

**Main page:** [Cisco Unified MeetingPlace, Release 7.0](#)

**Up one level:** [Troubleshooting](#)

## Contents

- [1 LDAP Authentication Problem](#)
  - ◆ [1.1 Related Topics](#)
- [2 Windows Authentication Problem](#)
  - ◆ [2.1 Related Topics](#)
  - ◆ [2.2 Adding a URL String to Internet Explorer's Trusted Zone](#)
    - ◇ [2.2.1 Procedure](#)
    - ◇ [2.2.2 Related Topics](#)
  - ◆ [2.3 Modifying Internet Explorer's Internet Zone to Automatically Pass Windows Credentials](#)
    - ◇ [2.3.1 Procedure](#)

## LDAP Authentication Problem

**Problem:** Cisco Unified MeetingPlace Web Conferencing is configured for LDAP authentication, but users are not being properly authenticated.

**Solution:** Check the Cisco Unified MeetingPlace eventlog. LDAP messages appear in the eventlog every time an authentication is performed. If the authentication is successful, you will see a message such as the following: LDAP Authenticated user: <username>

If the authentication fails, one of the following error messages will be logged in the eventlog:

**Error Message:** LDAP could not find user: <username>

**Explanation:** The user was not found (LDAP\_NO\_SUCH\_OBJECT).

**Error Message:** LDAP could not authenticate user: <username>

**Explanation:** User had bad credentials (LDAP\_INVALID\_CREDENTIALS); this is typically caused by using the wrong password.

**Error Message:** ldap\_simple\_bind\_s failed with error <hexadecimal number>

**Explanation:** This message is logged when the authentication fails for any other reason besides user not found or bad credentials. The hexadecimal number in the error code indicates the failure reason. Descriptions of the hexadecimal codes can be found at <http://msdn2.microsoft.com/en-us/library/aa367014.aspx>.

#### Related Topics

- [Monitoring and Maintaining Cisco Unified MeetingPlace Web Conferencing](#)

## Windows Authentication Problem

**Problem:** Internet Explorer prompts me for my Windows login information when I try to access Cisco Unified MeetingPlace even though I am already logged on to my computer with my domain Windows account.

**Possible Cause:** You configured Windows authentication but used an IP address or FQDN when setting your Web Server Hostname [Home Page] parameter. If the server name in a URL request to the Web Server contains any periods, such as the dots in an IP address or a FQDN, the request is automatically routed to Internet Explorer's Internet Zone, which is configured to not pass Windows credentials to the Web Server.

**Solution:** Add the URL string for Cisco Unified MeetingPlace to Internet Explorer's Trusted Zone or modify Internet Explorer's Internet Zone to automatically pass Windows credentials and log users into a website.

#### Related Topics

- [Adding a URL String to Internet Explorer's Trusted Zone](#)
- [Modifying Internet Explorer's Internet Zone to Automatically Pass Windows Credentials](#)

## Adding a URL String to Internet Explorer's Trusted Zone

This is the preferred method for working around Internet Explorer's Internet Zone configuration.

**Caution!** If you choose this workaround, you must apply this change to all end user computers.

#### Procedure

1. Open Internet Explorer.
2. Select **Tools > Internet Options**.
3. Click the **Security** tab.
4. Click **Trusted Zone**.

5. Click **Edit**.
6. Add the URL of your Web Server in the Trusted Sites window.  
For example, if you set your Web Server Hostname [Home Page] parameter to *abc.company.com*, then enter *http://abc.company.com* in the list of trusted websites and click **Add**.
7. Click **OK**.

#### Related Topics

- [Configuring Cisco Unified MeetingPlace Web Conferencing Security Features](#)

## Modifying Internet Explorer's Internet Zone to Automatically Pass Windows Credentials

**Caution!** If you choose this workaround, you must apply this change to all end-user computers.

#### Procedure

1. Open Internet Explorer.
2. Select **Tools > Internet Options**.
3. Click the **Security** tab.
4. Click **Internet Zone > Custom Level**.  
The Security Settings window displays.
5. Scroll down to the User Authentication section.
6. Click **Authenticate Logon with Current Username and Password** for Logon.
7. Click **OK**.