By default, Cisco Unified MeetingPlace Web Conferencing prompts users for login credentials by using an HTML web form, then authenticates them against the Cisco Unified MeetingPlace user profile database. However, you can choose to authenticate Cisco Unified MeetingPlace against third-party authentication software that provides different authentication behaviors. This can include different login windows, authentication against other user profile databases, or both.

Integration with third-party authentication software can provide the following benefits:

- Centralized user database-Facilitates profile management.
- Single Sign-On (SSO)-Allows users who have already been authenticated once to have access to all resources and applications on the network without having to re-enter their credentials.

  For SSO to work, you must ensure that Cisco Unified MeetingPlace user IDs are set up so that they match the corresponding user IDs used by the third-party authentication software. Because Cisco Unified MeetingPlace user IDs are case-sensitive, we recommend that you create them with all lowercase characters, and that you use Cisco Unified MeetingPlace Directory Services for directory synchronization. This way, matching user IDs between Cisco Unified MeetingPlace and third-party authentication software is easily accomplished.

Note: Cisco Unified MeetingPlace Web Conferencing automatically converts case so that Cisco Unified MeetingPlace user IDs and corresponding user IDs used by third-party authentication software match.

Web Conferencing provides the following authentication configuration options:

- HTTP Basic Authentication (Domain)
- LDAP
- LDAP, then MeetingPlace
- MeetingPlace
- Trust External Authentication
- Windows Integrated Authentication

Note: Having a Cisco Unified MeetingPlace profile does not guarantee users access to the Cisco Unified MeetingPlace system. Login behaviors vary depending on the authentication configuration and login options that you choose.

Contents

Restrictions: User Authentication and Load Balancing

In a Cisco Unified MeetingPlace load-balancing cluster, all users must enter the Cisco Unified MeetingPlace system through a designated Cisco Unified MeetingPlace web server. In such circumstances, you only need to configure the designated web server for your chosen authentication method. You can configure all other web servers in the cluster to use the default authentication method-MeetingPlace Web Form Authentication.

If, however, you want to configure other web servers in the cluster to use the same authentication method as a failover strategy, you can. However, depending on the type of authentication method used, this configuration can result in undesirable SSO behaviors.

For example, if you configure HTTP Basic Authentication or Windows Integrated Authentication, Cisco Unified MeetingPlace will prompt users for login credentials each time there is a web server redirect. This is because you are altering the hostname in the authentication configuration each time you redirect traffic to an active web server through a DNS change. If you configure LDAP or MeetingPlace authentication, users will not be prompted again for login credentials during a web conferencing redirect.

Allowing Cisco Unified MeetingPlace for Outlook Authentication

If your Cisco Unified MeetingPlace system includes the Cisco Unified MeetingPlace for Outlook integration, you must configure Cisco Unified MeetingPlace Web Conferencing to allow Outlook to authenticate. Do the following procedure.

Before You Begin

Verify that the Cisco Unified MeetingPlace user IDs and Windows domain user IDs of your users match.

To Configure Cisco Unified MeetingPlace for Outlook Authentication

1. Update the Cisco Unified MeetingPlace Web Conferencing registry key to allow Outlook authentication.
    1. From your desktop, choose **Start > Run** , then enter **regedit** .
    2. Locate HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\MeetingPlace WebPublisher\mpagent and change to **RemoteUserAllowed** .
    3. To allow Outlook to authenticate, choose **1** .
2. Configure Cisco Unified MeetingPlace for Outlook to use integrated windows authentication.
    1. Open Explorer and navigate to the **\MPWEB\mpoutlook** folder.
    2. Double-click **configclients.exe** .
    3. From the Outlook control panel, choose the **Logins** tab and check **Use Integrated Windows Authentication** .
    4. Click **OK** .
    5. Close the Outlook Configuration Client utility.

3. If you are configuring Web Conferencing user authentication, continue with the information at the top of the About User Authentication page to determine your authentication mode.