



How-To Integrate CanIt-PRO with Active Directory:

April, 2006

Summary

Several organizations use Active Directory to manage their user accounts. This paper describes how to integrate CanIt-PRO with an Active Directory system. It will cover setting up the integration, testing it and common problems that can occur.

Getting Active Directory Information

The first step of the process is to obtain the information required by CanIt-PRO for the Active Directory integration. The following table lists the data that is required and where it can be obtained from:

Data Item	Location
Server IP/Name	The IP address or fully qualified domain name (FQDN) of the Active Directory domain controller. If you have more than one domain controller then you may want to get this information for all of these.
Active Directory Domain	The domain of the Active Directory system. This should be easily accessible from the domain controller configuration.
User account	A user account is required to access the Active Directory system. This user only needs to have read access to the system.

Once this information is obtained you will now need to convert the Active Directory Domain to a value that can be understood by the CanIt-PRO system. For each value that is separated by a period you will need to change that into a dc=value entry. The following list of examples should help in converting the domain into an base DN value.

Domain Name	Base DN Value
domain.com	dc=domain,dc=com
complex.ad.domain	dc=complex,dc=ad,dc=domain

Configuring User Lookup Method

Once you have all of the information needed from your Active Directory system you can begin to configure CanIt-PRO by creating a User Lookup method. This feature is accessed via the Setup menu item and selecting the "User Lookups" sub menu option.

Clicking on the link "Add a New User Lookup" will start the process of creating a new lookup method. The first step is to assign a name for this method. Any name is acceptable here so long as it only contains numbers, letters, dashes, underscores and periods. When finished click on the "Next >>" button.

You will want to select "LDAP (Active Directory)" from the drop down list provided. This will pre-populate some values found on the next page that are specific to an Active Directory implementation. You can also optionally add a comment for this lookup value. Clicking on the "Next >>" button will move onto the next step in the process.

How-To: Active Directory Integration

On this page you will see several fields that can be filled in. The following table defines the values that should be edited and which values should be entered:

Field	Value
Use this method for authentication	This value should be set to yes if you want to use your Active Directory system to allow end users to authenticate. NOTE, that by selecting yes, this does not automatically enable authentication via Active Directory, more on this later.
LDAP server(s)	This is a listing of the Active Directory Domain servers you obtained earlier. If you have more than one separate each entry with a comma.
Load-balance LDAP servers	If you would like to have CanIt load balance the access across all of the servers mentioned in the above field select yes. Otherwise the list of servers will be used in a fall back mode.
Base DN	This is the Base DN created from the Active Directory Domain Name.
Bind DN	The user ID of the account you have obtained to read from the Active Directory system.
Bind Password	The password for the above account.
Strip domain name from login prior to authentication	If you plan on using multiple authentication mappings than this will strip out the domain name of the login account prior to using it for authentication purposes. This assumes that users will log into the CanIt-PRO system with their full email address.

Once the values in this form have been filled out you will want to proceed to the next step by clicking on the "Next >>" button.

A summary page is then displayed that allows you to review the items you have entered in on the previous page. Verify the values here are correct then finish the User Lookup creation process by clicking on the "Finish" button.

Testing User Lookup Method

To verify that your Active Directory User Lookup method is setup correctly CanIt-PRO provides a testing feature. This is accessed by going to the User Lookups page (under the Setup menu item). Beside the User Lookup method should be a link "Test". By clicking on this link you will be taken to the Test page.

This page allows you to test how this method will behave when performing authentication as well as how it will stream email addresses to end user accounts. For

How-To: Active Directory Integration

the first item you will need to enter in the username and password of an account in the Active Directory system. If you want to see how email addresses are mapped to streams just enter in the email address in the form. Clicking on the “Run the Test” button will run the test.

The output of each test is then displayed to you. At the end of each test it will inform you if the test was successful or if it failed. If the tests fail then you will want to check the output for possible causes. If the tests are successful then your CanIt-PRO system is successfully able to access your Active Directory system.

Possible Authentication Errors

The following table gives some possible items that can be seen in the output of the authentication test:

Message	Possible Causes
Could not connect to SERVER:PORT	● The CanIt system is unable to communicate to the AD server SERVER on port PORT
Could not bind to SERVER:PORT as BindDN	● The user account information entered for the User Lookup is not correct
No result from search	● This indicates that the user account you entered was not found in the Active Directory system
Could not bind to SERVER:PORT as USER	● The test account password does not match what is in Active Directory.

For the above table the value of SERVER is used for the Active Directory Server IP Address/Domain name. The value of PORT is used to indicate the Port that was used to connect to the Active Directory server. The value of BindDN is the user account used in the User Lookup configuration. The value of USER is the username entered in the form.

In addition to the above error messages extra information may also be included on these lines. This extra information may be useful in finding the cause of the problem. The above is not a complete listing of possible errors but a list of the most common ones found.

Possible Stream Mapping Errors

The following table gives some possible items that can be seen in the output of the stream mapping test:

How-To: Active Directory Integration

Message	Possible Causes
could not connect to LDAP server SERVER	● The CanIt system is unable to communicate to the AD server SERVER
Unable to bind to server	● The user account information entered for the User Lookup is not correct
Could not search for query	● The user account entered in the User Lookup does not have the ability to search the Active Directory system
No user found for query	● A user was unable to be found for the given EMAIL address
Could not find a StreamAttr value for the query	● The record found that matches the given email address doesn't have an associated User ID value.

For the above table the value of SERVER is used for the Active Directory Server IP Address/Domain name.

In addition to the above error messages extra information may also be included on these lines. This extra information may be useful in finding the cause of the problem. The above is not a complete listing of possible errors but a list of the most common ones found.

Using Active Directory for Stream Mapping

Once you have your Active Directory User Lookup setup you can then use this to map email addresses to streams for individual users. This is done by adding an entry in the Domain Mappings table. This is done by accessing the Domain Mappings sub menu item from the Setup menu.

From here you will want to enter in the domain name you wish to have email addresses mapped via the Active Directory system. From the drop down menu you would select the Active Directory User Lookup method that you created earlier. For example if you wanted to have domain.com mapped and my Active Directory User Lookup was called AD-UserLookup then I would enter in the text box 'domain.com' and select AD-UserLookup from the drop down menu and click the "Submit Changes" button. Once this is done any mail being received to this domain will be mapped to streams using the Active Directory User Lookup method mentioned.

If all of your domains will be mapped using this Lookup method then you can enter in a value of '*' for the domain mapping. This will cause all email filtered by the CanIt-PRO system to be streamed using the Active Directory method given.

Using Active Directory For Authentication

Once you have your Active Directory User lookup setup you can use this to authenticate your users through CanIt-PRO. You will need to add an entry to the Authentication Mapping table. This is done by accessing the Authentication Mappings sub menu item from the Setup menu.

From here you will want to enter in the domain name you wish to use your Active Directory User Lookup to authenticate users. From the drop down menu you will want to select the name of the User Lookup method that you created earlier for Active Directory. Your users will now need to log into the system with their full email address.

If all of your domains will use the Active Directory method then you can use the '*' value for the domain name. This will also remove the need for users to include their domain name with their login id.