The following sections describe particular terms of agreement that you should be aware of when configuring or using this product.

See the following sections:

- Configuration Restrictions
- Cisco Policy for Use of Third-Party Software
- Terms for Single Sign On Software Integration
- Terms of Support for Single Sign On Software Integration

## Contents

- 1 Configuration Restrictions
- 2 Cisco Policy for Use of Third-Party Software
- 3 Terms for Single Sign On Software Integration
- 4 Terms of Support for Single Sign On Software Integration

## Configuration Restrictions

Cisco Unified MeetingPlace Web Conferencing deployments that are customized beyond the built-in configuration capabilities of the product, or beyond the documented configuration settings, procedures, or instructions, are not supported by Cisco Systems.

Examples of such customizations include, but are not limited to, the following: modifying web page templates, changing HTML or Javscript code, changing IIS running parameters or applying custom ASP pages or ISAPI filters, modifying SQL server configuration or authentication method, and modifying Windows OS security through IPSec policies and NTFS ACL.

## Cisco Policy for Use of Third-Party Software

The Cisco Unified MeetingPlace Web Conferencing documentation describes the system, end user, and other requirements for the use of the Web Conferencing software. Failure to meet these requirements or the introduction of unsupported third-party products may interfere with the operation of the Web Conferencing software, and may affect Cisco support for the Web Conferencing product.

## Terms for Single Sign On Software Integration

- 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.
- SSO software integrations require proper configuration of Cisco Unified MeetingPlace Web Conferencing systems through the Admin pages. If your SSO software integration requires a change in the Web Conferencing product source code, your SSO integration becomes an SSO customization, and we do not support customizations by either customers or any other parties.
- 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 Conferencing product, 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 Web Conferencing features and operations.
- Customers are responsible for ensuring stability of integrated Web Conferencing-SSO systems, 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
- SSO software often includes a web-server extension, called the IIS ISAPI extension or filter. Web Conferencing installs and uses four IIS extensions. Any incompatibility between an SSO software extension and the Web Conferencing 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 Conferencing outage, resulting in a full system restart, ending of in-progress meetings, and disconnecting of Web Conferencing users. 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 Web Conferencing system, any changes in overall configuration, including Web Conferencing upgrades and SSO package upgrades, can potentially break integrated Web Conferencing-SSO systems.

## Terms of Support for Single Sign On Software Integration

- Customers must inform Cisco TAC that their Cisco Unified MeetingPlace Web Conferencing servers have third-party SSO packages installed and configured with Web Conferencing when opening a service request for Web Conferencing, Cisco Unified MeetingPlace for Outlook, or Cisco Unified MeetingPlace for 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 if the problem is on the SSO side or the Web Conferencing 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 Web Conferencing 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.