Main page: Cisco Unified MeetingPlace, Release 8.0

Up one level: Configuration

Note: This topic does *not* apply to deployments in which users schedule meetings from the Cisco WebEx site. For information about Cisco WebEx integration deployments, see the *Planning Guide for Cisco Unified MeetingPlace* at http://docwiki.cisco.com/wiki/Cisco_Unified_MeetingPlace%2C_Release_8.0_--_Planning_Your_Deployment.

- About User Authentication for the Web Server
- How to Configure MeetingPlace Authentication for the Web Server
- How to Configure LDAP Authentication for the Web Server
- How to Configure LDAP Then MeetingPlace Authentication for the Web Server
- How to Configure Trust External Authentication for the Web Server
- How to Configure HTTP Basic Authentication (Domain) for the Web Server
- How to Configure Windows Integrated Authentication for the Web Server
- Accessing Cisco Unified MeetingPlace Web When Locked-Out Due to Incorrect User Authentication Setup

Contents

About User Authentication for the Web Server

By default, Cisco Unified MeetingPlace prompts web users to sign in by using an HTML web form, then authenticates them against the Cisco Unified MeetingPlace user profile database. You may, however, choose to authenticate Cisco Unified MeetingPlace web users against third-party authentication software that provides different authentication behaviors. This can include different sign-in windows, authentication against other user profile databases, or both.

User Authentication Options for the Cisco Unified MeetingPlace Web Server

The Cisco Unified MeetingPlace Web Server software provides the following authentication configuration options:

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

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. You can configure the Cisco Unified MeetingPlace Web Server to automatically convert case so that Cisco Unified MeetingPlace user IDs and corresponding user IDs used by third-party authentication software match.

Note: While all authentication methods can be applied to internal or external servers, some authentication methods may not make sense for a DMZ environment. For more information about using Cisco Unified MeetingPlace Web Servers in the DMZ, see the Configuring Segmented Meeting Access for Cisco Unified MeetingPlace module.

Restrictions: User Authentication and Cluster Configuration

In a Cisco Unified MeetingPlace cluster configuration, 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. Depending on the type of authentication method used though, 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 to sign in 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 to sign in again during a Web Server redirect.

How to Configure MeetingPlace Authentication for the Web Server

Authenticating users against the profile database on the Cisco Unified MeetingPlace Application Server is the default user authentication option. You have two options when configuring this type of authentication:

- Signing in with an HTML-based web page form. This is the default option.
- Signing in against a sign-in window rendered by your web browser.

Regardless of the sign-in page users see, user IDs and passwords are sent to the Cisco Unified MeetingPlace Application Server for authentication. Both profiles and user passwords must match. Profiles are not case-sensitive.

- Configuring MeetingPlace Authentication for the Web Server
- Verifying MeetingPlace Authentication for the Web Server by Using the HTTP Form

Configuring MeetingPlace Authentication for the Web Server

Before You Begin

Read the Restrictions: User Authentication and Cluster Configuration.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Web Server**.

4. Select the name of the Web Server that you want to configure in the "View" section of the page.
5. Scroll to the Web Authentication section.
6. Select **MeetingPlace** for "Step 1: Directory".
7. Select one of the following options for "Step 2: Login Method":
    - Select **Web Page Form** to see an HTML-based Cisco Unified MeetingPlace sign-in window. This is the default authentication method.
    - Select' '**HTTP Basic Authentication** to see a sign-in window rendered by your web browser.
8. Select **Submit** and wait five minutes for the new configuration to take effect.

What to Do Next

(Optional) Proceed to the Verifying MeetingPlace Authentication for the Web Server by Using the HTTP Form.

Verifying MeetingPlace Authentication for the Web Server by Using the HTTP Form

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

Before You Begin

Complete the Configuring MeetingPlace Authentication for the Web Server.

Procedure

1. Open a web browser and navigate to Cisco Unified MeetingPlace.
2. Verify the following end-user behaviors:
    - When you access the Cisco Unified MeetingPlace home page, you see an Enter Network Password window.
    - After you enter your end-user Cisco Unified MeetingPlace user ID and password, you are authenticated to the Cisco Unified MeetingPlace Application Server.
    - The Welcome page displays your name in firstname, lastname order.
    - Sign In and Sign Out links do not display.

How to Configure LDAP Authentication for the Web Server

LDAP authentication compares user credentials against the profile database on an LDAPv2-compliant directory server. After users are authenticated by the LDAP server, they are automatically signed in to Cisco Unified MeetingPlace as long as their LDAP user IDs also exist in Cisco Unified MeetingPlace. You can also authenticate users against a multiple LDAP forest configuration.

With LDAP authentication, the following restrictions apply:

- The Cisco Unified MeetingPlace Web Server software supports only unencrypted LDAP, that is, queries to the LDAP server are in clear text.
- Users cannot sign in with their Cisco Unified MeetingPlace passwords for their same LDAP user names.
- LDAP profiles are used for authentication; Cisco Unified MeetingPlace profiles are ignored.

Note: To authenticate Cisco Unified MeetingPlace web users against the LDAP server, make sure that the LDAP server directory is designed to have all users in one container rather than broken into multiple containers (each representing a child OU).

Configuring LDAP Authentication for the Web Server

Before You Begin

Read the Restrictions: User Authentication and Cluster Configuration.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Web Server**.
4. Select the name of the Web Server that you want to configure in the "View" section of the page.
5. Scroll to the Web Authentication section.
6. Select **LDAP** for "Step 1: Directory".
7. Enter the LDAP hostname in the field provided.
   Example: *ldap.domain.com*
8. Enter the Distinguished Name (DN) information for your directory in the field provided noting the following considerations:
   - Cisco Unified MeetingPlace user profile login names are limited to 17 characters; therefore, the LDAP match must be 17 characters or less.
   - You can only enter one value for the LDAP Distinguished Name (DN) field. If your users are segregated into multiple organizational units (OUs), you can work around this issue by using either the DOMAIN\USER or user@ou.domain.com format for the DN. When configuring the LDAP Distinguished Name field, enter just %USERNAME%, without specifying an OU, DC, or other parameter.
     Note: All users in the LDAP server directory must be in one container rather than broken into multiple containers each representing a child OU.
   - *%USERNAME%* is the username that the user enters when logging in.
   - Before sending the request to the LDAP server *%USERNAME%* is replaced with the username that the user enters in the login username field. No additional modifications are made to the DN value.
   - *%USERNAME%* is case-sensitive, that is, all upper case.
   - If you match any of the following circumstances, leave the DN field blank (empty) instead of entering %USERNAME%:

- You are authenticating against a multiple LDAP forest configuration. Example: CN=*%USERNAME%*, OU=People, DC=mydomain, DC=com
- The LDAP server you are using is the LDAP interface on a Microsoft Active Directory server. If this is the case, you must leave the DN field blank for authentication to work. When configured in this manner, the format of the usernames that the user enters must be DOMAIN\USER or user@ou.domain.com.
- You want to send user passwords as protected (that is, not as clear text). Entering a value for the DN field sends passwords as clear text.

Note: If you choose to enter a value for the DN field, it is your responsibility to establish a secure connection between the Cisco Unified MeetingPlace web server and the LDAP server. This is not the same as configuring SSL configuration on the web server. The SSL feature in Cisco Unified MeetingPlace protects traffic between the client and web server. You will require a secure connection between the web server and the LDAP server.

- Consult your LDAP expert for your DN information.

9. Select how you want user names transformed for "Username Conversion Function." Selecting **None** applies no transformation to the original user ID string.
10. Select one of the following for "Step 2: Login Method."
    - Select **Web Page Form** to see an HTML-based Cisco Unified MeetingPlace sign-in window.
    - Select **HTTP Basic Authentication** to see a sign-in window rendered by your web browser.
11. Select **Submit** and wait five minutes for the new configuration to take effect.

Troubleshooting Tips

If you chose HTTP Basic Authentication as your sign-in method, restart the Cisco Unified MeetingPlace Web Master Service after configuring your LDAP authentication. If you do not, users who change their passwords in LDAP will be able to sign in to Cisco Unified MeetingPlace by using both their old and new passwords until the Web Master Service is restarted or after approximately 60 minutes.

What to Do Next

Based on your configuration, proceed to one of the following topics:

- Verifying LDAP Authentication for the Web Server by Using the Web Page Form
- Verifying LDAP Authentication for the Web Server by Using the HTTP Form

Verifying LDAP Authentication for the Web Server by Using the Web Page Form

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

Before You Begin

Complete the Configuring LDAP Authentication for the Web Server.

Procedure

1. Open a web browser and navigate to Cisco Unified MeetingPlace.
2. Verify the following end-user behaviors:
    - If you have a Cisco Unified MeetingPlace profile, you can sign in with your LDAP password.
    - You cannot sign in as a profiled user without a password.

Related Topics

- Configuring LDAP Authentication for the Web Server

Verifying LDAP Authentication for the Web Server by Using the HTTP Form

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

Before You Begin

Complete the Configuring LDAP Authentication for the Web Server.

Procedure

1. Open a web browser and navigate to Cisco Unified MeetingPlace.
2. Verify the following end-user behaviors:
    - When you access the Cisco Unified MeetingPlace home page, you see an Enter Network Password window.
    - After you enter your LDAP profile user ID and password, you are authenticated to the Cisco Unified MeetingPlace Application Server.
    - The Welcome page displays your name in firstname, lastname order.
    - Sign In and Sign Out links do not display.

Related Topics

- Configuring LDAP Authentication for the Web Server

How to Configure LDAP Then MeetingPlace Authentication for the Web Server

This authentication mode attempts to authenticate users against two directories if the need arises. When users first sign in, they are authenticated against the LDAP directory. If this authentication fails, the sign-in information is sent to the Cisco Unified MeetingPlace Application Server for a possible match. This behavior

allows a company to give non-LDAP users, such as guests or contractors, access to Cisco Unified MeetingPlace.

Prerequisites for Configuring LDAP Then MeetingPlace Authentication for the Web Server

- To authenticate Cisco Unified MeetingPlace web users against the LDAP server, make sure that the LDAP server directory is designed to have all users in one container rather than broken into multiple containers (each representing a child OU).
- If a match is made in the LDAP database, the user must provide the proper LDAP password. Three attempts with the incorrect password will lock the LDAP profile of the user.
- Only users who are not found in the LDAP directory are eligible for authentication through the Cisco Unified MeetingPlace directory.
- User IDs in the Cisco Unified MeetingPlace profile database are not case-sensitive.

Related Topics

- How to Configure LDAP Then MeetingPlace Authentication for the Web Server

Configuring the LDAP Then MeetingPlace Authentication for the Web Server

Before You Begin

Read the Restrictions: User Authentication and Cluster Configuration.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Web Server**.
4. Select the name of the Web Server that you want to configure in the "View" section of the page.
5. Scroll to the Web Authentication section.
6. Select **LDAP, then MeetingPlace** for "Step 1: Directory".
7. Enter the LDAP hostname in the field provided.
   Example: *ldap.domain.com*
8. Enter the Distinguished Name (DN) information for your directory in the field provided noting the following considerations:
   - Cisco Unified MeetingPlace user profile login names are limited to 17 characters; therefore, the LDAP match must be 17 characters or less.

- You can only enter one value for the LDAP Distinguished Name (DN) field. If your users are segregated into multiple organizational units (OUs), you can work around this issue by using either the DOMAIN\USER or user@ou.domain.com format for the DN. When configuring the LDAP Distinguished Name field, enter just %USERNAME%, without specifying an OU, DC, or other parameter.
  Note: All users in the LDAP server directory must be in one container rather than broken into multiple containers each representing a child OU.
- *%USERNAME%* is the username that the user enters when logging in.
- Before sending the request to the LDAP server *%USERNAME%* is replaced with the username that the user enters in the login username field. No additional modifications are made to the DN value.
- *%USERNAME%* is case-sensitive, that is, all upper case.
- If you match any of the following circumstances, leave the DN field blank (empty) instead of entering %USERNAME%:
  - You are authenticating against a multiple LDAP forest configuration. Example: CN=*%USERNAME%*, OU=People, DC=mydomain, DC=com
  - The LDAP server you are using is the LDAP interface on a Microsoft Active Directory server. If this is the case, you must leave the DN field blank for authentication to work. When configured in this manner, the format of the usernames that the user enters must be DOMAIN\USER or user@ou.domain.com.
  - You want to send user passwords as protected (that is, not as clear text). Entering a value for the DN field sends passwords as clear text.

  Note: If you choose to enter a value for the DN field, it is your responsibility to establish a secure connection between the Cisco Unified MeetingPlace web server and the LDAP server. This is not the same as configuring SSL configuration on the web server. The SSL feature in Cisco Unified MeetingPlace protects traffic between the client and web server. You will require a secure connection between the web server and the LDAP server.
- Consult your LDAP expert for your DN information.

9. Select how you want user names transformed for "Username Conversion Function."
   Selecting None applies no transformation to the original user ID string.
10. Select one of the following for "Step 2: Login Method":
    - Select **Web Page Form** to see an HTML-based Cisco Unified MeetingPlace sign-in window.
    - Select **HTTP Basic Authentication** to see a sign-in window rendered by your web browser.
11. Select **Submit** and wait five minutes for the new configuration to take effect.

What to Do Next

Based on your configuration, proceed to one of the following topics:

- Verifying LDAP Then MeetingPlace Authentication for the Web Server by Using the Web Page Form
- Verifying LDAP Then MeetingPlace Authentication for the Web Server by Using the HTTP Form

Verifying LDAP Then MeetingPlace Authentication for the Web Server by Using the Web Page Form

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

Before You Begin

Complete the Configuring the LDAP Then MeetingPlace Authentication for the Web Server.

Procedure

1. Open a web browser and navigate to Cisco Unified MeetingPlace.
2. Verify the following end-user behaviors:
    - You can sign in with your LDAP password.
    - You cannot sign in without a password.
    - If you have a Cisco Unified MeetingPlace profile, you can sign in and schedule meetings.
    - If you do not have a Cisco Unified MeetingPlace profile, you can only attend and search public meetings.

Related Topics

- How to Resolve Authentication Problems in the Troubleshooting the Cisco Unified MeetingPlace Web Server module.

Verifying LDAP Then MeetingPlace Authentication for the Web Server by Using the HTTP Form

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

Before You Begin

Complete the Configuring the LDAP Then MeetingPlace Authentication for the Web Server.

Procedure

1. Open a web browser and navigate to Cisco Unified MeetingPlace.
2. Verify the following end-user behaviors:
    - You can sign in with your LDAP password.
    - You cannot sign in without a password.
    - If you have a Cisco Unified MeetingPlace profile, you can sign in and schedule meetings.
    - This option does not allow you to sign in to Cisco Unified MeetingPlace as a guest, that is, without a Cisco Unified MeetingPlace profile.

Related Topics

- How to Resolve Authentication Problems in the Troubleshooting the Cisco Unified MeetingPlace Web Server module.

How to Configure Trust External Authentication for the Web Server

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 sign-in 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: Users cannot sign in to Cisco Unified MeetingPlace as guests after you have configured this authentication mode.

- Terms for Single Sign On Software Integration with the Web Server
- Terms of Support for Single Sign On Software Integration with the Web Server
- Restrictions for Configuring Trust External Authentication for the Web Server
- Configuring Trust External Authentication for the Web Server
- Verifying Trust External Authentication for the Web Server

Terms for Single Sign On Software Integration with the Web Server

Customer Premise Equipment (CPE) customers who implement SSO software integrations on their Cisco Unified MeetingPlace Web Servers do so at their own risk and are responsible for understanding the technical implementations and feasibility of SSO integrations on their systems.

By allowing SSO software integrations, we do not claim support for any SSO software packages or vendors.

Using SSO software integrations requires proper configuration of the Cisco Unified MeetingPlace Web Server software through the Web Administration pages. If your SSO software integration requires a change in the Cisco Unified MeetingPlace Web Server software product source code, your SSO integration becomes an SSO customization, and we do not support customizations by either customers or any other parties.

Any CPE customers who want to integrate SSO packages can contact Cisco Managed Services to obtain a Service Request to implement SSO. This service is offered as a convenience and does not change the scope of the SSO integration: this service is an integration and configuration of the Web Server software, not a customization of the product code.

Customers must first implement SSO software integrations on test or lab servers and verify that the integrated systems work, including the Cisco Unified MeetingPlace scheduling and joining operations.

Customers are responsible for ensuring stability of SSO-integrated Web Servers, including communicating with SSO software vendors for the following reasons:

- To obtain necessary fixes and support
- To troubleshoot functional problems and technical problems, including crashes triggered by the SSO package

Many SSO software products include a web-server extension, called the IIS ISAPI extension or filter. The Cisco Unified MeetingPlace Web Server software installs and uses four IIS extensions. Any incompatibility between an SSO software extension and the Web Server software extensions can make IIS non-functional or unstable. Any crash of the SSO IIS extension can cause IIS to crash and can generate a full Web Server outage, resulting in a full system restart and disconnection of users from the Cisco Unified MeetingPlace web user portal. Any memory leak in the SSO package or module can make IIS or the whole server unstable, as well.

Although SSO software integration is productized for the Cisco Unified MeetingPlace Web Server software, any changes in overall configuration, including Cisco Unified MeetingPlace upgrades and SSO package upgrades, can potentially break SSO-integrated Cisco Unified MeetingPlace systems.

Terms of Support for Single Sign On Software Integration with the Web Server

Customers must inform Cisco TAC that their Cisco Unified MeetingPlace Web Servers have third-party SSO packages installed and configured when opening a service request for Cisco Unified MeetingPlace, Cisco Unified MeetingPlace for Microsoft Outlook, or Cisco Unified MeetingPlace for IBM Lotus Notes.

Customers must be able to provide SSO integration details upon request. Inability to provide details can result in Cisco TAC not being able to proceed with service requests.

If a service request is about troubleshooting the SSO integration, Cisco TAC can review the logs and identify whether the problem is on the SSO side or the Cisco Unified MeetingPlace Web Server software side. If the problem is on the SSO side, information will be provided to customers, so they can further troubleshoot with their SSO vendors.

If the service request is about troubleshooting a Cisco Unified MeetingPlace problem that does not seem to be connected to the SSO integration, Cisco TAC will proceed per the normal support process. If TAC discovers that the SSO integration plays a role in the problem, information will be provided to customers, so they can further troubleshoot with their SSO vendors.

If Cisco TAC believes the problem is triggered by an SSO package, Cisco TAC can require customers to disable the SSO package to troubleshoot further.

Microsoft Debug Diagnostic tool, also called DebugDiag, may be required for troubleshooting IIS crashes and memory leaks to determine if these problems are produced by the SSO package.

Restrictions for Configuring Trust External Authentication for the Web Server

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

Related Topics

- How to Configure Trust External Authentication for the Web Server

Configuring Trust External Authentication for the Web Server

Before You Begin

- Read the Restrictions: User Authentication and Cluster Configuration.
- Read the Terms for Single Sign On Software Integration with the Web Server.
- Read the Terms of Support for Single Sign On Software Integration with the Web Server.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Web Server**.
4. Select the name of the Web Server that you want to configure in the "View" section of the page.
5. Scroll down to the Web Authentication section.
6. Select **Trust External Authentication** for "Step 1: Directory."
7. Enter an appropriate value for an external service for "HTTP Header Containing Username."
   Example: Enter HTTP_SM_USER for SiteMinder
8. Select how you want user names transformed for "Username Conversion Function."
   Selecting None applies no transformation to the original user ID string.
9. Select **Submit** and wait five minutes for the new configuration to take effect.

What to Do Next

(Optional) Proceed to the Verifying Trust External Authentication for the Web Server.

Verifying Trust External Authentication for the Web Server

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

Before You Begin

Complete the Configuring Trust External Authentication for the Web Server.

Procedure

1. Open your web browser and navigate to the Cisco Unified MeetingPlace 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 sign in with your SiteMinder password and schedule meetings.

How to Configure HTTP Basic Authentication (Domain) for the Web Server

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 sign-in window that is rendered by their web browser.
2. Users enter valid domain user IDs and passwords.
   Cisco Unified MeetingPlace profile PINs are ignored and not used in the authentication operation.
3. If the Web Servers accept the sign-in credentials and the user IDs also exist in Cisco Unified MeetingPlace profile databases, users are signed in automatically to Cisco Unified MeetingPlace and are granted access to the Cisco Unified MeetingPlace home page.

Note: The Cisco Unified MeetingPlace profile user ID 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 Base 64-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.

Configuring HTTP Basic Authentication (Domain) for the Web Server

Before You Begin

Read the Restrictions: User Authentication and Cluster Configuration.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Web Server**.
4. Select the name of the Web Server that you want to configure in the "View" section of the page.
5. Scroll down to the Web Authentication section.
6. Select **HTTP Basic Authentication (Domain)** for "Step 1: Directory."
   "Step 2: Login Method" is automatically set to HTTP Basic Authentication and cannot be changed.
7. Enter your "Default Logon Domain."
8. Select how you want user names transformed for "Username Conversion Function."
   Selecting None applies no transformation to the original user ID string.
9. Select **Submit** and wait five minutes for the new configuration to take effect.

What to Do Next

(Optional) Proceed to the Verifying HTTP Basic Authentication (Domain) for the Web Server.

Verifying HTTP Basic Authentication (Domain) for the Web Server

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

Before You Begin

Complete the Configuring HTTP Basic Authentication (Domain) for the Web Server.

Procedure

1. Open a web browser and navigate to Cisco Unified MeetingPlace.
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 Cisco Unified MeetingPlace when you enter your domain user ID and password.
   - If you have a Cisco Unified MeetingPlace profile, your name displays on the Welcome page as firstname, lastname and the Sign In link no longer displays.
   - You can only sign 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.

How to Configure Windows Integrated Authentication for the Web Server

- Windows Integrated Authentication

- Sign-In Behavior with Windows Integrated Authentication
- Configuring Windows Integrated Authentication for the Web Server
- Verifying Windows Integrated Authentication for the Web Server
- Configuring SiteMinder for Use With the Cisco Unified MeetingPlace Web Server Software

Windows Integrated Authentication

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, the browser prompts users to enter their user IDs and passwords. The Windows sign-in credentials are encrypted before being passed from the client to the Web Server.

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

Windows Integrated Authentication (WIA) is secure, but has the following limitations:

- Only Microsoft Internet Explorer versions 4.0 and later 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.
- WIA does not work on Web Servers with SSL enabled.

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.

Refer to Microsoft online documentation to further ensure or verify that your network supports WIA.

Related Topics

- How to Configure Secure Sockets Layer for the Web Server in the Configuring Security Features for the Cisco Unified MeetingPlace Web Server module

Sign-In Behavior with Windows Integrated Authentication

When WIA Works Properly:

- Users sign 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 signed in to Cisco Unified MeetingPlace and granted access to the home page. Cisco

Unified MeetingPlace user passwords are ignored and not used in the SSO operation.

The home page does not have Sign In links to the HTML-based sign-in form because users are already signed in through the SSO process.

- If their NT account user IDs do not match any user IDs in the Cisco Unified MeetingPlace directory, users see the Cisco Unified MeetingPlace home page, but with Sign In links to the HTML-based sign-in form. Users must then enter valid Cisco Unified MeetingPlace user IDs and passwords.
- (System administrators only) If a user selects Sign Out from the Cisco Unified MeetingPlace Web Administration, then the user is signed out and returns to the home page. To sign back in, the user may select Sign In and enter the valid Cisco Unified MeetingPlace user ID and password.

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 sign-in credentials.

Note: Cisco Unified MeetingPlace user IDs are not case-sensitive.

Related Topics

- Read the Terms for Single Sign On Software Integration with the Web Server.
- Read the Terms of Support for Single Sign On Software Integration with the Web Server.

Configuring Windows Integrated Authentication for the Web Server

Before You Begin

Read the Restrictions: User Authentication and Cluster Configuration.

Restrictions

- Each user must have an account (local or Active Directory) on the Windows NT server and must also have a Cisco Unified MeetingPlace profile user ID that matches the account name.
- Users must be using Microsoft Internet Explorer version 4.0 or later.
- WIA works only under the browser Intranet Zone connections. By default, only pages without any dots in the URL are considered to be in the Intranet Zone.
- WIA does not work across proxy servers or other firewall applications.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Web Server**.
4. Select the name of the Web Server that you want to configure in the "View" section of the page.
5. Scroll down to the Web Authentication section.
6. Select **Windows Integrated Authentication** for "Step 1: Directory."
   "Step 2: Login Method" is automatically set to HTTP Basic Authentication and cannot be changed.
7. Select how you want user names transformed for "Username Conversion Function."
   Selecting None applies no transformation to the original user ID string.
8. Select **Submit** and wait five minutes for the new configuration to take effect.

What to Do Next

(Optional) Proceed to the Verifying Windows Integrated Authentication for the Web Server.

Verifying Windows Integrated Authentication for the Web Server

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

Before You Begin

Complete the Configuring Windows Integrated Authentication for the Web Server.

Procedure

1. Open a web browser and navigate to Cisco Unified MeetingPlace.
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 sign 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 sign-in information even if you sign in by using your domain Windows account.

See How to Resolve Authentication Problems in the Troubleshooting the Cisco Unified MeetingPlace Web Server module for a workaround to this problem.

See Setting Your Web Server Options in the Quick Start Configuration for Cisco Unified MeetingPlace Web User Portal for Scheduling and Joining Meetings module for information about configuring your Web Server Home Page hostname.

Configuring SiteMinder for Use With the Cisco Unified MeetingPlace Web Server Software

If your deployment includes the SiteMinder application for authentication and single-sign on support, you will need to make the following changes to the SiteMinder configuration so that it can interoperate properly with the Cisco Unified MeetingPlace Web Server software.

String Blocking in URLs

SiteMinder looks for invalid strings in all URLs before processing. The Web Server software uses internal URLs that include the "." character (period), which is blocked by the default SiteMinder configuration. The default block is:

badurlchars="./, /., /*, *., ~, \, %00-%1f,%7f-%ff"

In order for the Web Server software to function properly, remove /. from the badurlchars string, for example:

badurlchars="./, /*, *., ~, \, %00-%1f,%7f-%ff"

Localhost Redirection and Hostname Blocking in URLs

The Web Server software uses internal URLs that include connecting to the localhost/loopback on port 8002, for example, http://localhost:8002. When SiteMinder receives a localhost request, it resolves localhost to the actual host name of the server. SiteMinder then looks up the host name in its list of hosts and matches it to the name of an agent. In order for the Web Server software to function properly, you must add this agent name to the exception list so that it is not blocked by SiteMinder.

The following example shows the SiteMinder logging for a localhost request on port 8002:

```
[5812/7912][Tue Apr 24 14:00:07
2007][..\..\..\CSmHttpPlugin.cpp:219][INFO:2] PLUGIN: Read HTTP_HOST
value 'localhost:8002'.

[5812/7912][Tue Apr 24 14:00:07
2007][..\..\..\CSmHttpPlugin.cpp:270][INFO:2] PLUGIN: ProcessResource -
Resolved Host 'YOURHOSTNAME:8002'.

[5812/7912][Tue Apr 24 14:00:40
2007][..\..\..\CSmHttpPlugin.cpp:290][INFO:1] PLUGIN: ProcessResource -
Resolved Agentname 'yourhostname-unprotected' for HTTP_HOST
'YOURHOSTNAME:8002'.
```

In the first line, SiteMinder processes the request to localhost on port 8002. In the second line, localhost is resolved to the actual hostname of the computer (in this example, YOURHOSTNAME). In the third line, YOURHOSTNAME:8002 is resolved to the agent defined in your SiteMinder configuration as yourhostname-unprotected. It is this agent name that must be allowed (not blocked) by SiteMinder in order for the request to succeed.

Accessing Cisco Unified MeetingPlace Web When Locked-Out Due to Incorrect User Authentication Setup

If you configure the Web Server to use anything other than the MeetingPlace native sign-in form for user authentication, you may not be able to sign in to Cisco Unified MeetingPlace through the web due to incomplete user authentication configuration. For example, you configured LDAP, then MeetingPlace user authentication, but failed to enter a valid LDAP hostname or to ensure that the LDAP user IDs existed in MeetingPlace. In such circumstances, you are unable to sign in to the Cisco Unified MeetingPlace web user portal, and therefore you cannot use the Web Administration to correct your configuration errors.

To restore access to the Cisco Unified MeetingPlace web user portal, you can do one of the following:

- Sign in to the Cisco Unified MeetingPlace Web Server, open a web browser, and browse to http://localhost:8002. You will be signed in using the *admin* profile and can access the Web Administration to fix the problem.
- Edit the SQL database and reset the mode to MeetingPlace native sign-in form.

The following procedure describes how to update the Cisco Unified MeetingPlace Web Server user authentication mode in SQL Server.

Procedure

1. Open a DOS command window.
2. Sign in to the SQL server by entering **C:\osql -U** *userid* **-P** *password*, replacing *userid* and *password* with the appropriate value.
3. Specify that you want to access the MPWEB database.

1. Enter **use mpweb**.
2. Enter **go**.

4. Enter **Update web set AuthMode = 1.**
5. Enter **Update web set AuthLoginMode = 1**.
6. Enter **go**.

The following tables provide mode definitions as a reference.

AUTHMODE Command	Value
#define SQLCONFIG_AUTHMODE_NONE	0
#define SQLCONFIG_AUTHMODE_MP	1
#define SQLCONFIG_AUTHMODE_LDAP	2
#define SQLCONFIG_AUTHMODE_LDAPMP	3
#define SQLCONFIG_AUTHMODE_TRUSTEXT	4
#define SQLCONFIG_AUTHMODE_BASIC_DOMAIN	5
#define SQLCONFIG_AUTHMODE_WIA	6

AUTHMODE Command	Value
#define SQLCONFIG_AUTHLOGINMODE_NONE	0
#define SQLCONFIG_AUTHLOGINMODE_WEB	1
#define SQLCONFIG_AUTHLOGINMODE_HTTP	2