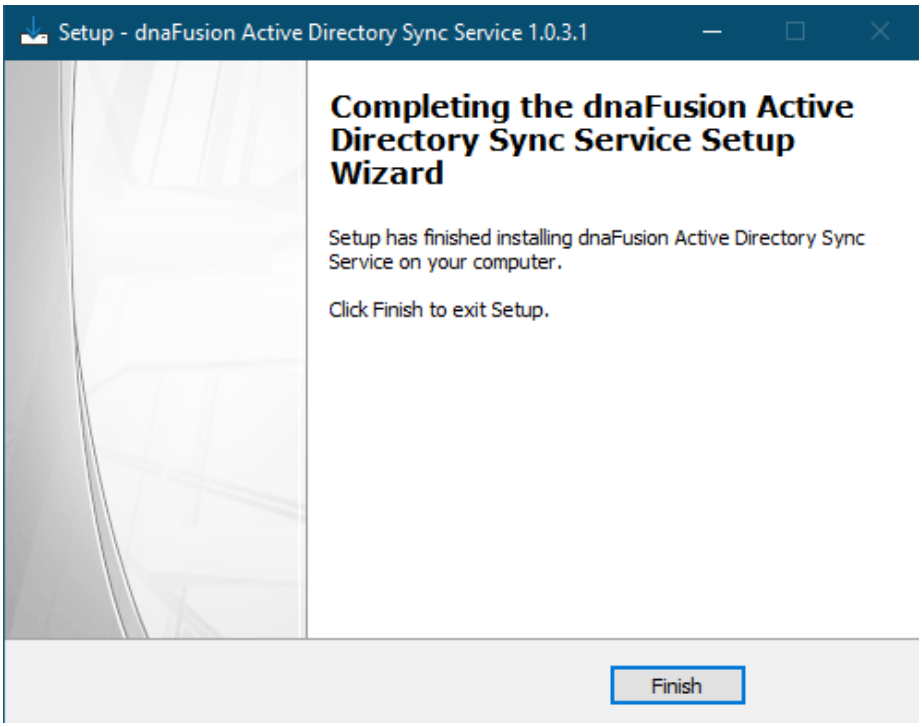


The AD Sync Service account should be the same account as used in the DNADrvr32 service.

3. **Click** “Install” to begin service installation with provided settings.



4. **Click** “Finish” once the service installation has completed.



Different Features with AD Sync Service:

Override profiles: When properly configured, you can use this service to allow profiles to be synced without any additional configuration being done within the DNA Fusion application. This is accomplished through the use of a new element called ***<OverrideProfiles>*** which is added to the ***<Option>*** section of the configuration XML as the example shown below.

```
<SyncConfig>
  <Ignore>
    <Operator>
      <Name>admin</Name>
    </Operator>
  </Ignore>
  <Options>
    <DefaultPassword>Random</DefaultPassword>
    <Interval>1</Interval>
    <IntervalRate>Hours</IntervalRate>
    <PurgeMethod>Disable</PurgeMethod>
    <SyncOnStartup>true</SyncOnStartup>
  </Options>
  <Queries>
    <Path></Path>
  </Queries>
</SyncConfig>
```

Configuration File Key Points:

When configuring the script in the override files there are a few key items to pay attention to:

<PurgeMethod>: The Purge method should be set to ***Disable*** . Although this setting can be set to ***Remove*** , setting it to disable will allow you to shut off any accounts without accidentally deleting operators unintentionally.

<Name> and </Operator>: When adding "Operators" to ignore, each operator must be separated with the ***<Operator>*** tag at the beginning of every ***<Name>Operator1</Name>*** sequence and ***</Operator>*** at the end, for example:

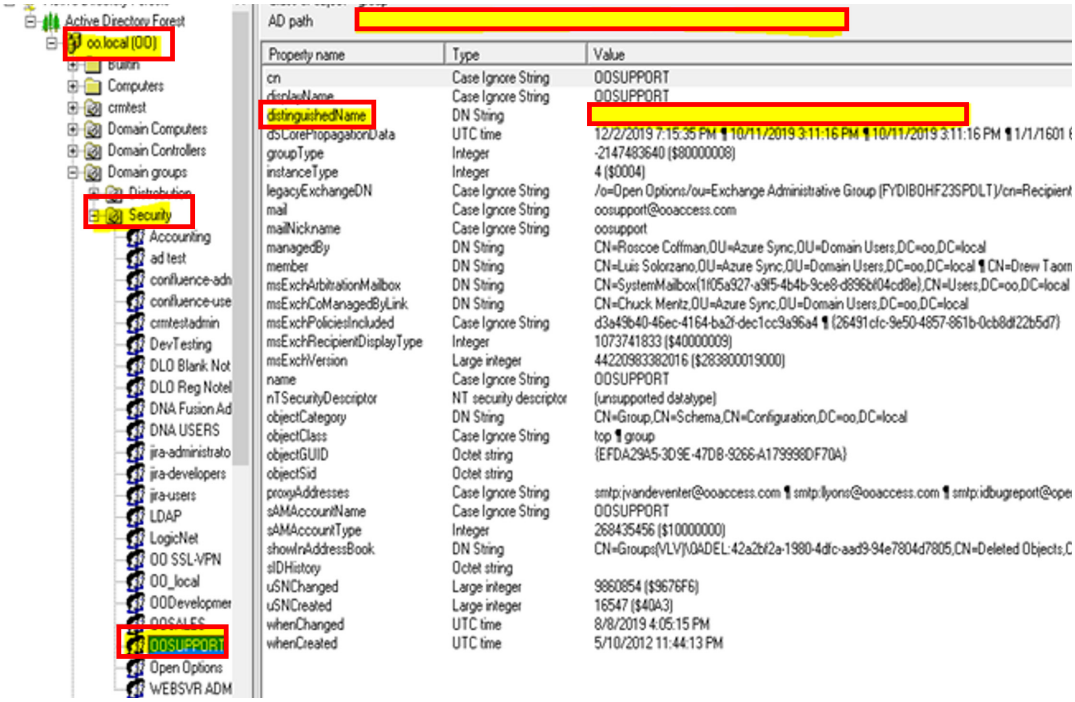
<Ignore>
<Operator>
<Name>Operator1</Name>
</Operator>
<Operator>
<Name>Operator2</Name>
</Operator>
<Operator>
<Name>Operator3</Name>
</Operator>
</Ignore>

<Interval> and <IntervalRate>: The interval rate can be set to Hours and Minutes. While the rate is user dependent, we recommend the settings of either 1 hour or 15 or 30 minutes to start in order to reduce large delays in updates or updates happening too continuously to allow for proper DNA Fusion operation.

<SyncOnStartup>: When set to "True" the plugin will commence sync'ing with AD within approximately a minute after start up or, if set to, False it will begin at the predetermined refresh interval.

Integrating the AD Service:

The settings of ***<Path>***, ***<Individual>***, ***<Group>*** and ***<MemberOf>*** should be taken directly from the active directory address listing and be based on the Operator who is creating the AD Sync as pictured below based on the AD:



Note: While each Operator of DNA Fusion can have different AD groups assigned to them, care should be taken when determining which groups will be assigned to which Operator.

Server Login Override: When required, you will now be able to provide details for logging into the AD Server that you will be using. This can now be accomplished through the Queries section by adding the elements of ***<Server>***, ***<UserName>*** and ***<Password>*** to facilitate updates from the AD. This service is optional and an example can be seen below:

```
<Queries>
    <Server>192.168.1.253</Server>
    <UserName>ADTest\Administrator</UserName>
    <Password>Password1</Password>
    <Path>LDAP://192.168.1.253/dc=adtest,dc=local</Path>
    <Group>(&amp;(objectCategory=person)(memberof:1.2.840.113556.1.4.1941:={0}))</Group>
    <Individual>(&amp;(objectCategory=Person)(sAMAccountName={0}))</Individual>
    <MemberOf>(&amp;(objectCategory=organizationalPerson)(memberof:1.2.840.113556.1.4.1941:={0})(sAMAccountName={1}))</MemberOf>
</Queries>

```

Email Sync: Email sync will now sync based on the AD user operator email taken from the AD profile's "userPrincipleName"

This Page Intentionally Left Blank