



Built right. Just for you.

AD SYNCHRONIZATION GUIDE



greenhousedata.com

*Green House Data
340 Progress Circle
Cheyenne, WY 82007*

Contents

OVERVIEW..... 3

Prerequisites.....3

ACTIVE DIRECTORY SYNCHRONIZATION SERVICE INSTALLATION 3

Prerequisites.....3

How to Install3

FAQ 5

Troubleshooting FAQ.....5

What happens if synchronization does not occur for some time due to an internet outage for maintenance on a local Domain Controller? 5

How can I check the status of the synchronization process between my local domain and Green House Data’s hosted platform? 5

How can I determine which Domain Controller is functioning as the “listener” for Green House Data’s Synchronization Service?..... 5

Where can I view the AD Sync logs? 5

I accidentally deleted a local user and they no longer exist within Green House Data’s Control Panel, can they be recovered? 5

General FAQ.....6

How does Green House Data’s Active Directory Synchronization Service connect to Green House Data’s Control Panel? 6

When do passwords become synchronized with Green House Data’s Control Panel? 6

What ports do I need to allow for communication between Green House Data’s Control Panel and our Domain Controllers? 6

If I make a change within Green House Data’s Control Panel, will the changes be reflected within my local domain? 6

What attributes are synchronized by default from my local domain to Green House Data’s Control Panel? 6

What additional attributes can be synchronized from my local domain to Green House Data’s Control Panel and how can I accomplish this? 7

Can I rename or change the AD Sync account password we created within the Control Panel?..... 7

Can I synchronize password expiration data with Green House Data’s Control Panel?..... 8

How can I find what accounts have the UPN and PrimarySMTP mismatched? 8

OVERVIEW

Green House Data's Active Directory Synchronization Service (AD Sync) provides an ongoing, one-way synchronization from your Active Directory (AD) environment(s) to your hosted domains within the Control Panel. The service allows you to synchronize your Domain Controllers (DCs) to Green House Data's Hosted Platform. The sync'ed user's properties will appear read-only within the Control Panel.

Green House Data's Active Directory Synchronization Service must be installed on all DCs within your forest to synchronize any changes that occur.

Prerequisites

Prior to the installation of AD Sync, it is highly recommended that your users' UPN and primary SMTP address match. A Green House Data engineer can assist in determining mismatched UPNs and primary SMTP addresses for existing and new customers.

Create a new user within your customer domain called **ADSync@yourdomain.com** as this will be used during the installation process.

Your Domain Controllers need to communicate to Green House Data's infrastructure over port 443 and no inbound ports are required for communication.

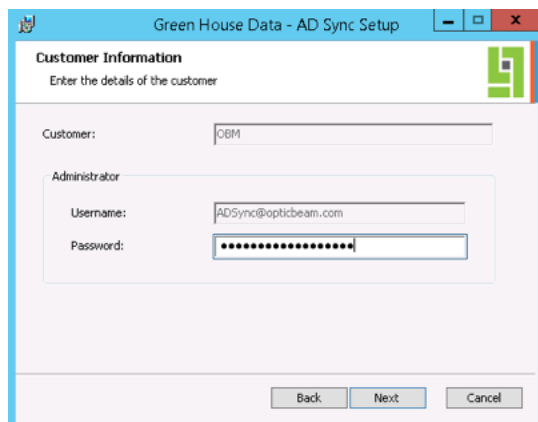
ACTIVE DIRECTORY SYNCHRONIZATION SERVICE INSTALLATION

Prerequisites

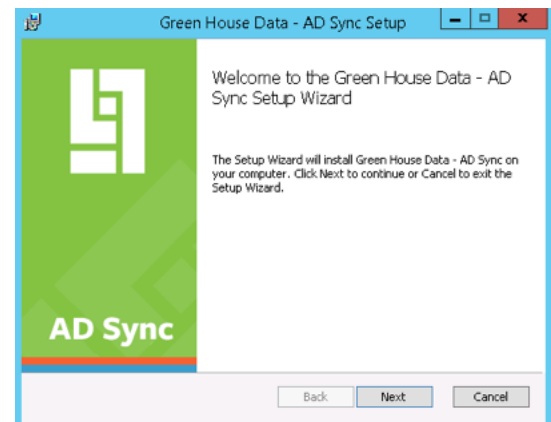
1. Create an Active Directory group called ADSync

How to Install

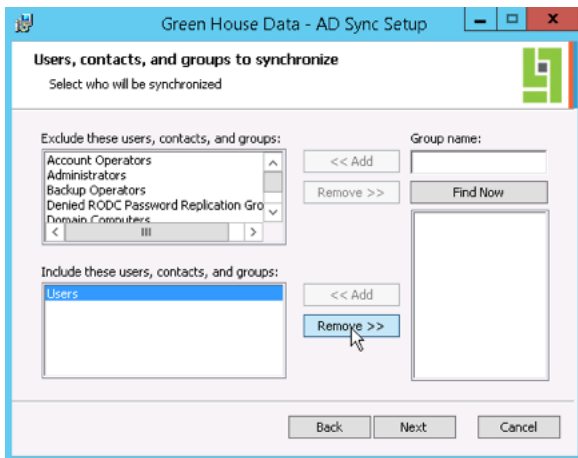
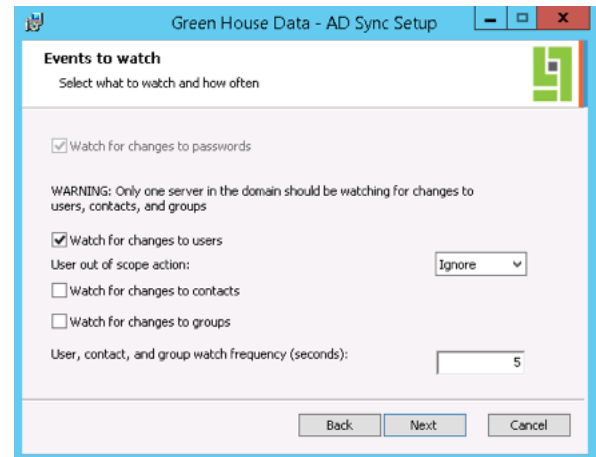
1. Login to <https://cp.greenhousedata.com> using the created AD Sync username and password.
2. Select Services > AD Sync > AD Sync Download
3. Select the Download link to start the download
4. Copy the file to all of your Domain Controllers
5. Run ADSyncSetup.exe (on each of your Domain Controllers)
6. Click Next
7. Input the password (set when creating the account) and click Next



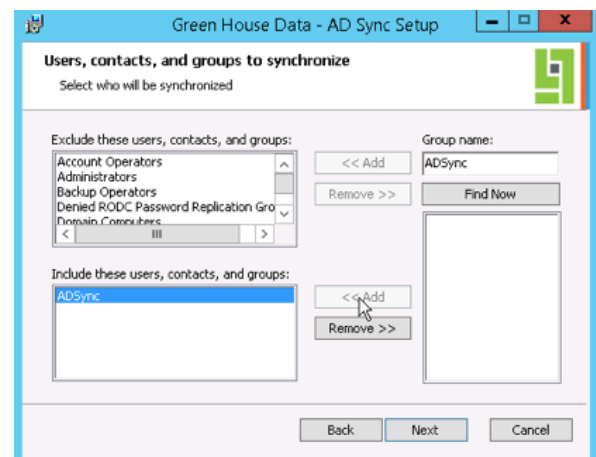
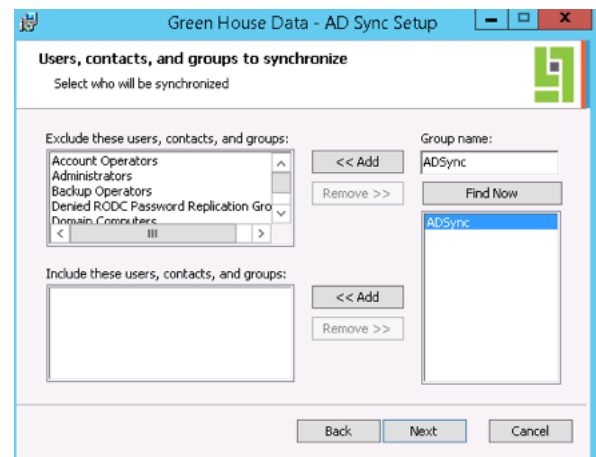
The screenshot shows the 'Customer Information' screen of the AD Sync Setup wizard. It prompts the user to enter the details of the customer. The 'Customer' field contains 'CBM'. The 'Administrator' section includes a 'Username' field with 'ADSync@opticbeam.com' and a 'Password' field with masked characters. Navigation buttons for 'Back', 'Next', and 'Cancel' are at the bottom.



8. Select the checkbox “Watch for changes to user”
 IMPORTANT: Only select this if it is the first domain controller within your forest.
9. Click Next
10. Highlight Users within the “Include these users, contacts and groups” list
11. Click Remove >>



12. Within the Group Name field, input ADSync
13. Click Find Now
14. Select ADSync from the list
15. Click << Add
16. Click Next
17. Click Next
18. Click Next
19. Click Next
20. Click Next
21. Click Install
22. Click Finish
23. Click Yes to restart your system
24. After your domain controller restarts, add all the users you wish to have synchronized to the ADSync Active Directory group.
25. Have all the users in the ADSync group change their passwords.



FAQ

Troubleshooting FAQ

What happens if synchronization does not occur for some time due to an internet outage for maintenance on a local Domain Controller?

All changes are stored within the AD Sync Queue and once connectivity has been restored, the changes will be processed on a first-in, first-out basis.

How can I check the status of the synchronization process between my local domain and Green House Data's hosted platform?

Visit <https://cp.greenhousedata.com>, login with the AD Synchronization account that was setup and select Services > AD Sync > AD Sync Server Monitor. This will display all servers that have checked in and provided updates.

How can I determine which Domain Controller is functioning as the "listener" for Green House Data's Synchronization Service?

Generally, the first AD Sync service that is installed within the local forest becomes the "listener" for your domain; you can review the ADSync.exe.config file located at "C:\Program Files\AD Sync", look for the value called UserSync and if this is set to True, then this is your "listener" domain controller. Otherwise, the service on the domain controller is only watching for password changes.

Where can I view the AD Sync logs?

There are two places to view logs:

1. Open Event Viewer on the Domain Controller where the service is installed and review the Application log for events from Source "Green House Data - AD Sync".
2. Review the daily log files that are stored at "C:\Program Files\Green House Data - AD Sync\Logs".

I accidentally deleted a local user and they no longer exist within Green House Data's Control Panel, can they be recovered?

If a user object was deleted from the local Active Directory domain while still a member of the synchronization group, Green House Data's AD Sync Service will automatically remove it from the Control Panel and any associated services.

You will need to create a new account or restore the user object from a tombstone within the local Active Directory domain, add the user as a member of the synchronization group, and notify support@GreenHouseData.com to reconnect the disconnected mailbox.

General FAQ

How does Green House Data's Active Directory Synchronization Service connect to Green House Data's Control Panel?

The AD Sync service monitors changes within the SYSVOL share using a filter driver installed during setup and it monitors for in-memory transactions on user, contact and group objects.

Once a change has been detected, the service establishes an HTTPS (encrypted) connection to Green House Data's Control Panel and the changes are then processed within the Control Panel.

Changes that are detected include attribute changes, accounts being disabled/enabled and also object deletions.

IMPORTANT: Only local Active Directory objects that are members of the AD Sync group will be synchronized to Green House Data's Control Panel.

When do passwords become synchronized with Green House Data's Control Panel?

Passwords only become synchronized AFTER AD Sync has been installed and the password has been changed within the local domain.

What ports do I need to allow for communication between Green House Data's Control Panel and our Domain Controllers?

Your Domain Controllers need to communicate to our infrastructure over port 443 and no inbound ports are required for communication.

If I make a change within Green House Data's Control Panel, will the changes be reflected within my local domain?

No, the synchronization process is only one-way.

What attributes are synchronized by default from my local domain to Green House Data's Control Panel?

- fullName
- firstName
- lastName
- password
- physicalDeliveryOfficeName
- department
- userPrincipalName
- description
- telephoneNumber
- wWWHomePage
- streetAddress

- postOfficeBox
- |
- co
- info
- s
- postalCode
- homePhone
- pager
- mobile
- facsimileTelephoneNumber
- ipPhone
- title
- manager.sAMAccountName
- objectSid
- userEnabled

What additional attributes can be synchronized from my local domain to Green House Data's Control Panel and how can I accomplish this?

- division
- company
- extensionAttribute2
- extensionAttribute3
- extensionAttribute4
- extensionAttribute5
- extensionAttribute6

In order to add the additional attributes, perform the following:

1. Stop the Green House Data – AD Sync Service
2. Edit the SetUser.xml configuration file located at “C:\Program Files\AD Sync\Requests”
3. Under the additionalproperties tag, copy and paste an existing property and modify the data with the additional attribute.

Example of company:

```
<property templatedependency=” company “>  
  <name> company </name>  
  <value>{company}</value>  
</property>
```

4. Start the Green House Data – AD Sync Service

Can I rename or change the AD Sync account password we created within the Control Panel?

Yes, the password and account name can be changed after the synchronization has been configured, but it is not recommended as passwords changed during this time period will not be synchronized. See below for the steps (How to re-install and/or perform an upgrade) after the password or account change has been made.

Can I synchronize the password expiration data with Green House Data's Control Panel?

No, Green House Data's Active Directory Synchronization Service does not currently support the replication of the expiration date from your Domain Controllers.

How can I find what accounts have the UPN and PrimarySMTP mismatched?

From your on-prem Exchange server, if it's at minimum Exchange 2007 SP2, you can run the command below which will export the mismatched addresses out to a CSV.

```
Get-Mailbox -ResultSize 100 | where {$_.PrimarySmtpAddress -notlike $_.UserPrincipalName} | select Alias, Identity, UserPrincipalName, PrimarySmtpAddress, EmailAddresses, DisplayName | Export-Csv mismatch.csv -NoTypeInformation
```