December | 14

Technical Publications

ZULTYS

INNOVATE | COMMUNICATE | COLLABORATE

Administrator Manual

LDAP Integration

Author: Zultys Technical Support Department

Information in this document is subject to change without notice. Every effort has been made to ensure that the information in this document is accurate. Zultys, Inc. is not responsible for printing or clerical errors. Any troubleshooting suggestions or suggestions for resolving common issues included in this document are recommendations made by Zultys Technical Support team and are not guaranteed to resolve every issue the reader may encounter.

1 Contents

1 INTRODUCTION 5

2 LDAP CONFIGURATION 6

2.1 ADDING A CONNECTION/SERVER 6
2.2 REMOVING A CONNECTION/SERVER 8
2.3 TESTING A CONNECTION/SERVER 8
2.4 REORDERING THE SERVERS 9

3 LDAP SYSTEM SERVICE STATUS 9

4 CONFIGURING USERS FOR AUTHENTICATION THROUGH LDAP 10

5 INSTALLATION OF SECURITY CERTIFICATES 12

5.1 DIGITAL SECURITY CERTIFICATES 12
5.2 INSTALL A CERTIFICATE FROM A CERTIFICATE AUTHORITY 12
5.2.1 ADD TRUSTED CERTIFICATE 13
5.2.2 ADD CERTIFICATE CHAIN 13

6 TROUBLESHOOTING 13

Trademark Information

Zultys and the Zultys logo design are registered trademarks of Zultys, Inc. MXIE is a trademarks of Zultys, Inc.
All other trademarks are the property of their respective owners.

Edition notice

This edition applies to version 1 of Zultys LDAP Integration and all subsequent releases and modifications until otherwise indicated in new editions.

Zultys Inc.
785 Lucerne Drive
Sunnyvale, CA 94085
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Zultys, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Zultys, Inc. retains title to, and ownership of, all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g. a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Zultys, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

1 Introduction

Zultys MX Software Version 6.0 adds the ability to include authentication through integration with an LDAP (Lightweight Directory Access Protocol) server. With LDAP authentication, users can login using the same password whether by local area network, intranet, e-mail, etc.

To use LDAP authentication, LDAP service first must be enabled on each MX phone system.

An LDAP authentication privilege then is assigned to each user. Through the MX Administrator UI, an MX Administrator can configure a user's profile to authenticate either by using a local password, which is stored and verified on the MX, or from an LDAP server. An LDAP authentication privilege can be removed at any time from the user's profile, as well.

Users with LDAP authentication use their domain passwords to login to the MXIE unified communications interface, Zultys Communicator for iPhone/Android, Zultys Salesforce Adapter, Zultys Outlook Communicator and Flex.

Users with administrator privileges that have LDAP authentication enabled in their user profile will use their domain passwords to login to the MX Administrator UI to administrate the MX. The built in Administrator account will always use the local MX authentication system to authenticate locally. This is by design to ensure administrative access to the MX in the event of total loss of connection to any LDAP server(s).

No LDAP cache is used by the MX and there is no automatic fail-over to local passwords. If an LDAP server is unreachable, authentication cannot be provided to users or administrators and their login attempt will be rejected. A best practice is to use two or more LDAP servers to achieve redundancy and reliability in case of an LDAP server failure. Secondary LDAP servers are only searched when the primary LDAP server is not reachable/not responding. If a LDAP search returns zero results from the primary LDAP Server, the search will not continue to the secondary LDAP server, it will end with zero results.

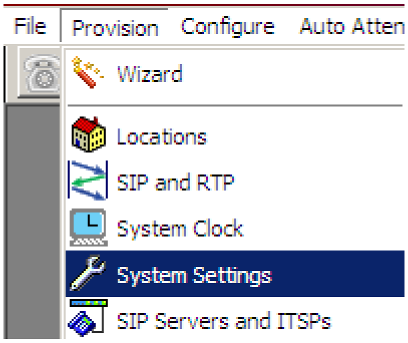
2 LDAP Configuration

In order to use LDAP authentication, you need to add a LDAP server/connection.

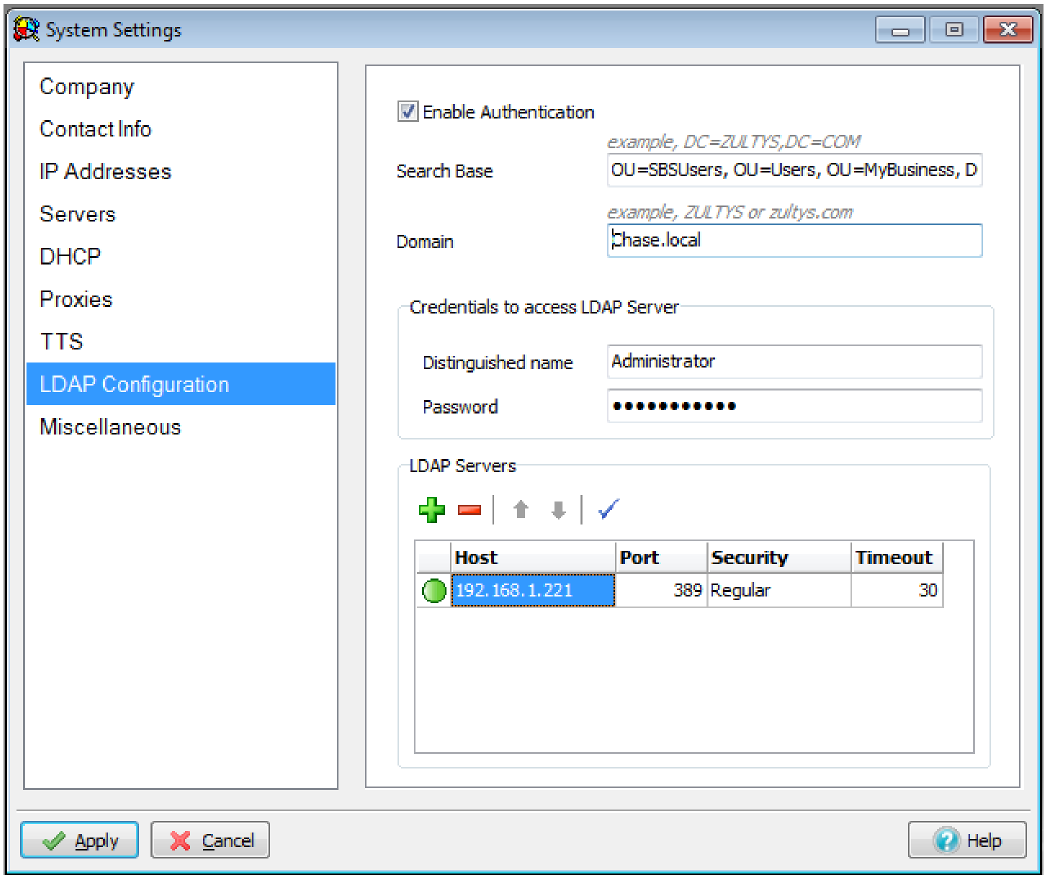
2.1 Adding a connection/server

1. Open MX Administrator

2. Click *Provision –> System settings (*This can also be set up using the Wizard as part of the initial setup)



3. A **System Settings** window opens. Click *LDAP Configuration* in left pane.



☑ Enable Authentication

Search Base: OU=SBSUsers, OU=Users, OU=MyBusiness, D (example, DC=ZULTYS,DC=COM)

Domain: Chase.local (example, ZULTYS or zultys.com)

Credentials to access LDAP Server

Distinguished name: Administrator

Password: ●●●●●●●●●●●

LDAP Servers

	Host	Port	Security	Timeout
●	192.168.1.221	389	Regular	30

4. Click on the checkbox to *Enable Authentication*.

5. Key in the data fields.

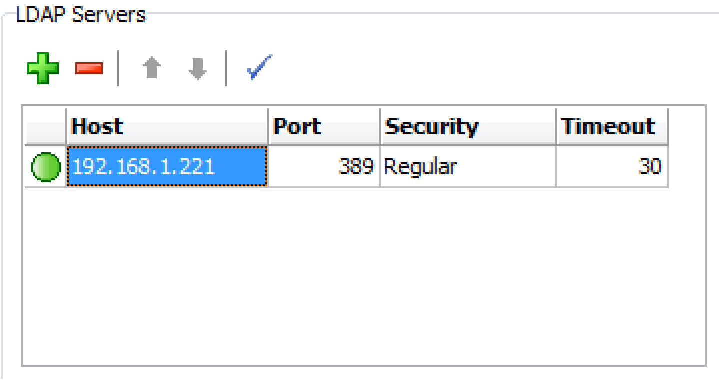
   - **Search Base**: This is the LDAP path to where all the users reside in the LDAP directory
   - **Domain**: This is the LDAP domain
   - **Distinguished Name**: Name/Account used to log into the LDAP directory to search for user credentials
   - **Password**: Password associated with the distinguished name

6. In the *LDAP Servers* block, click on the green + button (✚), to add an LDAP server.

7. Enter data for *Host*, *Port*, *Security* and *Timeout*.

   - **Host:** IP of FQDN of LDAP Server
   - **Port:** Port used to communicate with the LDAP server
   - **Security:** Security options

  - **Regular:** unencrypted communications
  - **SSL/TLS:** SSL/TLS Protocol used in encryption
  - **Start TLS:** StartTLS Protocol used in encryption
- **Timeout:** time out in seconds


LDAP Servers

	Host	Port	Security	Timeout
●	192.168.1.221	389	Regular	30

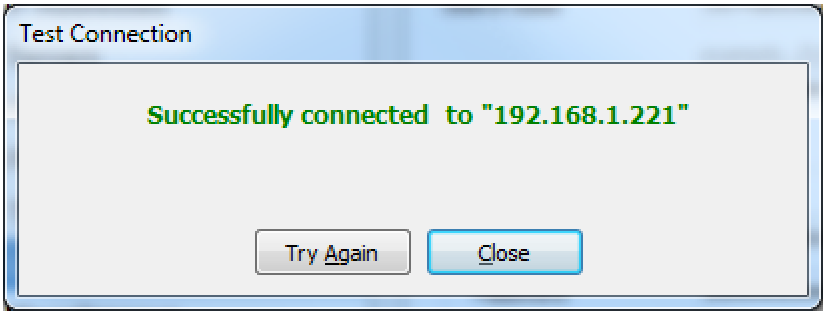
8. For redundancy, additional servers should be added. If one server is unreachable, the MX system automatically will attempt to use a secondary server. Click on the + button again to add additional servers.
9. Click on the *Apply* button when done.

2.2 Removing a connection/server

To remove a server highlight server entry and click on the red minus sign (−), there is no warning, it is simply removed.

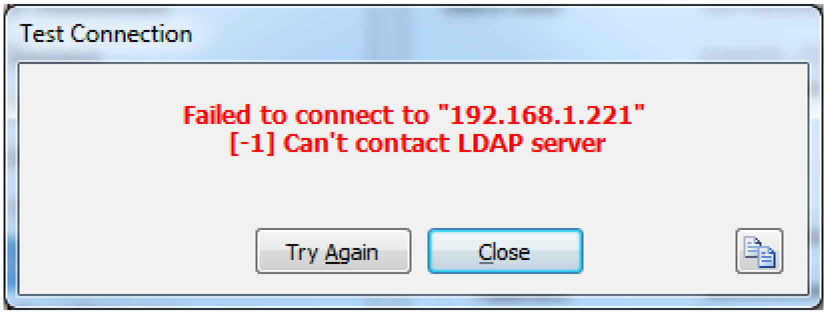
2.3 Testing a connection/server

Clicking on the blue check mark (✓), will allow you to test the connection to the LDAP server, if it is a successful connection the following message will be displayed.


Test Connection

Successfully connected to "192.168.1.221"

If the test fails to connect to the LDAP server the following message will be displayed, and it will indicate the reasons for failing.



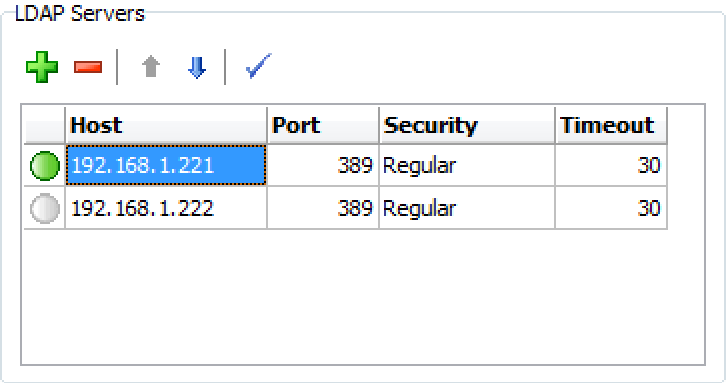
Failed to connect to "192.168.1.221"
[-1] Can't contact LDAP server

2.4 Reordering the servers

You can change the order of the connections/servers by highlighting the appropriate server and clicking the up and down arrows (⬆ ⬇).

3 LDAP System Service Status

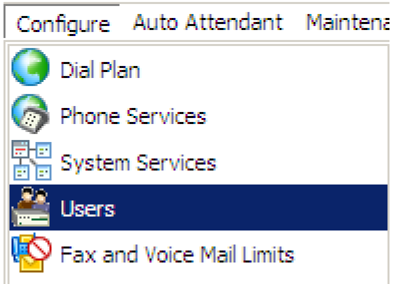
The status of the connection between the MX and the LDAP server is indicated by a green circular icon next to the LDAP server entry in the LDAP server table. If the connection is lost between the MX and the LDAP server the circular icon will change to a grey color to indicate it is not able to communicate with the LDAP Server.



	Host	Port	Security	Timeout
●	192.168.1.221	389	Regular	30
○	192.168.1.222	389	Regular	30

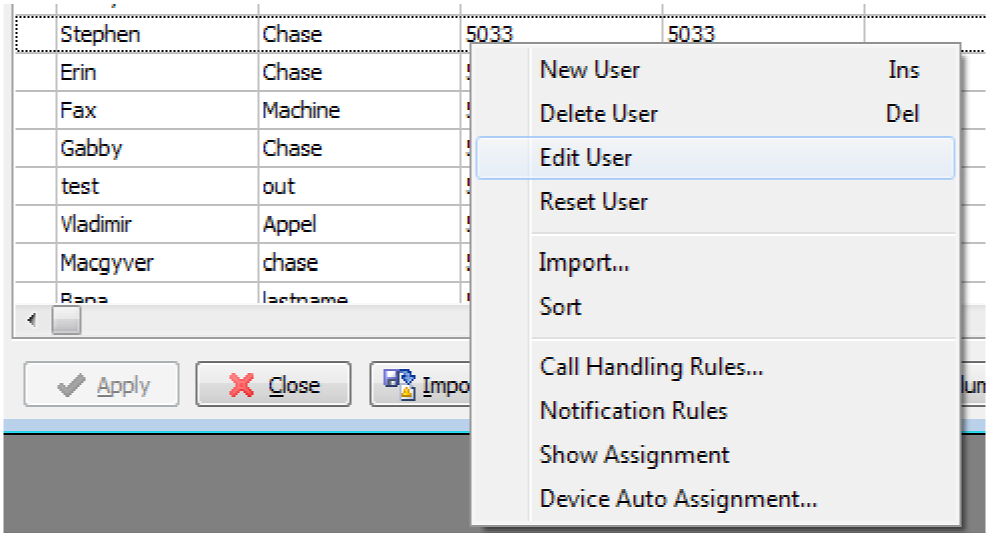
4 Configuring Users for Authentication through LDAP

1. Click on *Configure* -> *Users*



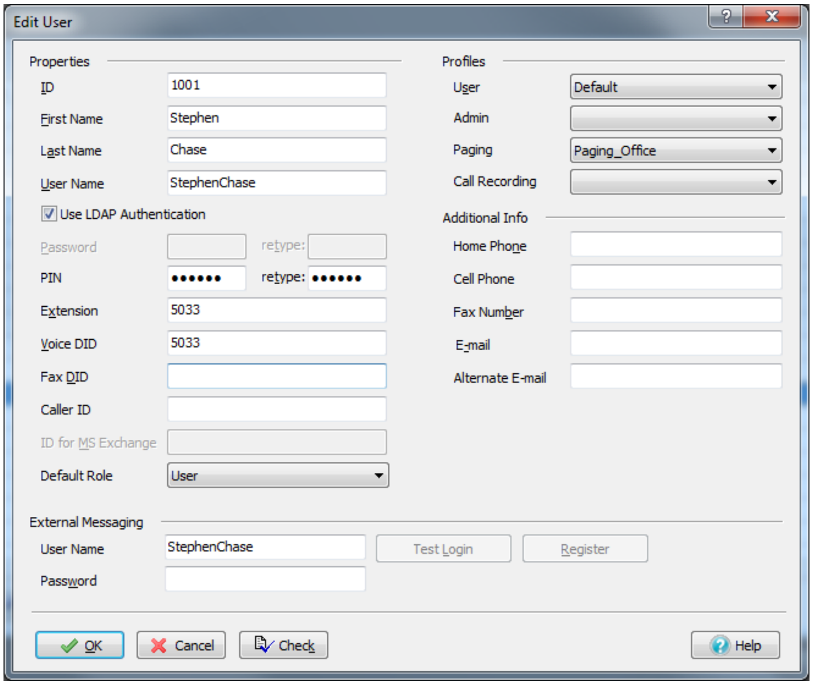
2. In the opening Users window, highlight the User's name and right-click on the name.

3. Select *Edit User*.



Stephen	Chase	5033	5033
Erin	Chase		
Fax	Machine		
Gabby	Chase		
test	out		
Vladimir	Appel		
Macgyver	chase		
Bana	lastname		

4. An Edit User window opens.



Properties

ID	1001
First Name	Stephen
Last Name	Chase
User Name	StephenChase
☑ Use LDAP Authentication	
Password	retype:
PIN	•••••• retype: ••••••
Extension	5033
Voice DID	5033
Fax DID	
Caller ID	
ID for MS Exchange	
Default Role	User

Profiles

User	Default
Admin	
Paging	Paging_Office
Call Recording	

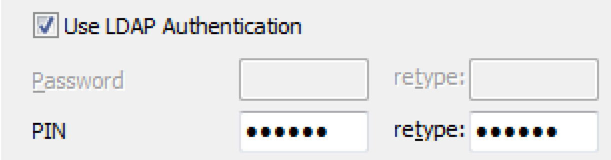
Additional Info

Home Phone	
Cell Phone	
Fax Number	
E-mail	
Alternate E-mail	

External Messaging

User Name	StephenChase
Password	

5. Click on the checkbox to enable *Use LDAP Authentication*. This will enable the individual user to use LDAP authentication, the password field will automatically grey out. A PIN should be added for this user from the users MXIE client.



☑ Use LDAP Authentication

Password		retype:	
PIN	••••••	retype:	••••••

6. **Password:** (local or through LDAP) is used with all computer clients including the MXIE Unified Communications interface, Zultys Mobile Communicator clients and the MX Administrator.

   When LDAP authentication is selected, Password fields are unavailable and are shown grayed.

7. **PIN**: Since the password is the same as your computer login via the LDAP server, this is usually a secure password that is alpha numeric, which cannot be entered on a telephone keypad. The Pin is used to access your voicemail via the telephone, or any time you are required to provide authentication to the MX via a telephone. The PIN is a numeric only field.

5 Installation of Security Certificates

The Lightweight Directory Access Protocol (LDAP) is used to read from and write to Active Directory. By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL) / Transport Layer Security (TLS) technology. You can enable LDAP over SSL (LDAPS) by installing a properly formatted certificate provided by the LDAP server administrator on the MX manually.

If your LDAP server requires Secure Sockets Layer (SSL) / Transport Layer Security (TLS) secured connection between the MX and your LDAP Server you must install the LDAP servers Certificate (provided by the server's administrator) on the MX manually. When using certificate chains, ALL certificates must be installed on the MX, if any of the chain is missing, the connection will fail.

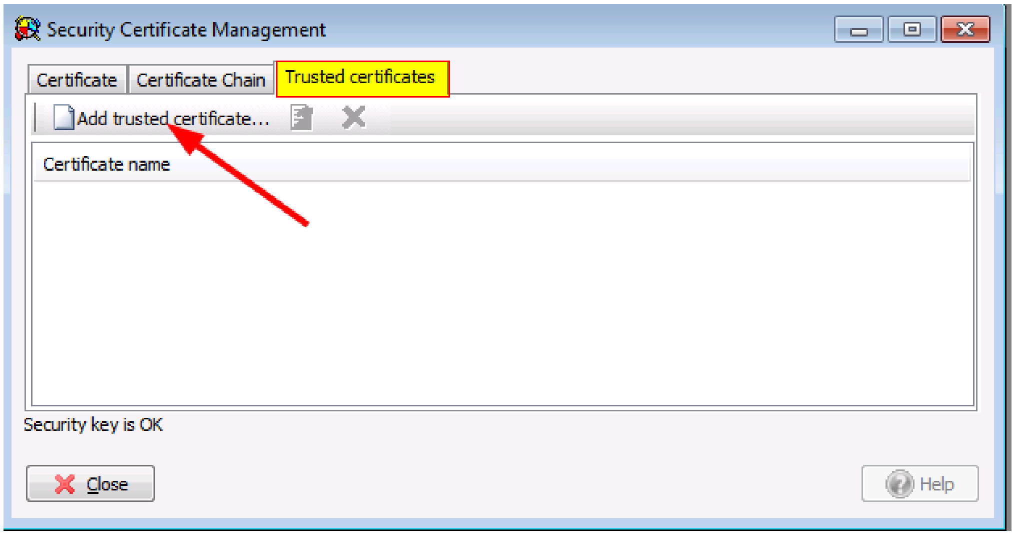
5.1 Digital Security Certificates

For LDAP servers that use a Secure Sockets Layer (SSL) / Transport Layer Security (TLS) secured connection between the server and your MX. A digital security certificate is required to enable a connection to the MX. A security certificate is a digital document assuring users that their transmission is encrypted, secure and connected to the right server, and it also informs the company that the communication is from who they claim to be.

If that certificate has been signed and approved by an independent certification authority (CA) then the Zultys MX and 3rd Party LDAP Server accepts the two endpoints as legitimate and proceeds with the connection.

5.2 Install a Certificate from a Certificate Authority

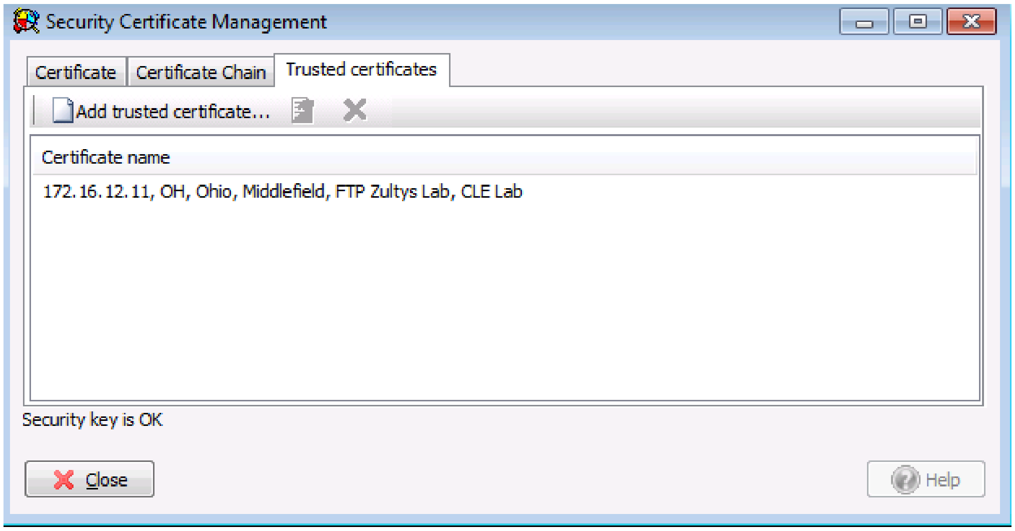
1. Navigate to *Maintenance -> Security Certificate Management*.



Security key is OK

5.2.1 Add Trusted Certificate

1. Click *Add trusted certificate* button from the trusted certificate tab.
2. Navigate to certificate file location and select the file.
3. Certificate will be automatically added.
4. If required, upload a certificate chain.



Certificate name
172.16.12.11, OH, Ohio, Middlefield, FTP Zultys Lab, CLE Lab

Security key is OK

5.2.2 Add Certificate Chain

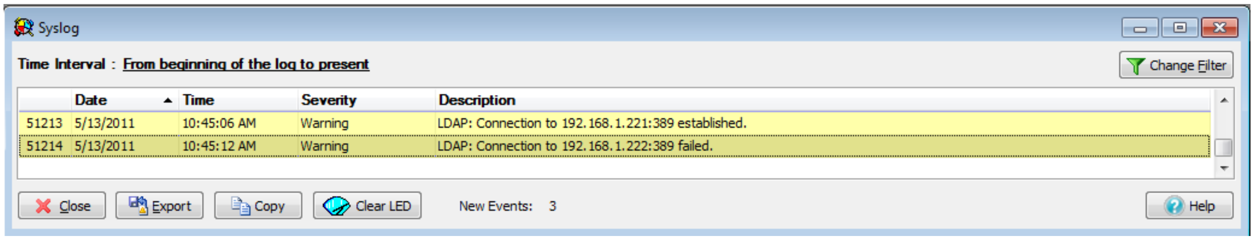
1. Click on the *Upload* button.
2. Choose Certificate Chain.
3. Navigate to certificate file location and select the file.
4. Certificate will be automatically added.

6 Troubleshooting

Troubleshooing issues with LDAP integration

- Confirm network connectivity
  - Verify IP or FQDN
  - If using FQDN, verify MX DNS server
  - Can you ping the server from the MX
- Login Issues
  - Check the Search Base, and verify it is correct and the users are in that location
  - Check Domain
  - Check Authentication credentials

The MX's built in Syslog will also capture all errors and report them



Time Interval : From beginning of the log to present

	Date	Time	Severity	Description
51213	5/13/2011	10:45:06 AM	Warning	LDAP: Connection to 192.168.1.221:389 established.
51214	5/13/2011	10:45:12 AM	Warning	LDAP: Connection to 192.168.1.222:389 failed.

New Events: 3