
Data Sheet D: Integration with Active Directory

The Snap Solution integrates with Active Directory for the purposes of retrieving the user and group information and populating it into the Snap targeting database. This information can then be utilized for targeting content to certain users and groups.

The integration point between the Snap Solution and Active Directory is the Snap Client software. All queries against Active Directory are performed by the Snap Client software. The Snap Client software is the application that is installed on user's PCs and forms the client component of the Snap Solution.

The Snap Client periodically queries Active Directory for information about the current user and relays that information through to the Snap Server where it is saved in the Snap targeting database.

At no point does the Snap Server software communicate with Active Directory. (This is in contrast to some other solutions where the server components integrate directly with Active Directory).

Data exchanged is encrypted. As with all communications between Snap Client and Snap Server, the data exchanged is encrypted to protect the confidentiality of the information in transit.

Technical Details

- **The Snap Client maintains a cached copy of the directory information relating to the user.** The cached directory information is stored in a file within the user profile.
- **The Snap Client will refresh the directory information from Active Directory.** The refresh will occur whenever the age of the cached directory information is at least 6 hours old. This refresh will also occur the first time that a particular user logs onto a PC, because the cached directory information will not exist at that time.
- **If the Snap Client detects a change** to the cached directory information as a result of the directory refresh, it will relay the new directory information to the Snap Server the next time that the client communicates with the server. This means that the directory information is only sent to the server whenever a change occurs.
- **ADSI** - The Snap Client communicates with Active Directory using Active Directory Service Interfaces (ADSI) which is a standard component of the Windows operating system used for interacting with Active Directory. The underlying communication protocol is LDAP.
- **The Snap Client authenticates to Active Directory** using the credentials of the logged-on user. This happens transparently through the use of ADSI.
- **The process for retrieving information from Active Directory is as follows:**
 1. The current user's Distinguished Name (DN) is obtained from ADSI.
 2. The User object in Active Directory is bound to by its DN. For example: LDAP://CN=Joe Bloggs,OU=Users,DC=example,DC=com
 3. A subset of attributes of the User object are retrieved from Active Directory and stored in the cached directory information. (See reference at end of this document of the list of User attributes retrieved).
 4. Each value of the memberOf attribute of the User object specifies the DN of a group that the user belongs to. For each group DN value in the memberOf attribute:
 - (a) the Group object is bound to, for example: LDAP://CN=All Sales Staff,OU=Distribution Lists,DC=example,DC=com
 - (b) a subset of attributes of the Group object are retrieved from Active Directory and stored in the cached directory information. (See reference at end of this document of the list of Group attributes retrieved).
 - (c) the memberOf attribute of each Group object is processed recursively to take into account nested group memberships.

- **Multiple domains or nested groups.** Multiple domains (forests) and nested groups are supported. Where multiple domains are in use or where nested groups are utilized, the Active Directory information that is obtained by the Snap Client is presented as a flattened structure within the Snap Content Management System.
- **There is a timeout of 120 seconds in completing a directory refresh.** If the timeout is reached, the refresh is aborted and retried every 5 minutes.
- **Filtering information obtained.** Facility exists, when creating the Snap Client MSI to apply filters to the LDAP query restricting AD information that is obtained by the Snap Client and related back to the Snap Servers.

List of User Attributes Retrieved

c	facsimileTelephoneNumber	sAMAccountName
cn	givenName	sn
co	homePhone	st
company	info	streetAddress
department	initials	telephoneNumber
description	ipPhone	title
displayName	l	url
extensionAttribute1	mail	userPrincipalName
extensionAttribute2	manager	wwwHomePage
extensionAttribute3	memberOf	
extensionAttribute4	mobile	
extensionAttribute5	objectGUID	
extensionAttribute6	otherFacsimileTelephoneNumber	
extensionAttribute7	otherHomePhone	
extensionAttribute8	otherIpPhone	
extensionAttribute9	otherMobile	
extensionAttribute10	otherPager	
extensionAttribute11	otherTelephone	
extensionAttribute12	pager	
extensionAttribute13	physicalDeliveryOfficeName	
extensionAttribute14	postOfficeBox	
extensionAttribute15	postalCode	

List of Group Attributes Retrieved

cn
 displayName
 description
 managedBy
 objectGUID
 info
 memberOf

Future Developments

- Development is scheduled for quarter 3 of 2010 that will extend the information that the Snap Client retrieves from Active Directory so that in the main, the full Active Directory structure of organizational units (OUs) will be mirrored within the Snap targeting database.
- Administrators, with the appropriate level of permissions, will be able to apply filters to restrict specific directory elements from populating the Snap targeting database. This will ensure only directory information relevant for communications targeting purposes is ever relayed through to the Snap targeting database.
- These same Administrators will be able to configure the directory information (filters and concatenation) within the Snap targeting database to create targeting structures to suit the needs of the business. This will include the ability to create a targeting hierarchy of domains, OUs, groups and attributes.
- Where there is no logical means of creating desired targeting groups from the Active Directory schema, a Group Registration Alert will instead be used to capture User responses to check-the-box questions relating to group membership options. User responses will result in the automatic generate and population of the specified groups.