

SOPHOS

Sophos NAC Advanced LDAP implementation guide

Product version: 3.2

Document date: March 2011



Contents

1 About This Document.....	3
2 LDAP Implementation Checklist.....	4
3 LDAP Implementation.....	5
4 LDAP Troubleshooting Issues.....	18
5 Technical Support.....	20
6 Legal Notices.....	21

1 About This Document

This document contains information about the following for Sophos NAC Advanced:

- LDAP Implementation Checklist
- LDAP Implementation Details
- LDAP Troubleshooting Issues

1.1 Intended Audience

The intended audience for this documentation is an IT generalist for a small- to medium-sized business. The audience may include IT specialists for businesses with more than 25,000 endpoints. If you have more than 1,000 endpoints, Sophos Professional Services are recommended. Professional Services works with your security team to devise and implement a software deployment plan.

2 LDAP Implementation Checklist

You must complete all the tasks in this checklist to successfully configure LDAP. All tasks are completed using instructions contained in this document, unless noted.

Task	Description	Completed
LDAP Implementation		
1.	Install and configure Sophos NAC Advanced using the <i>Sophos NAC Advanced installation guide</i> Installation Checklist. When you reach the LDAP implementation task, use this <i>LDAP Implementation Guide</i> .	
2.	Create an LDAP configuration file.	
3.	Configure registry settings on the Compliance Application Server to recognize the LDAP configuration file.	
4.	Run the Password Encryption tool to encrypt the bind password in the LDAP configuration file.	
5.	Change the authentication protocol in the Registration Interface to PAP. Important: PAP forces passwords to be sent in clear text; therefore, we recommend that you use LDAP over SSL. To use LDAP over SSL, you must install a certificate on your domain controller or directory server. Refer to your vendor documentation for information on this configuration.	
6.	Specify PAP authentication in the Remote Access Policy (Windows Server 2003) or Network Policy (Windows Server 2008).	
7.	Create a Connection Request Policy.	
LDAP Implementation (Optional Task)		
8.	Verify that the service account you specified in the LDAP configuration file has the correct Active Directory permissions. Note: LDAP authenticates to Active Directory using the previously created Connection Request Policy.	

3 LDAP Implementation

To use existing LDAP directories with the RADIUS Enforcer enforcement mechanism, complete the following steps:

1. Create an LDAP configuration file.
2. Configure registry settings on the Compliance Application Server to recognize the configuration file.
3. Run the Password Encryption tool to encrypt the bind password in the LDAP configuration file.
4. Change the authentication protocol in the Registration Interface to PAP.
5. Specify PAP authentication in the Remote Access Policy.
6. Create a Connection Request Policy.

3.1 Create an LDAP Configuration File

For the LDAP implementation with Sophos NAC Advanced to work correctly, you must create an LDAP configuration file with appropriate configuration file settings for your LDAP directory.

1. Using a text editor, create an LDAP configuration file with the appropriate LDAP configuration file settings.

Note: Use the sample LDAP configuration files as a reference. For more information, see [LDAP Configuration File Settings](#) (page 8).

2. Save the LDAP configuration file with a file name of your choice that has a .config file extension. For example, LDAPconfiguration.config.
3. Copy the LDAP configuration file to all Compliance Application Servers.

Note: We recommend that you place the LDAP configuration file in the c:\Program Files\Sophos\NAC\Authgateway folder.

3.1.1 Sample Configuration Files

The following configuration files are samples. A copy of the LDAPsample.config file is located in the default location: c:\Program Files\Sophos\NAC\Authgateway on the Compliance Application Server.

For information on specific configuration file settings, see [LDAP Configuration File Settings](#) (page 8).

Configuration Sample 1 - Standard Implementation

The following sample configuration file works with standard LDAP implementations, such as OpenLDAP™ or Novell® eDirectory™.

```
<? xml version="1.0" encoding="utf-8"?>
<configuration>
  <ldapSettings>
    <ldapGroupLookup value="All" />
    <ldapComplianceCheck value="All" />
    <lookupSettings value="All">
      <method type="GroupObject" />
      <hosts>
        <host address="10.0.1.2" port="389" ssl="no" />
        <host address="brasslite" port="389" />
        <host address="MyLDAP" port="636" ssl="yes" />
      </hosts>
      <BaseDN>
        <DN type="user" value="dc=example,dc=com" />
        <DN type="group" value="ou=mygroups,dc=example,dc=com" />
      </BaseDN>
      <ssl certstore="MY" />
      <bindDN value="cn=manager,dc=example,dc=com" />
      <bindPW value="AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAYtMu5iWVl0
66Z678F74kuAQAAAACAAAAAADZgAAqAAAABAAAABSeKDd9Kq3SRHwvaY
yewMwAAAAAASAAACgAAAAEAAAAITxtlveN79O33PeYldTOS4I_u65?AAb
MniRlN1FZIUAAAABfM6mmt62tTxcwm66ikA8laRM9M=" />
      <timeout value="5" />
      <userAttribute value="uid" />
      <userFilter value="objectClass=Person" />
      <groupAttribute value="cn" />
      <groupFilter value="objectClass=GroupOfUniqueNames" />
      <groupAttributeName value="UniqueMember" />
    </lookupSettings>
    <ldapAttributes>
      <attribute name="carlicense" />
      <attribute name="homepostaladdress" />
      <attribute name="businesscategory" />
    </ldapAttributes>
    <radiusAttributeMaps>
      <map ldapattr="carlicense" radiusattrnumber="25"
attrtype="String" replace="ou=$1,ou=Engineering">
      <![CDATA[ ( . +)]]></map>
      <map ldapattr="homepostaladdress" radiusattrnumber="11"
attrtype="String" replace="$1"><![CDATA[ ( . +)]]></map>
      <map ldapattr="businesscategory" radiusattrnumber="26"
vsaname="5428" vsanumber="200" vsatype="Text"
replace="$1"><![CDATA[ ( . +)]]></map>
    </radiusAttributeMaps>
  </ldapSettings>
</configuration>
```

Configuration Sample 2 - LDAP Using Active Directory Implementation

The following sample configuration file works with LDAP implementations that connect to Active Directory.

Note: This sample configuration is provided primarily for testing. We recommend that you use the Sophos NAC Advanced default group functionality when using Active Directory. If that is not possible, you can use the following implementation.

```
<? xml version ="1.0" encoding ="utf-8"?>
<configuration>
  <ldapSettings>
    <ldapGroupLookup value="All" />
    <ldapComplianceCheck value="All" />
    <lookupSettings value="All">
      <method type="GroupObject" />
      <hosts>
        <host address="10.0.1.2" port="389" ssl="no" />
        <host address="brasslite" port="389" />
        <host address="MyLDAP" port="636" ssl="yes" />
      </hosts>
      <BaseDN>
        <DN type="user" value="dc=example,dc=com" />
        <DN type="group" value="ou=mygroups,dc=example,dc=com" />
      </BaseDN>
      <ssl certstore="MY" />
      <bindDN value="cn=manager,dc=example,dc=com" />
      <bindPW value="AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAYtMu5iWVl0
66Z678F74kuAQAAAACAAAAAADZgAAqAAAABAAAABSeKDd9Kq3SRHwvaY
yewMwAAAAAASAAACgAAAAEAAAAITxtlveN79O33PeYldTOS4I_u65?AAb
MniRlN1FZIUAAAABfM6mmt62tTxcwm66ikA8laRM9M=" />
      <timeout value="5" />
      <userAttribute value="samaccountname" />
      <userFilter value="objectClass=Person" />
      <groupAttribute value="cn" />
      <groupFilter value="objectClass=Group" />
      <groupAttributeName value="Member" />
    </lookupSettings>
    <ldapAttributes>
      <attribute name="carlicense" />
      <attribute name="homepostaladdress" />
      <attribute name="businesscategory" />
    </ldapAttributes>
    <radiusAttributeMaps>
      <map ldapattr="carlicense" radiusattrnumber="25"
attrtype="String" replace="ou=$1,ou=Engineering">
        <![CDATA[(.)]]></map>
      <map ldapattr="homepostaladdress" radiusattrnumber="11"
attrtype="String" replace="$1"><![CDATA[(.)]]></map>
      <map ldapattr="businesscategory" radiusattrnumber="26"
vsaname="5428" vsanumber="200" vsatype="Text"
replace="$1"><![CDATA[(.)]]></map>
```

```

    </radiusAttributeMaps>
  </ldapSettings>
</configuration>

```

3.1.2 LDAP Configuration File Settings

The following table contains the LDAP configuration file elements, attributes, descriptions, and possible values.

Element	Attribute	Description and Possible Values
<configuration>		
ldapSettings		Section that contains all LDAP directory settings.
<ldapSettings>		
ldapGroupLookup	value	Value that specifies which lookupSettings section should be referenced in the configuration file when the RADIUS Enforcer is performing a group lookup.
ldapComplianceCheck	value	Value that specifies which lookupSettings section in the configuration file should be referenced when the RADIUS Enforcer is performing a policy compliance check.
lookupSettings		Section that contains settings on where and how to locate information in the LDAP directory when the RADIUS Enforcer is performing a user group lookup or policy compliance check.
ldapAttributes		Section that identifies the LDAP attributes to retrieve from the directory to be mapped to RADIUS attributes during a policy compliance check.
radiusAttributeMaps		Section that identifies the RADIUS attributes to which the LDAP attributes are mapped during a policy compliance check.
<lookupSettings> (multiple lookupSettings sections can be defined, as necessary)		
method	type	Method in which the RADIUS Enforcer will look up a user's group in the LDAP directory. Supported values are: <ul style="list-style-type: none"> ■ GroupObject: Indicates that group names are stored as objects in the LDAP directory, and the RADIUS Enforcer must search for group objects that the user is a member of. ■ UserAttribute: Indicates that group names are contained in a user's attributes and that the RADIUS

Element	Attribute	Description and Possible Values
		Enforcer must search for user objects to determine which groups a user is a member of.
hosts		Section that contains the LDAP directory host machine settings.
host	address	IP address or hostname of the LDAP directory host machine.
	port	Port that is used when connecting to the LDAP directory host machine.
	ssl	When value=Yes, SSL is used to access the LDAP directory host machine.
BaseDN		Section that contains the Base Distinguished Name (DN) of the LDAP directory.
DN	type	Designates the DN type used to determine location when the RADIUS Enforcer searches the LDAP directory. This value should be located above all possible OUs for groups and users in the directory hierarchy. Supported values are: <ul style="list-style-type: none"> ■ User: This value is used for both user group lookups and policy compliance checks when searching for a matching user object in the LDAP directory. ■ Group: This value is used when searching for group objects that the user is a member of. This value is only used when the method type is GroupObject.
	value	Designates the actual base DN used as a starting location when the RADIUS Enforcer searches the LDAP directory. This value should be located above all possible OUs for groups and users in the directory hierarchy.
ssl	certstore	String that specifies the name of the certificate store. Currently, this value must only contain "MY". <p>Note: This value is required only if you configured SSL for any of the specified hosts.</p>
bindDN	value	User ID used to perform all LDAP searches. Leave this field blank for anonymous binds. <p>Note: When using LDAP to authenticate to Active Directory, this service account must have read permission for the CN or OU subtree where the domain user accounts reside and read permission for group membership.</p>

Element	Attribute	Description and Possible Values
bindPW	value	<p>Password for the associated bindDN account. Leave this field blank for unauthenticated binds.</p> <p>Important: This field is encrypted and must be set using the Password Encryption tool. For more information, see Run the Password Encryption Tool to Encrypt the Bind Password (page 13).</p>
timeout	value	Designates the amount of time, in seconds, the RADIUS Enforcer waits to receive data from the LDAP directory before moving on to its next process.
userAttribute	value	<p>Designates the name of the attribute that contains the user name in the LDAP directory. This value is combined with userFilter (below) to form an LDAP search filter.</p> <p>This value is used when the method type is GroupObject or UserAttribute.</p>
userFilter	value	<p>Optional filter string combined with userAttribute (above) to form a complete LDAP search string when searching for a matching user object. The resulting search filter will take the following form:</p> <p>(amp;(userFilter)(userAttribute=<user name>))</p> <p>This value is used when the method type is GroupObject or UserAttribute.</p>
groupAttribute	value	Designates the name of the attribute that contains the group name on a matching user or group object. The value of this attribute behaves differently depending on which method is used for group lookup. For UserAttribute group lookups, this attribute will be located on the matching user object. For GroupObject group lookups, this attribute will be located on the matching group objects that the user is a member of.
groupAttributeName	value	<p>Designates the name of the attribute that contains the list of users belonging to that group in the LDAP directory. This value is combined with groupFilter (below) to form an LDAP search filter.</p> <p>This value is only used when the method type is GroupObject.</p>
groupFilter	value	<p>Optional filter string combined with groupAttributeName (above) to form a complete LDAP search string. The resulting search filter will take the following form:</p> <p>(amp;(groupFilter)(groupAttributeName=<user's DN>))</p>

Element	Attribute	Description and Possible Values
		This value is only used when the method type is GroupObject.
groupSearchMax	value	Maximum number of groups returned for each user from the LDAP directory to the RADIUS Enforcer when performing GroupObject type group lookups. The default value is 100. Note: This field is not included in the sample configuration file. If you have users who are in more than 100 groups, you may need to add this field to your configuration file and either specify a value larger than 100 or set the value to 0 to return all groups.
<ldapAttributes>		
attribute	name	Name of the user's attribute that you want to map to a RADIUS attribute during a policy compliance check.
<radiusAttributeMaps>		
map	ldapattr	Name of an LDAP attribute that you identified in the ldapAttributes section that you want to map to a RADIUS attribute.
	radiusattrnumber	Number of the RADIUS attribute that you want to map to the corresponding LDAP attribute. Example: RADIUS attribute Class is 25. RADIUS attribute Filter-Id is 11. Note: To specify a vendor-specific attribute, this attribute must be set to 26.
	attrtype	Data type of the RADIUS attribute that you want to map to the corresponding LDAP attribute. Supported values are: String or Integer .
	vsaname	ID number of the vendor-specific RADIUS attribute that you want to map to the corresponding LDAP attribute. This value is only used for vendor-specific attributes.
	vsanumber	Number of the vendor-specific RADIUS attribute that you want to map to the corresponding LDAP attribute. This value is only used for vendor-specific attributes.

Element	Attribute	Description and Possible Values
	vsatype	Data type of the vendor-specific RADIUS attribute that you want to map to the corresponding LDAP attribute. Supported values are: Text or Integer . This value is only used for vendor-specific attributes.
	replace	Regular expression replacement value used to map the LDAP attribute to the RADIUS attribute. The replace string is used in conjunction with the regular expression in the cdata section to find strings in the LDAP attribute and convert them to the desired format. The text of the map element is the find portion of the regular expression and must be formatted as follows: "<![CDATA[MyFindExpression]]>" For more information on regular expressions, see http://msdn2.microsoft.com/en-us/library/az24scfc(vs.71).aspx .

3.2 Configure Registry Settings on the Application Servers and RADIUS Enforcer Servers

If you want to configure the RADIUS Enforcer to use LDAP, you must configure the following settings in the registry on all Compliance Application Servers and RADIUS Enforcer servers. These registry settings must be manually configured because they are not specified by the Sophos Compliance Application Server installation.

HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\NAC\AuthGateway		
Registry Setting Name	Type	Value Description
LDAPConfigFilename	String	String that specifies the full file path and name of the LDAP configuration file you create. Both the RADIUS Enforcer and the AuthGatewayConfig.exe file use this setting to locate the configuration file.
UseLDAPAuthAuthZ	DWORD	Specifies that LDAP authentication and authorization will be used instead of RADIUS. Important: You must restart IAS or Network Policy Server and the Sophos COM+ package for this change to be implemented. <ul style="list-style-type: none"> ■ 0 = LDAP is disabled ■ 1 = LDAP is enabled

3.3 Run the Password Encryption Tool to Encrypt the Bind Password

To encrypt the bind password in the configuration file, you must run the Password Encryption tool from a command prompt with the appropriate parameters.

Note: If you want to re-use a configuration file on multiple servers, you must run the Password Encryption tool on each server to update and encrypt the bind password since the encryption of the password is server-specific.

1. Locate the Password Encryption tool, or `AuthGatewayConfig.exe`, on the Compliance Application Server. The default location of this tool is `c:\Program Files\Sophos\NAC\Authgateway`.
2. Ensure that the `LDAPConfigFilename` registry setting points to the configuration file you created.
3. From a command prompt, go to the directory where the `AuthGatewayConfig.exe` file is located.
4. Type `AuthGatewayConfig.exe <bindDN><bindPW>`, in which `<bindDN>` and `<bindPW>` are replaced with the appropriate bind user ID and bind password values, and press **Enter**. A message displays stating that the bind password was successfully updated.

Important: The `bindDN` must be typed exactly as it appears in the configuration file you created.

3.4 Change the Authentication Protocol in the Registration Interface to PAP

Sophos NAC Advanced defaults to using the MSChapV2 RADIUS authentication protocol. For LDAP implementations, you must change the authentication protocol in the Registration Interface to PAP.

Important: PAP forces passwords to be sent in clear text; therefore, we recommend that you use LDAP over SSL. To use LDAP over SSL, you must install a certificate on your domain controller or directory server. Refer to your vendor documentation for information on this configuration.

1. Locate the Registration Interface `Web.config` file for the Registration Interface on the Compliance Application Server. If you installed the Sophos NAC Advanced software in the default location, the file can be found in the following location:
`c:\inetpub\wwwroot\RegistrationInterface\web.config`.
2. Open the `Web.config` file in Notepad.
3. Locate the **authInterface** section and the **radius** subsection.
4. Change the **mschapv2** value in this line `<add key="authType" value="mschapv2" />` to **pap**.

5. Save and close the file.

The modified radius subsection in the Registration Interface web.config file must appear as:

```
<radius>
  <add key="authType" value="pap" />
  <add key="serverRetries" value="1" />
  <add key="listRetries" value="1" />
</radius>
```

6. Repeat these steps on all Compliance Application Servers.

3.5 Specify PAP Authentication in Remote Access Policy (Windows Server 2003)

You must create a Remote Access Policy for both VPN and LAN implementations. For an LDAP implementation to work properly with Sophos NAC Advanced, you must specify PAP authentication in the Remote Access Policy in IAS.

1. From the Compliance Application Server Start menu, click **Administrative Tools > Internet Authentication Service**.

IAS opens.

2. Click **Remote Access Policies**.
3. Right-click on the name of the Remote Access Policy that is being used with Sophos NAC Advanced, and then select **Properties**.
4. Click **Edit Profile**.
5. Click the **Authentication** tab.
6. Select the **Unencrypted authentication (PAP, SPAP)** check box if it is not selected, and then click **OK**.
7. Click **OK** to return to the IAS main window.
8. Repeat these steps on all Compliance Application Servers.

3.6 Specify PAP Authentication in Network Policy (Windows Server 2008)

You must create a Network Policy for both VPN and LAN implementations. For an LDAP implementation to work properly with Sophos NAC Advanced, you must specify PAP authentication in the Network Policy in Network Policy Server.

1. From the Compliance Application Server Start menu, click **Administrative Tools > Network Policy Server**.

Network Policy Server opens.

2. Under Policies, click **Network Policies**.
3. Right-click on the name of the Network Policy that is being used with Sophos NAC Advanced, and then select **Properties**.
4. Click the **Constraints** tab.
5. In the **Authentication Methods** section, select the **Unencrypted authentication (PAP, SPAP)** check box if it is not selected, and then click **OK**.
6. Repeat these steps on all Compliance Application Servers.

3.7 Create a Connection Request Policy (Windows Server 2003)

For an LDAP implementation to work properly with Sophos NAC Advanced, you must specify a Connection Request Policy on all Compliance Application Servers.

1. From the Compliance Application Server Start menu, click **Administrative Tools > Internet Authentication Service**. IAS opens. Double-click **Connection Request Processing**. Right-click **Connection Request Policies**. Click **New > Connection Request Policy**.
2. Click **Next** to continue.
3. Select the **A custom policy** option button.
4. Type a policy name.
5. Click **Next** to continue.
6. Click **Add** to add attributes.
7. Select the appropriate attribute, and then click **Add**.
Note: Typically, the Day-And-Time-Restrictions attribute is specified.
8. Specify the appropriate time of day constraints, and then click **OK**.
Note: Typically, the time of day constraints are set to 24 hours/7 days a week permitted. To obtain this constraint, select the Permitted option button.
9. Click **Next** to continue.
10. Click **Edit Profile**.
11. Select the **Accept users without validating credentials** option button, and then click **OK**.
12. Click **Next** to continue.
13. Click **Finish**.

Note: If other Connection Request Policies exist on the Compliance Application Server, ensure that this Connection Request Policy is specified as lower priority.

14. Repeat these steps on all Compliance Application Servers.

3.8 Create a Connection Request Policy (Windows Server 2008)

For an LDAP implementation to work properly with Sophos NAC Advanced, you must specify a Connection Request Policy on all Compliance Application Servers.

1. From the Compliance Application Server Start menu, click **Administrative Tools > Network Policy Server**.

Network Policy Server opens.

2. Under Policies, right-click **Connection Request Policies**, and click **New**.
3. Type a policy name, and leave **Unspecified** as the network connection method.
4. Click **Next** to continue.
5. Click **Add** to add conditions.
6. Select the appropriate condition, and then click **Add**.

Note: Typically, the Day And Time Restrictions condition is specified.

7. Specify the appropriate time of day constraints, and then click **OK**.

Note: Typically, the time of day constraints are set to 24 hours/7 days a week permitted. To obtain this constraint, select the Permitted option button.

8. Click **Next** to continue.
9. In the **Authentication** section, select the **Accept users without validating credentials** option button, and then click **Next**.
10. Click **Next** to continue. You do not need to set attributes for this policy.
11. Click **Finish**.

Note: If other Connection Request Policies exist on the Compliance Application Server, ensure that this Connection Request Policy is specified as lower priority.

12. Repeat these steps on all Compliance Application Servers.

3.9 Use LDAP to Authenticate to Active Directory

Some enterprises use both LDAP and Active Directory. To use LDAP to authenticate to Active Directory you must:

- Verify that the service account you specified in the LDAP configuration file has the correct Active Directory permissions.
- Use the previously created Connection Request Policy.

3.9.1 Verify the Required Service Account has the Correct Permissions

The service account permissions you specified in the LDAP configuration file must have the following permissions:

- Read permission for the CN or OU subtree where the domain user accounts reside.
- Read permission for group membership.

Note: This service account is specified in the bindDN element of the LDAP configuration file.

4 LDAP Troubleshooting Issues

This section contains troubleshooting issues pertaining to LDAP.

4.1 Server Communication Issues

This section contains troubleshooting information about server communication issues.

Cause	Resolution
LDAP Application Event Log Issues	
<p>Issue:</p> <p>Event log error message containing: "LDAPDataAgent: BSB, unable to authenticate search user, XXX. YYY"</p> <p>OR</p> <p>Event log error message containing: "LDAPDataAgent: GetUserGroup, unable to re-authenticate search user, XXX. YYY", where XXX is the search user defined in the LDAP configuration file and YYY is the error message received from the LDAP server.</p>	
Bad bindDN	Confirm that the bindDN value is correct in LDAP configuration file.
Bad bindPW (password associated with bindDN account)	Reset the bindPW value using the Password Encryption tool (AuthGatewayConfig.exe).
<p>Issue: Event log informational message containing: "LDAPDataAgent: BSB, error search for user, XXX, using filter, YYY. No such object. Invalid BaseDN?", where XXX is the user's uid and YYY is an LDAP search filter.</p>	
User base DN is invalid or incorrect.	Confirm that the base DN value of type "User" is correct in the LDAP configuration file.
<p>Issue: Event log error message containing: "LDAPDataAgent: ZZZ, Exception while loading LDAP Config.", where ZZZ is a function name.</p>	
Unable to locate the LDAP configuration file.	Confirm that the value specified in the registry path HKLM\Software\Sophos\AuthGateway\LDAPConfigFilename (REG_SZ) is correct.
Invalid LDAP configuration file.	For more information, view the detailed event message further down in the same event, or view the previous event log entry.
<p>Issue: Event log error or warning message containing: "LDAPDataAgent: ZZZ, LDAP Exception (AAA). BBB. While attempting to connect to server, CCC", where ZZZ is a function name, AAA is the error number, BBB is the error description, and CCC is the LDAP server name or IP address.</p>	

Cause	Resolution
LDAP Server CCC is down.	Confirm that server CCC is functioning properly, OR modify the LDAP configuration file to use another LDAP server.
Pending search to server CCC timed out.	Do any of the following, in no particular order: <ul style="list-style-type: none"> ■ Specify a narrower search filter in the LDAP configuration file. ■ Increase the timeout value in the LDAP configuration file. ■ Change the configuration file's LDAP server list to use LDAP servers under less load.
SSL failure(s).	Do any of the following, in no particular order: <ul style="list-style-type: none"> ■ Verify CCC matches Subject in the LDAP server's SSL certificate. ■ Verify that the issuing Certificate Authority (CA) is listed in the Trusted Root Authorities list on the Compliance Application Server certificate store. ■ Verify if the certificate issued to server CCC is valid (e.g. has not expired, has the correct name, is a trusted source, etc.).
Issue: Event log warning message containing: "LDAPDataAgent: LDAP Disconnect (AAA). BBB. From server, CCC"	
LDAP Server CCC unexpectedly terminated the LDAP connection.	Confirm that server CCC is functioning properly, OR modify the LDAP configuration file to use another LDAP server.

5 Technical Support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

6 Legal Notices

Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.