

[Cisco Unified MeetingPlace Release 6.1](#) > [Web Conferencing](#) > [Configuring](#) > [Configuring User Authentication](#)

The HTTP basic authentication method is a widely used industry-standard method for collecting user ID and password information. It works as follows:

1. Users are prompted by a pop-up login window that is rendered by their web browser.
2. Users enter valid domain user IDs and passwords. Cisco Unified MeetingPlace profile passwords are ignored and not used in the authentication operation.
3. If the web servers accept the login credentials and the user IDs also exist in Cisco Unified MeetingPlace profile databases, users are logged in automatically to Cisco Unified MeetingPlace and are granted access to the Cisco Unified MeetingPlace home page.

Note: Cisco Unified MeetingPlace profile user IDs are case sensitive and must match the domain user ID of the user.

The advantage of HTTP Basic Authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that the password is Base64 encoded before being sent over the network. Since Base64 is not a true encryption, it can be easily deciphered. You can mitigate this security risk by implementing Secure Socket Layer (SSL) on the web server.

See the following procedures:

- [To Configure HTTP Basic Authentication \(Domain\)](#)
- [To Verify the HTTP Basic Authentication \(Domain\) Configuration](#)

To Configure HTTP Basic Authentication (Domain)

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 **HTTP Basic Authentication (Domain)** .
"Step 2: Login Method" is automatically set to HTTP Basic Authentication and cannot be changed.
6. Click **Submit** and wait five minutes for the new configuration to take effect.
7. (Optional) To verify your configuration, continue with the [To Verify the HTTP Basic Authentication \(Domain\) Configuration](#).

To Verify the HTTP Basic Authentication (Domain) Configuration

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

1. Open a web browser and navigate to Cisco Unified MeetingPlace Web Conferencing.
2. Verify the following end-user behaviors:
 - ◆ You see an Enter Network Password dialog when accessing the home page.
 - ◆ If you have a local account on the Windows server and a matching profile user ID, you are authenticated to the Audio Server when you enter your domain user ID and password.
 - ◆ If you have a Cisco Unified MeetingPlace profile, your name appears on the Welcome page as firstname, lastname and the Sign In link no longer displays.
 - ◆ You can only log in to Cisco Unified MeetingPlace if you are authenticated by the Cisco Unified MeetingPlace web server.
 - ◆ In IIS, the MPWeb/Scripts folder is set to Basic Authentication.