LDAP Synchronization Agent Configuration Guide for

BLACKSHIELD CLOUD  BLACKSHIELD SERVER

Powerful Authentication Management for Service Providers and Enterprises

Version 3.x

Authentication Service Delivery Made EASY™
Contact Information

CRYPTOCARD’s technical support specialists can provide assistance when planning and implementing CRYPTOCard in your network. In addition to aiding in the selection of the appropriate authentication products, CRYPTOCard can suggest deployment procedures that provide a smooth, simple transition from existing access control systems and a satisfying experience for network users. We can also help you leverage your existing network equipment and systems to maximize your return on investment.

CRYPTOCARD works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through a CRYPTOCard channel partner, please contact your partner directly for support needs.

To contact CRYPTOCard directly:

<table>
<thead>
<tr>
<th>United Kingdom</th>
<th>North America</th>
</tr>
</thead>
<tbody>
<tr>
<td>2430 The Quadrant, Aztec West, Almondsbury, Bristol, BS32 4AQ, U.K.</td>
<td>600-340 March Road, Kanata, Ontario, Canada K2K 2E4</td>
</tr>
<tr>
<td>Phone: +44 870 7077 700</td>
<td>Phone: +1 613 599 2441</td>
</tr>
<tr>
<td>Fax: +44 870 7077071</td>
<td>Fax: +1 613 599 2442</td>
</tr>
<tr>
<td><a href="mailto:support@cryptocard.com">support@cryptocard.com</a></td>
<td><a href="mailto:support@cryptocard.com">support@cryptocard.com</a></td>
</tr>
</tbody>
</table>

For information about obtaining a support contract, see our Support Web page at http://www.cryptocard.com

Publication History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011.11.28</td>
<td>Feature changes</td>
<td>2.3</td>
</tr>
<tr>
<td>2011.08.31</td>
<td>Feature changes</td>
<td>2.2</td>
</tr>
<tr>
<td>2011.07.04</td>
<td>Added Feature Update</td>
<td>2.1</td>
</tr>
<tr>
<td>2011.05.09</td>
<td>Minor updates</td>
<td>2.0</td>
</tr>
<tr>
<td>2011.03.14</td>
<td>Initial release</td>
<td>1.0</td>
</tr>
</tbody>
</table>
## Contents

Applicability ................................................................................................................................. 5

Overview ........................................................................................................................................ 6

Features .......................................................................................................................................... 7

Preparation and Prerequisites .......................................................................................................... 7

Configuring the Agent .................................................................................................................... 8

BlackShield ID LDAP Sync Agent Configuration Tool ........................................................................ 13

  Status Tab ...................................................................................................................................... 13

    LDAP Configuration .................................................................................................................... 13

    LDAP Sync Groups ...................................................................................................................... 13

    Last Sync Status .......................................................................................................................... 14

    Transaction Details ..................................................................................................................... 14

  Configuration Tab .......................................................................................................................... 15

    LDAP Configuration .................................................................................................................... 15

    LDAP Credentials ....................................................................................................................... 16

    LDAP Sync Group(s) .................................................................................................................... 17

    LDAP Schema Configuration ....................................................................................................... 18

Other Synchronization Options ........................................................................................................... 18

  Mobile Number Country Code ....................................................................................................... 18

  LDAP Scan Interval ......................................................................................................................... 18

  Group Sync Options ....................................................................................................................... 19

  Key Set .......................................................................................................................................... 19

  BlackShield ID Synchronization Server .......................................................................................... 19

Notification Tab .................................................................................................................................... 20

  SMTP Configuration ....................................................................................................................... 20

  E-Mail Test ..................................................................................................................................... 21

  E-Mail Message Templates ............................................................................................................. 21
## Applicability

This integration guide is applicable to:

<table>
<thead>
<tr>
<th>Summary</th>
<th>BlackShield Cloud</th>
<th>BlackShield SPE Server (3.x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Windows Versions</td>
<td>Windows XP SP 3</td>
<td>Windows 2003 R2 Server</td>
</tr>
<tr>
<td></td>
<td>Windows 2008 SP2 and Windows 2008 R2</td>
<td>Windows Vista SP2</td>
</tr>
<tr>
<td></td>
<td>Windows 7</td>
<td></td>
</tr>
<tr>
<td>Supported Architecture</td>
<td>32-bit</td>
<td>64-bit</td>
</tr>
<tr>
<td>Additional Software Components</td>
<td></td>
<td>.Net 2.0</td>
</tr>
<tr>
<td>Network Port</td>
<td>TCP Port 8456</td>
<td>TCP Port 389</td>
</tr>
<tr>
<td></td>
<td>TCP Port 636 (optional)</td>
<td></td>
</tr>
<tr>
<td>Support LDAP Directory Servers</td>
<td>Active Directory</td>
<td>Sun One 6.x</td>
</tr>
<tr>
<td></td>
<td>Novell eDirectory 8.x</td>
<td></td>
</tr>
<tr>
<td>LDAP Directory Server Access</td>
<td>Read-only</td>
<td></td>
</tr>
<tr>
<td>Supported LDAP Groups</td>
<td>Single LDAP Group</td>
<td>Multiple LDAP Groups</td>
</tr>
</tbody>
</table>
Overview

The LDAP Synchronization Agent has been developed to simplify the task of user creation in BlackShield Cloud. Without the agent, the administrator must manually input user information via the web based management interface. Once installed, the LDAP Synchronization Agent monitors LDAP groups for membership changes and updates user information in BlackShield Cloud to reflect these changes.

1. Organization imports their synchronization agent key file into the LDAP Synchronization Agent, configures a connection to their LDAP Directory Server then selects one or more LDAP groups.

2. The LDAP Synchronization Agent queries the LDAP Directory server for all users within the selected LDAP Group(s).

3. For each member of the group: The first name, last name, username, email address, address, phone, mobile and selected LDAP group(s) are exported by the LDAP Synchronization Agent and queued for transmission.

4. The LDAP Synchronization Agent pushes all user and group information to the BlackShield Cloud which in turn creates each user and group in the Virtual Server.

5. The LDAP Synchronization Agent queries the LDAP Directory server every 20 minutes (default synchronization period) and pushes all user and group information to the BlackShield Cloud.

6. Additions, deletions and updates are pushed to BlackShield Cloud during each synchronization.
Features

Most organizations maintain information about their users in an LDAP directory such as Active Directory. The purpose of the Synchronization Agent is to auto-populate BlackShield Cloud with users maintained in one of these user sources.

Key features of the agent are:

- Can be used with almost any LDAP Directory Server.
- Can accommodate custom LDAP schemas.
- Does not write to the LDAP Directory Server.
- Does not require an administrator account to connect to the LDAP Directory Server.
- Can synchronize multiple LDAP Directory Servers.
- Uses AES encryption between the LDAP Synchronization Agent and the BlackShield Cloud.
- Supports SSL between the LDAP Synchronization Agent and the LDAP Directory Server.

Preparation and Prerequisites

You will need the following to install and configure the LDAP Synchronization Agent:

- The BlackShield Cloud account total license capacity must be equal to or greater than the amount of users synchronized from LDAP. LDAP groups do not count towards capacity.
- The synchronization agent key file generated by your Virtual Server (MASSyncConfigFile.bmc). This is generated from the LDAP Sync Agent Settings link in the Authentication Processing Module within the COMMS tab of your Virtual Server.
- The agent Installer (BlackShield ID LDAP Sync Agent x64.exe or BlackShield ID LDAP Sync Agent.exe for 64-bit and 32-bit systems respectively)
- The IP address/host name and port number of your LDAP Directory Server.
- An account name and password that can be used by the LDAP Synchronization Agent to connect to the LDAP Directory Server.
- TCP Port 389 or 636 open between the LDAP Synchronization Agent and the LDAP Directory Server.
- TCP Port 8456 open between the LDAP Synchronization Agent and BlackShield Cloud.
Configuring the Agent

Configuring the LDAP Synchronization agent consists of 10 steps:

Step 1. Download the LDAP Sync Agent key file for your Virtual Server within BlackShield Cloud

Step 2. Import the LDAP Sync Agent key file into the LDAP Synchronization agent.

Step 3. Configure the connection information for the LDAP Directory Server.

Step 4. Select the LDAP Group(s) to synchronize.

Step 5. Set the LDAP scan interval.


Step 7. Customized Email Message Templates (optional).


Step 9. Start Synchronization

Step 10. Allow Sync Permission

1. Log into BlackShield Cloud Manager.

   Select Virtual Servers, Your Account Name, COMMS tab.

   Expand Authentication Processing then select LDAP Sync Agent Settings.

   Select the Download button then save the MASSyncConfigFile.bmc file. This file is loaded into the LDAP Synchronization Agent.
2. After running the installer:
Launch the Agent from the CRYPTOCard Program group.

In the Current Organization section, click the Add button. Browse to the location of the MASSyncConfigFile.bmc and load the file.

The Current Organization section will update showing the name of your Virtual Server.

3. Select the Configuration tab. In the LDAP Configuration section, click the Configure button.

Enter the host name or IP address and port number of the LDAP Directory server. Select SSL if you have a certificate installed on the server.

If you have one or more failover LDAP directory servers that the agent should connect to in the event that the primary cannot be reached, indicate this by selecting a corresponding number from the Number of Failover dropdown.
Select a schema from the dropdown list.

Possible default values are:
- Active Directory
- eDirectory
- SunOne directory

Enter a User DN and password created for the agent.

The User DN contains the username (and location of the user within LDAP) that will be used by the agent to connect to the LDAP Directory Server. If using Active Directory, this value should be entered in an email format.

Example: The BaseDN in the figure is dc=ts, DC=cryptocard, DC=com. So the User DN should be defined as username@ts.cryptocard.com.

The user account does not need write capability as the agent only reads from the directory.

The Base DN acts as the starting point in the directory for the agent to search for users.

Append Base DN: This will add the Base DN to the information defined in User DN. Do not select this option if the User DN value has been entered in an email format.

The agent will automatically find all containers with users, starting from the BaseDN. You can exclude containers or add containers by checking the manually edit option.
4. The next step is to configure the LDAP group memberships which are used to determine which users are synchronized. In other words, containers determine where to look for users while group membership determines which users in a container will be synchronized.

Use the arrow buttons to add or remove highlighted Available Groups to/from Synchronized Groups.

5. Click Configure in the Other Synchronization Options group.

If required, modify the LDAP Scan Interval and/or the Groups to Sync option.

6. Select the Notification Tab. In SMTP Configuration select Configure.

Enter a from Email address, the Hostname/IP address of the SMTP server, port number and if required, the user name and password credentials to log onto the SMTP server.

7. In Email Message Templates select Customize.

Select the message condition from the dropdown and modify the Subject and Body content as required.
8. In Event Recipient Lists select Add.

Enter one or more valid email addresses to the recipient email list and set the event.

9. To start / stop synchronization, click the Start / Stop buttons in Service Status.

10. To allow Sync Agent Permission, click the Change Permission link in the Sync Permission column under the LDAP Sync Agent Hosts task of the Authentication Processing module on the COMMS tab of your Blackshield Console.

Change the Sync Agent Host Permission to Allow and click Apply.
BlackShield ID LDAP Sync Agent Configuration Tool

The BlackShield ID LDAP Sync agent configuration tool allows for the modification of various features available within the agent.

Status Tab

The Status tab deals primarily with supplying information on LDAP Sync Groups and their transaction details.

LDAP Configuration

**LDAP Connection Status**
Displays the current connection status between the agent and the LDAP Directory server.

**LDAP Configuration Info**
Displays the connection information for the LDAP Server. This dialog does not display any password information.

**LDAP Sync Groups**
Lists all LDAP Groups configured to synchronize against the BlackShield Cloud.
Last Sync Status

**LAST SYNC TIME**
Displays the last synchronization attempt by the agent.

**SCAN DURATION**
Displays the amount of time required to scan all groups to retrieve user information.

**# OF UNIQUE OBJECTS**
Displays the amount of LDAP objects discovered during the last scheduled scan.

**# OF DIFFERENCES**
Displays the amount of LDAP objects differences between the local persistent cache and the LDAP Directory server during the last scheduled scan.

**SENT TRANSACTIONS**
Displays the amount of updates sent to the BlackShield Cloud.

**TOTAL USERS SYNC’D**
Displays the amount of users currently synchronized with the BlackShield Cloud.

Transaction Details

**ID**
Displays the number of the current transaction record.

**STATUS**
Displays the status of the transaction.

**SCAN STARTED**
Displays the start date and time of an LDAP Directory server scan.

**SCAN ENDED**
Displays the end date and time of an LDAP Directory server scan.

**SENT TO BLACKSHIELD**
Displays the date and time the transaction was delivered to BlackShield Cloud.

**REFRESH**
Amount of time before transaction details will be updated.

**SAVE AS**
Saves all transaction details to a file.

**CLEAR**
Permanently deletes all transaction details.
Configuration Tab

The Configuration tab deals primarily with LDAP configuration and scanning intervals.

LDAP Configuration

This section is used to configure the connection between the agent and the LDAP Directory server.

**HOST NAME OR IP**
Specifies the location of the LDAP server.

**PORT**
By default TCP port 389 is used. If required, the Active Directory Global Catalog (TCP port 3268) may be used.

**USE SSL**
If the LDAP server has been configured to use a certificate this option may be select. If the option is selected change the Port value to 636.

**NUMBER OF FAILOVER**
May configure up to 4 other failover LDAP servers. All LDAP servers must have access to the same BaseDN.
**LDAP Schema**
Includes default LDAP schema support for Active Directory (2003/2008), eDirectory 8.x and Sun One 6.x

Additional schemas may appear if configured under LDAP Schema Configuration.

---

**LDAP Credentials**

**User DN**
If using Active Directory, the value should be entered in an email format

Example: The BaseDN in the figure is dc=ts, DC=cryptocard, DC=com. So username “cclldap” could be defined in UserDN as cclldap@ts.cryptocard.com.

If using another LDAP Server the User DN may be more complicated, for example

uid=cclldap, ou=Users, dc=ts, dc=cryptocard, dc=com

**Base DN:**
Specifies the top level of the LDAP Server.

**Append Base DN**
This will add the Base DN to the information defined in User DN.

Example: If I specified a User DN of uid=cclldap and selected Append Base DN the following would be submitted to the LDAP Server when connecting

uid=cclldap, dc=ts, dc=cryptocard, dc=com

**Password**
Used in combination with User DN as credentials to connect to the LDAP Server.
MANUAL DN CONFIGURATION

Allows for manually editing the location where users can be found.

LDAP Sync Group(s)

LDAP groups may be selected from Available Groups and placed into Synchronized Group(s).

If the group is not visible, enter the name of the group in the Available Groups field.

Synchronization will not take place if Synchronized Group(s) contains no groups.

If a selected LDAP group is deleted on the LDAP Directory Server, all synchronization will be halted until the group is removed from the agent or recreated on the LDAP Directory Server.

If you’d like to remove all LDAP users from BlackShield Cloud, you must place an empty LDAP group in Synchronized Group(s).
LDAP Schema Configuration

The schema management dialog allows for the creation of a custom schema. This can be used to view LDAP objects which are not visible by default within the LDAP Synchronization agent.

Other Synchronization Options

Mobile Number Country Code

**COUNTRY CODE TO PREPEND**

The agent automatically strips all non-numeric characters from the data in the “Cell Number” mapping (refer to point 7 above). In addition, if a numeric value is entered into this field, the agent will prepend this value to the “Cell Number” mapping under the following conditions:

- If the Cell Number has 00 as the leading digits, the agent will remove the leading 00. Example: 0041-77889991111 becomes 4177889991111

- If the Cell Number has 0 as the leading digit, the agent will strip the 0 and prepend the country code. Example using 31 as prepend country code: 0778-89991111 becomes 3177889991111

- If the Cell Number leading digit is 1 through 9, the agent will prepend the country code. Example using 31 as prepend country code: 778-89991111 becomes 3177889991111

LDAP Scan Interval

This value determines how frequently the agent will scan LDAP for changes and apply them to BlackShield Cloud. The default value is 20 minutes.
Group Sync Options

The Group Sync options allow you to control the LDAP groups that get migrated into BlackShield Cloud. The default value is *Sync filter groups only*.

The following options are available:

**All**: All LDAP groups will be imported into BlackShield Cloud.

**With members only**: Only the LDAP groups assigned to synchronized users are imported into BlackShield Cloud.

**Sync filter groups only**: Only the monitored LDAP sync group is imported into BlackShield Cloud.

**None**: No LDAP groups will be imported into BlackShield Cloud.

**Key Set**

Displays the account specific synchronization agent key being used in BlackShield Cloud. This information must match with the Key Set found under Virtual Servers, Account Name, COMMS, Authentication Processing, LDAP Sync Agent Settings within BlackShield Cloud.

**BlackShield ID Synchronization Server**

Displays the location of the BlackShield Cloud LDAP synchronization servers and the TCP port.
Notification Tab

The Notification tab deals primarily with SMTP Server configuration and alert messages.

SMTP Configuration

**CONFIGURE SMTP SETTINGS**

Enter a from Email address, the Hostname/IP address of the SMTP server, port number.

If required, the user name and password credentials to log onto the SMTP server may be entered.
E-Mail Test

**ENTER EMAIL ADDRESS**
This section is used to test the SMTP configuration.

E-Mail Message Templates

The agent can send notification if it is unable to connect to LDAP or connect to BlackShield.

Event Recipient Lists

**LIST NAME**
Display name for the event.

**RECIPIENT E-MAIL**
Enter a valid email address then select Add.

**RECIPIENT E-MAIL LIST**
Displays a list of all email addresses to notify.

**EVENTS**
Place a checkmark on LDAP or Sync Server Connection issue.