APPTIX™

EMAIL • CALL • UNITE

Technical Overview

Active Directory Synchronization

Document Revision: March 15, 2010

Description of Active Directory Synchronization

Active Directory Synchronization (AD Sync) is a utility that performs a one way synchronization from a customer's Active Directory (AD) database to the Apptix OnDemand (AOD) hosted AD database. This utility provides customers a single point to create, modify or delete Exchange, SharePoint and Office Communicator accounts. AD Sync will make the end user experience even better with password synchronization which synchronizes their local domain password with the AOD domain, providing end users with one password. New customers migrating to Apptix will benefit greatly by being able to easily duplicate their Active Directory structure with Apptix using the AD Sync utility.

The unobtrusive Sync Agent is installed on a server in the customer's network, and securely transmits all of the AD changes over a secure Internet connection. All synchronization is one-way from the customer's AD to Apptix's platform, which reduces the permissions needed by Apptix at the customer AD, and prevents Apptix from writing any data to the customer AD. Configurable Instant Services Provisioning allows unattended provisioning of the Exchange mailboxes, SharePoint site access rights, and OCS user accounts to the newly registered AD users.

Features and Benefits of AD Sync

The following features are available in the AD Sync utility.

1. **User Accounts Synchronization** - AD Sync allows for the customer administrators to manage a local copy of the corporate AD and synchronize the following AD "events" to the hosted AD version on AOD:
    - New Users, Contacts
    - Deleted Users, Contacts
    - Change to Distribution Lists
    - Password changes
    - Updated attributes such as mailing address, phone number, etc.
2. **Synchronizing user password changes** - The Password Filter and Password Change Listener securely deliver the password change requests to AOD to ensure the unified sign-in experience. During the initial synchronization the passwords for the new users are auto-generated. After that, when a user changes password in external AD, it is passed to AOD by AD Password Change Filter component. If the customer opts to not synchronize passwords, the Password Filter and Password Change Listener are do not need to be installed.
3. **Partial Domain synchronization** - customers can choose a set of Active Directory Organization Units to be synchronized to AOD and apply additional filter conditions for the user accounts / contacts.
4. **Selective Attribute synchronization** - customers can limit the set of attributes to be synchronized. See the section below that outlines these attributes.
5. **Address Book Synchronization** - Changes to contacts in local Exchange Address Book would be automatically propagated to the hosted Exchange Address Book
6. **Configurable Synchronization** - All data synchronization can be configured by the administrator from Apptix's Control Panel. The administrator has the ability to configure what data is synchronized, and when the data is synchronized. The following list outlines some of the configurations that can be made to the data synchronization'
    - Configurable delays between synchronization times/delays (3 hours by default)
    - Configurable new user creation options (to create Exchange mailbox, SharePoint accounts, OCS)
    - Configurable behavior on user deletion (e.g. to delete associated Exchange mailbox or just disable)
    - Password synchronization can be enabled or disabled
    - Synchronization of Contacts can be enabled or disabled
    - Synchronization of Distribution list changes can be enabled or disabled
    - One or more customer Organization Units (OUs) within customer AD can be selected for synchronization
    - Filters on users, contact, distribution lists or any attributes can be configured to "ignore" during synchronization
7. **Instant User Provisioning** - Newly created AD users can be instantly provisioned in AOD without manual intervention by the local administrator

8. **Instant Services Provisioning** – Services can be enabled automatically and seamlessly for users that are added to AOD. The services that can be provisioned in AOD include:
    a. Exchange Mailbox
    b. SharePoint Site Access Rights
    c. OCS User Account
9. **Security -** All synchronization is a secure, one-way synch from the customer's network into the AOD platform. Apptix will never write data from the hosted AD to the customer's AD. This reduces the permissions and service accounts Apptix needs at the local AD level.
    a. SSL encryption over public networks
    b. Encryption for passwords within local network

Synchronization of user data can be established prior to, or after, the user's mailbox is created and in use in AOD. Likewise, the synchronization can be disabled at any time, and re-established with no affect on the accounts and services of the end user.

NOTE: AD Sync is not a single sign-on tool. The utility allows for passwords to be synchronized from the customer's local AD to the Apptix AOD AD. The end users will still need to login to the hosted services (Exchange, SharePoint, OCS, etc), only now, their password will be the same as their local domain password.

Selective Attribute Synchronization

Customers can restrict the set of attributes that are synchronized to the online services. The following table provides the complete list of the attributes supported for User and Contact objects:

Synchronizable attributes. "■"- mandatory, "◘" - optional, "-" - not applicable.

POA Attribute	AD Attribute(s) Involved	User	Contact	Comments
Display name	displayName mailNickname givenName + sn	■	■	The 1st non empty combination of AD properties is used
External DN	distinguishedName	■	■	
-	uSNChanged	■	■	Attribute is used internally for an entity changing detection.
Login	userPrincipalName mailNickname SAMAccountName	■	-	The first non empty AD property is used
Enabled	userAccountControl	■	-	
External email	targetAddress	-	■	
Alias	mailNickname	◘	◘	AD property is available in case when Exchange is installed in a customer's AD.
First Name	givenName	◘	◘	
Last Name	sn	◘	◘	
Description	description	◘	◘	
Office	physicalDeliveryOfficeName	◘	◘	
Telephone	telephoneNumber	◘	◘	
Web Page	wWWHomePage	◘	◘	
Primary Email	mail	◘	-	

POA Attribute	AD Attribute(s) Involved	User	Contact	Comments
Password	objectSid	◘	-	The **objectSid** property is mandatory if password synchronization is enabled. Passwords changes are traced with special password filter installed on each Domain Controller.
Street	streetAddress	◘	◘	
City	l	◘	◘	
State / Province	st	◘	◘	
Zip / Postal code	postalCode	◘	◘	
Country	c	◘	◘	
Country	co	◘	◘	
Home Phone	homePhone	◘	◘	
Pager	pager	◘	◘	
Mobile Phone	mobile	◘	◘	
Fax	facsimileTelephoneNumber	◘	◘	
IP Phone	ipPhone	◘	◘	
Title	title	◘	◘	
Department	department	◘	◘	
Company	Company	◘	◘	
-	Initials	◘	◘	
-	postOfficeBox	◘	◘	
-	info	◘	◘	
Email addresses / SIP addresses	proxyAddresses	◘	◘	
Group membership	memberOf	◘	◘	There will be implemented a complex logic for membership relations importing
Show in Address Book	msExchHideFromAddressLists	-	◘	The **show_in_address_book** is equal to (*NOT* **msExchHideFromAddressLists**).

Technical Description of AD Sync

Upon the completion of the customer qualifications section of this document, Apptix's Implementation Team will review the document, and contact the customer directly to discuss and schedule a time and date to install the AD Sync utility.

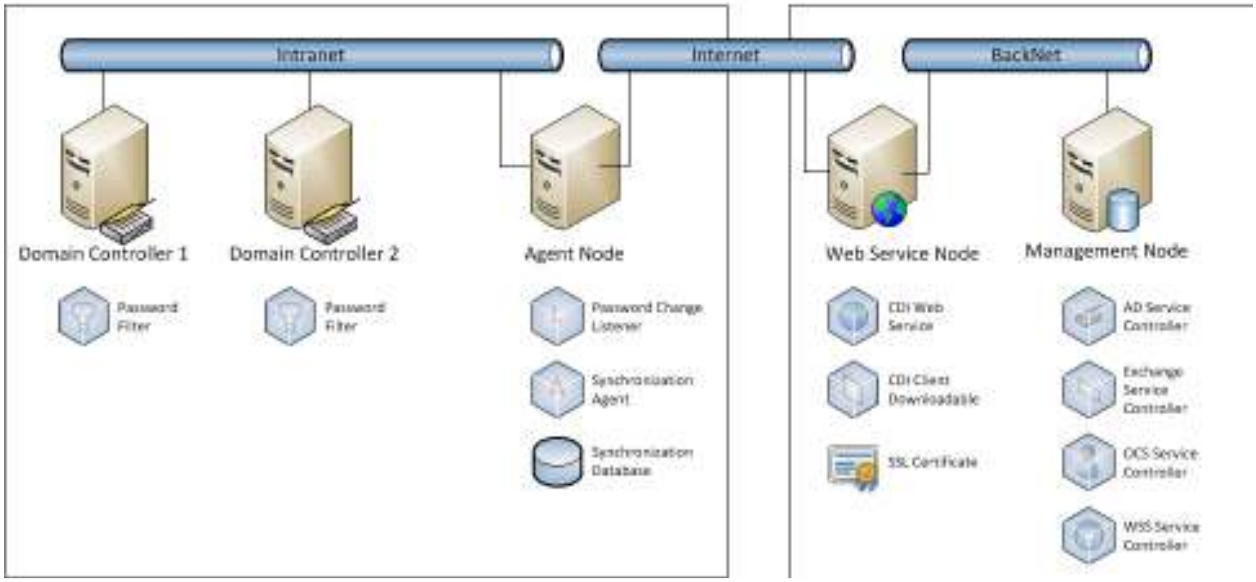
This utility is not a self-provisioning utility. Apptix's Implementation Team will work with the customer to ensure that the utility is properly activated within AOD, and the agents are correctly installed in the customer's network.

NOTE: Once AD Sync is activated and configured all modifications to the hosted AOD AD, must be made at the local AD level. The ability to modify the hosted AD will no longer be available to the customer administrators.

The AD Sync Utility is made up of the following two (2) agents to be installed in the customer's AD:

1. **Password Filter** – installed on domain controllers
2. **Synchronization Agent Node** – installed on a member server, or virtual machine, within the local domain

How AD Sync Works



Customer Premise Apptix Datacenter

1. The Password Filter runs on **every** Domain Controller in the customer's domain. It intercepts all the password changes and sends the new password data to the Password Change Listener.
2. The Password Change Listener runs on an Agent Node server, in the customer's domain. It encrypts the new passwords and writes them into the Password Synchronization Queue. The new password is delivered by the Synchronization Agent, which runs on the same Agent Node server.
3. The Synchronization Agent scans the customer's Active Directory for changes, and communicates the changes via a secure web connection, to the Web Service Node within AOD.
4. The Web Service Node is in Apptix' Datacenter. This node updates the hosted AOD Active Directory with the changes received from the Agent Node, and provisions the new services within the platform.

Hardware Requirements

The following hardware is required to run the Password Filter Agent:

1. Runs on every domain controller in customer's domain
2. Windows 2003 Server, or better, running as a Domain Controller
3. Optional, depending on if the customer chooses to synchronize passwords
4. A reboot of the domain controller is necessary after installation

The following hardware is required to run the Synchronization Agent Node:

1. A standalone server or virtual machine
2. Windows 2003 Server Release 2 or higher
3. A member of the customer's local domain
4. **Not** a Domain Controller
5. Trusted SSL certificate at the machine level

Firewall Rules

To ensure proper communication between the servers on the customer's premises, the following rules should be enabled:

Intra Communications

From	To	Protocol	Port
Synchronization Agent Node	Customer AD Domain Controller	TCP	389 (LDAP), 3268 (Global Catalog)
		TCP, UDP	88 (Kerberos)
Customer AD Domain Controller	Synchronization Agent Node	TCP, UDP	135 (DCOM

Outgoing Connections

From	To	Protocol	Port
Synchronization Agent Node	AOD Web Service Node	TCP	443 (HTTPS)

Customer Qualifications Checklist

Below are questions that should be answered prior to Apptix's Implementation Team engaging with the customer.

1. Are you a new or existing Apptix customer?
    - ○ New Apptix customer
    - ○ Existing Apptix Customer
        - AOD Account Number:
        - Customer Name:
2. What version of Windows is your organization running?
    - ○ Windows 2003
    - ○ Windows 2008
3. How many domains do you have, and what are their names?
        - Number of domains:
        - Name of domains:
4. How many domain controllers do you have?
5. How many Organizational Units (OU) do you have?
6. Will all of the OUs be synchronized with the AD Sync Utility?
    - ○ Yes
    - ○ No
7. How many users exist in your local AD?
8. How many users exist in your AOD account? (new customers only)
9. Do you have an available member server or virtual machine to run the Synchronization Agent Node?
    - ○ Yes
    - ○ No
10. What services are you looking to auto-provision (check all that apply)?
    - ○ Exchange
    - ○ SharePoint
    - ○ Office Communication Services 2007
11. Are you going to auto provision new users from your local AD to AOD?
    - ○ Yes
    - ○ No
12. Are you going to synchronize contacts and distribution lists? Approximately how many?
    - ○ Yes
    - ○ No
13. Are you going to synchronize passwords?
    - ○ Yes
    - ○ No
14. Please provide a diagram of your existing AD structure.
15. Please provide an LDIF (LDAP (Lightweight Directory Access Protocol) Data Interchange Format) dump from your existing AD.