Adeptia Suite 6.2

Active Directory Integration Guide

Release Date September 26, 2014

Adeptia Inc.
443 North Clark Ave,
Suite 350
Chicago, IL 60610, USA
Phone: (312) 229-1727

DOCUMENT INFORMATION

Adeptia Suite

Single Sign On Configuration Guide

Adeptia Suite Version 6.2

Printed February 2014

Printed in USA

Adeptia Support Information

For support queries, please contact us at *support@adeptia.com*.
Access the Adeptia Web site at the following URL:

www.adeptia.com

Copyright

Trademarks

Confidentiality

CONFIDENTIAL AND PROPRIETARY INFORMATION OF Adeptia. The information set forth herein represents the confidential and proprietary information of Adeptia. Such information shall only be used for the express purpose authorized by Adeptia and shall not be published, communicated, disclosed or divulged to any person, firm, corporation or legal entity, directly or indirectly, or to any third person without the prior written consent of Adeptia.

Disclaimer

Adeptia, Inc. provides this publication "as is" without warranty of any kind, either express or implied. In no event shall Adeptia be liable for any loss of profits, loss of business, loss of use or data, interruption of business, or for indirect, special, punitive, incidental, or consequential damages of any kind.

No part of this work covered by copyright herein may be reproduced in any form or by any means—graphic, electronic, or mechanical—including photocopying, recording, taping, or storage in an information retrieval system, without prior written permission of the copyright owner.

This publication is subject to replacement by a later edition. To determine if a later edition exists, contact www.adeptia.com.

TABLE OF CONTENTS

1

PREFACE

This document provides guidelines for integrating Adeptia Suite with Active Directory (LDAP Server).

TARGET AUDIENCE

This document is intended for the users who want to integrate Adeptia Suite with their LDAP Server and use Single Sign On authentication.

CONTACTS/REPORTING PROBLEMS

These sections present contact information for different situations.

Sales

In case of any sales queries, please contact us at *sales@adeptia.com*.

Support

For support queries, please contact us at *support@adeptia.com*.

Latest updates and information

For the latest updates and information, please visit us at *www.adeptia.com*.

Adeptia Web site

Access the Adeptia Web site at the following URL:
www.adeptia.com

2

OVERVIEW

You can configure Adeptia Suite to authenticate users, using one of the following methods:

- Form-based Authentication without LDAP
- Form-based Authentication with LDAP
- Single Sign On with LDAP

Form-based Authentication without LDAP

This is Adeptia's built-in authentication method. It uses Adeptia's database to authenticate the users.

Form-based Authentication with LDAP

In this authentication:

- User enters URL into browser and is directed to Login page
- User enters Domain user id (without any domain prefix) and password
- Adeptia uses LDAP Login Module to authenticate from Active Directory
- User credentials are retrieved for authorization & Home page is loaded based on authorized access

Single Sign On with LDAP

In this authentication:

- User logs in to PC with domain User ID
- User enters the Adeptia Login URL in the browser
- User is able to log in to the Adeptia Server without providing login credentials

3

CONFIGURING FORM-BASED LDAP AUTHENTICATION

This section explains how to configure Adeptia Suite to use Form-based LDAP authentication.

Prerequisites

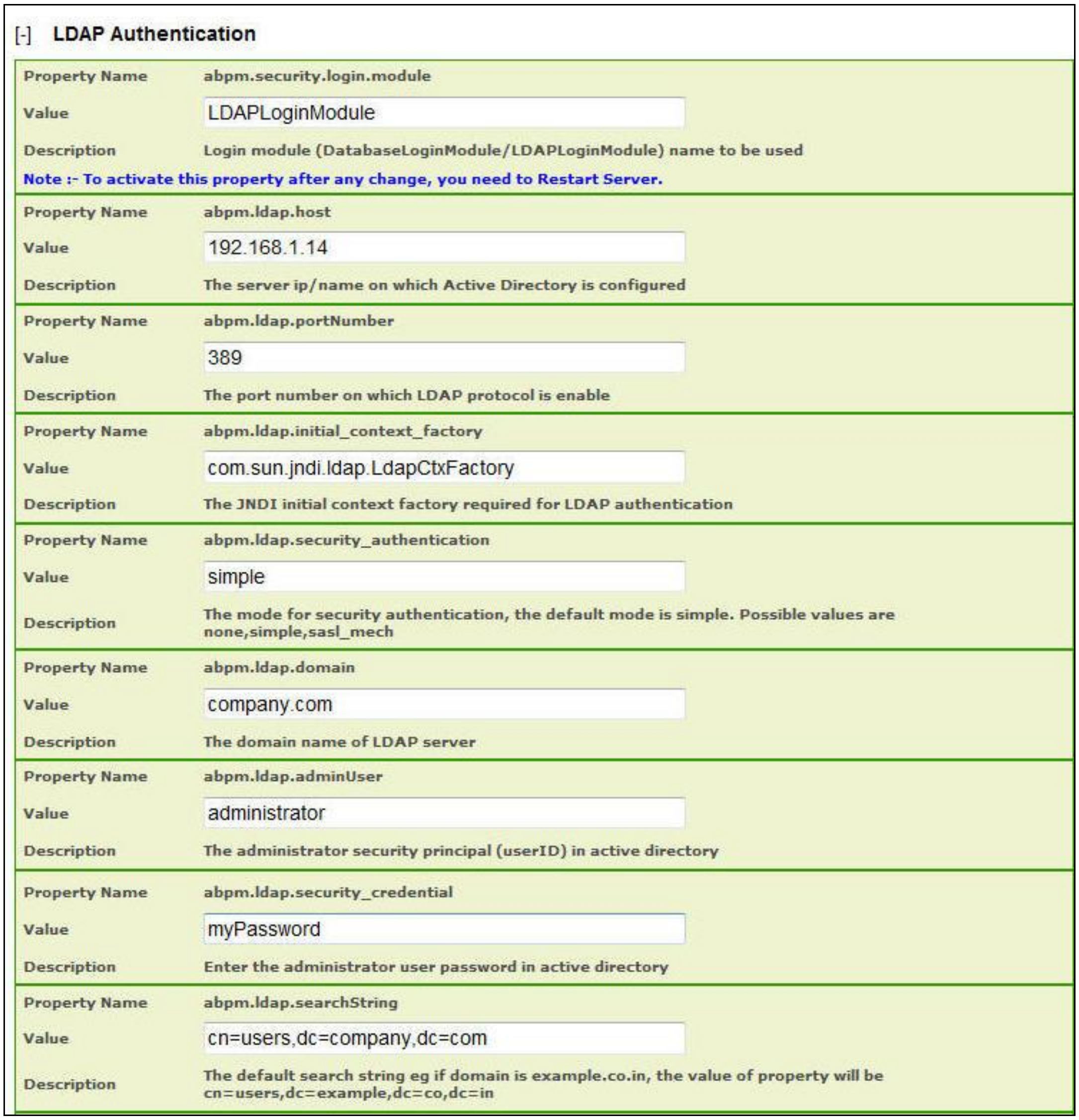
The client machine, where Adeptia Suite will be running, must be part of the Active Directory.

Steps

1. Start Kernel and WebRunner.
2. Login as *admin* user. Password of admin user is *indigo1.*
3. Create a group in Adeptia Suite that will be used as default group for LDAP users.

> ℹ In case the LDAP user, through which you will log into Adeptia Suite, belongs to Active Directory default group **Domain Users** group, then this user becomes the part of the default group in Adeptia Suite. ID of this group will be defined in *abpm.ldap.businessUsers*.
>
> To know how to create a group, refer to Adeptia *Suite Administrator Guide.*

4. Expand *System* and then *LDAP Authentication* (see figure below).



[-] **LDAP Authentication**

Property Name	abpm.security.login.module
Value	LDAPLoginModule
Description	Login module (DatabaseLoginModule/LDAPLoginModule) name to be used
Note :- To activate this property after any change, you need to Restart Server.	
Property Name	abpm.ldap.host
Value	192.168.1.14
Description	The server ip/name on which Active Directory is configured
Property Name	abpm.ldap.portNumber
Value	389
Description	The port number on which LDAP protocol is enable
Property Name	abpm.ldap.initial_context_factory
Value	com.sun.jndi.ldap.LdapCtxFactory
Description	The JNDI initial context factory required for LDAP authentication
Property Name	abpm.ldap.security_authentication
Value	simple
Description	The mode for security authentication, the default mode is simple. Possible values are none,simple,sasl_mech
Property Name	abpm.ldap.domain
Value	company.com
Description	The domain name of LDAP server
Property Name	abpm.ldap.adminUser
Value	administrator
Description	The administrator security principal (userID) in active directory
Property Name	abpm.ldap.security_credential
Value	myPassword
Description	Enter the administrator user password in active directory
Property Name	abpm.ldap.searchString
Value	cn=users,dc=company,dc=com
Description	The default search string eg if domain is example.co.in, the value of property will be cn=users,dc=example,dc=co,dc=in

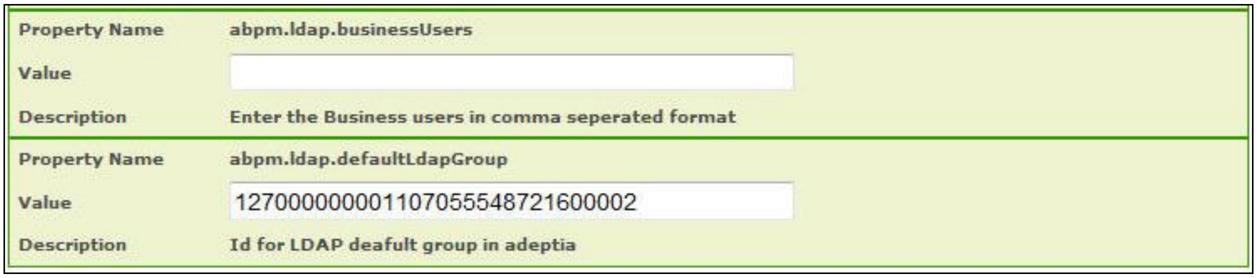
5. Configure the LDAP properties as per the details given in the above figure.

Mapping LDAP Group with Adeptia's Roles

There are three roles in Adeptia that are referred as user type. They are Administrator, Developer and Business.

By default all LDAP users are treated as developer, however, you can configure LDAP users as Business user type.

1. To map LDAP user as business user, enter the name of the users, who you want to be defined as business user in *abpm.ldap.businessUsers*. These names should be separated by commas.
2. To map users of Active directory default group **Domain User** group with Adeptia group, enter the ID of the group, which you have created in *Step 4* of this section in *abpm.ldap.defaultldapGroup* (see figure below).



Property Name	abpm.ldap.businessUsers
Value	
Description	Enter the Business users in comma seperated format
Property Name	abpm.ldap.defaultLdapGroup
Value	127000000001107055548721600002
Description	Id for LDAP deafult group in adeptia

a. To know the Id of the group, go to *Group Manage Page,* and click the name of the group. This will display all the details of the group along with its id.

b. For Admin you can only use Adeptia root **admin** user. However, you are configured with LDAP but root user will still be authenticated from Adeptia.

3. Click **Save** and restart the Kernel and WebRunner.

4

CONFIGURING SINGLE SIGN ON WITH LDAP

In order to use Single Sign On feature in Adeptia Suite, you need to configure:

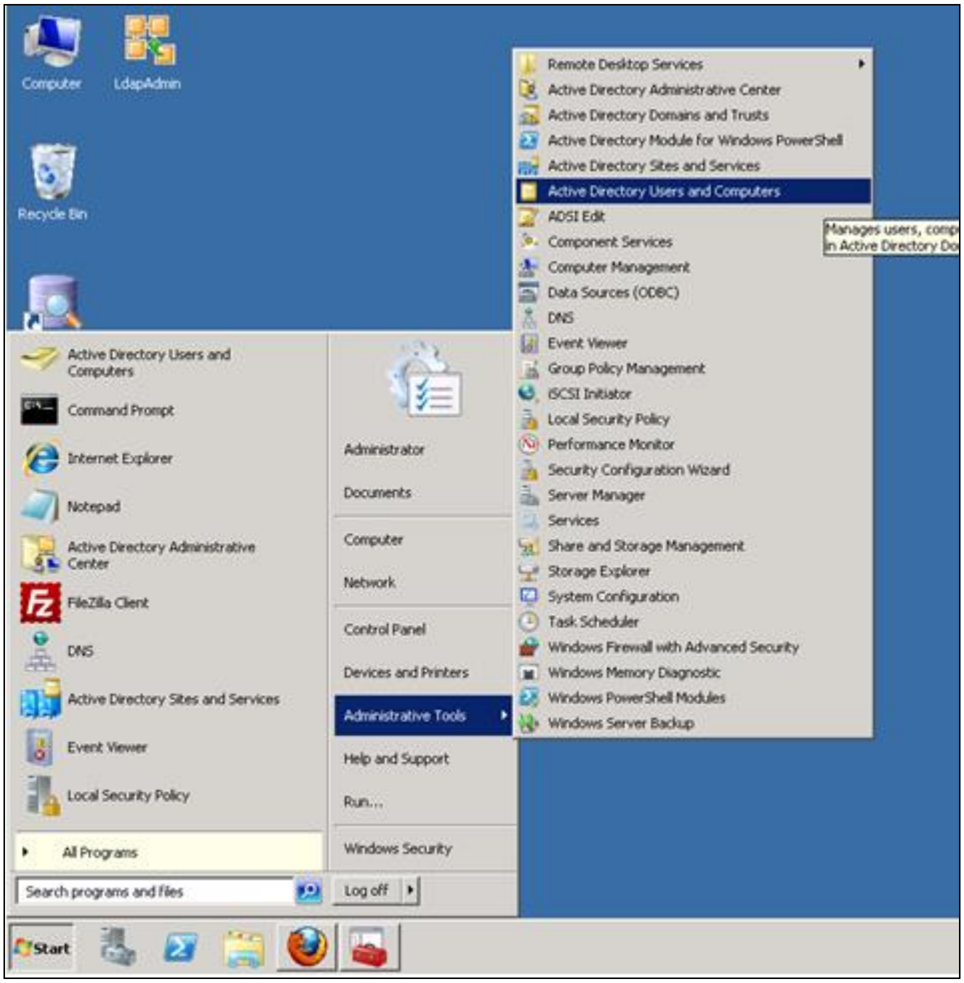
- Active Directory Server (LDAP Server).
- Client Machine where Adeptia Suite will be installed.
- Machine from where Adeptia Suit will be accessed.

CONFIGURATION ON ACTIVE DIRECTORY SERVER

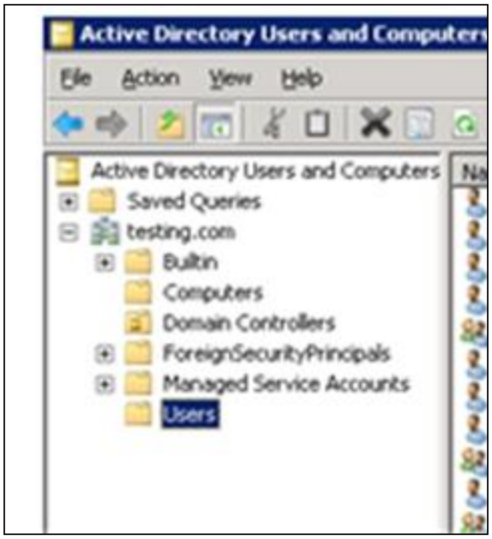
This section describes the configuration, which you need to do for Active Directory Server.

Steps

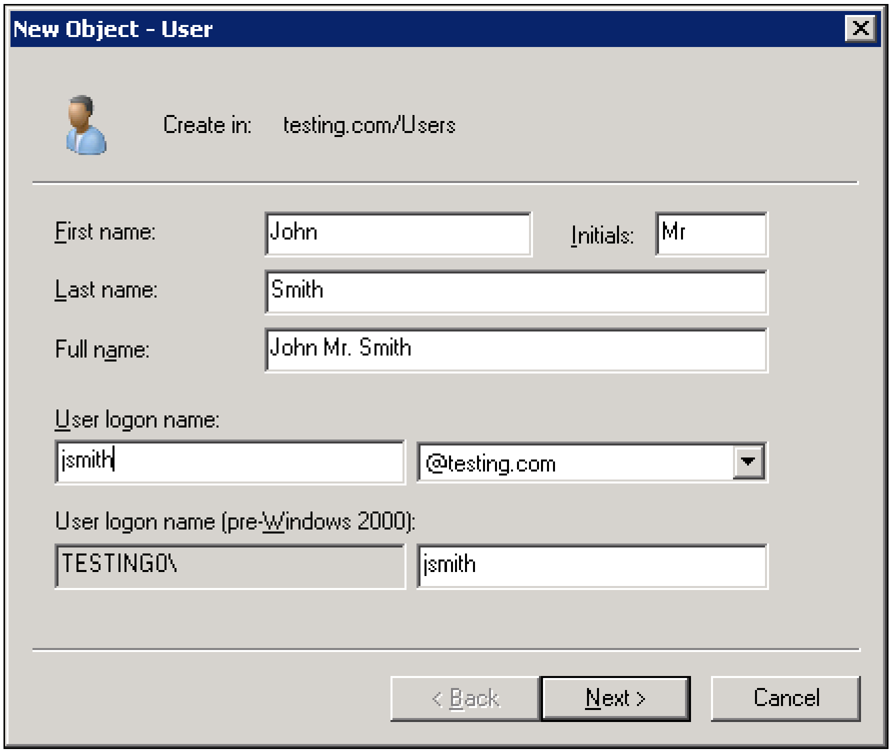
1. Log in to Active Directory Server as Administrator user.
2. Go to *Start > All Programs > Administrative Task,* and select *Active Directory Users and Computers* (see figure below).



3. The *Active Directory Users and Computers* screen is displayed (see figure below).



4. Select *Users* and create a New user as shown in figure below.



First name: John

Initials: Mr

Last name: Smith

Full name: John Mr. Smith

User logon name: jsmith @testing.com

User logon name (pre-Windows 2000): TESTING0\ jsmith

Do not use host name of the client machine (where Adeptia Suite will be installed) as username.

5. Once the user is created, execute the following commands to generate the Service Principal Name.

   setspn -a HTTP/<dns_name> <account_name>

   Here:

   <dns_name> is the hostname**.**domain name of the Active Directory server.

   <account_name> is the logon name of the User that you have created.

   For Example:

   setspn –a HTTP/SER-41.company.com jsmith

6. Now execute the following commands to generate the key tab file for server authentication.

   ktpass -out <keytab.file.location> -princ <spn>@<realm.kerberos.caps> -mapUser <active.directory.NetbiosName\accountName> -mapOp set -pass <active.directory.AccountPassword>

   Here:

<spn> should be similar to as specified in previous command.

<realm.kerberos.caps> - shall be in caps and match with kerberos configuration file (defined later)

Assuming that the hostname name is *SER-41*, the command would be:

ktpass -out C:/keytab/server.keytab -princ HTTP/SER-41.company.com@COMPANY.COM -mapUser Server\jsmith -mapOp set -pass p@ssw0rd

Here, **Server** is the netbios name of the active directory.

CONFIGURATION ON CLIENT MACHINE WHERE ADEPTIA SUITE WILL BE INSTALLED

Prerequisites

The client machine must be a part of Active Directory and you must be logged in with the User, which is used to set SPN command in the previous section.

Steps

1. Login in to the Client machine, where Adeptia Suite will be installed, as local administrator and configure the user (which is used in setspn command) as local administrator.
2. Now, login with this user and install Adeptia Suite Version 6.2.
3. Apply the provided patch.

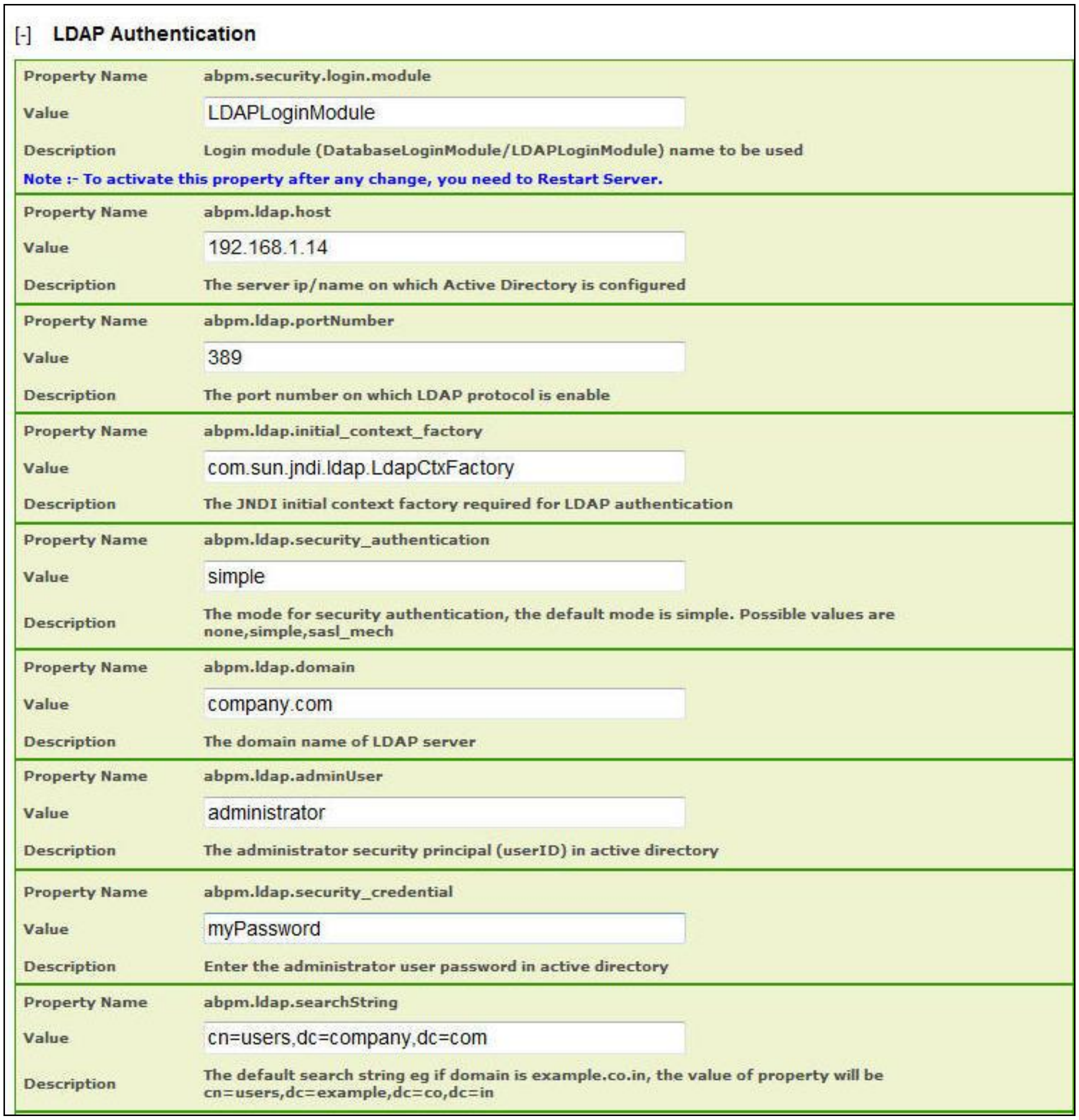
> ℹ By default, the Adeptia Suite will be installed with built-in authentication. Below are the steps to configure Adeptia Suite to use Single Sign On feature with Active directory.
>
> To know how to create a group, refer to Adeptia *Suite Administrator Guide.*

4. Change the login module using following steps:
   a. Start Kernel and WebRunner.
   b. Login as *admin* user.
   c. Create a group in Adeptia Suite that will be used as default group for LDAP users.

> ℹ
> - In case the LDAP user through which you will login into Adeptia Suite, belongs to Active Directory default group “Domain Users” group, then this user becomes the part of this default group in Adeptia Suite. ID of this group will be defined in *abpm.ldap.businessUsers*.
> - To know how to create a group, refer to Adeptia *Suite Administrator Guide.*

d. Go to *Administer > Setup > Application Settings* and then click *Update System Properties.*

e. Expand *System* and then *LDAP Authentication* (see figure below).



[-] **LDAP Authentication**

Property Name	abpm.security.login.module
Value	LDAPLoginModule
Description	Login module (DatabaseLoginModule/LDAPLoginModule) name to be used
Note :- To activate this property after any change, you need to Restart Server.	
Property Name	abpm.ldap.host
Value	192.168.1.14
Description	The server ip/name on which Active Directory is configured
Property Name	abpm.ldap.portNumber
Value	389
Description	The port number on which LDAP protocol is enable
Property Name	abpm.ldap.initial_context_factory
Value	com.sun.jndi.ldap.LdapCtxFactory
Description	The JNDI initial context factory required for LDAP authentication
Property Name	abpm.ldap.security_authentication
Value	simple
Description	The mode for security authentication, the default mode is simple. Possible values are none,simple,sasl_mech
Property Name	abpm.ldap.domain
Value	company.com
Description	The domain name of LDAP server
Property Name	abpm.ldap.adminUser
Value	administrator
Description	The administrator security principal (userID) in active directory
Property Name	abpm.ldap.security_credential
Value	myPassword
Description	Enter the administrator user password in active directory
Property Name	abpm.ldap.searchString
Value	cn=users,dc=company,dc=com
Description	The default search string eg if domain is example.co.in, the value of property will be cn=users,dc=example,dc=co,dc=in

f. Configure the LDAP properties as per the details given in the above figure.

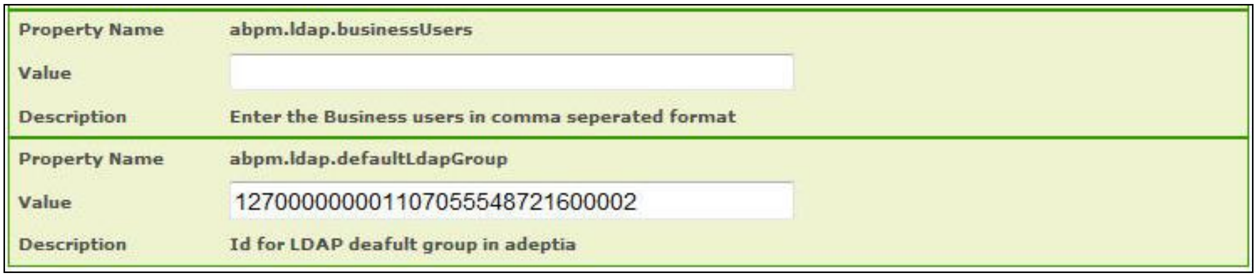
Mapping LDAP Group with Adeptia's Roles

There are three roles in Adeptia that are referred as user types. They are **Administrator**, **Developer** and **Business**.

By default all LDAP users are treated as developer, however, you can configure LDAP users to Business user type.

a. To map LDAP user as business user, enter the name of the users, who you want to be defined as business user in *abpm.ldap.businessUsers*. These names should be separated by commas.

b. To map users of Active directory default group **Domain User** group with Adeptia group, enter the ID of the group, which you have created in *Step 4* of this section in *abpm.ldap.defaultldapGroup* (see figure below).



Property Name	abpm.ldap.businessUsers
Value	
Description	Enter the Business users in comma seperated format
Property Name	abpm.ldap.defaultLdapGroup
Value	127000000001107055548721600002
Description	Id for LDAP deafult group in adeptia

- To know the Id of the group, go to *Group Manage Page* and click the name of the group. This will display the all the details of the group along with its id.
- For Admin you can only use Adeptia root "admin" user. However, you are configured with LDAP but root user will still get authenticated from Adeptia.

c. Click **Save.**

5. Enable SPNEGO filter using below steps:

   a. Go to ./Serverkernel/SSO folder; copy the *web.xml* into *./ServerKernel/web/WEB-INF* folder.

   b. Edit this file in a text editor and do the modifications as explained below.

```
<init-param>
    <param-name>spnego.krb5.conf</param-name>
    <param-value>/krb5.ini</param-value>
</init-param>

<init-param>
    <param-name>spnego.login.conf</param-name>
    <param-value>/login.conf</param-value>
</init-param>
```

   c. Enter the absolute path of the files highlighted in the above figure. For example: If you have installed Adeptia Suite in C:\Program Files, the path would be as shown in the figure below:

```
<init-param>
    <param-name>spnego.krb5.conf</param-name>
    <param-value>C:\Program 
Files\AdeptiaSuite\AdeptiaSuite-
```

```
6.2\AdeptiaServer\ServerKernel\etc\krb5.ini</param-value>
          </init-param>

          <init-param>
              <param-name>spnego.login.conf</param-name>
              <param-value> C:\Program 
Files\AdeptiaSuite\AdeptiaSuite-
6.2\AdeptiaServer\ServerKernel\etc\login.conf</param-value>
          </init-param>
```

d. Replace the Username and Password highlighted in the figure below, with the user name and password of the user, which is used in setspn command.

```
        <init-param>
              <param-name>spnego.preauth.username</param-name>
              <param-value>Username</param-value>
          </init-param>

          <init-param>
              <param-name>spnego.preauth.password</param-name>
              <param-value>Password</param-value>
          </init-param>
```

e. Also, define the realm in caps as shown in the figure below.

```
<login-config>
         <auth-method>SPNEGO</auth-method>
         <realm-name>COMPANY.COM</realm-name>
             </login-config>
```

f. Save the file.

6. Configure keytab using the steps as explained below:

a. Go to ./ServerKernel/etc and edit the *login.conf* file in text editor (see figure below).

```
spnego-server {
       com.sun.security.auth.module.Krb5LoginModule required
        storeKey=true
        isInitiator=false
        useKeyTab=true
        keyTab="C:/KeyTab/server.keytab"
        principal="HTTP/SER-41.company.com"
        debug=true;
};
```

b. Define the path, where you want to keep the keytab file.

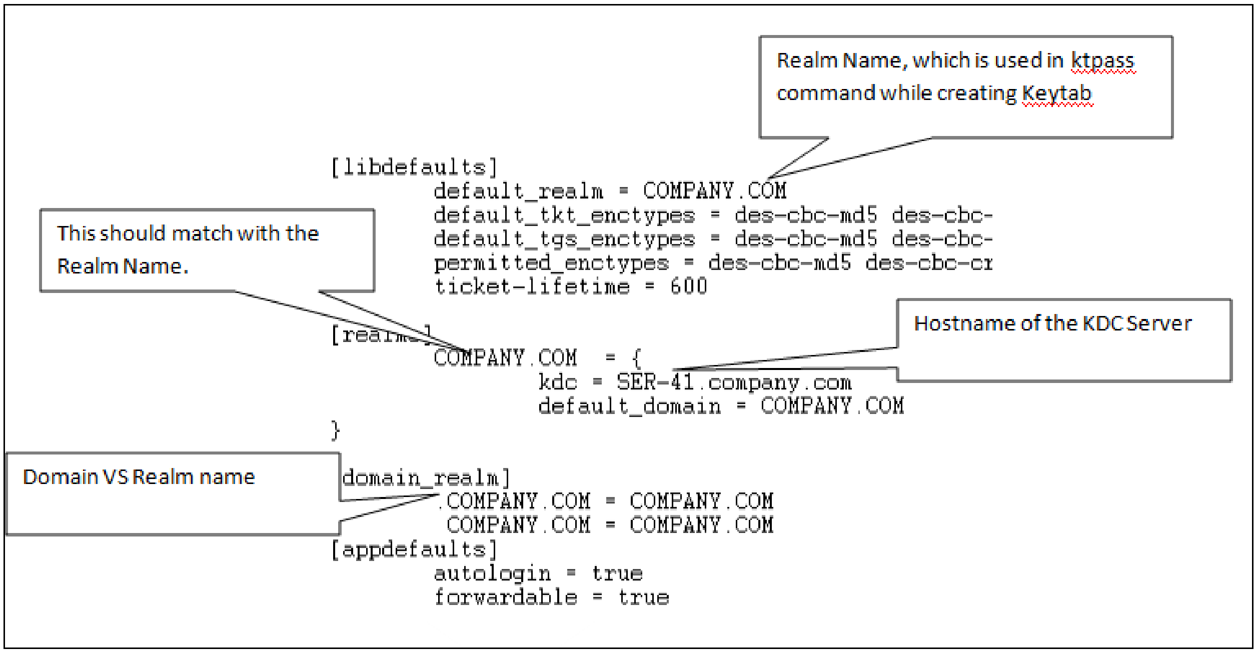
c. Copy the keytab file (which you have generated on Active Directory server), in the location specified in the login.conf within *KeyTab* attribute. This file should be placed at client machine where Adeptia Suite will be installed.

d. Also, enter the Service Principal name (which you have defined using setspn command) within *principal* attribute.

e. Save the file.

7. Configure the Kerberos configuration file using below steps.

   a. Go to *./ServerKernel/etc* folder and edit the *krb5.ini* file in text editor (see figure below).



Realm Name, which is used in ktpass command while creating Keytab

This should match with the Realm Name.

Hostname of the KDC Server

Domain VS Realm name

```
[libdefaults]
        default_realm = COMPANY.COM
        default_tkt_enctypes = des-cbc-md5 des-cbc-
        default_tgs_enctypes = des-cbc-md5 des-cbc-
        permitted_enctypes = des-cbc-md5 des-cbc-cr
        ticket-lifetime = 600

[realms]
        COMPANY.COM  = {
                kdc = SER-41.company.com
                default_domain = COMPANY.COM
}

[domain_realm]
        .COMPANY.COM = COMPANY.COM
         COMPANY.COM = COMPANY.COM
[appdefaults]
        autologin = true
        forwardable = true
```

   b. Configure the *krb5.ini* file as shown in the figure below.

8. Save the file.

9. Configure JASS Login Service using below step:

   a. Go to ./ServerKernel/SSO/jetty/contexts folder. This folder contains webapp.xml file. Copy this file to *./ServerKernel/etc/jetty/contexts* folder of Adeptia Suite.

   b. Edit the *webapp.xml* file in text editor (see figure below) and configure the realm as shown in the figure below:

```
<Set name="loginService">
    <New class="org.eclipse.jetty.plus.jaas.JAASLoginService">
         <Set name="name">COMPANY.COM</Set>
         <Set name="loginModuleName">spnego-client</Set>
       </New>
   </Set>
```

c. Save the file.

10. Restart Kernel and Webrunner.

CONFIGURATION ON MACHINE FROM WHERE ADEPTIA SUITE WILL BE ACCESSED

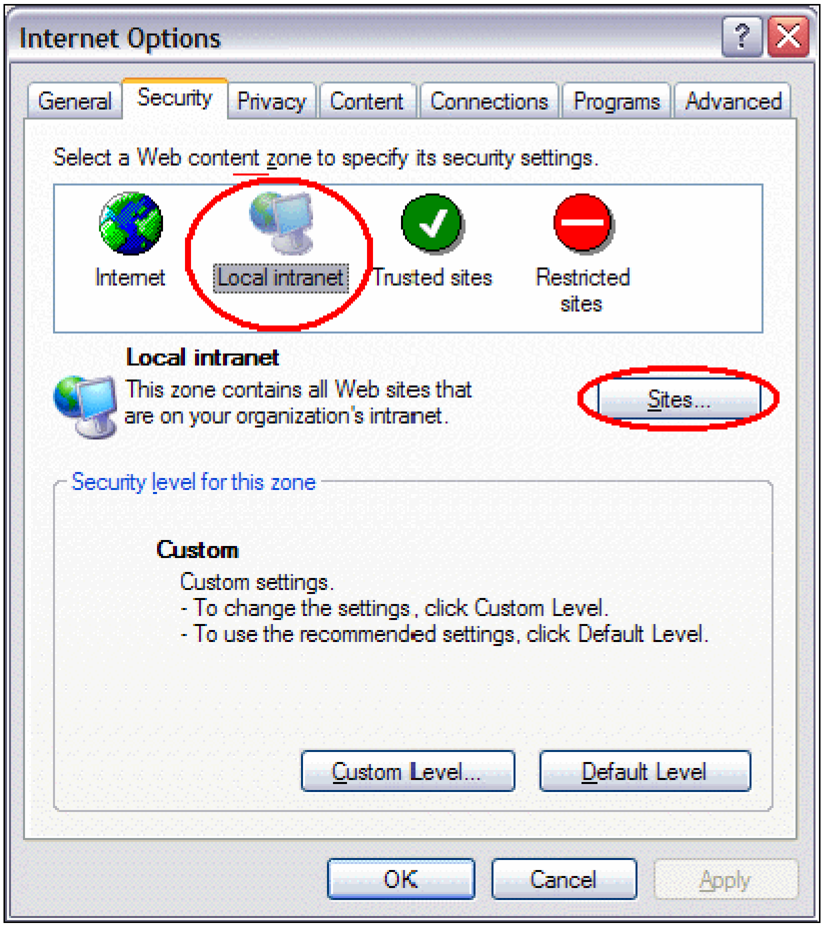
This section covers the configuration that you need to do within Internet Explorer from where Adeptia Suite will be accessed.

Prerequisites

The machine from where you will access Adeptia Suite must be a part of the domain, and you must be logged in with domain user account.

Steps

1. Open the Internet Explorer.
2. Go to *Tools > Internet Option.*
3. Select the Security tab, select the Local intranet and click the Sites button (see figure below).



Select a Web content zone to specify its security settings.

Local intranet

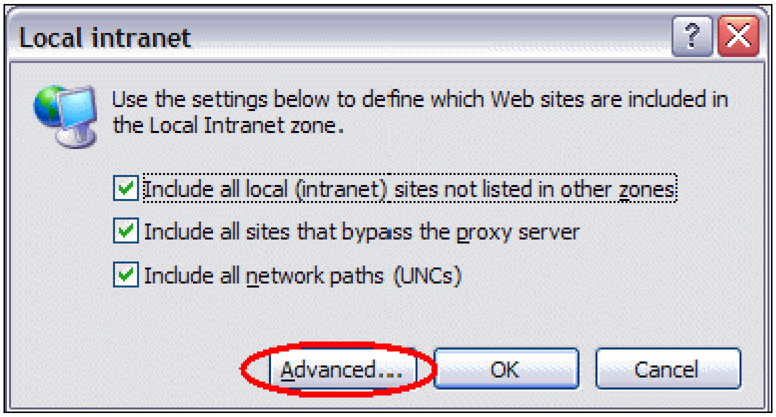
This zone contains all Web sites that are on your organization's intranet.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

4. We need to add the active directory host to a trusted list of URL's. Click the **Advanced** button (see figure below).



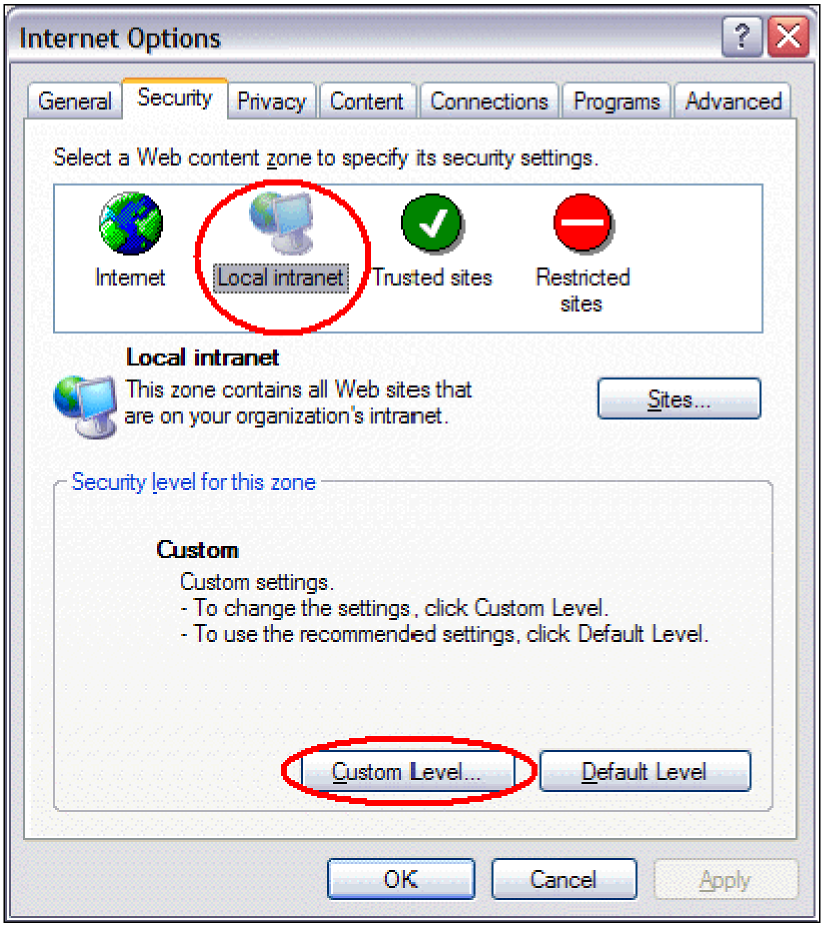
Use the settings below to define which Web sites are included in the Local Intranet zone.

☑ Include all local (intranet) sites not listed in other zones

☑ Include all sites that bypass the proxy server

☑ Include all network paths (UNCs)

5. This opens a dialog where the URL's of the servers where Adeptia Suite is installed, can be added (see figure below).
6. Next step is to configure the automatic authentication handling in the browser. Go back to the Security tab and select the Custom Level.



Select a Web content zone to specify its security settings.

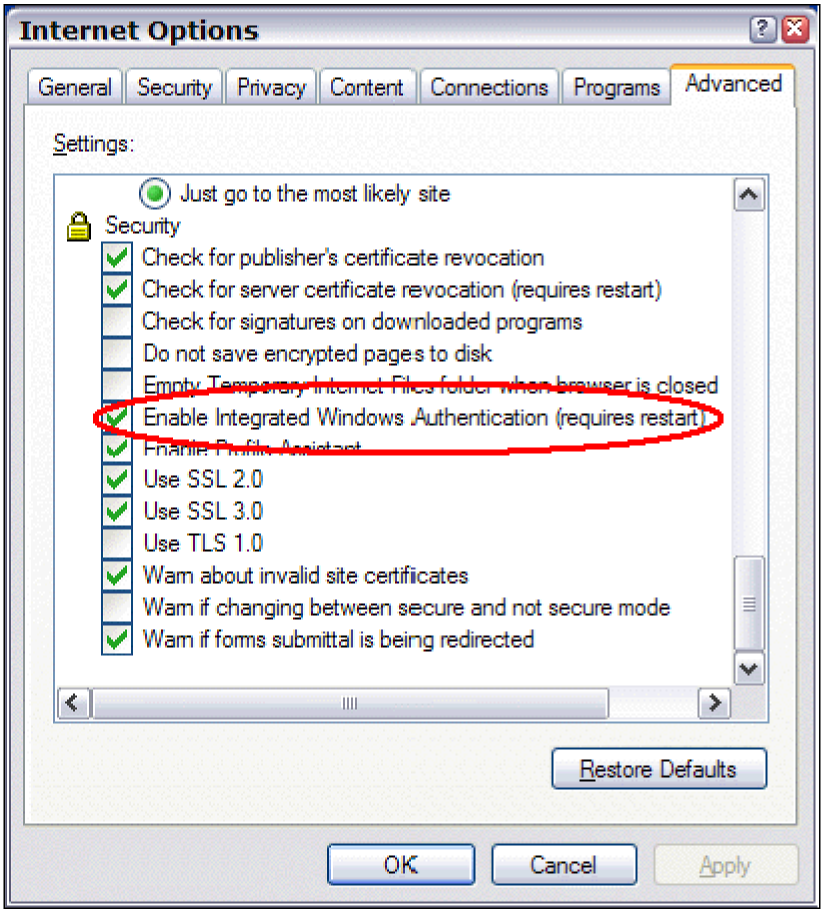
Local intranet

This zone contains all Web sites that are on your organization's intranet.

Custom

Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

7. Select the Advanced tab, scroll down to the Security section (see figure below).



Settings:

- ● Just go to the most likely site
- Security
  - ☑ Check for publisher's certificate revocation
  - ☑ Check for server certificate revocation (requires restart)
  - ☐ Check for signatures on downloaded programs
  - ☐ Do not save encrypted pages to disk
  - ☐ Empty Temporary Internet Files folder when browser is closed
  - ☑ Enable Integrated Windows Authentication (requires restart)
  - ☑ Enable Profile Assistant
  - ☑ Use SSL 2.0
  - ☑ Use SSL 3.0
  - ☐ Use TLS 1.0
  - ☑ Warn about invalid site certificates
  - ☐ Warn if changing between secure and not secure mode
  - ☑ Warn if forms submittal is being redirected

8. Make sure that the *Enable Integrated Windows Authentication* setting is checked.
9. Click **OK** to close this dialog box.