Trust External Authentication represents a broad-range of enterprise security software that provides functions like authentication, resource access authorization, Single Sign On (SSO), and intrusion detection. Typically, this software protects your web server by installing a DLL plug-in into the web server service, for example IIS. This DLL plug-in, also called ISAPI Filter, intercepts user login credentials and passes them to a corporate authentication and authorization server. The software must be able to output user IDs in the HTTP header so that they can be passed to Cisco Unified MeetingPlace for authentication.

Note: User IDs in the Cisco Unified MeetingPlace profile database are case sensitive. Users cannot log in to Cisco Unified MeetingPlace as guests after you have configured this authentication mode.

Before configuring this authentication mode, make sure that you read the following terms of agreement in Web Conferencing Terms of Use:

- Terms for Single Sign On Software Integration
- Terms of Support for Single Sign On Software Integration

Restrictions

When configuring Trust External authentication, make sure that the /mpweb/scripts/public/ directory is not protected by SSO. Protecting this directory will prevent Cisco Unified MeetingPlace Web Conferencing from functioning properly.

See the following procedures:

- To Configure Trust External Authentication
- To Verify the Trust External Authentication Configuration

To Configure Trust External Authentication

When user IDs are sent to the Cisco Unified MeetingPlace Audio Server, Web Conferencing can apply transformation to user IDs.

If you are also using Cisco Unified MeetingPlace for Outlook, complete the Allowing Cisco Unified MeetingPlace for Outlook Authentication before beginning this procedure.

1. Sign in to Cisco Unified MeetingPlace Web Conferencing.
2. From the Welcome page, click **Admin** , then click **Web Server** .
3. From the "View" section of the page, click the name of the web server that you want to configure.
4. Scroll down to the Web Authentication section.
5. For "Step 1: Directory," choose **Trust External Authentication** .

6. For "HTTP Header Containing Username," enter an appropriate value for an external service, such as HTTP_SM_USER for SiteMinder.
7. For "Username Conversion Function," choose how you want user names transformed. **None** applies no transformation to the original user ID string.
8. Click **Submit** and wait five minutes for the new configuration to take effect.
9. (Optional) If you want to verify your configuration, continue with the To Verify the Trust External Authentication Configuration.

To Verify the Trust External Authentication Configuration

Use a Cisco Unified MeetingPlace end user profile when completing the this procedure.

1. Open your web browser and navigate to the Cisco Unified MeetingPlace Web Conferencing home page.
2. Verify the following end-user behaviors:
    - Using a SiteMinder environment, you are immediately authenticated to MeetingPlace with your SiteMinder user ID and password.
    - If you have a Cisco Unified MeetingPlace profile, you can log in with your SiteMinder password and schedule meetings.