

Configuração SSO para o sistema do Cisco Unified MeetingPlace Web Conferencing

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar a autenticação SSO no server das Conferências web](#)

[Instruções passo a passo](#)

[Pesquise defeitos o processo de autenticação SSO](#)

[Instruções passo a passo](#)

[Informações Relacionadas](#)

[Introdução](#)

Para a segurança aumentada, você pode configurar o único sinal na autenticação (SSO) para o Cisco Unified MeetingPlace Web Conferencing. A autenticação SSO usa um certificado para autenticar clientes.

Este documento descreve o processo para configurar e pesquisar defeitos a autenticação SSO para o Cisco Unified MeetingPlace Web Conferencing.

[Pré-requisitos](#)

[Requisitos](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Você instalou e a liberação configurada 5.4 do Cisco Unified MeetingPlace Web Conferencing.
- Você estabeleceu uma conexão federada ao server da federação de Cisco.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre

convenções de documentos.

[Configurar a autenticação SSO no server das Conferências web](#)

Este procedimento fornece instruções para configurar a autenticação SSO no server do Cisco Unified MeetingPlace Web Conferencing.

[Instruções passo a passo](#)

Conclua estes passos:

1. No menu iniciar do Windows, clique a **corrida**.
2. Na caixa de diálogo da corrida, no campo abrir, incorpore o **regedit**.
3. No indicador do editor de registro, consulte a esta
chave: `HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\MeetingPlace WebPublisher\Authenticators\SSOAuth`
4. No menu da edição, clique **novo > valor de série**.
5. No campo de nome, entre em **VerificationURL**.
6. Clicar com o botão direito o valor de série e o clique **altera**.
7. Na caixa de diálogo da corda da edição, no campo de dados do valor, incorpore o **file> do server gateway>/<authorization do <federation de http://** e clique a **APROVAÇÃO**.
8. Retire o editor de registro.
9. Em seu campo de endereço do navegador, incorpore a URL de seu server das Conferências web e pressione-a **entram**.
10. No Home Page das Conferências web, use seu Gerente-nível ID do sistema e senha a fim assinar dentro, a seguir clique-os **assinam dentro agora**.
11. Na página de boas-vindas, clique o **Admin**.
12. Na página de administração, clique o **servidor de Web**.
13. Na página do servidor de Web, na seção da vista, clique seu server.
14. Na seção da edição, confirme que a caixa de verificação da **autenticação do servidor de Web da confiança** está verificada.
15. Se você mudou o ajuste, o clique **submete-se**.

[Pesquise defeitos o processo de autenticação SSO](#)

Este procedimento ajuda-o a diagnosticar problemas com autenticação SSO.

[Instruções passo a passo](#)

Conclua estes passos:

1. Termine estes substeps a fim testar o comportamento das Conferências web: Em seu campo de endereço do navegador, incorpore o **gateway> das Conferências do <Web de http://** e pressione-o **entram**. Use suas credenciais do help desk a fim entrar às Conferências web. Se você pode entrar normalmente e as Conferências web funcionam normalmente, o problema é com o processo de autenticação SSO. Tac Cisco do contato.
2. Termine estas etapas a fim testar a resposta de servidor de PingFederate: Em seu campo de endereço do navegador, incorpore o **gateway> do server do <federation de http://** e

pressione-o **entram**. Se a página de login de PingFederate é indicada, o server de PingFederate é executado corretamente sobre a porta padrão. Em seu campo de endereço do navegador, incorpore o **gateway> do server do <federation de https://** e pressione-o **entram**. Se a página de login de PingFederate é indicada, o server de PingFederate é executado corretamente sobre a porta padrão sobre o SSL.

3. Termine esta etapa a fim de testar a resposta do servidor SQL: Em seu campo de endereço do navegador, incorpore o **file> do server gateway>/<authorization do <federation de http://? a=a&b=b**. Se uma página em branco se publica com o “falso” nela, a conexão ao server da federação está obstruída. Tac Cisco do contato. Se alguma outra página ou texto se publicam, a conexão ao server da federação é bem sucedida.

[Informações Relacionadas](#)

- [Páginas de suporte do Cisco Unified MeetingPlace](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)