Windows Integrated Authentication (WIA) uses an algorithm to generate a hash based on the credentials and computers that users are using. WIA then sends this hash to the server; user passwords are not sent to the server.

If WIA fails for some reason, such as improper user credentials, users are prompted by their browsers to enter their user IDs and passwords. The Windows logon credentials are encrypted before being passed from the client to the web server.

Note: You can configure Internet Explorer version 4.0 or later versions to initially prompt for user information if needed. For more information, see the Internet Explorer documentation.

Although Windows Integrated Authentication (WIA) is secure, it does have the following limitations:

- Only Microsoft Internet Explorer version 4.0 or later versions support this authentication method.
- WIA does not work across proxy servers or other firewall applications.
- WIA works only under the browser Intranet Zone connections and for any trusted sites you have configured.
- Cisco Unified MeetingPlace UserIDs must be all lower case.
- You cannot have SSL enabled if you are configuring WIA.

Therefore, WIA is best suited for an intranet environment where both users and the web server are in the same domain and where administrators can ensure that every user has Microsoft Internet Explorer. The web server must be in a Windows domain.

To further ensure or verify that your network supports WIA, refer to Microsoft online documentation.

Contents

Login Behavior with Windows Integrated Authentication

The following describes the login behavior when using WIA:

- Users log in to their workstations by using their Windows NT domain accounts.

- If their NT account user IDs also exist in the Cisco Unified MeetingPlace profile database, users are automatically logged in to Cisco Unified MeetingPlace and granted access to the home page. Cisco Unified MeetingPlace profile passwords are ignored and not used in the SSO operation.

  The home page does not have Sign In links to the HTML-based login form because users are already logged in through the SSO process. For SSO terms of agreement, see Web Conferencing Terms of Use.

- If their NT account user IDs do not match any user IDs in the Cisco Unified MeetingPlace directory, users see the Cisco Unified MeetingPlace Web Conferencing home page, but with Sign In links to the HTML-based login form. Users must then enter valid Cisco Unified MeetingPlace user IDs and passwords.

Note: Cisco Unified MeetingPlace user IDs are case sensitive. Web Conferencing converts case from lower case to upper case and vice versa automatically. However, if you are using a segmented meeting access configuration with one server (SMA-1S), case conversion affects the internal server only.

The following describes the login behavior when WIA does not work properly:

- Users see a popup window prompting them for their Cisco Unified MeetingPlace user IDs and passwords.
- If their credentials are authenticated in the Cisco Unified MeetingPlace directory, users see the Cisco Unified MeetingPlace home page.
- If authentication fails, users are prompted continually for their valid login credentials.

See the following procedures:

- To Configure Windows Integrated Authentication
- To Verify the Windows Integrated Authentication Configuration

To Configure Windows Integrated Authentication

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

Note the following restrictions:

- Users must have local accounts on Windows servers with matching profile user IDs.
- Only Microsoft Internet Explorer version 4.0 or later supports this authentication method.
- WIA works only under the browser Intranet Zone connections.
- WIA does not work across proxy servers or other firewall applications.
- You cannot have any dots in your URL. Using IP or FQDN causes users to be prompted for login credentials.

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 **Windows Integrated Authentication** .
   "Step 2: Login Method" is automatically set to HTTP Basic Authentication and cannot be changed.
6. For Require Web Server Authentication, enter **Yes**.
   Note: For more information on web server authentication, see Configuring User Authentication for Web Conferencing.
7. Click **Submit** and wait five minutes for the new configuration to take effect.
8. (Optional) To verify your configuration, continue with the To Verify the Windows Integrated Authentication Configuration.

To Verify the Windows Integrated Authentication 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:
   - If you are on the same domain, you are immediately authenticated to the web server and see the Welcome page with your name displayed in firstname, lastname order. The Sign In link does not display.
   - If you are on a different domain, you see an Enter Network Password window that includes the Domain field.
   - If you are on a different domain, enter your Windows NT account user ID and password. You are then authenticated to the Cisco Unified MeetingPlace web server and see the Welcome page with your name displayed in firstname, lastname order. The Sign In link does not display.
   - Only users authenticated by the web server can log in.
   - In IIS, the MPWeb/Scripts folder is set to Integrated Windows Authentication.

Troubleshooting Tips

If you configured your web server Home Page hostname by using an IP address or FQDN, you will be prompted for your Windows login information even if you log in by using your domain Windows account.

For a workaround to this problem, see the Troubleshooting Problems with Windows Authentication.

For information about configuring your web server Home Page hostname, see the Configuring the Web Server.