



Guia de Administração do Cisco WebEx Meetings Server Versão 2.5

Primeira publicação: 30 de Julho de 2014

Última modificação: 14 de Outubro de 2014

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



1

CAPÍTULO

Visão geral do sistema

- Informações sobre o licenciamento de produtos, página 1
- Sobre a documentação do produto, página 1
- Termos, página 2

Informações sobre o licenciamento de produtos

Links de informações de licenciamento para este produto:

- <http://www.webex.com/license.html>
- http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
- <http://www.webex.com/CiscoWebExMeetingsServerSEULA.html>

Sobre a documentação do produto

Os Guias do Cisco WebEx Meetings Server fornecem procedimentos detalhados de planejamento, implantação e gerenciamento do seu sistema:

Estes incluem instalação e listas de verificação de rede, para que você possa coletar informações e tomar decisões antes da implantação real.

Além disso, cobrimos procedimentos de alteração do sistema, pós-implantação, tais como:

- Adicionar um sistema de Alta Disponibilidade (HA)
- Expandir seu sistema para um tamanho de sistema maior
- Atualizar ou modernizar o sistema para a versão mais recente

O guia administrativo do Cisco WebEx Meetings Server descreve como usar os recursos disponíveis para você no site da Administração e inclui as seguintes seções:

- Painel — o painel exibe o monitor do seu sistema e inclui links nas suas configurações de alarme, página **Tendências de Reunião**, página **Histórico de Recursos**, páginas do sistema e páginas de configurações. Consulte [Sobre o Seu Painel](#) para obter mais informações.

- Gerenciamento do Usuário: Adicionar, importar, ativar e reativar os usuários, configurar os códigos de monitoramento e enviar e-mail aos usuários no seu sistema com estes recursos. Consulte [Gerenciando Usuários, na página 111](#) para obter mais informações.
- Sistema: Configure as propriedades do sistema, URLs do site e site de administração, servidores, configurações SNMP e licenças com estes recursos. Consulte [Configurando Seu Sistema, na página 135](#) para obter mais informações.
- Definições: Configure as suas definições incluindo informações da empresa, recursos de marca, definições de reunião, áudio, vídeo, mobilidade, qualidade de serviço, senhas, definições de e-mail, downloads e definições de segurança com estes recursos. Consulte [Definindo as Configurações, na página 161](#) para obter mais informações.
- Gerenciamento de relatório: Configura e visualiza seus relatórios mensais. Consulte [Gerenciando relatórios, na página 237](#) para obter mais informações.
- Informações e acesso ao suporte: Abra e visualize os casos de suporte, configure recursos de depuração e realize testes de sistema e reunião, usando estes recursos. Consulte [Usando os Recursos de Suporte, na página 265](#) para obter mais informações.

Termos

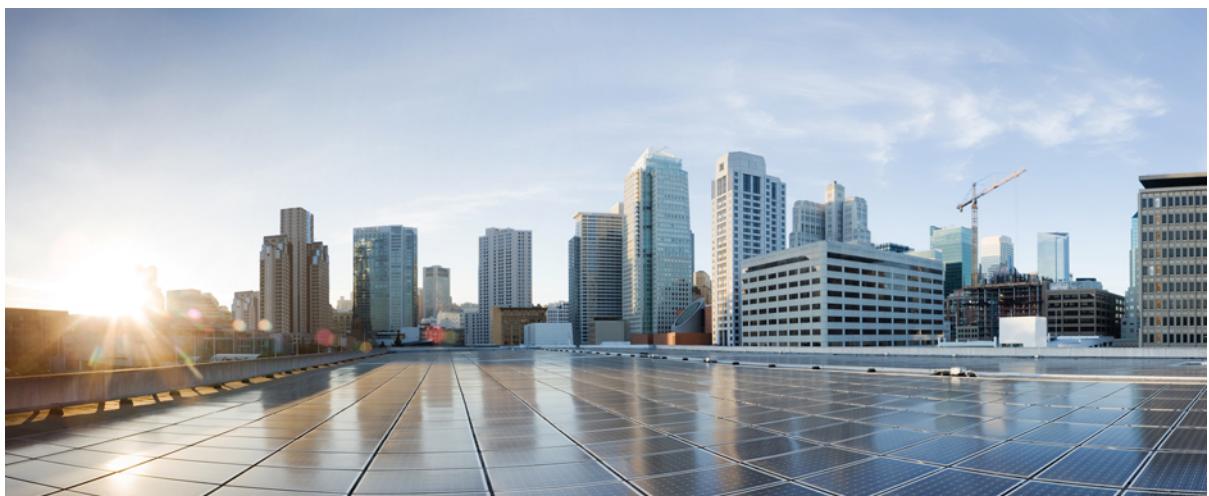
Os termos usados para descrever este produto.

Centro de dados — O hardware físico, que inclui, pelo menos, um dispositivo que contém uma instância de um sistema.

Alta disponibilidade — Um sistema redundante que existe localmente em paralelo com o sistema primário. Se o sistema principal falhar, o sistema de alta disponibilidade substitui a funcionalidade que falhou e um alerta é enviado. O failover é transparente para os usuários.

Servidor — Uma única instância do Cisco WebEx Server. Vários centros de dados podem ser unidos e funcionar como um único sistema.

Sistema — A aplicação do sistema do Cisco WebEx Server que inclui um ou mais centros de dados físicos.



PARTE

Guia de Implantação do Cisco WebEx Meetings Server

- [Usando o VMware vSphere com seu sistema, página 5](#)
- [Implantando um sistema automaticamente, página 11](#)
- [Implantando um sistema manualmente, página 31](#)
- [Configurando o Seu Servidor de E-mail, Fuso Horário e Local, página 49](#)
- [Alterando o sistema após a implantação, página 55](#)
- [Adicionar um Sistema de Alta Disponibilidade, página 57](#)
- [Expandindo o seu Sistema para Tamanho de Sistema Maior, página 63](#)
- [Atualizando o Sistema, página 69](#)
- [Atualizando o Sistema, página 77](#)
- [Testando o Sistema, página 85](#)



CAPÍTULO 2

Usando o VMware vSphere com seu sistema

- Usando VMware vSphere, página 5
- Configurando o Organizador ESXi para Usar um Servidor NTP., página 6
- Criando um Backup Usando o VMware vCenter, página 6
- Tirando uma Foto Instantânea utilizando o VMware vCenter, página 7
- Anexando um Arquivo VMDK Existente para uma Nova Máquina Virtual, página 8

Usando VMware vSphere

As máquinas virtuais para o seu sistema são implantadas com o VMware vSphere. O Cisco WebEx Meetings Server deve ser instalado em máquinas virtuais VMware, sujeito às seguintes restrições:

- Use o VMware vSphere 5.0, 5.0 Update 1, 5.0 Update 2, 5.1, 5.1 Update 1 ou 5.5.
Versões anteriores do vSphere não são suportadas.
- Use o VMware ESXi 5.0, 5.0 Update 1, 5.0 Update 2, 5.1, 5.1 Update 1 ou 5.5.
O uso de versões ESXi anteriores resulta em mensagens de erro confusas sobre o **hardware não suportado** que não listam explicitamente o problema.
- Verifique se o servidor DNS configurado no organizador ESXi pode resolver os nomes dos organizadores das máquinas virtuais que são implantadas no organizador ESXi.
- Você deve usar o VMware vCenter para gerenciar os organizadores ESXi no qual o sistema Cisco WebEx Meetings Server é implantado.
- Ao desligar uma máquina virtual, sempre selecione **Ligar > Desligar visitante** para cada máquina virtual. (Não use a opção **Desligar**.)



Observação

Para detalhes sobre as configurações VMware suportadas, consulte os *Requisitos do sistema e guia de planejamento do Cisco WebEx Meetings Server*.

Configurando o Organizador ESXi para Usar um Servidor NTP.

Configure o organizador ESXi para usar o Network Time Protocol (NTP) para a sincronização do relógio do dispositivo e verifique se os servidores NTP são acessíveis. Em um ambiente com vários centros de dados, a sincronização dos relógios dos centros de dados é fundamental para manter o compartilhamento de dados entre os centros de dados. Para instruções detalhadas, consulte a documentação VMware ESXi.

Etapa 1 Usando o cliente vSphere, selecione o organizador ESXi na painel de inventário.

Etapa 2 Selecione **Configuração > Configuração de horário** na seção Software.

Etapa 3 Selecione **Propriedades**.

Etapa 4 Selecione **Cliente NTP Habilitado**.

Etapa 5 Selecione **Opções** para definir as configurações do servidor NTP.

Recomendamos que você selecione **Iniciar e parar com organizador** para diminuir a possibilidade do tempo do organizador ESXi se tornar errado.

Criando um Backup Usando o VMware vCenter

Os backups são sistemas de arquivos tradicionais, que aproveitam a tecnologia VMware e SAN-baseados na transferência de dados. A Recuperação de Dados VMware® cria backups de máquinas virtuais sem interromper a sua utilização ou os dados e serviços que providenciam. A Recuperação de Dados utiliza uma aplicação de máquina virtual e um plug-in de cliente para gerenciar e restaurar backups. O dispositivo de backup é fornecido em formato de virtualização aberta (OVF). O plug-in de Recuperação de Dados requer o Cliente VMware vSphere.

A Recuperação de Dados administra backups existentes, removendo os backups à medida que se tornam mais velhos. Ela também suporta a deduplicação para remover dados redundantes. Antes de fazer qualquer procedimento de alteração no sistema, recomendamos que você crie um backup de cada uma das máquinas virtuais usando o VMware Data Recovery (disponível no VMware vSphere versão 5.0) ou vSphere Data Protection (disponível em vSphere versão 5.1). (VMware Data Recovery/vSphere Data Protection estão incluídos no VMware vSphere, exceto no vSphere Essentials Kit. Consulte http://www.vmware.com/pdf/vdr_11_admin.pdf para obter mais informações.)

Os backups também podem ser criados usando um servidor de armazenamento. Consulte [Configurando um Servidor de Armazenamento, na página 146](#) para obter mais informações.

As *fotos instantâneas* de máquinas virtuais são uma "fotografia" do seu sistema em um ponto específico no tempo e não são as mesmas que os backups. Por motivos de desempenho, certifique-se de usar backups da sua máquina virtual e mantê-los em um local de armazenamento que seja diferente das unidades físicas contendo suas máquinas virtuais. Para obter mais informações sobre fotos instantâneas e problemas de desempenho conhecidos, consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).

Etapa 1 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#))

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

- Etapa 2** Siga as instruções da documentação do VMware vSphere e use o VMware Data Recovery (chamado VMware vSphere Data Protection a partir da versão vSphere 5.1) para criar um backup do sistema e de cada uma das máquinas virtuais. Para detalhes completos sobre este backup, consulte o *Guia de Administração do VMware Data Recovery* ou o *Guia de Administração do vSphere Data Protection*.

Observação Recomendamos que você exclua os backups depois que o procedimento de alteração do sistema estiver completo, você tiver testado o sistema e esteja satisfeito com os resultados. A restauração de um centro de dados a partir de backups antigos ou fotos instantâneas pode causar um comportamento inesperado.

Tirando uma Foto Instantânea utilizando o VMware vCenter

Fotos instantâneas das máquinas virtuais são utilizadas para recuperar rapidamente uma máquina virtual depois de um procedimento de alteração do sistema. As fotos instantâneas são *fotografias* do seu sistema em um ponto específico no tempo e não são as mesmas que os backups (consulte [Criando um Backup Usando o VMware vCenter, na página 6](#)). Recomendamos que, além de tirar fotos instantâneas, você faça o backup do seu sistema.



Observação

Se o arquivo do disco da máquina virtual original é perdido, você não pode recuperar a máquina virtual com as fotos instantâneas.

As fotos instantâneas são armazenadas nas unidades físicas contendo as suas máquinas virtuais. Se você não excluir essas fotos instantâneas em tempo hábil, os usuários finais podem começar a experiência de áudio e vídeo degradada, devido a um problema conhecido que afeta o desempenho da máquina virtual. Portanto, recomendamos que você use backups e mantenha os backups das máquinas virtuais em um local de armazenamento que seja diferente das unidades físicas contendo suas máquinas virtuais. Além disso, as fotos instantâneas podem ser utilizadas para atualizações, mas para atualizações do sistema recomendamos que você exclua todos as fotos instantâneas e faça backup do sistema original antes de executar uma atualização.

Para mais informações sobre este conhecido problema com as fotos instantâneas VMware, acesse o site da VMware e leia o documento, *Melhores práticas para executar VMware vSphere no armazenamento anexado à Rede*. Você também pode procurar no VMware KnowledgeBase por **impacto no desempenho causado pela foto instantânea** para obter informações adicionais.

Antes de fazer a maioria dos procedimentos de alteração do sistema, recomendamos que você faça o backup do sistema (especialmente ao realizar uma atualização ou expansão) ou tire uma foto instantânea (ao executar uma atualização) de cada uma das máquinas virtuais. Você pode fazer backup do seu sistema utilizando o VMware Data Recovery (VMware vSphere Data Protection a partir do vSphere versão 5.1) ou tirar uma foto

instantânea de cada máquina virtual. (A Recuperação de Dados Vmware/Proteção de Dados vSphere está incluída com o VMware vSphere, exceto no kit vSphere Essentials.)

Certifique-se de ler a seção de preparação para o procedimento específico. Listamos considerações específicas para cada procedimento.



Lembrar

Se o seu sistema é composto por várias máquinas virtuais, selecione **Ligar > Desligar convidado** e tire uma foto instantânea de cada máquina virtual em seu sistema. Rotule a foto instantânea de cada máquina virtual com o mesmo prefixo, por exemplo, 20 de agosto, assim você sabe que essas fotos instantâneas foram feitas ao mesmo tempo.

Recomendamos que você mantenha as fotos instantâneas não mais do que 24 horas. Se você quiser mantê-las por mais tempo, recomendamos que você crie um backup. Para mais informações sobre o VMware Data Recovery (VMware vSphere Data Protection a partir da versão vSphere 5.1), consulte [Criando um Backup Usando o VMware vCenter](#), na página 6.

Etapa 1

Coloque o sistema em modo de manutenção. Para obter detalhes completos, consulte [Sobre o Modo de Manutenção](#), na página 107.

Certifique-se que não há reuniões ativas e que você selecionou um horário onde haverá um impacto mínimo aos seus usuários.

Etapa 2

No VMware vCenter, selecione **Ligar > Desligar convidado** para cada uma das máquinas virtuais.

Etapa 3

Selecione **Foto instantânea > Tirar foto instantânea** para cada máquina virtual.

Etapa 4

Digite um nome para a foto instantânea e selecione **OK**.

Próximos passos

- Conclua o procedimento e teste o seu sistema para confirmar que ele é bem sucedido.
- Se você precisar reverter para uma foto instantânea, certifique-se de que a foto instantânea para cada máquina virtual foi tirada ao mesmo tempo. Ligar um sistema com fotos instantâneas inadequadas pode resultar em corrupção do banco de dados.

Anexando um Arquivo VMDK Existente para uma Nova Máquina Virtual

Esta seção descreve como anexar um Disco de Máquina Virtual (VMDK) a partir de uma máquina virtual de administração existente para uma nova máquina virtual de administração usando VMware vCenter. Este procedimento é usado quando você expande ou atualiza seu sistema. (Nós reutilizamos os dados armazenados do sistema no disco rígido 4 da máquina virtual de administração).

**Cuidado**

Faça uma cópia do arquivo VMDK do disco rígido 4 e copie-o diretamente para a pasta da máquina virtual da máquina virtual de administração no sistema atualizado ou expandido. Se você simplesmente anexar o disco rígido 4, então, os dados ainda são armazenados na pasta da máquina virtual da máquina virtual de administração antiga. Se você excluir acidentalmente a máquina virtual de administração existente no inventário vCenter, o sistema atual irá perder o acesso ao disco rígido 4.

**Importante**

Certifique-se de copiar o arquivo VMDK base original para o disco rígido de 4, e não uma foto instantânea deste arquivo VMDK.

**Observação**

Se você estiver usando armazenamento Direct-attached (DAS), você deve migrar o VMDK para um número de unidade lógica (LUN) onde a nova máquina virtual de administração pode acessá-lo.

**Observação**

Referimo-nos à máquina virtual de Administração antes do procedimento de alteração do sistema como a máquina virtual de administração *atual*. A máquina virtual de Administração, após a expansão ou a atualização, é chamada de máquina virtual de Administração de *atualização*.

-
- Etapa 1** Navegue o inventário no Vmware vCenter e encontre a máquina virtual de Administração atual do seu sistema.
- Etapa 2** Clique com o botão direito no nome da máquina virtual e selecione **Editar Configurações...**.
A janela **Propriedades da Máquina Virtual** é exibida.
- Etapa 3** Selecione a guia **Hardware**, então selecione **Hard disk 4**.
- Etapa 4** Para referência futura, copie e cole em outro documento o local do **Arquivo em Disco**.
Isto especifica o local do VMDK no Vmware vCenter.
A sequência é semelhante a [EMC-LUN10-RAID5] webex-sysA-admin/webex-sysA-admin_3.vmdk. Se você já atualizou seu sistema, o nome do arquivo não segue a convenção de nomeação da máquina virtual existente.
- Etapa 5** Anote o local de armazenamento para o disco rígido 4 e o nome da pasta da máquina virtual.
A sequência do nome da pasta é semelhante a [EMC-LUN8-RAID5] webex-sysB-admin.
- Etapa 6** Feche a janela **Editar Configurações...** sem fazer nenhuma alteração.
- Etapa 7** Altere a visualização do vCenter em Datastore e em visualização de Cluster Datastore. Selecione **Visualizar > Inventário > Grupos de Datastores e Datastore**.
- Etapa 8** Selecione o local de armazenamento onde a sua máquina virtual de Administração existente está localizada (a partir do passo 5) e selecione **Procurar esse datastore**.
- Etapa 9** Selecione o local de armazenamento onde a máquina virtual de Administração recém implantada (para o sistema expandido ou atualizado) está localizada e selecione **Procurar esse datastore**.
- Etapa 10** Organize as duas janelas do navegador de armazenamento de dados (para a máquina virtual de Administração atual e expandida ou atualizada) lado a lado para que você possa ver ambas as pastas da máquina virtual de Administração.
- Etapa 11** Abra as duas pastas da máquina virtual e copie o VMDK da pasta da máquina virtual de Administração atual para a pasta da máquina virtual de Administração expandida ou atualizada.

- a) Na pasta da máquina virtual de administração atual, localize o VMDK que está associado com disco rígido 4. Consulte o local do arquivo que você anotou na Etapa 4 para confirmar a exatidão.
- b) Clique com o botão direito do mouse no arquivo e selecione **Copiar**.
- c) Clique com o botão direito do mouse dentro da pasta da máquina virtual de Administração expandida ou atualizada e selecione **Colar**. Quando a operação de colar for concluída, feche as janelas de datastore.
- d) Retorne a visualização do vCenter a uma lista de organizadores e clusters, selecionando **Visualizar > Inventário > Organizadores e Clusters**.

- Etapa 12** Navegue no inventário no VMware vCenter e encontre a máquina virtual de Administração expandida ou atualizada para seu sistema.
- Etapa 13** Clique com o botão direito do mouse no nome da máquina virtual expandida ou atualizada e selecione **Editar Configurações...**. A janela **Propriedades da Máquina Virtual** é exibida.
- Etapa 14** Selecione a guia **Hardware**, então selecione **Hard disk 4**.
- Etapa 15** Selecione **Remover**. Esta ação não remove a unidade virtual imediatamente. Em vez disso, a unidade virtual existente é agendada para remoção.
- Etapa 16** Selecione **Adicionar**. O assistente **Adicionar Hardware** é exibido.
- Etapa 17** Selecione **Hard Disk**, então **Próximo**.
- Etapa 18** Selecione **Usar um disco virtual existente**, então **Próximo**.
- Etapa 19** Selecione **Procurar** e navegue até o armazenamento de dados onde a máquina virtual de Administração expandida ou atualizada está localizada. Navegue até a pasta nova máquina virtual de Administração. Clique duas vezes nesta pasta, então selecione o disco virtual que você copiou no passo 11. Selecione **OK**.
- Etapa 20** Na lista suspensa **Nó do Dispositivo Virtual**, selecione **SCSI (0:3)**, em seguida selecione **Próximo**.
- Etapa 21** Reveja suas alterações, e se elas estiverem corretas, selecione **Terminar**. Caso contrário, selecione **Voltar** e corrija quaisquer erros. Quando o assistente for concluído, um novo disco marcado para adição na guia **Hardware** será exibido.
- Etapa 22** Comprometer as operações de Adicionar e Remover, selecionando **OK**.
- Etapa 23** Visualizar essa tarefa de reconfiguração da máquina virtual no Vmware vCenter no painel **Tarefas Recentes** para garantir que não há erros.



CAPÍTULO 3

Implantando um sistema automaticamente

- Conceitos gerais para implantação do sistema, página 11
- Checklist de Instalação, página 14
- As informações necessárias para uma Implantação Automática, página 15
- Implementando o arquivo OVA do cliente VMware vSphere, página 18
- Selecionando o Seu Idioma para Instalação, página 21
- Confirmando a Implantação, página 22
- Escolhendo Qual Sistema Instalar, página 22
- Escolhendo o tipo de implantação, página 22
- Fornecendo Credenciais Vmware vCenter, página 23
- Escolha as Configurações do vCenter para a sua Máquina Virtual de Mídia, página 24
- Inserindo informações de Rede para a Máquina Virtual de Mídia, página 24
- Adicionando o Acesso Público, página 24
- Inserindo o Endereço VIP Público, página 26
- Inserindo o Endereço VIP Privado, página 27
- URLs do Site WebEx e da Administração WebEx, página 27
- Confirmando que sua rede está configurada corretamente, página 29
- Implantação das máquinas virtuais, página 29
- Verificando o sistema, página 29

Conceitos gerais para implantação do sistema

Tamanhos do sistema

Os sistemas são identificados pelo número de usuários simultâneos suportados:

- 50 usuários simultâneos (também conhecido como sistema *micro*)

- Suporta normalmente uma empresa entre 500 e 1000 funcionários
- Sistema primário [sem Alta Disponibilidade {HA}] compreende uma máquina virtual de administração e um proxy reverso da internet opcional (para acesso público)
 - 250 usuários simultâneos (também conhecido como sistema *pequeno*)
 - Suporta normalmente uma empresa entre 2500 e 5000 funcionários
 - O sistema primário (sem HA) compreende uma máquina virtual de administração, uma máquina virtual de mídia e um proxy reverso da internet opcional (para acesso público)
 - 800 usuários simultâneos (também conhecido como sistema *médio*)
 - Suporta normalmente uma empresa entre 8000 e 16.000 funcionários
 - O sistema primário (sem HA) compreende uma máquina virtual de administração, uma máquina virtual de mídia e um proxy reverso da internet opcional (para acesso público)
 - 2000 usuários simultâneos (também conhecido como sistema *grande*)
 - Suporta normalmente uma empresa entre 20.000 e 40.000 funcionários
 - Sistema primário (sem HA) compreende uma máquina virtual de administração, três máquinas virtuais de mídia, duas máquinas web e um proxy reverso da internet opcional (para acesso público)

Termos usados durante a implantação

URL do site WebEx — uma URL http segura para que os usuários organizem e participem de reuniões em um ambiente de centro de dados único.

URL de administração WebEx — URL http segura para que os administradores configurem, monitorem e gerenciem o sistema em um ambiente de centro de dados único.

VIP público — endereço de IP virtual para a URL do site WebEx.

VIP privado — endereço de IP virtual para a URL do site de administração ou o endereço de IP virtual para a URL do site WebEx (para usuários internos apenas, se você tem um DNS split-horizon).

URL WebEx comum — usada pelo DNS para redirecionar o usuário ao centro de dados, onde o usuário executa tarefas relacionadas às reuniões, tais como agendamento ou organização de reuniões. Qual centro de dados DNS é transparente para o usuário. A URL WebEx comum é simplesmente uma localização conveniente para um usuário entrar no sistema. Se um centro de dados cair, nada muda para o usuário, incluindo a URL usada para acessar as reuniões, porque o DNS irá redirecionar o usuário para o centro de dados sobrevivendo.

URL de Administração Comum — é muitas vezes referida como simplesmente a *URL de Administração*. Ela é usada pelo DNS para redirecionar um administrador para o centro de dados de gerenciamento de onde o administrador faz logon no sistema. O centro de dados que o DNS escolhe é transparente para o administrador (no entanto, a sequência na barra da URL muda dependendo de qual centro de dados o administrador está usando para acessar o sistema). A URL de Administração Comum é simplesmente um alvo conveniente que um administrador usa para entrar no sistema.

URLs de Administração Locais — são específicas para cada centro de dados em um sistema com Vários centros de dados (MDC). Ao efetuar logon através da URL de Administração Comum, o DNS redireciona o administrador para a URL de Administração Local para o centro de dados de gerenciamento. Quaisquer modificações no sistema, tais como a atribuição de uma licença para um usuário, são realizadas no centro de dados de gerenciamento e replicadas para todos os centros de dados no sistema de MDC.

Um administrador pode escolher um centro de dados específico para modificar a partir do aplicativo CWMS, mas selecionar um outro centro de dados para modificar não altera a URL de Administração Local, porque o acesso do administrador para o sistema continua a ser o centro de dados escolhido pelo DNS quando o administrador efetua logon no sistema. As modificações do administrador para outro centro de dados no sistema de MDC passa pelo centro de dados de gerenciamento escolhido pelo DNS para o centro de dados de destino.

Um sistema de MDC terá um mínimo de duas URLs de Administração Locais, uma para cada centro de dados no sistema.

URLs locais que são específicas para cada centro de dados.

Informações do perfil do sistema

Completa este gráfico do seu sistema.

URL do site comum		
URL da administração comum		
Endereços de IP virtuais DC1 e DC2		
	Centro de dados 1	Centro de dados 2
URLs do site local		
URLs de administração local		
Endereços de IP virtuais públicos		
Endereço de IP virtuais privados		
Servidor DNS		
Endereço de IP da máquina virtual de administração		
Endereço de IP da máquina virtual de mídia 1		
Endereço de IP da máquina virtual de mídia 2		
Endereço de IP da máquina virtual de mídia 3		
Endereço de IP da máquina virtual da Web 1		
Endereço de IP da máquina virtual da Web 2		

Endereço de IP da máquina virtual DMZ (opcional)		
Endereço de e-mail do administrador CWMS		
Senha		
Remote Access ¹		
Senha		
Endereço de IP do Call Manager		
ID do administrador do Cisco Call Manager		
Senha do Cisco Call Manager		
Números de discagem de entrada CWMS		
Números de Telefone		

¹ As contas de acesso remoto não serão ativadas até a conta ser ativada.

Checklist de Instalação



Restrição

Você deve usar o VMware vCenter para gerenciar os organizadores ESXi no qual o sistema Cisco WebEx Meetings Server é implantado.

Alterações da Rede

Consulte o checklist de rede apropriado para a sua implantação. Considere o seguinte:

- Acesso público: se os usuários fora de seu firewall podem organizar e acessar reuniões a partir da Internet ou dispositivos móveis ou não.
A Cisco recomenda o acesso público, uma vez que resulta em uma melhor experiência de usuário para a sua equipe móvel.
- Tipo de configuração DNS em sua empresa: DNS split-horizon ou DNS sem split-horizon (configuração DNS mais comum). Para mais informações sobre a configuração DNS, consulte o *Guia de planejamento do Cisco WebEx Meetings Server*.
- Abra a porta 10200 a partir do desktop do administrador para a máquina virtual de Administração. A porta 10200 é usada pelo navegador durante a implantação.

Selecione a lista de verificação apropriada para sua implantação:

- Checklist de Rede para um Sistema com Acesso Público e DNS não Split-Horizon
- Checklist da Rede para um Sistema Com Acesso Não Público
- Checklist da Rede para um Sistema com Acesso Público e DNS Split-Horizon

Info. necessárias

As informações necessárias variam se você está fazendo uma implantação de sistemas automática (suportado por 50 usuários simultâneos, 250 usuários simultâneos e 800 usuários simultâneos) ou manual (com suporte para todos os tamanhos de sistemas). Recomendamos que você selecione uma implantação automática, a menos que você esteja implantando um sistema de 2000 usuários, que sempre exige uma implantação manual.

Selecione a lista de verificação apropriada para seu tipo de implantação:

- As informações necessárias para uma Implantação Automática, na página 15
- Informações necessárias para uma Implantação Manual, na página 35

As informações necessárias para uma Implantação Automática

Esta é a informação necessária para o seu sistema, em ordem.



Observação

Certifique-se de adicionar os FQDNs de máquinas virtuais, endereços IP, URLs de site WebEx e Administração e endereços VIP para seus servidores DNS antes de iniciar a implantação do sistema. Utilizamos esta informação para procurar endereços de IP para você durante a implantação.

Para evitar quaisquer problemas de DNS, você pode querer testar essas URLs e endereços de IP antes de iniciar a implantação do OVA. Caso contrário, a implantação do sistema irá falhar até que você corrija esses erros.

Nome do Campo	Descrição	Valor Para o Seu Sistema
URL vCenter	O endereço http seguro do servidor vCenter para as máquinas virtuais no seu sistema.	
Nome de usuário vCenter	O nome do usuário para implantar as máquinas virtuais em seu sistema. Este usuário deve ter privilégios de administrador: para implantar, configurar, ligar ou desligar, e excluir as máquinas virtuais.	
Senha vCenter	Senha do usuário vCenter.	
(apenas 250 e 800 usuários simultâneos do sistema)	Organizador ESXi para a máquina virtual de mídia.	
Organizador ESXi	Observação Este organizador ESXi deve estar no mesmo vCenter como a URL do vCenter acima.	

Nome do Campo	Descrição	Valor Para o Seu Sistema
(apenas 250 e 800 usuários simultâneos do sistema) Armazenamento de Dados	Armazenamento para a máquina virtual de mídia.	
(apenas 250 e 800 usuários simultâneos do sistema) Grupo de portas da Máquina Virtual	Grupo de porta para a máquina virtual de mídia. Observação A Cisco recomenda que você escolha o mesmo grupo de porta que você selecionou para a máquina de Administração virtual.	
(apenas 250 e 800 usuários simultâneos do sistema) FQDN para a máquina virtual de mídia	Nome de domínio totalmente qualificado (todos os caracteres minúsculos) para a máquina virtual de mídia.	
(apenas 250 e 800 usuários simultâneos do sistema) Endereço de IPv4 para a máquina virtual de mídia	Endereço de IPv4 para a máquina virtual de mídia. Vamos procurar automaticamente o endereço IPv4 correspondente para esta máquina virtual de mídia.	
(Apenas acesso público) Organizador ESXi	Organizador ESXi para a máquina virtual de Proxy Reverso da Internet. Observação A Cisco recomenda que você selecione um organizador ESXi diferente do qual você escolheu para a administração e outra máquina virtual interna. Para permitir o tráfego para o proxy reverso da internet, verifique se o organizador ESXi está configurado com um grupo de portas que pode rotear o VLAN cujo endereço IP é utilizado pelo proxy reverso da internet.	
(Apenas acesso público) Armazenamento de Dados	O armazenamento de dados da máquina virtual de Proxy Reverso da Internet.	

Nome do Campo	Descrição	Valor Para o Seu Sistema
(Apenas acesso público) Grupo de portas da Máquina Virtual	<p>O grupo de porta para a máquina virtual do Proxy Reverso de Internet.</p> <p>Observação Por razões de segurança, a Cisco recomenda que você selecione um grupo de porta diferente do qual você escolheu para máquina virtual de Administração.</p>	
(Apenas acesso público) FQDN para o Proxy Reverso da Internet	Nome de domínio totalmente qualificado (todos os caracteres minúsculos) para a máquina virtual de proxy reverso da internet.	
(Apenas acesso público) Endereço de IPv4 do Proxy Reverso da Internet	Endereço de IPv4 para a máquina virtual de Proxy Reverso da Internet. Vamos procurar automaticamente o endereço IPv4 correspondente para esta máquina virtual do Proxy Reverso de Internet.	
(Apenas acesso público) Entrada IPv4	Porta IPv4 para a máquina virtual de Proxy Reverso da Internet.	
(Apenas acesso público) Máscara de sub-rede do IPv4	Máscara de sub-rede para a máquina virtual de Proxy Reverso da Internet.	
(Apenas acesso público) Endereço de IPv4 do Servidor DNS Primário	Servidor DNS para a máquina virtual de Proxy Reverso da Internet.	
(Apenas acesso público) Endereço de IPv4 do Servidor DNS Secundário	Servidor DNS adicional para a máquina virtual de Proxy Reverso da Internet (Opcional).	
VIP público	Endereço de IP para a URL do site WebEx (os usuários do site acessam para organizar e participar de reuniões)	

Nome do Campo	Descrição	Valor Para o Seu Sistema
VIP privado	<ul style="list-style-type: none"> Endereço de IP para a URL do site de Administração (para que os administradores configurem, monitorem e gerenciem o sistema) Endereço de IP para a URL do site WebEx (apenas para usuários internos, se você tem um DNS split-horizon). 	
URL do Site WebEx	URL http segura (todos os caracteres minúsculos) para que os usuários organizem e participem de reuniões.	
URL da Administração WebEx	URL http segura (todos os caracteres minúsculos) para que os administradores configurem, monitorem e gerenciem o sistema.	

O que fazer a seguir

Com esta informação, iniciar a implantação do sistema, inserindo a URL de implantação em uma janela do navegador. (A URL de implantação é exibida na janela do console para a máquina virtual de Administração.)



Observação

Se o sistema for reiniciado antes que a configuração estiver concluída, uma nova senha é gerada e você deve usar a URL de implantação com a nova senha.

Implementando o arquivo OVA do cliente VMware vSphere

O modelo OVA cria dois NICs virtuais para cada máquina virtual. No entanto, apenas as máquinas virtuais de admin usam os dois NICs virtuais. Todas as outras máquinas virtuais do Cisco WebEx Meetings Server (CWMS), apenas um NIC virtual é usado e o outro é desligado.

Este procedimento é fornecido como uma orientação geral. As telas que você vê durante a implantação OVA depende das configurações do seu vCenter, do armazenamento e da rede e podem ser diferentes do que está descrito neste procedimento. Veja a sua documentação do Vmware vSphere para informações completas no assistente OVA.

Antes de iniciar

Obtenha o arquivo OVA do Servidor do Cisco WebEx Meetings para o seu sistema e coloque-o em um local que seja acessível do Vmware vSphere Use o cliente VMware vSphere para implantar a máquina virtual de Administração no seu sistema.

Você deve usar o VMware vCenter para gerenciar os organizadores ESXi no qual o sistema Cisco WebEx Meetings Server é implantado. Ao usar o cliente vSphere, inicie sessão no vCenter e implante o arquivo OVA na máquina virtual de Administração.

-
- Etapa 1** Inicie sessão no seu cliente VMware vSphere.
Certifique-se de iniciar sessão como um usuário que inclui privilégios de administrador: para implantar, configurar, ligar ou desligar, e excluir as máquinas virtuais.
- Etapa 2** Selecione **Arquivo > Implantar o modelo OVF...**
- Etapa 3** Selecione **Procurar** para navegar até o local do arquivo OVA. Selecione **Próximo**.
Você pode selecionar o link **Cisco WebEx Meetings Server** para ir para uma página da internet com informações detalhadas sobre este sistema.
- Etapa 4** Leia as Exigências de Licença do Usuário Final e selecione **Aceitar**, então selecione **Próximo**.
- Etapa 5** Navegue para e selecione o local, no inventário vCenter, onde você gostaria de colocar a máquina virtual de Administração.
- Etapa 6** Insira o nome da máquina virtual para o tamanho do sistema e selecione **Próximo**. Para obter mais informações sobre a seleção do tamanho correto para a sua empresa, consulte [Tamanhos do sistema, na página 11](#).
Você deve implantar a máquina virtual de Administração antes de implantar qualquer outra máquina virtual. Se você selecionar a implantação automática (recomendado), implantaremos as outras máquinas virtuais para você. Se você escolher a implantação manual (exigido para sistema de 2000 usuários simultâneos), então após a implantação da máquina virtual de Administração, você deve implantar as outras máquinas virtuais utilizando este mesmo assistente.
A Cisco recomenda que você inclua o tipo no nome da máquina virtual; por exemplo, "Admin" no nome da sua máquina virtual de Administração, para identificá-la facilmente no seu inventário do vCenter.
Todas as máquinas virtuais da internet para os seus sistemas devem estar na mesma sub-rede que a máquina virtual de Administração. (Dependendo do tamanho do sistema que você selecionar, você pode precisar de uma ou mais máquinas virtuais internas de web e mídia.)
- Etapa 7** A partir da lista suspensa, selecione a máquina virtual para o tamanho do seu sistema e selecione **Próximo**.
Certifique-se de implementar a máquina virtual de Administração antes de qualquer outra máquina virtual em seu sistema.
- Etapa 8** Navegue através do inventário vCenter e selecione o organizador ESXi ou cluster onde você deseja implantar as máquinas virtuais para o seu sistema. Selecione **Próximo**.
- Etapa 9** Se o cluster contém um conjunto de recursos, selecione o conjunto de recursos onde você deseja implantar o modelo OVA e selecione **Próximo**.
Os pools de recursos compartilham os recursos de CPU e memória ou trabalham com recursos do VMware, tais como DRS ou vMotion. Os pools de recursos devem ser dedicados a um único Organizador ESXi. Os pools de recursos VMware não são recomendados para uso com o Cisco WebEx Meetings Server.
- Etapa 10** Selecione o armazenamento de dados para a sua máquina virtual e o tipo de provisionamento para a sua máquina virtual. Você deve selecionar o **Thick Provisioning** e criar o máximo de espaço na unidade virtual necessário para o seu sistema. Com Thin Provisioning, o VMware aloca o espaço do sistema do arquivo em um *conforme necessário*, resultando em um desempenho ruim. O disco lazy zero é suficiente e o eager zero é aceitável, mas o disco eager zero levará mais tempo para ser concluído.
- Etapa 11** Configurar o mapeamento de rede. Para cada rede de origem, selecione uma rede de destino da lista suspensa na coluna **Destination Networks**. Selecione **Próximo**.
- Observação** Tanto a VM Network e a VIP Network devem ser mapeadas para o mesmo valor na coluna Destination Network. Você pode ignorar a mensagem de aviso sobre redes de múltiplas fontes mapeadas para a mesma rede do organizador.

Etapa 12 Insira as seguintes informações para a máquina virtual, então selecione **Próximo**:

- Nome do organizador da máquina virtual (não inclui o domínio aqui)
- Domínio para a máquina virtual
- Endereço de IPv4 (Eth0) da máquina virtual
- A máscara da sub-rede da máquina virtual
- Portão de endereço de IP
- O servidor DNS primário que contém entradas para o hostname e endereço de IP desta máquina virtual
- Servidor DNS secundário que contém entradas para o nome do organizador e o endereço de IP da máquina virtual
(Um sistema com apenas um servidor DNS configurado está em risco, porque cria um ponto único de falha.
Recomendamos que você configure um servidor DNS secundário para criar redundância de rede.)
- O idioma exibido durante o processo de instalação, seguindo a alimentação desta máquina virtual

Observação Para evitar problemas de DNS, você pode testar as URLs e endereços de IP antes de iniciar a implantação do OVA. A implantação falhará se houver erros.

Etapa 13 Confirme a informação que você inseriu. Se houver qualquer problema, selecione **Voltar** e altere os valores.

Etapa 14 Se você estiver atualizando um sistema manualmente, selecione **Concluir**, pule o balanço deste processo e continue com a próxima etapa em [Atualizando o sistema manualmente, na página 82](#). (Copiar dados do sistema original para o sistema de atualização usando a implantação manual deve ser realizado após o sistema atualizado ser implantado, mas ainda não ligado.) Caso contrário, verifique **Ligar após a implantação** e selecione **Concluir**.

Etapa 15 Se você estiver implementando uma máquina virtual de Administração, vai até o vCenter e abra uma janela de console para a máquina. Uma vez que é ligado, nós verificaremos as informações de rede que você inseriu durante a implantação OVA.

Se formos capazes de confirmar a conectividade, um marcador de seleção verde é exibido.

Se houver um problema, um X vermelho é exibido. Corrija o erro e tente novamente a implantação OVA.

Etapa 16 Anote a URL diferenciando maiúsculas de minúsculas exibida na janela do console.

Um administrador utiliza esta URL para continuar a implantação do sistema.

Se o sistema for reiniciado antes que a configuração esteja concluída, uma nova senha é gerada e você deve usar a URL com a nova senha.

Próximos passos

Se você está realizando uma implantação manual, recomendamos que você implante o resto das máquinas virtuais no seu sistema neste momento. Isso evita quaisquer problemas, incluindo o tempo limite ao ligar as máquinas virtuais.

Se a implantação for com sucesso, continue com a implantação do sistema em uma janela do navegador.

Se a implantação falhou, consulte [Verificando a Sua Configuração de Rede Após uma Falha na Implantação OVA, na página 20](#).

Verificando a Sua Configuração de Rede Após uma Falha na Implantação OVA

Confirme as entradas de rede para a máquina virtual.

**Importante**

Não utilize **Editar Configurações...** em nenhuma das máquinas virtuais no seu sistema, a não ser após uma implantação interrompida. Uma vez que o sistema estiver instalado e funcionando, você deve utilizar o site da Administração WebEx para fazer quaisquer outras edições nas configurações da máquina virtual. Se você utilizar o seu cliente vSphere, essas alterações não serão aceitas pelo sistema.

**Observação**

Para as etapas detalhadas, consulte a sua documentação Vmware vSphere.

Etapa 1

No cliente vSphere, selecione **Ligar > Desligar convidado** na máquina virtual.

Etapa 2

Encontre a máquina virtual no Inventário e clique com o botão direito do mouse em **Editar Configurações....**

Etapa 3

Selecione a guia **Opções**.

Etapa 4

Selecione **Propriedades** e confirme se todas as informações de rede foram inseridas corretamente. Se nenhuma alteração for necessária, reimplante o OVA com as configurações corretas.

Uma possível causa de um problema de rede é que o roteamento VLAN não está configurado corretamente para o organizador ESXi. Devido a máquina virtual estar nesse VLAN, a máquina virtual não terá conectividade de rede. A partir da rede onde o organizador ESXi reside, você deve ser capaz de executar o ping no endereço de IP de entrada padrão da VLAN que você utiliza nas máquinas virtuais no seu sistema.

Selecionando o Seu Idioma para Instalação

Determine seu idioma preferido para a configuração do sistema.

**Observação**

Não feche esta janela do navegador, até que a implantação do sistema seja concluída. Se você fechar o navegador antes, pode ser necessário reiniciar a implantação.

o sistema CWMS é o nome padrão do centro de dados após uma atualização para a versão 2.5; não é traduzido do inglês para qualquer dos outros idiomas.

Antes de iniciar

Certifique-se que você implantou a máquina virtual de Administração do VMware vCenter. Consulte [Implementando o arquivo OVA do cliente VMware vSphere, na página 18](#)

Etapa 1

Selecione o idioma do menu suspenso.

Etapa 2

Selecione **Próximo**.

Confirmando a Implantação

Para confirmar que você está implantando um novo sistema ou expandindo um sistema já existente, selecione **Próximo**.

Confirmando o Tamanho do Seu Sistema

Você selecionou o tamanho do seu sistema quando você implementou a máquina virtual de Administração, usando o arquivo OVA.

- Confirme se o tamanho do sistema que você selecionou durante a implantação do OVA está correto.
 - Se o tamanho do sistema que você selecionou estiver correto, então selecione **Próximo**.
 - Se o tamanho do sistema que você selecionou estiver errado, então selecione **Eu quero alterar o Tamanho do Sistema**.
 - a) Usando o cliente VMware vSphere, selecione **Ligar > Desligar convidado** nas máquinas virtuais de Administração com o tamanho do sistema errado.
 - b) Clique com o botão direito do mouse e selecione **Excluir a partir do Disco**.
 - c) Reimplante o arquivo OVA e selecione a máquina virtual de Administração para o tamanho do sistema correto.

Escolhendo Qual Sistema Instalar

Etapa 1 Determina o tipo de instalação.

- Se você estiver instalando este sistema pela primeira vez, então escolha **Instalar o sistema primário**.
- Se você já instalou um sistema primário e deseja um sistema de Alta Disponibilidade (HA) redundante, então escolha **Criar um sistema de Alta Disponibilidade (HA) redundante**.

Você não deve instalar um sistema HA antes de instalar o sistema primário, já que você não pode usar o sistema HA, a menos que o sistema primário tenha sido instalado.

Etapa 2 Selecione **Próximo**.

Escolhendo o tipo de implantação

Você pode escolher a implantação automática ou manual das máquinas virtuais do sistema. Sua decisão sobre a implantação manual ou automática depende do seguinte:

- Se você tem restrições de tempo, uma implantação automática é mais rápida do que uma implantação manual.

- Se preferir a orientação passo a passo, essa orientação é fornecida durante uma implantação automática.
- Se você está familiarizado com o VMware vCenter e não quer fornecer as credenciais do vCenter, selecione a implantação manual.

Recomendamos que você selecione **Automático**, a menos que você esteja implantando um sistema de 2000 usuários, que sempre exige a implantação manual.

Etapa 1 Selecione a implantação automática ou manual:

- **Automática:** Implantamos todas as máquinas virtuais necessárias para o seu sistema.
- **Manual:** Você deve implantar manualmente cada máquina virtual usando o VMware vCenter. Após responder algumas perguntas sobre seu sistema, será fornecido a você uma lista de máquinas virtuais necessárias para seu sistema.

Etapa 2 Selecione **Próximo**.

Fornecendo Credenciais Vmware vCenter

Se você selecionar uma implantação automática, o Cisco WebEx Meetings Server requer credenciais vCenter para implantar as máquinas virtuais para você.

Antes de iniciar

Todos os organizadores ESXi do seu sistema devem pertencer a mesma VMware vCenter.

Etapa 1 Insira a URL do https seguro para o vCenter onde o sistema será implantado.**Etapa 2** Insira o nome de usuário que nós usaremos para implantar as máquinas virtuais. O usuário do vCenter deve incluir privilégios de administrador que permitem que o administrador implante, configure, ligue e desligue, e exclua as máquinas virtuais.**Etapa 3** Insira a senha para este nome de usuário.**Etapa 4** Selecione **Próximo**.

Escolha as Configurações do vCenter para a sua Máquina Virtual de Mídia

A máquina virtual de mídia é necessária para a implantação de 250 usuários e 800 usuários do sistema.

Etapa 1 A partir da lista suspensa, escolha o organizador ESXi para máquina virtual de mídia.

Etapa 2 Escolha o armazenamento de dados para a máquina virtual de mídia.

Etapa 3 Escolha o grupo da porta da máquina virtual para a máquina virtual de mídia.

A Cisco recomenda que você escolha o mesmo grupo de porta que você selecionou para a máquina de Administração virtual.

Etapa 4 Selecione Próximo.

Inserindo informações de Rede para a Máquina Virtual de Mídia

Inserindo o nome de domínio totalmente qualificado da máquina virtual de mídia, o Cisco WebEx Meetings Server tenta preencher as informações de rede.



Observação

A máquina virtual de mídia deve estar na mesma sub-rede que as máquinas virtuais de Administração. Não edite o domínio, o portão de IPv4, a máscara de sub-rede ou os servidores DNS para a máquina virtual de mídia.

Etapa 1 Insira o FQDN da máquina virtual de Mídia.

Você já deve ter inserido o endereço de IP e o hostname da máquina virtual de mídia em seus servidores DNS. O Cisco WebEx Meetings Server procura e preenche o **Endereço IPv4**.

Etapa 2 Selecione Próximo.

Adicionando o Acesso Público

Se você adicionar acesso público usando IRP, os usuários fora do firewall podem organizar ou participar de reuniões a partir da Internet ou dispositivos móveis. As máquinas virtuais IRP podem ser adicionadas a um sistema a qualquer momento em uma base de centro de dados. Adicionar IRP a um centro de dados em um ambiente com Vários centros de dados (MDC) dá aos usuários fora do firewall acesso a todo o sistema. Para impedir acesso externo, todas as máquinas virtuais IRP devem ser removidas de um sistema.

Por razões de segurança, recomendamos que você localize o Proxy Reverso da Internet em uma sub-rede diferente da sub-rede ocupada pela máquina virtual de Administração. Isso garante o nível de isolamento da rede entre o proxy reverso da internet e as suas máquinas virtuais internas (Administrador e mídia, se for o caso).

Em um ambiente de Vários centros de dados (MDC), os centros de dados não podem ser expandidos ou atualizados. Os centros de dados secundários devem ser removidos do MDC, tornando-os um ambiente de Centro de dados único (SDC). O ambiente MDC pode ser restaurado após os centros de dados serem modificados e verifica-se que a versão e os tamanhos dos centros de dados coincidem.

Antes de iniciar

Não é necessário conectar o servidor de armazenamento à um servidor de Proxy Reverso da Internet (PRI).

Se houver um firewall entre as máquinas virtuais de Administração e as máquinas virtuais IRP, o endereço de IP temporário deve ser permitido através do firewall.

Etapa 1 Escolha se os usuários externos podem ou não organizar ou participar de reuniões.

- Se você deseja adicionar acesso público, confirme que **Criar uma máquina virtual de Proxy Reverso da Internet** está selecionado.
- Se você deseja que apenas os usuários internos (aqueles atrás do firewall da empresa) organizem ou participem de reuniões, então desmarque **Criar uma máquina virtual de Proxy Reverso da Internet**.

Etapa 2 Selecione **Próximo**.

Próximos passos

- Com acesso público: [Escolhendo as Configurações vCenter para Proxy Reverso da Internet \(IRP\), na página 25](#)
- Sem acesso público: [Inserindo o Endereço VIP Privado, na página 27](#)
- Para as conexões de clientes IPv6: [Configurando IPv6 para conexões de clientes, na página 141](#)

Escolhendo as Configurações vCenter para Proxy Reverso da Internet (IRP)

Antes de iniciar

Certifique-se que as portas do firewall exigidas pelo VMware vCenter estão abertas para que o vCenter implante a máquina virtual de proxy reverso da internet (IRP). Para mais informações sobre as portas do firewall necessárias, consulte o *Guia de Planejamento do Cisco WebEx Meetings Server*.

Etapa 1 A partir da lista suspensa, escolha o organizador ESXi para máquina virtual IRP.

Etapa 2 Escolha o armazenamento de dados para o IRP.

Etapa 3 Escolha o grupo de porta da máquina virtual.

Etapa 4 Selecione **Próximo**.

Inserir informações de rede no Proxy Reverso da Internet (IRP)

Etapa 1 Insira o nome de organizador e o endereço de IP dos servidores de Proxy Reverso da Internet (IRP) no DNS para permitir a pesquisa de uma rede externa.

Se você tem servidores DNS que permitem pesquisa de redes internas, adicione o nome de organizador e o endereço de IP dos servidores IRP nestes servidores DNS também. Isto permite uma conexão segura entre as máquinas virtuais internas e os servidores IRP.

Etapa 2 Insira o seguinte:

Se você inseriu o nome de organizador e o endereço de IP da máquina virtual de proxy reverso da Internet nos seus servidores DNS, então pesquisaremos e preencheremos o campo **Endereço de Ipv4**.

- Nome de Domínio Totalmente Qualificado (FQDN)
- Entrada IPv4
- Máscara de sub-rede do IPv4
- Endereço de IPv4 do Servidor DNS Primário
- Endereço de IPv4 do servidor DNS Secundário (Opcional)

Etapa 3 Selecione **Próximo**.

Inserindo o Endereço VIP Públco

- Este endereço VIP público deve ser visível a partir da Internet e da rede interna (DNS de horizonte dividido apenas).
- Este endereço de VIP público deve estar na mesma sub-rede que o Proxy Reverso da Internet.
- Se você não tiver um DNS split-horizon, então todos os usuários usam o endereço VIP Público para organizar e participar de reuniões.
- Se você tiver um DNS split-horizon e adicionou o acesso público, então os usuários externos usam o endereço VIP Público para organizar e participar de reuniões.

Para mais informações sobre o DNS split-horizon e sem split-horizon, e o acesso público, consulte o *Guia de Planejamento do Cisco WebEx Meetings Server*.



Observação

Se você estiver criando um sistema de Alta Disponibilidade (HA), você não precisa reinserir esta informação, como usaremos as informações que você inseriu no sistema primário.

- Insira o endereço IPv4 VIP público e selecione **Próximo**.

Inserindo o Endereço VIP Privado

Os administradores configuram, monitoram e mantém o sistema através da URL do site de administração que mapeia o endereço VIP privado.

Se você tem um DNS split-horizon, então os usuários internos também usam o endereço VIP Privado para organizar e participar de reuniões.

Se você estiver adicionando um sistema de Alta Disponibilidade (HA), você não precisa reinserir esta informação; usaremos as informações que você inseriu no sistema primário.

Antes de iniciar

O endereço de IP virtual privado (VIP) deve estar na mesma sub-rede que as suas máquinas virtuais internas (Administração e Mídia, se aplicável).

- Insira o endereço VIP privado IPv4 e selecione **Próximo**.

URLs do Site WebEx e da Administração WebEx

URL do Site WebEx

Usuários acessam a URL do site WebEx para agendar, organizar ou participar de reuniões. Esta URL resolve para o endereço VIP privado ou endereço VIP público, dependendo se você está ou usando um DNS split-horizon.

- Resolve para o endereço VIP público para todos os usuários, quando você não tem DNS split-horizon.
- Resolve para o endereço VIP público para os usuários externos, quando você tem DNS split-horizon.
- Resolve para o endereço VIP privado para os usuários internos, quando você tem DNS split-horizon.



Observação

As portas 80 e 443 devem ser abertas para a URL do site WebEx.

URL da Administração WebEx

Os administradores acessam a URL da Administração WebEx para configurar, gerenciar e monitorar o sistema. Esta URL resolve para o endereço VIP privado.



Observação

As portas 80 e 443 devem ser abertas para a URL de administração WebEx.

Nomes para as URLs do Site WebEx e da Administração WebEx.

Você pode escolher quase todos os nomes para essas URLs, compreendendo todos os caracteres minúsculos. No entanto, você não pode usar os seguintes como o nome do organizador nas URLs:

- o mesmo nome que os nomes dos organizadores para qualquer uma das máquinas virtuais no sistema

- autenticação
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-cliente-serviços
- E-mails
- manutenção
- manager
- orion
- oriondata
- oriontemp
- NBR
- npp
- probe
- reminder
- RAIZ
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- Versão
- WBXService
- WebEx

Inserindo as URLs do site WebEx comum e do site de administração

A URL do site comum permite que os usuários agendem e organizem reuniões e accessem gravações de reuniões. A URL do site de administração fornece gerenciamento do sistema. Se você estiver adicionando um sistema de Alta Disponibilidade (HA), não é necessário inserir novamente esta informação; as URLs do sistema primário devem coincidir com as URLs do sistema HA. (Consulte [Conceitos gerais para implantação do sistema](#), na página 11 para obter descrições das URLs.)

Etapa 1 Insira as URLs seguras do site de administração WebEx e do site comum WebEx (<https://>).

A URL do site comum WebEx deve ser diferente da URL de administração WebEx.

Não reutilize os nomes dos organizadores das máquinas virtuais na parte do nome do organizador da URLs WebEx.

Etapa 2 Selecione **Próximo**.

Confirmando que sua rede está configurada corretamente

Esta tela fornece links para ajuda on-line para as alterações de rede necessárias para o seu sistema. A ajuda on-line fornece detalhes sobre as alterações do servidor DNS bem como as configurações do firewall.

Você deve fazer alterações no servidor DNS e firewall que nos permitem testar a conectividade de rede.

Se você ainda não tiver feito isso, conclua a configuração de rede e selecione **Próximo**.

Se você estiver testando uma implantação automática, implantamos as máquinas virtuais necessárias para seu sistema quando você selecionar **Próximo**.

Se você estiver testando uma implantação manual, insira os nomes dos organizadores nas máquinas virtuais e implante-as (se você ainda não as implantou).

Quando a implantação estiver concluída, teste ligando-as e verifique se todas as máquinas virtuais ligaram com sucesso.

Implantação das máquinas virtuais

Baseado nas informações que você inseriu antes, implantamos as máquinas virtuais necessárias para seu sistema.

A implantação requer vários minutos para concluir. Não saia desta página até que todas as máquinas virtuais tenham sido implantadas e ligadas (ou mensagens de erro serão exibidas indicando que a implantação falhou).

Quando a coluna de status mostra todas as verificações verdes, a implantação está concluída sem erros. Selecione **Próximo**.

Se forem indicados erros, corrija-os e selecione **Próximo** para reimplantar o sistema. Você pode selecionar **Baixar arquivo de registro** para obter o arquivo de registro para esta implantação. O log fornece um registro da implantação, que pode ser usado para solucionar problemas de uma implantação que falhou.

Observação

Antes de reimplantar um sistema, certifique-se de desligar e excluir as máquinas virtuais envolvidas com os erros; caso contrário, durante uma reimplantação, você pode ver mensagens de erro sobre as máquinas virtuais existentes.

Verificando o sistema

A verificação do sistema verifica os parâmetros de configuração do seu sistema. Isso inclui a confirmação de que as máquinas virtuais possuem a configuração mínima necessária e a validação das URLs do site WebEx e de Administração WebEx.

A verificação do sistema leva alguns minutos para concluir. Não saia desta página até que todas as verificações tenham sido concluídas com sucesso, ou a verificação do sistema falha e mostra mensagens de erro indicando o problema.

Se você recarregou a página antes da conclusão das verificações, você será retornado a primeira página desta implantação de sistema. Quando as verificações forem concluídas com êxito, a primeira página do utilitário de configuração será exibida.

A URL do site de Administração usada durante o processo de implantação é o nome de organizador da máquina virtual de Administração. Durante a configuração básica, o nome de organizador é substituído pela URL do site de Administração. Como resultado, a primeira vez que você iniciar a sessão no site de Administração, o sistema poderá solicitar que você aceite a exceção no certificado.

- Complete um dos seguintes:

- Se não houver erros e o estado mostrar todas as verificações verdes, selecione **Próximo** e continue com [Configurando um servidor de e-mail \(SMTP\), na página 49](#). Em raros casos, você pode ver **Não testado**. Isso não significa que existe algum problema com as máquinas virtuais. Ele simplesmente afirma que as verificações do sistema não foram concluídas; por exemplo, a entrada pode ser exibida porque houve uma perda temporária de conectividade de rede. Depois de concluir a implantação, você pode iniciar sessão no site da Administração e verificar esses recursos.
 - Se há um problema com a conectividade de rede, verifique se a URL do Site WebEx, as URLs de Administração e os endereços de IP foram inseridos corretamente. Verifique se estes sites estão na mesma sub-rede e se os parâmetros foram corretamente inseridos nos servidores DNS.
 - Se houver problemas com o sistema para atender a capacidade mínima do sistema, você tem duas opções:
 - Desligue todas as máquinas virtuais do VMware vCenter e as exclua manualmente. Em seguida, tente novamente a implantação do sistema em um sistema com recursos que atendem ou excedem os requisitos mínimos.
 - Prossiga com a instalação atual. Se você fizer, você deve reconhecer que renuncia o direito de solicitar suporte técnico da Cisco. Confirme, verificando a mensagem de erro na caixa de seleção e selecione **Próximo**.
 - Se houver algum problema com uma ou mais de suas máquinas virtuais, desligue as máquinas virtuais com os erros e as exclua manualmente usando o VMware vCenter. Corrija os problemas e tente novamente a implantação do sistema.
- Selecione **Continuar** para ir para a configuração básica onde você configura o servidor de e-mail ([Configurando um servidor de e-mail \(SMTP\), na página 49](#)) e identifica um administrador ([Criando contas de administrador, na página 51](#)). Se outro administrador completar a configuração básica, envie esta URL para esse administrador.



CAPÍTULO 4

Implantando um sistema manualmente

- Conceitos gerais para implantação do sistema, página 31
- Checklist de Instalação, página 34
- Informações necessárias para uma Implantação Manual, página 35
- Implementando o arquivo OVA do cliente VMware vSphere, página 36
- Selecionando o Seu Idioma para Instalação, página 39
- Confirmando a Implantação, página 40
- Confirmando o Tamanho do Seu Sistema, página 40
- Escolhendo Qual Sistema Instalar, página 40
- Escolhendo o tipo de implantação, página 40
- Adicionando o Acesso Público, página 41
- Inserindo o Endereço VIP Público, página 43
- Inserindo o Endereço VIP Privado, página 43
- URLs do Site WebEx e da Administração WebEx, página 44
- Inserindo as URLs do site WebEx comum e do site de administração, página 45
- Confirmando que sua rede está configurada corretamente, página 45
- Implantação de máquinas virtuais, página 46
- Verificando o sistema, página 47

Conceitos gerais para implantação do sistema

Tamanhos do sistema

Os sistemas são identificados pelo número de usuários simultâneos suportados:

- 50 usuários simultâneos (também conhecido como sistema *micro*)
 - Suporta normalmente uma empresa entre 500 e 1000 funcionários

- Sistema primário [sem Alta Disponibilidade {HA}] compreende uma máquina virtual de administração e um proxy reverso da internet opcional (para acesso público)
- 250 usuários simultâneos (também conhecido como sistema *pequeno*)
 - Suporta normalmente uma empresa entre 2500 e 5000 funcionários
 - O sistema primário (sem HA) compreende uma máquina virtual de administração, uma máquina virtual de mídia e um proxy reverso da internet opcional (para acesso público)
- 800 usuários simultâneos (também conhecido como sistema *médio*)
 - Suporta normalmente uma empresa entre 8000 e 16.000 funcionários
 - O sistema primário (sem HA) compreende uma máquina virtual de administração, uma máquina virtual de mídia e um proxy reverso da internet opcional (para acesso público)
- 2000 usuários simultâneos (também conhecido como sistema *grande*)
 - Suporta normalmente uma empresa entre 20.000 e 40.000 funcionários
 - Sistema primário (sem HA) compreende uma máquina virtual de administração, três máquinas virtuais de mídia, duas máquinas web e um proxy reverso da internet opcional (para acesso público)

Termos usados durante a implantação

URL do site WebEx — uma URL http segura para que os usuários organizem e participem de reuniões em um ambiente de centro de dados único.

URL de administração WebEx — URL http segura para que os administradores configurem, monitorem e gerenciem o sistema em um ambiente de centro de dados único.

VIP público — endereço de IP virtual para a URL do site WebEx.

VIP privado — endereço de IP virtual para a URL do site de administração ou o endereço de IP virtual para a URL do site WebEx (para usuários internos apenas, se você tem um DNS split-horizon).

URL WebEx comum — usada pelo DNS para redirecionar o usuário ao centro de dados, onde o usuário executa tarefas relacionadas às reuniões, tais como agendamento ou organização de reuniões. Qual centro de dados DNS é transparente para o usuário. A URL WebEx comum é simplesmente uma localização conveniente para um usuário entrar no sistema. Se um centro de dados cair, nada muda para o usuário, incluindo a URL usada para acessar as reuniões, porque o DNS irá redirecionar o usuário para o centro de dados sobrevivendo.

URL de Administração Comum — é muitas vezes referida como simplesmente a *URL de Administração*. Ela é usada pelo DNS para redirecionar um administrador para o centro de dados de gerenciamento de onde o administrador faz logon no sistema. O centro de dados que o DNS escolhe é transparente para o administrador (no entanto, a sequência na barra da URL muda dependendo de qual centro de dados o administrador está usando para acessar o sistema). A URL de Administração Comum é simplesmente um alvo conveniente que um administrador usa para entrar no sistema.

URLs de Administração Locais — são específicas para cada centro de dados em um sistema com Vários centros de dados (MDC). Ao efetuar logon através da URL de Administração Comum, o DNS redireciona o administrador para a URL de Administração Local para o centro de dados de gerenciamento. Quaisquer modificações no sistema, tais como a atribuição de uma licença para um usuário, são realizadas no centro de dados de gerenciamento e replicadas para todos os centros de dados no sistema de MDC.

Um administrador pode escolher um centro de dados específico para modificar a partir do aplicativo CWMS, mas selecionar um outro centro de dados para modificar não altera a URL de Administração Local, porque o acesso do administrador para o sistema continua a ser o centro de dados escolhido pelo DNS quando o administrador efetua logon no sistema. As modificações do administrador para outro centro de dados no sistema de MDC passa pelo centro de dados de gerenciamento escolhido pelo DNS para o centro de dados de destino.

Um sistema de MDC terá um mínimo de duas URLs de Administração Locais, uma para cada centro de dados no sistema.

URLs locais que são específicas para cada centro de dados.

Informações do perfil do sistema

Completa este gráfico do seu sistema.

URL do site comum		
URL da administração comum		
Endereços de IP virtuais DC1 e DC2		
	Centro de dados 1	Centro de dados 2
URLs do site local		
URLs de administração local		
Endereços de IP virtuais públicos		
Endereço de IP virtuais privados		
Servidor DNS		
Endereço de IP da máquina virtual de administração		
Endereço de IP da máquina virtual de mídia 1		
Endereço de IP da máquina virtual de mídia 2		
Endereço de IP da máquina virtual de mídia 3		
Endereço de IP da máquina virtual da Web 1		
Endereço de IP da máquina virtual da Web 2		

Endereço de IP da máquina virtual DMZ (opcional)		
Endereço de e-mail do administrador CWMS		
Senha		
Remote Access ²		
Senha		
Endereço de IP do Call Manager		
ID do administrador do Cisco Call Manager		
Senha do Cisco Call Manager		
Números de discagem de entrada CWMS		
Números de Telefone		

² As contas de acesso remoto não serão ativadas até a conta ser ativada.

Checklist de Instalação



Restrição

Você deve usar o VMware vCenter para gerenciar os organizadores ESXi no qual o sistema Cisco WebEx Meetings Server é implantado.

Alterações da Rede

Consulte o checklist de rede apropriado para a sua implantação. Considere o seguinte:

- Acesso público: se os usuários fora de seu firewall podem organizar e acessar reuniões a partir da Internet ou dispositivos móveis ou não.
A Cisco recomenda o acesso público, uma vez que resulta em uma melhor experiência de usuário para a sua equipe móvel.
- Tipo de configuração DNS em sua empresa: DNS split-horizon ou DNS sem split-horizon (configuração DNS mais comum). Para mais informações sobre a configuração DNS, consulte o *Guia de planejamento do Cisco WebEx Meetings Server*.
- Abra a porta 10200 a partir do desktop do administrador para a máquina virtual de Administração. A porta 10200 é usada pelo navegador durante a implantação.

Selecione a lista de verificação apropriada para sua implantação:

- Checklist de Rede para um Sistema com Acesso Público e DNS não Split-Horizon
- Checklist da Rede para um Sistema Com Acesso Não Público
- Checklist da Rede para um Sistema com Acesso Público e DNS Split-Horizon

Info. necessárias

As informações necessárias variam se você está fazendo uma implantação de sistemas automática (suportado por 50 usuários simultâneos, 250 usuários simultâneos e 800 usuários simultâneos) ou manual (com suporte para todos os tamanhos de sistemas). Recomendamos que você selecione uma implantação automática, a menos que você esteja implantando um sistema de 2000 usuários, que sempre exige uma implantação manual.

Selecione a lista de verificação apropriada para seu tipo de implantação:

- As informações necessárias para uma Implantação Automática, na página 15
- Informações necessárias para uma Implantação Manual, na página 35

Informações necessárias para uma Implantação Manual

Em uma implantação manual, você cria todas as máquinas virtuais para o seu sistema usando o assistente OVA do seu cliente vSphere. Você, então, instala o sistema usando uma implantação manual.

Você deve escolher uma implantação manual se você estiver implantando um sistema de usuário 2000.



Observação

Certifique-se de adicionar os FQDNs de máquinas virtuais, endereços IP, URLs de site WebEx e Administração e endereços VIP para seus servidores DNS antes de iniciar a implantação do sistema. Vamos usar essa informação para verificar a conectividade de rede no final da implantação.

Para evitar quaisquer problemas de DNS, você pode querer testar essas URLs e endereços de IP antes de iniciar a implantação do OVA. Caso contrário, a implantação do sistema irá falhar até que você corrija esses erros.

Esta é a informação necessária para o seu sistema, em ordem.

Nome do Campo	Descrição	Valor Para o Seu Sistema
VIP público	Endereço de IP para a URL do site WebEx (os usuários do site acessam para organizar e participar de reuniões)	
VIP privado	<ul style="list-style-type: none"> Endereço de IP para a URL do site de Administração (para que os administradores configurem, monitorem e gerenciem o sistema) Endereço de IP para a URL do site WebEx (apenas para usuários internos, se você tem um DNS split-horizon). 	

Nome do Campo	Descrição	Valor Para o Seu Sistema
URL do Site WebEx	URL http segura (todos os caracteres minúsculos) para que os usuários organizem e participem de reuniões.	
URL da Administração WebEx	URL http segura (todos os caracteres minúsculos) para que os administradores configurem, monitorem e gerenciem o sistema.	
FQDN para as máquinas virtuais internas	Dependendo do tamanho do sistema que você selecionou, o nome de domínio totalmente qualificado (todos os caracteres minúsculos) das máquinas virtuais da web e de mídia.	
(Apenas acesso público) FQDN do Proxy Reverso da Internet	Se você planeja adicionar o acesso público, então você precisa inserir o nome de domínio totalmente qualificado (todos os caracteres minúsculos) da máquina virtual de Proxy Reverso da Internet.	

O que fazer a seguir

Com esta informação, iniciar a implantação do sistema, inserindo a URL de implantação em uma janela do navegador. (A URL de implantação está escrita na janela do console para a máquina virtual de Administração).



Observação

Se o sistema for reiniciado antes que a configuração estiver concluída, uma nova senha é gerada e você deve usar a URL de implantação com a nova senha.

Implementando o arquivo OVA do cliente VMware vSphere

O modelo OVA cria dois NICs virtuais para cada máquina virtual. No entanto, apenas as máquinas virtuais de admin usam os dois NICs virtuais. Todas as outras máquinas virtuais do Cisco WebEx Meetings Server (CWMS), apenas um NIC virtual é usado e o outro é desligado.

Este procedimento é fornecido como uma orientação geral. As telas que você vê durante a implantação OVA depende das configurações do seu vCenter, do armazenamento e da rede e podem ser diferentes do que está descrito neste procedimento. Veja a sua documentação do Vmware vSphere para informações completas no assistente OVA.

Antes de iniciar

Obtenha o arquivo OVA do Servidor do Cisco WebEx Meetings para o seu sistema e coloque-o em um local que seja acessível do Vmware vSphere Use o cliente VMware vSphere para implantar a máquina virtual de Administração no seu sistema.

Você deve usar o VMware vCenter para gerenciar os organizadores ESXi no qual o sistema Cisco WebEx Meetings Server é implantado. Ao usar o cliente vSphere, inicie sessão no vCenter e implante o arquivo OVA na máquina virtual de Administração.

-
- Etapa 1** Inicie sessão no seu cliente VMware vSphere.
Certifique-se de iniciar sessão como um usuário que inclui privilégios de administrador: para implantar, configurar, ligar ou desligar, e excluir as máquinas virtuais.
- Etapa 2** Selecione **Arquivo > Implantar o modelo OVF...**
- Etapa 3** Selecione **Procurar** para navegar até o local do arquivo OVA. Selecione **Próximo**.
Você pode selecionar o link **Cisco WebEx Meetings Server** para ir para uma página da internet com informações detalhadas sobre este sistema.
- Etapa 4** Leia as Exigências de Licença do Usuário Final e selecione **Aceitar**, então selecione **Próximo**.
- Etapa 5** Navegue para e selecione o local, no inventário vCenter, onde você gostaria de colocar a máquina virtual de Administração.
- Etapa 6** Insira o nome da máquina virtual para o tamanho do sistema e selecione **Próximo**. Para obter mais informações sobre a seleção do tamanho correto para a sua empresa, consulte [Tamanhos do sistema, na página 11](#).
Você deve implantar a máquina virtual de Administração antes de implantar qualquer outra máquina virtual. Se você selecionar a implantação automática (recomendado), implantaremos as outras máquinas virtuais para você. Se você escolher a implantação manual (exigido para sistema de 2000 usuários simultâneos), então após a implantação da máquina virtual de Administração, você deve implantar as outras máquinas virtuais utilizando este mesmo assistente.
A Cisco recomenda que você inclua o tipo no nome da máquina virtual; por exemplo, "Admin" no nome da sua máquina virtual de Administração, para identificá-la facilmente no seu inventário do vCenter.
Todas as máquinas virtuais da internet para os seus sistemas devem estar na mesma sub-rede que a máquina virtual de Administração. (Dependendo do tamanho do sistema que você selecionar, você pode precisar de uma ou mais máquinas virtuais internas de web e mídia.)
- Etapa 7** A partir da lista suspensa, selecione a máquina virtual para o tamanho do seu sistema e selecione **Próximo**.
Certifique-se de implementar a máquina virtual de Administração antes de qualquer outra máquina virtual em seu sistema.
- Etapa 8** Navegue através do inventário vCenter e selecione o organizador ESXi ou cluster onde você deseja implantar as máquinas virtuais para o seu sistema. Selecione **Próximo**.
- Etapa 9** Se o cluster contém um conjunto de recursos, selecione o conjunto de recursos onde você deseja implantar o modelo OVA e selecione **Próximo**.
Os pools de recursos compartilham os recursos de CPU e memória ou trabalham com recursos do VMware, tais como DRS ou vMotion. Os pools de recursos devem ser dedicados a um único Organizador ESXi. Os pools de recursos VMware não são recomendados para uso com o Cisco WebEx Meetings Server.
- Etapa 10** Selecione o armazenamento de dados para a sua máquina virtual e o tipo de provisionamento para a sua máquina virtual. Você deve selecionar o **Thick Provisioning** e criar o máximo de espaço na unidade virtual necessário para o seu sistema. Com Thin Provisioning, o VMware aloca o espaço do sistema do arquivo em um *conforme necessário*, resultando em um desempenho ruim. O disco lazy zero é suficiente e o eager zero é aceitável, mas o disco eager zero levará mais tempo para ser concluído.
- Etapa 11** Configurar o mapeamento de rede. Para cada rede de origem, selecione uma rede de destino da lista suspensa na coluna **Destination Networks**. Selecione **Próximo**.
- Observação** Tanto a VM Network e a VIP Network devem ser mapeadas para o mesmo valor na coluna Destination Network. Você pode ignorar a mensagem de aviso sobre redes de múltiplas fontes mapeadas para a mesma rede do organizador.

Etapa 12 Insira as seguintes informações para a máquina virtual, então selecione **Próximo**:

- Nome do organizador da máquina virtual (não inclui o domínio aqui)
- Domínio para a máquina virtual
- Endereço de IPv4 (Eth0) da máquina virtual
- A máscara da sub-rede da máquina virtual
- Portão de endereço de IP
- O servidor DNS primário que contém entradas para o hostname e endereço de IP desta máquina virtual
- Servidor DNS secundário que contém entradas para o nome do organizador e o endereço de IP da máquina virtual
(Um sistema com apenas um servidor DNS configurado está em risco, porque cria um ponto único de falha.
Recomendamos que você configure um servidor DNS secundário para criar redundância de rede.)
- O idioma exibido durante o processo de instalação, seguindo a alimentação desta máquina virtual

Observação Para evitar problemas de DNS, você pode testar as URLs e endereços de IP antes de iniciar a implantação do OVA. A implantação falhará se houver erros.

Etapa 13 Confirme a informação que você inseriu. Se houver qualquer problema, selecione **Voltar** e altere os valores.

Etapa 14 Se você estiver atualizando um sistema manualmente, selecione **Concluir**, pule o balanço deste processo e continue com a próxima etapa em [Atualizando o sistema manualmente, na página 82](#). (Copiar dados do sistema original para o sistema de atualização usando a implantação manual deve ser realizado após o sistema atualizado ser implantado, mas ainda não ligado.) Caso contrário, verifique **Ligar após a implantação** e selecione **Concluir**.

Etapa 15 Se você estiver implementando uma máquina virtual de Administração, vai até o vCenter e abra uma janela de console para a máquina. Uma vez que é ligado, nós verificaremos as informações de rede que você inseriu durante a implantação OVA.

Se formos capazes de confirmar a conectividade, um marcador de seleção verde é exibido.

Se houver um problema, um X vermelho é exibido. Corrija o erro e tente novamente a implantação OVA.

Etapa 16 Anote a URL diferenciando maiúsculas de minúsculas exibida na janela do console.

Um administrador utiliza esta URL para continuar a implantação do sistema.

Se o sistema for reiniciado antes que a configuração esteja concluída, uma nova senha é gerada e você deve usar a URL com a nova senha.

Próximos passos

Se você está realizando uma implantação manual, recomendamos que você implante o resto das máquinas virtuais no seu sistema neste momento. Isso evita quaisquer problemas, incluindo o tempo limite ao ligar as máquinas virtuais.

Se a implantação for com sucesso, continue com a implantação do sistema em uma janela do navegador.

Se a implantação falhou, consulte [Verificando a Sua Configuração de Rede Após uma Falha na Implantação OVA, na página 20](#).

Verificando a Sua Configuração de Rede Após uma Falha na Implantação OVA

Confirme as entradas de rede para a máquina virtual.

**Importante**

Não utilize **Editar Configurações...** em nenhuma das máquinas virtuais no seu sistema, a não ser após uma implantação interrompida. Uma vez que o sistema estiver instalado e funcionando, você deve utilizar o site da Administração WebEx para fazer quaisquer outras edições nas configurações da máquina virtual. Se você utilizar o seu cliente vSphere, essas alterações não serão aceitas pelo sistema.

**Observação**

Para as etapas detalhadas, consulte a sua documentação Vmware vSphere.

Etapa 1

No cliente vSphere, selecione **Ligar > Desligar convidado** na máquina virtual.

Etapa 2

Encontre a máquina virtual no Inventário e clique com o botão direito do mouse em **Editar Configurações....**

Etapa 3

Selecione a guia **Opções**.

Etapa 4

Selecione **Propriedades** e confirme se todas as informações de rede foram inseridas corretamente. Se nenhuma alteração for necessária, reimplante o OVA com as configurações corretas.

Uma possível causa de um problema de rede é que o roteamento VLAN não está configurado corretamente para o organizador ESXi. Devido a máquina virtual estar nesse VLAN, a máquina virtual não terá conectividade de rede. A partir da rede onde o organizador ESXi reside, você deve ser capaz de executar o ping no endereço de IP de entrada padrão da VLAN que você utiliza nas máquinas virtuais no seu sistema.

Selecionando o Seu Idioma para Instalação

Determine seu idioma preferido para a configuração do sistema.

**Observação**

Não feche esta janela do navegador, até que a implantação do sistema seja concluída. Se você fechar o navegador antes, pode ser necessário reiniciar a implantação.

o sistema CWMS é o nome padrão do centro de dados após uma atualização para a versão 2.5; não é traduzido do inglês para qualquer dos outros idiomas.

Antes de iniciar

Certifique-se que você implantou a máquina virtual de Administração do VMware vCenter. Consulte [Implementando o arquivo OVA do cliente VMware vSphere, na página 18](#)

Etapa 1

Selecione o idioma do menu suspenso.

Etapa 2

Selecione **Próximo**.

Confirmando a Implantação

Para confirmar que você está implantando um novo sistema ou expandindo um sistema já existente, selecione **Próximo**.

Confirmando o Tamanho do Seu Sistema

Você selecionou o tamanho do seu sistema quando você implementou a máquina virtual de Administração, usando o arquivo OVA.

- Confirme se o tamanho do sistema que você selecionou durante a implantação do OVA está correto.
 - Se o tamanho do sistema que você selecionou estiver correto, então selecione **Próximo**.
 - Se o tamanho do sistema que você selecionou estiver errado, então selecione **Eu quero alterar o Tamanho do Sistema**.
 - a) Usando o cliente VMware vSphere, selecione **Ligar > Desligar convidado** nas máquinas virtuais de Administração com o tamanho do sistema errado.
 - b) Clique com o botão direito do mouse e selecione **Excluir a partir do Disco**.
 - c) Reimplante o arquivo OVA e selecione a máquina virtual de Administração para o tamanho do sistema correto.

Escolhendo Qual Sistema Instalar

Etapa 1 Determina o tipo de instalação.

- Se você estiver instalando este sistema pela primeira vez, então escolha **Instalar o sistema primário**.
- Se você já instalou um sistema primário e deseja um sistema de Alta Disponibilidade (HA) redundante, então escolha **Criar um sistema de Alta Disponibilidade (HA) redundante**.

Você não deve instalar um sistema HA antes de instalar o sistema primário, já que você não pode usar o sistema HA, a menos que o sistema primário tenha sido instalado.

Etapa 2 Selecione **Próximo**.

Escolhendo o tipo de implantação

Você pode escolher a implantação automática ou manual das máquinas virtuais do sistema. Sua decisão sobre a implantação manual ou automática depende do seguinte:

- Se você tem restrições de tempo, uma implantação automática é mais rápida do que uma implantação manual.

- Se preferir a orientação passo a passo, essa orientação é fornecida durante uma implantação automática.
- Se você está familiarizado com o VMware vCenter e não quer fornecer as credenciais do vCenter, selecione a implantação manual.

Recomendamos que você selecione **Automático**, a menos que você esteja implantando um sistema de 2000 usuários, que sempre exige a implantação manual.

Etapa 1 Seleccione a implantação automática ou manual:

- **Automática:** Implantamos todas as máquinas virtuais necessárias para o seu sistema.
- **Manual:** Você deve implantar manualmente cada máquina virtual usando o VMware vCenter. Após responder algumas perguntas sobre seu sistema, será fornecido a você uma lista de máquinas virtuais necessárias para seu sistema.

Etapa 2 Seleccione **Próximo**.

Adicionando o Acesso Público

Se você adicionar acesso público usando IRP, os usuários fora do firewall podem organizar ou participar de reuniões a partir da Internet ou dispositivos móveis. As máquinas virtuais IRP podem ser adicionadas a um sistema a qualquer momento em uma base de centro de dados. Adicionar IRP a um centro de dados em um ambiente com Vários centros de dados (MDC) dá aos usuários fora do firewall acesso a todo o sistema. Para impedir acesso externo, todas as máquinas virtuais IRP devem ser removidas de um sistema.

Por razões de segurança, recomendamos que você localize o Proxy Reverso da Internet em uma sub-rede diferente da sub-rede ocupada pela máquina virtual de Administração. Isso garante o nível de isolamento da rede entre o proxy reverso da internet e as suas máquinas virtuais internas (Administrador e mídia, se for o caso).

Em um ambiente de Vários centros de dados (MDC), os centros de dados não podem ser expandidos ou atualizados. Os centros de dados secundários devem ser removidos do MDC, tornando-os um ambiente de Centro de dados único (SDC). O ambiente MDC pode ser restaurado após os centros de dados serem modificados e verifica-se que a versão e os tamanhos dos centros de dados coincidem.

Antes de iniciar

Não é necessário conectar o servidor de armazenamento à um servidor de Proxy Reverso da Internet (PRI).

Se houver um firewall entre as máquinas virtuais de Administração e as máquinas virtuais IRP, o endereço de IP temporário deve ser permitido através do firewall.

Etapa 1 Escolha se os usuários externos podem ou não organizar ou participar de reuniões.

- Se você deseja adicionar acesso público, confirme que **Criar uma máquina virtual de Proxy Reverso da Internet** está selecionado.

- Se você deseja que apenas os usuários internos (aqueles atrás do firewall da empresa) organizem ou participem de reuniões, então desmarque **Criar uma máquina virtual de Proxy Reverso da Internet**.

Etapa 2 Seleccione Próximo.

Próximos passos

- Com acesso público: [Escolhendo as Configurações vCenter para Proxy Reverso da Internet \(IRP\), na página 25](#)
- Sem acesso público: [Inserindo o Endereço VIP Privado, na página 27](#)
- Para as conexões de clientes IPv6: [Configurando IPv6 para conexões de clientes, na página 141](#)

Escolhendo as Configurações vCenter para Proxy Reverso da Internet (IRP)

Antes de iniciar

Certifique-se que as portas do firewall exigidas pelo VMware vCenter estão abertas para que o vCenter implante a máquina virtual de proxy reverso da internet (IRP). Para mais informações sobre as portas do firewall necessárias, consulte o *Guia de Planejamento do Cisco WebEx Meetings Server*.

Etapa 1 A partir da lista suspensa, escolha o organizador ESXi para máquina virtual IRP.

Etapa 2 Escolha o armazenamento de dados para o IRP.

Etapa 3 Escolha o grupo de porta da máquina virtual.

Etapa 4 Seleccione Próximo.

Inserir informações de rede no Proxy Reverso da Internet (IRP)

Etapa 1 Insira o nome de organizador e o endereço de IP dos servidores de Proxy Reverso da Internet (IRP) no DNS para permitir a pesquisa de uma rede externa.

Se você tem servidores DNS que permitem pesquisa de redes internas, adicione o nome de organizador e o endereço de IP dos servidores IRP nestes servidores DNS também. Isto permite uma conexão segura entre as máquinas virtuais internas e os servidores IRP.

Etapa 2 Insira o seguinte:

Se você inseriu o nome de organizador e o endereço de IP da máquina virtual de proxy reverso da Internet nos seus servidores DNS, então pesquisaremos e preencheremos o campo **Endereço de Ipv4**.

- Nome de Domínio Totalmente Qualificado (FQDN)
- Entrada Ipv4

- Máscara de sub-rede do IPv4
- Endereço de IPv4 do Servidor DNS Primário
- Endereço de IPv4 do servidor DNS Secundário (Opcional)

Etapa 3 Selecione **Próximo**.

Inserindo o Endereço VIP PÚBLICO

- Este endereço VIP público deve ser visível a partir da Internet e da rede interna (DNS de horizonte dividido apenas).
- Este endereço de VIP público deve estar na mesma sub-rede que o Proxy Reverso da Internet.
- Se você não tiver um DNS split-horizon, então todos os usuários usam o endereço VIP Público para organizar e participar de reuniões.
- Se você tiver um DNS split-horizon e adicionou o acesso público, então os usuários externos usam o endereço VIP Público para organizar e participar de reuniões.

Para mais informações sobre o DNS split-horizon e sem split-horizon, e o acesso público, consulte o *Guia de Planejamento do Cisco WebEx Meetings Server*.



Observação

Se você estiver criando um sistema de Alta Disponibilidade (HA), você não precisa reinserir esta informação, como usaremos as informações que você inseriu no sistema primário.

- Insira o endereço IPv4 VIP público e selecione **Próximo**.

Inserindo o Endereço VIP Privado

Os administradores configuram, monitoram e mantêm o sistema através da URL do site de administração que mapeia o endereço VIP privado.

Se você tem um DNS split-horizon, então os usuários internos também usam o endereço VIP Privado para organizar e participar de reuniões.

Se você estiver adicionando um sistema de Alta Disponibilidade (HA), você não precisa reinserir esta informação; usaremos as informações que você inseriu no sistema primário.

Antes de iniciar

O endereço de IP virtual privado (VIP) deve estar na mesma sub-rede que as suas máquinas virtuais internas (Administração e Mídia, se aplicável).

- Insira o endereço VIP privado IPv4 e selecione **Próximo**.

URLs do Site WebEx e da Administração WebEx

URL do Site WebEx

Usuários acessam a URL do site WebEx para agendar, organizar ou participar de reuniões. Esta URL resolve para o endereço VIP privado ou endereço VIP público, dependendo se você está ou usando um DNS split-horizon.

- Resolve para o endereço VIP público para todos os usuários, quando você não tem DNS split-horizon.
- Resolve para o endereço VIP público para os usuários externos, quando você tem DNS split-horizon.
- Resolve para o endereço VIP privado para os usuários internos, quando você tem DNS split-horizon.



Observação

As portas 80 e 443 devem ser abertas para a URL do site WebEx.

URL da Administração WebEx

Os administradores acessam a URL da Administração WebEx para configurar, gerenciar e monitorar o sistema. Esta URL resolve para o endereço VIP privado.



Observação

As portas 80 e 443 devem ser abertas para a URL de administração WebEx.

Nomes para as URLs do Site WebEx e da Administração WebEx.

Você pode escolher quase todos os nomes para essas URLs, compreendendo todos os caracteres minúsculos. No entanto, você não pode usar os seguintes como o nome do organizador nas URLs:

- o mesmo nome que os nomes dos organizadores para qualquer uma das máquinas virtuais no sistema
- autenticação
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-cliente-serviços
- E-mails
- manutenção
- manager
- orion

- oriondata
- oriontemp
- NBR
- npp
- probe
- reminder
- RAIZ
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- Versão
- WBXService
- WebEx

Inserindo as URLs do site WebEx comum e do site de administração

A URL do site comum permite que os usuários agendem e organizem reuniões e acessem gravações de reuniões. A URL do site de administração fornece gerenciamento do sistema. Se você estiver adicionando um sistema de Alta Disponibilidade (HA), não é necessário inserir novamente esta informação; as URLs do sistema primário devem coincidir com as URLs do sistema HA. (Consulte [Conceitos gerais para implantação do sistema, na página 11](#) para obter descrições das URLs.)

Etapa 1 Insira as URLs seguras do site de administração WebEx e do site comum WebEx (<https://>).
A URL do site comum WebEx deve ser diferente da URL de administração WebEx.

Não reutilize os nomes dos organizadores das máquinas virtuais na parte do nome do organizador da URLs WebEx.

Etapa 2 Selecione **Próximo**.

Confirmando que sua rede está configurada corretamente

Esta tela fornece links para ajuda on-line para as alterações de rede necessárias para o seu sistema. A ajuda on-line fornece detalhes sobre as alterações do servidor DNS bem como as configurações do firewall.

Você deve fazer alterações no servidor DNS e firewall que nos permitam testar a conectividade de rede.

Se você ainda não tiver feito isso, conclua a configuração de rede e selecione **Próximo**.

Se você estiver testando uma implantação automática, implantamos as máquinas virtuais necessárias para seu sistema quando você selecionar **Próximo**.

Se você estiver testando uma implantação manual, insira os nomes dos organizadores nas máquinas virtuais e implante-as (se você ainda não as implantou).

Quando a implantação estiver concluída, teste ligando-as e verifique se todas as máquinas virtuais ligaram com sucesso.

Implantação de máquinas virtuais

Após fornecer informações sobre as máquinas virtuais no sistema, nós tentaremos conectar para cada uma das máquinas virtuais implementadas para o seu sistema.



Observação

Não deixe esta página até que o sistema tenha sido conectado a todas as máquinas virtuais, ou a conexão falha com mensagens de erro indicando o problema.

Etapa 1 Insira os nomes de domínio totalmente qualificados (FQDN) para todas as máquinas virtuais adicionais, necessárias para o seu sistema. (Você inseriu o FQDN da máquina virtual de Administração antes, quando você o implementou do arquivo OVA.)

Etapa 2 Se você já não tiver feito isso, utilizando o VMware vCenter, implante todas as máquinas virtuais adicionais necessárias para o sistema.

Etapa 3 Ligue todas estas máquinas virtuais e verifique se elas ligaram com sucesso. Em seguida, selecione **Detectar máquinas virtuais**.

Estabelecemos conexões com essas máquinas virtuais. Isso poderá levar alguns minutos.

Etapa 4 Aguarde até que o estado **Conectado** seja exibido para todas as máquinas virtuais, então complete um dos seguintes:

- Se não houver erros, o estado mostra todas as verificações verdes. Se você estiver satisfeita com a configuração até agora, selecione **Próximo**. Caso contrário, você pode alterar os FQDNs das máquinas virtuais, novamente selecionando **Detectar máquinas virtuais**.

- Se você ver erros, corrija-os e selecione **Próximo** para continuar.

Observação Você pode selecionar **Baixar arquivo de registro** para obter o arquivo de registro para essa implantação, fornecendo um registro que pode ser usado para solucionar problemas de uma implantação que falhou.

- Se houver outros problemas com uma ou mais máquinas virtuais, do VMware vCenter, desligue as máquinas virtuais com os erros e elimine-as manualmente. (Se você não exclui-las, pode ser que você veja mensagens de erro respeito a essas máquinas virtuais). Após corrigir os problemas, reimplante as máquinas virtuais a partir do arquivo OVA e selecione **Detectar máquinas virtuais**.

Verificando o sistema

A verificação do sistema verifica os parâmetros de configuração do seu sistema. Isso inclui a confirmação de que as máquinas virtuais possuem a configuração mínima necessária e a validação das URLs do site WebEx e de Administração WebEx.

A verificação do sistema leva alguns minutos para concluir. Não saia desta página até que todas as verificações tenham sido concluídas com sucesso, ou a verificação do sistema falha e mostra mensagens de erro indicando o problema.

Se você recarregou a página antes da conclusão das verificações, você será retornado a primeira página desta implantação de sistema. Quando as verificações forem concluídas com êxito, a primeira página do utilitário de configuração será exibida.

A URL do site de Administração usada durante o processo de implantação é o nome de organizador da máquina virtual de Administração. Durante a configuração básica, o nome de organizador é substituído pela URL do site de Administração. Como resultado, a primeira vez que você iniciar a sessão no site de Administração, o sistema poderá solicitar que você aceite a exceção no certificado.

- Complete um dos seguintes:

- Se não houver erros e o estado mostrar todas as verificações verdes, selecione **Próximo** e continue com [Configurando um servidor de e-mail \(SMTP\), na página 49](#). Em raros casos, você pode ver **Não testado**. Isso não significa que existe algum problema com as máquinas virtuais. Ele simplesmente afirma que as verificações do sistema não foram concluídas; por exemplo, a entrada pode ser exibida porque houve uma perda temporária de conectividade de rede. Depois de concluir a implantação, você pode iniciar sessão no site da Administração e verificar esses recursos.
 - Se há um problema com a conectividade de rede, verifique se a URL do Site WebEx, as URLs de Administração e os endereços de IP foram inseridos corretamente. Verifique se estes sites estão na mesma sub-rede e se os parâmetros foram corretamente inseridos nos servidores DNS.
 - Se houver problemas com o sistema para atender a capacidade mínima do sistema, você tem duas opções:
 - Desligue todas as máquinas virtuais do VMware vCenter e as exclua manualmente. Em seguida, tente novamente a implantação do sistema em um sistema com recursos que atendem ou excedem os requisitos mínimos.
 - Prossiga com a instalação atual. Se você fizer, você deve reconhecer que renuncia o direito de solicitar suporte técnico da Cisco. Confirme, verificando a mensagem de erro na caixa de seleção e selecione **Próximo**.
 - Se houver algum problema com uma ou mais de suas máquinas virtuais, desligue as máquinas virtuais com os erros e as exclua manualmente usando o VMware vCenter. Corrija os problemas e tente novamente a implantação do sistema.
- Selecione **Continuar** para ir para a configuração básica onde você configura o servidor de e-mail ([Configurando um servidor de e-mail \(SMTP\), na página 49](#)) e identifica um administrador ([Criando contas de administrador, na página 51](#)). Se outro administrador completar a configuração básica, envie esta URL para esse administrador.



CAPÍTULO 5

Configurando o Seu Servidor de E-mail, Fuso Horário e Local

- Configurando um servidor de e-mail (SMTP), página 49
- Definindo o fuso horário, idioma e localidade, página 50
- Criando contas de administrador, página 51
- Sobre o teste do sistema, página 52

Configurando um servidor de e-mail (SMTP)

Configure um Servidor de e-mail para habilitar o sistema para enviar convites de reuniões e outras comunicações aos usuários.

É importante que o Servidor de e-mail esteja sempre operacional. O e-mail é o principal método de comunicação com os seus usuários, incluindo notificações de gravação, alterações de informações de reuniões, estado da conta e muitos outros anúncios importantes. (Consulte também [Adicionar usuários](#), na página 121).

 **Importante**

Os usuários são identificados no sistema pelo endereço de e-mail. Se um endereço de e-mail do usuário é alterado e o usuário permanece ativo, o endereço de e-mail no CWMS também deve ser alterado ou esse usuário não receberá notificações.



Observação

Não é necessário desativar o modo de manutenção para modificar estas propriedades.

-
- Etapa 1** Inicie sessão no site de Administração.
- Etapa 2** Selecione **Sistema** e selecione **Exibir Mais** na seção Servidores.
- Etapa 3** Na seção **Servidor SMTP**, selecione **Editar**.
- Etapa 4** Insira o nome de domínio totalmente qualificado (FQDN) de um servidor de e-mail que o sistema usará para enviar e-mails.
- Etapa 5** (Opcional) Selecione **TLS habilitado** para ativar o Transport Layer Security (TLS). (A autenticação básica está habilitada por padrão.)
- Etapa 6** (Opcional) Edite o campo **Porta** para alterar o valor padrão.
Os números de porta padrão SMTP são 25 ou 465 (porta SMTP segura).
- Observação** O nó da Web e o nó da Administração enviam solicitações SMTP para o servidor de e-mail configurado. Se houver um firewall entre as máquinas virtuais internas da Web e de Administração e o servidor de e-mail, o tráfego SMTP pode ser bloqueado. Para garantir que a configuração do servidor de e-mail e a notificação de e-mail funcionem corretamente, a porta 25 ou 465 (número de porta SMTP segura) deve estar aberta entre o servidor de e-mail e as máquinas virtuais da Web e de Administração.
- Etapa 7** (Opcional) Ative a autenticação do servidor de e-mail, selecione **Autenticação do servidor habilitada**. Se você ativar a autenticação, insira as credenciais **Nome de usuário** e **Senha** necessárias para o sistema acessar o servidor de e-mail corporativo.
Os e-mails do sistema são enviados pelo admin@<WebEx-site-URL>. Verifique se o servidor do e-mail pode reconhecer este usuário.
Para sistemas micro, pequenos ou médios, as notificações de e-mail vêm das máquinas virtuais de administração (sistema primário ou de alta disponibilidade).
Para sistemas grandes, as notificações de e-mail vêm das máquinas virtuais da web (sistema primário ou de alta disponibilidade). Em um sistema grande, existem três máquinas virtuais da web no sistema primário e uma máquina virtual da web no sistema de alta disponibilidade.
- Etapa 8** Selecione **Salvar**.
-

Próximos passos

Consulte também [Ativação ou desativação de usuários e administradores a partir da página Usuários](#), na página 124, [Adicionar usuários](#), na página 121 e [Editando Usuários](#), na página 122.

Definindo o fuso horário, idioma e localidade

Antes de iniciar

Se você estiver executando o Windows 7 e o seu site Cisco WebEx em uma Internet Explorer 10 abrir o navegador, você pode querer selecionar o documento internet Explorer 10 para certificar-se de que todos os botões no aplicativo funcionar corretamente.

- Selecione **Ferramentas > Ferramentas de desenvolvimento**.

- No topo da janela Ferramentas de desenvolvimento, selecione **Modo documento: Normas do IE7 > Normas do Internet Explorer 10.**

-
- Etapa 1** Do site da Administração, navegue até **Configurações > Informações da empresa**
Etapa 2 Selecione o **Fuso horário** local para este sistema a partir da lista suspensa.
Etapa 3 Selecione o **Idioma**.
Etapa 4 Selecione a **Localidade** do país
Etapa 5 Selecione **Salvar**.
-

Criando contas de administrador

O sistema cria uma conta de Primeiro administrador. Este administrador deve iniciar sessão no sistema, criar uma senha e adicionar outros administradores. Até então, nenhum outro administrador pode ter acesso ao sistema. Como parte do processo, o Primeiro administrador pode criar uma conta de Auditor, separando o administrador e o auditor. Isto pode ser feito como parte do processo de implantação ou o Primeiro administrador pode criar um Auditor (**Usuários > Editar usuários**). (Consulte [Adicionando uma função de auditor, na página 51.](#))

Antes de iniciar

Um servidor de correio para o sistema usar para enviar e-mails aos administradores deve ser configurado. Consulte [Configurando um servidor de e-mail \(SMTP\), na página 49](#) para obter instruções.

-
- Etapa 1** Insira o primeiro e último nome do administrador.
Etapa 2 Insira o endereço de e-mail completo do administrador e confirme-o inserindo-o novamente.
Etapa 3 (Opcional) Selecione **Criar uma conta de auditor** para adicionar um Auditor ao sistema.
Etapa 4 Selecione **Próximo** para criar a senha inicial.
Etapa 5 Insira uma senha e confirme-a inserindo-a novamente.
Etapa 6 Selecione **Enviar** para iniciar sessão no site da Administração WebEx.
Etapa 7 Inicie sessão no sistema e adicione administradores e usuários. Após a criação de cada nova conta, o sistema envia um e-mail para essa pessoa, dando boas-vindas e solicitando que ela inicie sessão e altere a senha inicial. Após o primeiro início de sessão, é oferecido a cada administrador um tutorial do sistema. Os administradores podem visualizar o tutorial imediatamente ou visualizá-lo sob demanda.
-

Adicionando uma função de auditor

O primeiro administrador tem a função de auditor, por padrão, e é o único que pode ativar a função de Auditor de outro usuário. Ao fazer isso, os privilégios do Auditor são tirados do Primeiro Administrador. Se um Auditor também é um Administrador do Sistema, essa pessoa tem uma função de Auditoria do Sistema.

A função de Auditor separa ações administrativas do monitoramento do sistema, como segue:

- Ative ou desative a auditoria.
- Configure o CWMS para sincronizar com os servidores syslog remotos.
- Execute a purgação de registros.
- Configure alarmes para a partição de registros.
- Gere capturas de registros.
- Se as funções de Administrador e Auditor não estão separadas, apenas as funções de Administrador e Organizadores existem; os administradores possuem toda a autoridade.
- Se as funções de Administrador e Auditor são separadas quando o sistema é implantado, uma função de Primeiro administrador é criada (descrita como a *conta de emergência*). Após a implantação do sistema, apenas a conta de emergência de Primeiro Administrador pode criar um Auditor, tirando os privilégios de Auditor dos administradores. O Primeiro Administrador pode criar quantos auditores como desejado após o sistema ter sido implantado.
- O Auditor é apenas local; ele não pode vir da sincronização com alguma base de usuários externos.
- Os parâmetros do Auditor (como o nome) podem ser modificados, mas uma vez criada, a função de Auditor não pode ser desativada ou designada a outra ID de usuário.
- Um Auditor não pode modificar os parâmetros do usuário.
- Um Auditor não tem privilégios de Organizador e não pode agendar reuniões usando a conta de Auditor. Um Auditor pode participar de reuniões como participante.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecionar **Usuários**.

Etapa 3

Selecione um usuário.

A janela **Editar usuários** é exibida.

Etapa 4

Selecione o tipo de conta de **Auditor**.

Etapa 5

Selecione **Salvar**.

É enviado um e-mail de boas-vindas ao Auditor.

Sobre o teste do sistema

A maioria dos testes do sistema são realizados utilizando o sistema CWMS, por exemplo por [Usando o Teste de Reuniões, na página 86](#) e [Utilizar o teste de recursos do sistema, na página 86](#).

Ao testar um sistema atualizado, você pode manter o sistema original até que você tenha terminado de testar o sistema atualizado (mas como eles compartilham alguns parâmetros, tais como endereços de IP, você não pode ligar os dois sistemas ao mesmo tempo). Quando estiver satisfeito com os resultados dos testes no sistema

atualizado, você pode remover (para sempre) o sistema original. Certifique-se de que seu sistema atualizado esteja em execução antes de remover o sistema original. Isso evita a remoção acidental do arquivo de disco da máquina virtual de base (VMDK), que pode ser acessado pelo sistema atualizado.

Alguns dos testes recomendados para executar no sistema são:

- Adicionar, editar, ativar e desativar usuários. Consulte [Gerenciando Usuários, na página 111.](#))
- Agende e realize uma reunião.
- Reagende uma reunião existente.
- Exclua uma série de reuniões agendadas.
- Adicione e abra um anexo de reunião a partir do convite de reunião.
- Grave uma reunião e reproduza a gravação.

O sistema também pode ser testado:

- [Confirmando que sua rede está configurada corretamente, na página 29](#)
- [Verificando o sistema, na página 29](#)
- [Verificando se o sistema primário e o sistema HA estão na mesma versão](#)
- Confirmando que o sistema primário irá ser transferido para o sistema HA, removendo a conexão física com o sistema primário e verificando se o Cisco WebEx está sendo executado no sistema HA.



Alterando o sistema após a implantação

Este capítulo descreve a preparação necessária antes de executar os procedimentos de alteração do sistema:

- [Atualizando o Sistema, na página 69](#)
- [Atualizando o Sistema, na página 77](#)
- [Expandindo o seu Sistema para Tamanho de Sistema Maior, na página 63](#)
- [Preparando para um Procedimento de Alteração do Sistema, página 55](#)

Preparando para um Procedimento de Alteração do Sistema

Os eventos que são de alteração do sistema e exigem preparação antecipada pelo administrador são:

- Adicionando ou removendo um sistema de alta disponibilidade (HA) Consulte [Adicionar um Sistema de Alta Disponibilidade, na página 57.](#))
- Atualizar o sistema para uma versão superior (usando um arquivo de atualização ISO). (Consulte [Preparando-se para atualizar um sistema existente.](#))
- Atualizar o sistema com a implantação de um sistema paralelo e transferir os dados do sistema original para o sistema atualizado (usando um arquivo OVA). (Consulte [Preparando para atualizar um centro de dados, na página 77.](#))
- Expansão do sistema para um tamanho maior. (Consulte [Preparando para a Expansão do Sistema, na página 63\).](#)



Observação

Como este procedimento exige acesso exclusivo ao sistema, os usuários não poderão acessar o sistema para reuniões. Certifique-se de agendar este procedimento durante um horário que seja menos prejudicial aos seus usuários.

Certifique-se de coordenar com outros administradores de sistemas antes de iniciar um procedimento de alteração de sistema. Outros administradores do sistema não devem acessar o sistema durante este procedimento. Se o fizerem, suas alterações não serão salvas e o resultado pode ser imprevisível.

Os backups não são necessários para essas ações. Se você não precisa criar backups de suas máquinas virtuais, então você não precisa concluir este procedimento. Entretanto, como uma boa prática, recomendamos a criação de um backup. Para detalhes completos sobre este backup, consulte [Criando um Backup Usando o VMware vCenter](#), na página 6, o *Guia de Administração do VMware Data Recovery* ou o *Guia de Administração do vSphere Data Protection*.



CAPÍTULO 7

Adicionar um Sistema de Alta Disponibilidade

- Preparando para adicionar Alta Disponibilidade (HA) em um sistema, página 57
- Implantando um sistema de alta disponibilidade (HA), página 58
- Vinculando um sistema de alta disponibilidade para um sistema primário, página 59
- Comportamento do sistema de alta disponibilidade após a falha de componentes, página 60
- Removendo a alta disponibilidade de um sistema, página 62

Preparando para adicionar Alta Disponibilidade (HA) em um sistema

Um sistema de alta disponibilidade (HA) é um sistema local, redundante, que é criado, em seguida, adicionado a um sistema primário. No caso de uma falha da máquina virtual, o sistema cai novamente no sistema de HA.

Se você está planejando adicionar HA a um sistema, você também está planejando atualizar o sistema, recomendamos que você adicione HA antes de atualizar o sistema, então atualize o sistema combinado (primário e HA); o sistema de HA é atualizado automaticamente quando o sistema principal é atualizado. Se você atualizar o sistema primeiro, para adicionar HA, você deve implantar de forma independente, depois atualizar o sistema HA (assim os sistemas primário e HA ficam na mesma versão).

O sistema de HA tem as seguintes restrições:

- Um sistema executando HA não pode registrar Vários centros de dados (MDC). (Para remover a HA, consulte [Removendo a alta disponibilidade de um sistema, na página 62](#)).
- O tamanho do sistema HA deve ser o mesmo que o sistema primário.
- O sistema HA deve estar na mesma versão original que o sistema primário.
Se você atualizar o sistema primário, o sistema HA deve ser atualizado.
- Se o sistema primário tem atualmente HA e você está implantando um novo sistema HA, você não pode reutilizar as máquinas virtuais no sistema HA original. Remova as máquinas virtuais HA antigas antes da implantação do novo sistema HA com novas máquinas virtuais.
- Como esse processo adiciona novas máquinas virtuais ao seu sistema, o certificado de segurança atual se tornará inválido e exigirá uma atualização a menos que você esteja usando um certificado autoassinado.

- Seu sistema HA deve ser configurado com o mesmo OVA e patch que seu sistema primário. Se as versões dos sistemas primário e de alta disponibilidade não são iguais, você será instruído a atualizar para a versão superior dos dois.
- As máquinas virtuais internas do sistema HA devem estar na mesma sub-rede que as máquinas virtuais internas do sistema primário.
- Se você adicionou o acesso público ao sistema primário, você deve adicioná-lo ao sistema HA. Além disso, a máquina virtual de Proxy Reverso da Internet do sistema HA deve estar na mesma sub-rede que a máquina virtual de Proxy Reverso da Internet do sistema primário.



Observação

A maioria dos recursos no seu sistema HA são proibidos. Por exemplo, você não tem acesso ao sistema HA para atualizar, configurar o SNMP, acessar o armazenamento ou configurar servidores de e-mail. Você pode ver as propriedades do sistema, mas a modificação do sistema HA é proibida.

Além disso, o balanceamento de carga não é configurável; é automático e incorporado no sistema.

Antes de Começar

As seguintes condições devem ser satisfeitas antes de adicionar HA a um sistema primário:

- Verifique:
 - O sistema primário alvo é implantado e não faz parte de um MDC.
 - Há uma rede redundante entre as máquinas virtuais.
 - A rede é uma rede de alta largura de banda de 10 Gbps.
 - Network Time Protocol (NTP) configurado no sistema HA e primário, e os relógios que são sincronizados.
- Crie um backup do sistema primário. Consulte [Criando um Backup Usando o VMware vCenter](#), na página 6.
- Verifique se todas as máquinas virtuais estão funcionando normalmente. Determine o estado da máquina virtual, visualizando o Monitoramento de Sistema como descrito em [Sobre o Seu Painel](#).
- Recomendamos que você tire uma fotografia da máquina virtual de alta-disponibilidade antes de proceder com este procedimento. Refaça o procedimento copiando a fotografia em caso de erro.
- Anote o nome de domínio totalmente qualificado (FQDN) da máquina virtual de alta disponibilidade; você deve saber o FQDN para adicionar alta disponibilidade ao sistema primário.

Implantando um sistema de alta disponibilidade (HA)

A Alta Disponibilidade (HA) é implantada como um sistema primário, exceto que durante a implantação o sistema a identifica como um sistema HA. O sistema HA é então ligado ao sistema primário que utiliza o sistema HA como uma alternativa em caso de falha do sistema primário. Uma falha no sistema primário é visível aos usuários.

Para adicionar HA a um sistema:

-
- Etapa 1** Implante um sistema paralelo usando [Implantando um sistema automaticamente, na página 11](#) ou [Implantando um sistema manualmente, na página 31](#). Quando o processo pergunta se você está implantando um sistema primário ou HA, escolha HA. Recomendamos que você use o mesmo processo para implantar o sistema HA que você usou para implantar o sistema primário. Se você não sabe qual processo foi usado para implantar o sistema primário, utilize o processo [Implantando um sistema automaticamente, na página 11](#), a menos que você esteja implantando um sistema grande (2000 usuários simultâneos). Todos os sistemas grandes requerem [Implantando um sistema manualmente, na página 31](#).
- Etapa 2** Verifique se as versões do sistema primário e HA coincidem:
- 1 Em uma janela de navegador separada, inicie sessão no site de Administração WebEx do sistema primário.
 - 2 Na guia **Painel**, verifique se o número da versão do sistema primário no painel **Sistema** corresponde à versão HA. Se as versões coincidem, continue.
- Se o sistema primário está em uma versão posterior do que o sistema HA, então você precisa reimplantar o sistema HA usando um arquivo OVA com uma versão correspondente ao software ou atualizar o sistema HA.
-

Próximos passos

Vincule o sistema HA ao sistema primário usando [Vinculando um sistema de alta disponibilidade para um sistema primário](#).

Ao atualizar um sistema de alta disponibilidade, depois de reiniciar o sistema e o processo de reinicialização parecer estar completo, recomendamos que você aguarde mais 15 minutos antes de iniciar o procedimento de adicionar sistema de alta disponibilidade.

Vinculando um sistema de alta disponibilidade para um sistema primário

Para vincular o sistema primário a um sistema de HA implantado completando a integração de HA no sistema primário:

Antes de iniciar

Verifique se este sistema não é parte de um sistema com Vários centros de dados (MDC). (HA não é suportado em um ambiente MDC).

Crie um sistema de alta disponibilidade (HA) usando o mesmo processo que você usou para criar o sistema primário descrito em [Implantando um sistema de alta disponibilidade \(HA\), na página 58](#).

-
- Etapa 1** Notifique os usuários e administradores de que o sistema está sendo colocado em modo de manutenção. Ao agendar uma janela de manutenção para executar esta tarefa, esteja ciente de que o sistema executa uma reinicialização do sistema quando você desativa o modo de manutenção. Uma reinicialização do sistema leva aproximadamente 30 minutos, dependendo do tamanho do seu sistema.

- Etapa 2** Inicie sessão no site de administração do sistema primário.
- Etapa 3** Selecione **Ativar o Modo de Manutenção**.
- Etapa 4** Na seção de Sistema, selecione o link **Exibir Mais**.
- Etapa 5** Selecione **Adicionar Sistema de Alta Disponibilidade**.
- Etapa 6** Siga as instruções na página **Propriedades do Sistema** para adicionar o sistema de HA.
- Etapa 7** Insira o nome de domínio totalmente qualificado (FQDN) da máquina virtual do site de Administração do sistema de alta disponibilidade e selecione **Continuar**.
A disponibilidade do sistema primário e do sistema de HA é validada. Se ambos os sistemas estão prontos, então você vai ver um botão verde **Adicionar**. (Não selecione-o se o sistema não estiver no modo de manutenção.) Se um dos sistemas não estiver pronto, uma mensagem de erro é exibida. Corrija o erro e tentar o procedimento novamente.
- Etapa 8** Selecione **Adicionar**.
Observação Se o "Código de erro: Base de dados-64" aparecer, repita este procedimento utilizando uma foto instantânea das máquinas virtuais de alta disponibilidade.
Seu sistema de alta disponibilidade é adicionado e automaticamente configurado para servir como um backup no caso de uma falha do sistema primário.
- Etapa 9** Selecione **Desative o Modo de Manutenção** e **Continuar** para confirmar.
O sistema reinicia. Você pode iniciar sessão novamente no site de Administração, após a reinicialização. (Para remover HA, consulte [Removendo a alta disponibilidade de um sistema, na página 62](#)).

Comportamento do sistema de alta disponibilidade após a falha de componentes

Quando mídia específica e componentes da plataforma executando em uma máquina virtual desligam, esses componentes são automaticamente reiniciados pelo sistema. As reuniões afetadas passam a falha para outros recursos disponíveis na mesma ou em outra máquina virtual no sistema (para outra que não seja um sistema autônomo de 50 usuários).

Sistemas de Alta Disponibilidade

Em sistemas de alta disponibilidade (HA), o Cisco WebEx Meetings Server irá se recuperar para estes componentes quando houver uma falha de componente único:

- Um serviço único em uma máquina virtual.
- Uma máquina virtual.
- Um único servidor físico ou blade, que organiza até duas máquinas virtuais (desde que o layout da máquina virtual esteja em conformidade com as especificações listadas no *Guia de planejamento do Cisco WebEx Meetings Server*).
- Um link de rede única, assumindo que a rede é provisionada em uma forma totalmente redundante.
- Um único nó do Cisco Unified Communications Manager (CUCM), assumindo que o CUCM é provisionado em uma forma redundante.

Após a falha do componente único, o sistema Cisco WebEx Meetings Server comporta-se como segue:

- Por um período de até três minutos, o compartilhamento de aplicativos, a conexão de voz de áudio usando o computador e vídeo podem ser interrompidos. O Cisco WebEx Meetings Server permite três minutos para a falha ser detectada e para reconectar automaticamente todos os clientes afetados da reunião. Os usuários não necessitam fechar seus clientes da reunião e voltar a participar da reunião.
- Algumas falhas podem causar a desconexão das conexões de teleconferência de áudio. Se isso acontecer, os usuários terão de se reconnectar manualmente. A reconexão deve ocorrer dentro de dois minutos.
- Para algumas falhas, nem todos os clientes e reuniões são afetados. As conexões da reunião são normalmente redistribuídas entre várias máquinas virtuais e organizadores.

Informações adicionais de um sistema de 2000 usuários

Um sistema de 2000 usuários fornece alguma funcionalidade de alta disponibilidade sem a adição de um sistema de HA. Para um sistema de 2000 usuários sem alta disponibilidade:

- Seu sistema ainda funciona após a perda de qualquer uma das máquinas virtuais de mídia ou web, mas a capacidade do sistema será prejudicada.
- A perda da máquina virtual de administração torna o sistema não utilizável.

Para um sistema de 2000 usuários com alta disponibilidade:

- A perda de qualquer uma das máquinas virtuais (administração, mídia ou web) não afeta o seu sistema. Seu sistema continuará funcionando em plena capacidade, mesmo com a perda de qualquer servidor físico que hospeda as máquinas virtuais primárias (administração e mídia ou web e mídia) ou as máquinas virtuais HA (administração e mídia ou web).
- Quando uma máquina virtual com falha é reiniciada, ela volta a participar do sistema e o sistema retorna ao seu estado normal de trabalho.
- Quando uma máquina virtual de mídia falha, as reuniões organizadas no servidor são brevemente interrompidas, mas a reunião falha em uma máquina virtual alternativa de mídia. Os usuários devem participar novamente das sessões de áudio do desktop e vídeo manualmente.
- Quando uma máquina virtual da web falha, as sessões web existentes organizadas nessa máquina virtual também falham. Os usuários devem iniciar sessão no site WebEx novamente e estabelecer uma nova sessão do navegador que será organizada em uma máquina virtual web alternativa.
- Quando uma máquina virtual de administração falha, todas as sessões de administrador existentes também falham. Os administradores devem iniciar sessão novamente no site da Administração e estabelecer uma nova sessão do navegador que será organizada em uma máquina virtual de administração alternativa. Além disso, pode haver uma breve interrupção a qualquer administrador existente ou nas sessões de reunião do usuário final.

Removendo a alta disponibilidade de um sistema

- Etapa 1** Inicie sessão no site da Administração.
- Etapa 2** Selecione **Ativar o Modo de Manutenção**.
- Etapa 3** Selecione **Exibir mais** na seção Sistema.
- Etapa 4** Selecione **Remover Sistema de Alta Disponibilidade**.
A página **Remover Sistema de Alta Disponibilidade** aparece exibindo o nome do domínio totalmente qualificado (FQDN) do seu sistema de alta disponibilidade.
- Etapa 5** Selecione **Continuar**.
Depois de ter removido um sistema de alta disponibilidade, você não pode adicionar o mesmo sistema de alta disponibilidade novamente no sistema. Para reconfigurar a alta disponibilidade, você precisa começar novamente através da reimplementação de um sistema de alta disponibilidade do arquivo OVA. Consulte [Adicionar um Sistema de Alta Disponibilidade, na página 57](#) para obter mais informações.
O seu sistema de alta disponibilidade está removido.
- Etapa 6** Abra o VMware vCenter e remova o sistema de alta disponibilidade usando o comando **Excluir do disco**.
- Etapa 7** Selecione **Desative o Modo de Manutenção** e **Continuar** para confirmar.
O sistema se reinicia.
-



CAPÍTULO 8

Expandindo o seu Sistema para Tamanho de Sistema Maior

- Preparando para a Expansão do Sistema, página 63
- Expandindo o Tamanho do Sistema, página 64

Preparando para a Expansão do Sistema

A expansão do sistema requer a implantação de um novo sistema primário, bem como a transferência dos dados do sistema a partir do sistema original para o sistema expandido. A expansão de um sistema exige que as licenças existentes do organizador sejam reorganizadas no sistema expandido. Consulte [Reorganizando licenças após uma grande modificação do sistema, na página 253.](#))

Um sistema de Vários centros de dados (MDC) não pode ser expandido. Para expandir um sistema MDC:

- Remova os centros de dados secundários (consulte [Removendo um centro de dados, na página 263](#)).
- Expanda o sistema de centro primário de dados simples.
- Obtenha licenças MDC para o sistema expandido e carregue as licenças no sistema primário.
- Crie um novo centro de dados secundário do mesmo tamanho que o centro de dados primário.
- Participe dos centros de dados (consulte [Unindo um centro de dados a um sistema MDC, na página 260](#)).

Considerações para um sistema expandido

Considere o seguinte:

- Um orçamento para qualquer hardware adicional.
- O número previsto de reuniões simultâneas e o tamanho médio ao longo dos próximos meses.
- Quando um sistema original é atualizado ou expandido, um sistema paralelo é criado. Se houver tempo restante no período de teste do sistema original, esse tempo é transferido para o sistema atualizado ou expandido. As licenças dos Organizadores permanentes válidas no sistema original podem ser transferidas para um sistema atualizado ou expandido ao *reorganizar* as licenças.

Obtendo as informações necessárias para a expansão do sistema

Obtenha o arquivo OVA usado para instalar a versão do sistema existente e completar a lista de verificação de expansão:

Nome do Campo	Valor atual para o seu sistema
URL do Site WebEx	
URL do Site de Administração	
Endereço VIP Privado	
Endereço VIP Público	

Expandindo o Tamanho do Sistema**Antes de iniciar**

Ao expandir um sistema com Vários centros de dados (MDC), é necessário primeiro remover os centros de dados secundários. Consulte [Removendo um centro de dados, na página 263.](#)

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Se você estiver expandindo um sistema MDC, remova todos, menos o centro de dados primário.

Consulte [Removendo um centro de dados, na página 263.](#)

Etapa 3

Se você estiver expandindo um sistema MDC, crie um novo centro de dados executando o Cisco WebEx Meeting Server para unir depois que o sistema primário for expandido.

Consulte [Registrando centros de dados para criar um sistema de vários centros de dados \(MDC\), na página 255.](#)

Etapa 4

Criar um backup do sistema original. Consulte [Criando um Backup Usando o VMware vCenter, na página 6.](#)

Etapa 5

Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior.](#)

Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#)

Ativar o modo de manutenção em todos os centros ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 6

Selecione **Continuar**.

Etapa 7

Selecione **Sistema > Ver mais**.

Etapa 8

Selecione **Expandir Tamanho do Sistema**.

Etapa 9

Selecione **Continuar**.

Seu sistema verifica a conectividade com as máquinas virtuais. Se há problemas de conectividade com uma ou mais máquinas virtuais, você deve corrigir os problemas antes de continuar. Se não houver problemas de conectividade, o sistema realiza um backup automático. Após a conclusão do backup, você será notificado de que você pode prosseguir com a sua expansão.

- Etapa 10** Usando o cliente VMware vSphere, selecione **Ligar > Desligar convidado** nas máquinas virtuais para o sistema original. Consulte [Implementando o arquivo OVA do cliente VMware vSphere, na página 18.](#))
- Etapa 11** Usando o cliente vSphere, implante a máquina virtual de Administração para o novo tamanho do sistema. Se você estiver executando uma expansão automática, criaremos as outras máquinas virtuais no seu sistema. Se você estiver executando uma expansão manual, você pode criar as outras máquinas virtuais no seu sistema.
- Etapa 12** Anexe o **Disco rígido 4** da máquina virtual de Administração do sistema para a máquina virtual de Administração para o sistema expandido. Consulte [Anexando um Arquivo VMDK Existente para uma Nova Máquina Virtual, na página 8.](#))
- Etapa 13** Ligue a máquina virtual de Administração para o sistema expandido e anote a URL de implantação. Se você estiver realizando uma expansão automática, ligaremos as outras máquinas virtuais no seu sistema. Se você estiver executando uma expansão manual, ligue as outras máquinas virtuais no seu sistema.
- Etapa 14** Insira a URL de implantação em um navegador da internet e continue a implantação do seu sistema expandido.
- Etapa 15** Selecione o seu idioma preferido para a implantação do sistema expandido. Consulte [Selecionando o Seu Idioma para Instalação, na página 21.](#))
- Etapa 16** Selecione **Expandir a capacidade do sistema existente > Próximo.**
- Etapa 17** Confirme o tamanho do sistema. (Consulte [Confirmando o Tamanho do Seu Sistema, na página 22.](#)) Este tamanho de sistema deve ser maior ou igual ao sistema original.
- Etapa 18** Selecione **Instalar um sistema primário.**
- Etapa 19** Selecione a implantação automática ou manual. Consulte [Escolhendo o tipo de implantação, na página 22.](#)) Se você escolheu implantação manual, continue para a próxima etapa. Se você escolheu a implantação automática:
- Insira as credenciais vCenter para que possamos implantar as máquinas virtuais para você. (Consulte [Fornecendo Credenciais Vmware vCenter, na página 23.](#))
 - Selecione o organizador ESXi, armazenamento de dados e o grupo de porta da máquina virtual para a máquina virtual de mídia. Consulte [Escolha as Configurações do vCenter para a sua Máquina Virtual de Mídia, na página 24.](#))
 - Insira o nome de domínio totalmente qualificado na máquina virtual de mídia. Se você já atualizou o servidor DNS com entradas para o sistema expandido, então pesquisaremos o endereço de IP para você. (Consulte [Inserindo informações de Rede para a Máquina Virtual de Mídia, na página 24.](#))
- Use o mesmo arquivo OVA que você usou para implantar o seu sistema original e implantar a máquina virtual de Administração para o novo tamanho de sistema.
- Seu sistema avisará quando a expansão estiver concluída.
- Etapa 20** Se você quiser o acesso público para o seu sistema expandido, certifique-se que a caixa de seleção **Criar uma máquina de virtual de Proxy Reverso da Internet** esteja marcada. Caso contrário, desmarque esta caixa de seleção. (Consulte [Adicionando acesso público ao seu sistema utilizando IRP, na página 138.](#)) Se você optou por adicionar o acesso público:
- Selecione o organizador ESXi, armazenamento de dados e o grupo de porta da máquina virtual para a máquina virtual de proxy reverso da Internet (IRP).
 - Informe o nome de organizador e as informações de rede para a máquina virtual IRP.
- Etapa 21** Insira o endereço VIP público para a URL do site WebEx. (Consulte [Inserindo o Endereço VIP Público, na página 26.](#))

Você pode inserir o mesmo endereço VIP público que você usa para o sistema original ou alterar para um novo endereço de IP. Se você alterá-lo, então faça as atualizações necessárias no servidor DNS.

- Etapa 22** Insira o endereço VIP privado para a URL do site WebEx. (Consulte [Inserindo o Endereço VIP Privado, na página 27.](#))
Você pode inserir o mesmo endereço VIP privado que você usa para o sistema original ou alterar para um novo endereço de IP. Se você alterá-lo, então faça as atualizações necessárias no servidor DNS.
- Etapa 23** Insira a URL do site WebEx comum. (Consulte [Inserindo as URLs do site WebEx comum e do site de administração, na página 28.](#))
Os participantes acessam esta URL para organizar e participar de reuniões Esta URL resolve o endereço VIP privado ou o endereço VIP público, dependendo se você está ou não usando um DNS split-horizon.
Você pode inserir a mesma URL do site WebEx que você usa para o seu sistema original ou alterar para uma nova. Se você alterá-lo, então faça as atualizações necessárias no servidor DNS.
Guarde a URL do site original no servidor DNS. Redirecione a URL do site original para a URL do novo site. Se os usuários tentarem usar a URL original e você não tiver redirecionado para a nova URL, eles não serão capazes de organizar ou participar de reuniões.
- Etapa 24** Insira a URL do site de administração WebEx para que os administradores acessem o site de Administração Cisco WebEx. (Consulte [Inserindo as URLs do site WebEx comum e do site de administração, na página 28.](#))
Esta URL resolve para o endereço VIP privado.
Você pode inserir a mesma URL do site WebEx que você usa para o sistema original ou alterar para uma nova. Se você alterá-lo, então faça as atualizações necessárias no servidor DNS.
Guarde a URL do site original no servidor DNS. Redirecione a URL do site original para a URL do novo site. Se os usuários tentarem usar a URL original e você não tiver redirecionado para a nova URL, eles não serão capazes de organizar ou participar de reuniões.
- Etapa 25** Verifique se você fez todas as alterações de configuração necessárias de rede, servidor DNS e firewall no seu sistema. Consulte [Confirmando que sua rede está configurada corretamente, na página 29.](#))
- Etapa 26** Uma vez que suas máquinas virtuais foram implantadas com sucesso, selecione **Próximo** para continuar com a verificação do sistema. Consulte [Implantação de máquinas virtuais, na página 46.](#))
Junto com a verificação do sistema, atualizamos o sistema expandido com atualizações necessárias para corresponder com a versão do software do sistema original, antes da expansão (Estas atualizações podem levar até 1 hora). Ao concluir, o sistema reinicia. Consulte [Verificando o sistema, na página 29.](#))
- Etapa 27** Selecione **Reiniciar.**
- Etapa 28** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 29** Se você está se expandindo um sistema MDC, una-o ao sistema MDC. Consulte [Unindo um centro de dados a um sistema MDC, na página 260.](#))
- Etapa 30** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior.](#)
Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Etapa 31 Selecione **Continuar**.

O sistema reinicia. Você pode iniciar sessão no site de Administração, após a reinicialização.

Observação Se você criou originalmente as máquinas virtuais usando o arquivo OVA do Cisco WebEx Meetings Server 2.0, então talvez você visualize uma mensagem de erro "Não é possível acessar o servidor". Se isso acontecer, use o cliente VMware vSphere e "Reiniciar convidado" para todas as máquinas virtuais no sistema.

Etapa 32 Teste o sistema expandido. Consulte [Sobre o teste do sistema, na página 52.](#))

Se a expansão for mal sucedida, então, desligue o sistema expandido e ligue o sistema original. Se necessário, entre em contato com o TAC da Cisco para mais assistência.

Etapa 33 Reorganize as licenças do Organizador ou as licenças MDC como apropriado para o sistema expandido. (Consulte [Reorganizando licenças após uma grande modificação do sistema, na página 253.](#))



CAPÍTULO 9

Atualizando o Sistema

- Sobre a atualização de um sistema, página 69
- Conectando a uma Imagem ISO da Unidade de CD/DVD, página 70
- Atualizando os centros de dados versão 2.5 e superior com inatividade do sistema, página 71
- Atualizando um sistema com vários centros de dados com tempo de inatividade zero, página 73

Sobre a atualização de um sistema

Em um sistema de centro de dados único (SDC), o centro de dados deve ser colocado no Modo de Manutenção. Em um sistema de Vários centros de dados (MDC), todos os centros de dados podem ser derrubados para a atualização, ou em alguns casos, os centros de dados podem ser derrubados um de cada vez. O processo para derrubar os centros de dados um de cada vez e o serviço de manutenção para os usuários são referidos como uma atualização com tempo de inatividade zero. Verifique as notas de versão para as quais a versão do Cisco WebEx Meeting Server é elegível para uma atualização com tempo de inatividade zero. Se você estiver executando uma atualização com tempo de inatividade zero, recomendamos que você atualize todos os outros centros de dados no sistema, logo que possível, após a atualização do primeiro centro de dados.

Uma *atualização* é definida como uma substituição do sistema para implantar grandes modificações que fizemos ao sistema. Por exemplo, substituir um sistema atualmente executando a versão 1.5 para executar a versão 2.0 que inclui suporte para um novo sistema operacional. Uma *atualização* é definida como a substituição de um sistema existente (original) para tirar vantagem das modificações que fizemos para melhorar o sistema. Uma *expansão* é definida como a ampliação de um sistema existente, mas não a alteração da versão do aplicativo. Por exemplo, você pode atualizar um sistema a partir da versão 1.5 para 1.5MR, atualizar um sistema 1.5 para 2.0 ou expandir um sistema de 800 usuários para 2000 usuários. Em todos os casos, os processos incluem a transferência de todos os dados a partir do sistema original para o sistema atualizado ou expandido.

Use a tabela a seguir para determinar se você deve executar uma atualização do sistema ou atualizar um centro de dados para executar uma versão específica do Cisco WebEx Meetings Server.

Versão instalada	Para a versão...	Atualizar	Atualizar
1.5MR3 ou superior	2.0 ou 2.5 ³	X	
1.0MR, 1.1MR ou 1.5MR	2.5	X	

Versão instalada	Para a versão...	Atualizar	Atualizar
2.0MR3 ou superior	2.5		X
2.5 Único centro de dados (SDC)	Qualquer 2.5MR		X
2.5 Vários centros de dados (MDC)	Qualquer 2.5MR		X

³ Recomendamos que qualquer versão de 1.0, 1.1 ou 1.5 seja atualizada para a versão 1.5MR3 dos arquivos OVA e ISO antes de atualizar para a versão 2.5.

O procedimento de atualização completo, incluindo o backup das suas máquinas virtuais, pode levar até uma hora, dependendo do:

- Tamanho do sistema
- Tamanho do banco de dados
- Velocidade do carregamento no vCenter



Observação

O sistema **CWMS** é o nome padrão do centro de dados após uma atualização para a versão 2.5; não é traduzido do inglês para algum dos outros idiomas.

Conectando a uma Imagem ISO da Unidade de CD/DVD

Para a atualização mais rápida, recomendamos que você monte a imagem ISO no armazenamento de dados vCenter. No entanto, se você colocá-la em um disco local acessível ao cliente vSphere, certifique-se que o cliente vSphere tenha uma conexão com fio na intranet da sua empresa (não sobre VPN).

Para colocar a imagem ISO no armazenamento de dados do vCenter e conectar ao CD/DVD, execute os seguintes passos:

-
- Etapa 1** Obtenha a imagem ISO desejada da Cisco em <http://www.cisco.com/cisco/software/navigator.html>.
 - Etapa 2** Verifique se você possui as permissões adequadas.
 - Etapa 3** Selecione o organizador ESXi para a máquina virtual de administração *do centro de dados a ser atualizado*. Selecione a guia **Sumário** e clique duas vezes no nome de **datastore1** em **Armazenamento**.
 - Etapa 4** Na janela **Datastore e Datastore clusters** selecione **Procurar esse datastore**.
 - Etapa 5** Selecione o ícone de seta verde (Carregar arquivo) e carregue a atualização do arquivo ISO.
 - Etapa 6** Selecione a máquina virtual de Administração no inventário VMware vCenter.
 - Etapa 7** Selecione o ícone de **CD/DVD** para a máquina virtual de Administração.
 - Etapa 8** Selecione **Unidade 1 de CD/DVD > Conectar à imagem ISO** em um disco local ou em um armazenamento de dados.
 - Etapa 9** Confirme se a unidade de CD/DVD está conectada.

- a) Clique com o botão direito do mouse no nome da máquina virtual de Administração no inventário vCenter e selecione **Editar Configurações...**
 - b) Na guia **Hardware**, selecione **CD/DVD drive 1**.
 - c) Se desmarcado, verifique a caixa de diálogo **Conectado**.
 - d) Selecione **OK**.
-

Próximos passos

Atualize o centro de dados, seguindo as instruções em [Atualizando os centros de dados versão 2.5 e superior com inatividade do sistema, na página 71](#).

Atualize o centro de dados com tempo de inatividade zero, seguindo as instruções em [Atualizando um sistema com vários centros de dados com tempo de inatividade zero, na página 73](#).

Atualizando os centros de dados versão 2.5 e superior com inatividade do sistema

Este procedimento descreve como atualizar um sistema com um Centro de dados único (SDC) ou um sistema com Vários centros de dados (MDC), onde o sistema é desligado, colocando todos os centros de dados em modo de manutenção.

Antes de iniciar

Você concluiu:

- Uma verificação das notas de versão para determinar se esta versão da versão do Cisco WebEx Meeting Server é elegível para uma atualização com tempo de inatividade zero. Se ela é elegível para a atualização com tempo de inatividade zero, siga o procedimento em [Atualizando um sistema com vários centros de dados com tempo de inatividade zero, na página 73](#).
- Colocar a imagem ISO no armazenamento de dados do vCenter e conectar com o CD/DVD como descrito em [Conectando a uma Imagem ISO da Unidade de CD/DVD, na página 70](#).

-
- | | |
|----------------|--|
| Etapa 1 | Obtenha o arquivo de atualização mais recente da Cisco em http://www.cisco.com/cisco/software/navigator.html . O pacote de atualização para o seu sistema inclui uma imagem ISO. Você não pode <i>pular</i> algumas versões do software. Por exemplo, você deve instalar o Cisco WebEx Meetings Server versão 1.1 (Build 1.1.1.9.A) antes de aplicar 1.5MR3. Verifique as notas de versão da versão correta para uso. Consulte também Sobre a atualização de um sistema, na página 69 . |
| Etapa 2 | Notifique outros administradores de sistema que não devem acessar qualquer centro de dados que está sendo atualizado durante este procedimento. Se o fizerem, suas alterações não serão salvas e o resultado pode ser imprevisível. |
| Etapa 3 | Limpe o cachê do seu navegador. Recursos estáticos são armazenados em cachê para melhorar o desempenho das páginas web; no entanto, o cachê de dados pode estar incorreto. Portanto, recomendamos que você limpe o cachê do navegador. |
| Etapa 4 | Inicie sessão nos sites de Administração. |

Não feche as janelas do navegador até que os centros de dados sejam reiniciados ou reinicializados, pois você pode não ser capaz de iniciar sessão novamente nos sites de Administração.

- Etapa 5** Ative o modo de manutenção para todos os centros de dados. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).
Ao ativar o modo de manutenção em todos os centros de dados ativos se encerra a atividade de conferência e os usuários já não poderão iniciar sessão no site WebEx, agendar ou participar de reuniões, ou reproduzir gravações de reuniões.
- Etapa 6** Faça backups de todas as máquinas virtuais em todos os centros de dados deste sistema (a menos que você está se recuperando de uma atualização sem êxito).
Consulte [Criando um Backup Usando o VMware vCenter](#), na página 6.)
- Etapa 7** Selecione **Sistema**.
- Etapa 8** Selecione o centro de dados que você deseja atualizar.
- Etapa 9** Selecione **Atualizar**.
A página **Atualizar sistema** é exibida.
- Etapa 10** Selecione **Atualizar > Continuar**.
A página **Validar imagem ISO** é exibida.
- Etapa 11** Selecione **Eu conectei à imagem ISO e estou pronto(a) para prosseguir > Continuar**.
A imagem ISO é lida para condições, tais como requisitos de tempo de inatividade.
A página **Atualizar sistema** é exibida.
- Etapa 12** Selecione **Fiz backups de todas as máquinas virtuais em todos os centros de dados > Continuar**. Não feche a janela do navegador; caso contrário, você não será capaz de retornar a esta página.
Elá pode levar até uma hora para completar uma atualização. Se você ver que o botão de reinício ainda não apareceu, verifique o estado da atualização do centro de dados primário para confirmar que não há erros na atualização e que ela está ocorrendo.
- Importante** Não desligue ou reinicie qualquer centro de dados enquanto outro centro de dados é atualizado; caso contrário, pode fazer com que a atualização falhe.
Uma vez que a atualização em todos os centros de dados for concluída, o botão **Reiniciar** é exibido, confirmando o sucesso da atualização.
- Etapa 13** Selecione **Continuar**.
- Cuidado** Uma vez que você selecionar **Continuar**, você não pode parar o processo de atualização. Se um problema surge durante o procedimento e não for concluído com sucesso, então você deve usar os backups para restaurar todos os centros de dados no sistema.
Não feche a janela do navegador, caso contrário você não será capaz de retornar a esta página. Se uma sessão do navegador é fechada ou perde a conexão, por qualquer motivo, você deve verificar a tela de abertura das máquinas virtuais para verificar se a atualização foi concluída com êxito, em seguida, reinicie o sistema manualmente.
- Importante** Não desligue ou reinicie qualquer centro de dados enquanto outro centro de dados é atualizado; caso contrário, pode fazer com que a atualização falhe.
Uma vez que a atualização for concluída, uma nova página é exibida, confirmando o sucesso da atualização.
Reiniciar se torna ativo quando todos os centros de dados no sistema são atualizados.
- Etapa 14** Selecione **Reiniciar** para reiniciar o sistema.
A página de logon no site de Administração Cisco WebEx é exibida.
- Etapa 15** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 16 Verifique as notas de versão para esta atualização, e determine se quaisquer tarefas de pós atualização são necessárias. Se as tarefas adicionais forem necessárias, as conclua antes de tirar o sistema do modo de manutenção.

Etapa 17 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Etapa 18 Teste o sistema. Consulte [Sobre o teste do sistema, na página 52](#) para testes recomendados.

Próximos passos

Recomendamos que você remova todos os backups quando você estiver satisfeito com a operação.

Atualizando um sistema com vários centros de dados com tempo de inatividade zero

Este procedimento descreve como atualizar um sistema com Vários centros de dados (MDC), onde o sistema continua a atender os usuários usando outro centro de dados enquanto este centro de dados é atualizado. Durante uma atualização com tempo de inatividade zero, não reinicie ou desligue qualquer centro de dados.

Antes de iniciar

Você concluiu:

- Uma verificação das notas de versão para determinar se esta versão da versão do Cisco WebEx Meeting Server é elegível para uma atualização com tempo de inatividade zero. Se ele não é elegível para atualização com tempo de inatividade zero, siga o procedimento em [Atualizando os centros de dados versão 2.5 e superior com inatividade do sistema, na página 71](#).
- Colocar a imagem ISO no armazenamento de dados do vCenter e conectar com o CD/DVD como descrito em [Conectando a uma Imagem ISO da Unidade de CD/DVD, na página 70](#).

Etapa 1 Obtenha o arquivo de atualização mais recente da Cisco em <http://www.cisco.com/cisco/software/navigator.html>. O pacote de atualização para o seu sistema inclui uma imagem ISO. Você não pode *pular* algumas versões do software. Por exemplo, você deve instalar o Cisco WebEx Meetings Server versão 1.1 (Build 1.1.1.9.A) antes de aplicar 1.5MR3. Verifique as notas de versão da versão correta para uso. Consulte também [Sobre a atualização de um sistema, na página 69](#).

Etapa 2 Notifique outros administradores de sistema que não devem acessar qualquer centro de dados que está sendo atualizado durante este procedimento. Se o fizerem, suas alterações não serão salvas e os resultados podem ser imprevisíveis.

Etapa 3 Limpe o cachê do seu navegador. Recursos estáticos são armazenados em cachê para melhorar o desempenho das páginas web; no entanto, o cachê de dados pode estar incorreto. Portanto, recomendamos que você limpe o cachê do navegador.

- Etapa 4** Inicie sessão nos sites de Administração.
Não feche as janelas do navegador até que os centros de dados sejam reiniciados ou reinicializados, pois você pode não ser capaz de iniciar sessão novamente nos sites de Administração.
- Etapa 5** Selecione **Sistema**.
- Etapa 6** Selecione o centro de dados que você deseja atualizar.
- Etapa 7** Selecione **Atualizar**.
A página **Atualizar sistema** é exibida.
- Etapa 8** Selecione **Atualizar > Continuar**.
A página **Validar imagem ISO** é exibida.
- Etapa 9** Selecione **Eu conectei à imagem ISO e estou pronto(a) para prosseguir > Continuar**.
A imagem ISO é lida para condições, tais como requisitos de tempo de inatividade.
A página **Atualizar sistema** é exibida.
- Etapa 10** Faça backups de todas as máquinas virtuais (a menos que você esteja se recuperando de uma atualização sem êxito).
(Consulte [Criando um Backup Usando o VMware vCenter](#), na página 6).
Importante O backup criado aqui pode ser usado para repetir uma atualização com tempo de inatividade zero que falhou. Se você tentar recuperar uma atualização com tempo de inatividade zero de qualquer outro backup, você pode perder dados ou danificar seu sistema. Pule esta etapa apenas se você estiver se recuperando de uma tentativa de atualização com tempo de inatividade zero que falhou recentemente.
- Etapa 11** Ligue todas as máquinas virtuais e repita a Etapa 2 até a Etapa 9, efetuando logon novamente no centro de dados.
Se você perdeu a conexão com a imagem ISO como resultado do processo de backup, restabeleça a conexão. Consulte [Conectando a uma Imagem ISO da Unidade de CD/DVD](#), na página 70.)
- Etapa 12** Selecione **Fiz backups de todas as máquinas virtuais em todos os centros de dados > Continuar**. Não feche a janela do navegador; caso contrário, você não será capaz de retornar a esta página.
Ele pode levar até uma hora para completar uma atualização. Se você ver que o botão de reinício ainda não apareceu, verifique o estado da atualização do centro de dados primário para confirmar que não há erros na atualização e que a atualização está ocorrendo.
Importante Não desligue ou reinicie qualquer centro de dados enquanto outro centro de dados é atualizado; caso contrário, pode fazer com que a atualização falhe.
Uma vez que a atualização neste centro de dados for concluída, o botão **Reiniciar** é exibido, confirmando o sucesso da atualização.
O backup feito como parte deste processo não é mais válido para a recuperação. Se a atualização falhar por algum motivo, você pode recuperar este centro de dados usando o backup criado como parte deste processo.
- Etapa 13** Selecione **Reiniciar**.
A tela de logon é exibida.
- Etapa 14** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 15** Navegue para o painel do centro de dados que acabou de ser atualizado.
A versão atualizada é exibida no painel.
- Etapa 16** Verifique as notas de versão para esta atualização, e determine se quaisquer tarefas de pós atualização são necessárias. Se as tarefas adicionais forem necessárias, as conclua antes de tirar o sistema do modo de manutenção.
- Etapa 17** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este

centro de dados é parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. O serviço de reuniões para usuários neste centro de dados é restaurado.

Próximos passos

Recomendamos que você remova todos os backups quando você estiver satisfeito com a operação.

Depois que este centro de dados estiver operacional e em um estado saudável, atualize outro centro de dados, repetindo este procedimento o mais rapidamente possível.



CAPÍTULO 10

Atualizando o Sistema

- [Preparando para atualizar um centro de dados, página 77](#)
- [Fazendo Upgrade Automático no Sistema, página 79](#)
- [Atualizando o sistema manualmente, página 82](#)

Preparando para atualizar um centro de dados

O seu sistema pode ser atualizado reimplantando-o com um arquivo OVA (Modelo de Servidor Virtual) atualizado. O procedimento de atualização cria um sistema paralelo e os dados do sistema original são transferidos para o sistema *atualizado* como parte do processo de atualização. Se o sistema atualizado falhar o teste, você pode reiniciar o sistema original para restaurar o serviço, corrigir os erros e reimplantar um sistema atualizado.

Uma *atualização* é definida como uma substituição do sistema para implantar grandes modificações que fizemos ao sistema. Por exemplo, substituir um sistema atualmente executando a versão 1.5 para executar a versão 2.0 que inclui suporte para um novo sistema operacional. Uma *atualização* é definida como a substituição de um sistema existente (original) para tirar vantagem das modificações que fizemos para melhorar o sistema. Uma *expansão* é definida como a ampliação de um sistema existente, mas não a alteração da versão do aplicativo. Por exemplo, você pode atualizar um sistema a partir da versão 1.5 para 1.5MR, atualizar um sistema 1.5 para 2.0 ou expandir um sistema de 800 usuários para 2000 usuários. Em todos os casos, os processos incluem a transferência de todos os dados a partir do sistema original para o sistema atualizado ou expandido.

Use a tabela a seguir para determinar se você deve executar uma atualização do sistema ou atualizar um centro de dados para executar uma versão específica do Cisco WebEx Meetings Server.

Versão instalada	Para a versão...	Atualizar	Atualizar
1.5MR3 ou superior	2.0 ou 2.5 ⁴	X	
1.0MR, 1.1MR ou 1.5MR	2.5	X	
2.0MR3 ou superior	2.5		X

Versão instalada	Para a versão...	Atualizar	Atualizar
2.5 Único centro de dados (SDC)	Qualquer 2.5MR		X
2.5 Vários centros de dados (MDC)	Qualquer 2.5MR		X

⁴ Recomendamos que qualquer versão de 1.0, 1.1 ou 1.5 seja atualizada para a versão 1.5MR3 dos arquivos OVA e ISO antes de atualizar para a versão 2.5.

A atualização do sistema pode ser realizada de forma automática ou manual. **Recomendamos que você faça a atualização do sistema usando o processo automático.**

Ao fazer a atualização:

- Não tente *atualizar* um sistema para uma versão gradual; *atualize* para a próxima versão completa do aplicativo. Por exemplo, *atualize* seu sistema de 1.5 para 2.0. *Atualize* seu sistema de 1.1 a 1.5.
- Verifique se as configurações de data/hora de todas as VMs correspondem:
 - Certifique-se para que a data e a hora estejam corretas e que o Network Time Protocol (NTP) esteja em execução. Consulte [Configurando um Servidor NTP.](#))
 - Confirme que a configuração NTP em cada organizador ESXi esteja configurada para iniciar e parar com o organizador.
 - Se for necessário modificar a configuração para corrigir qualquer um desses problemas, verifique se todas as VMs nos organizadores são graciosamente desligadas.
- Quando você atualiza um Servidor de Reuniões Cisco WebEx, os registros capturados salvos no sistema *original* não são transferidos para o sistema de Serviços de Reuniões Cisco WebEx *atualizado*. Portanto, você deve primeiro capturar e baixar quaisquer registros e capturas de registro que você precise do sistema original antes de iniciar a atualização.
- A VM de admin de atualização deve estar no mesmo organizador ESXi que a VM de administração original.
- Quando um sistema original é atualizado ou expandido, um sistema paralelo é criado. Se houver tempo restante no período de teste do sistema original, esse tempo é transferido para o sistema atualizado ou expandido. As licenças dos Organizadores permanentes válidas no sistema original podem ser transferidas para um sistema atualizado ou expandido ao *reorganizar* as licenças.
-



Observação

Nos referimos ao sistema atual antes de iniciar a atualização como o sistema *original*. O sistema atual após a atualização é chamado de sistema *atualizado*.

Antes de começar uma atualização automática ou manual

Antes de fazer a atualização em um sistema manualmente ou automaticamente, as seguintes questões deveriam ser abordadas:

- Obtenha o arquivo OVA usado para a atualização.

- Remova todas as fotos instantâneas VMware do sistema original (existente). Não tome nenhuma foto instantânea durante o processo de atualização.
- Crie um backup para cada máquina virtual no seu sistema (existente) original. Consulte [Criando um Backup Usando o VMware vCenter, na página 6.](#)
- Planeje uma parada para manutenção. Durante o processo de atualização, o sistema original é colocado em modo de manutenção e requer acesso exclusivo ao sistema; os usuários não poderão acessar o sistema para reuniões durante este período. Agende esta atualização para um horário que menos atrapalhe os seus usuários.
- Planeje o aumento do tamanho dos armazenamentos de dados, uma vez que o sistema original e o sistema atualizado compartilham armazenamentos de dados até o teste do sistema atualizado estar completo e o sistema original removido.
- Verifique se os nomes de organizadores e endereços IP do sistema original são reutilizados no sistema atualizado. Também, se as máquinas virtuais internas para ambos os sistemas estão na mesma sub-rede. Se você tiver adicionado o acesso público, as máquinas virtuais de Proxy Reverso da Internet para o sistema original e o sistema atualizado devem estar na mesma sub-rede.
- Verifique se o nome do organizador do vCenter pode ser resolvido pelo servidor DNS. Teste o link fazendo um ping no nome do organizador.

Observação

o sistema CWMS é o nome padrão do centro de dados após uma atualização para a versão 2.5; não é traduzido do inglês para qualquer dos outros idiomas.

Fazendo Upgrade Automático no Sistema

Este procedimento lista as tarefas de alto nível necessárias para concluir uma atualização automática. Ela inclui links para as seções do *Guia de Administração do Cisco WebEx Meetings Server* (em <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html>), que fornece detalhes sobre os passos necessários para completar cada tarefa.

Antes de iniciar

Antes de atualizar um sistema usando o processo de atualização automática:

- Em um ambiente de Vários centros de dados (MDC), os centros de dados não podem ser expandidos ou atualizados. Os centros de dados secundários devem ser removidos do MDC, tornando-os um ambiente de Centro de dados único (SDC). O ambiente MDC pode ser restaurado após os centros de dados serem modificados e verifica-se que a versão e os tamanhos dos centros de dados coincidem.
- Informe os outros administradores de sistemas que não poderão acessar ou fazer alterações ao sistema original durante a atualização, pois suas alterações poderão produzir resultados imprevisíveis.
- Informe os outros administradores de sistemas que não poderão acessar ou fazer alterações ao sistema original durante a atualização, pois suas alterações poderão produzir resultados imprevisíveis.
- Forneça e configure um endereço de IP e um nome de organizador adicionais que serão usados temporariamente para a máquina virtual de administração no sistema atualizado. Este pode ser qualquer endereço de IP disponível na VLAN. O nome do organizador pode ser qualquer um que você quiser,

uma vez que este endereço de IP e o nome do organizador serão lançados no final do processo de atualização.

O sistema original e o sistema atualizado são ligados durante este processo. O endereço de IP e o nome do organizador temporários evitam conflitos de IP durante esta parte do processo. Depois que os dados são transferidos do sistema original para o sistema modificado, o sistema original é desligado. No final do processo, o sistema modificado é retirado do modo de manutenção e reinicializado.

Durante a reinicialização, o endereço de IP e o nome do organizador temporários são lançados e o sistema modificado usa o endereço de IP da máquina virtual de administração original e o nome do organizador.

Se houver um firewall entre as máquinas virtuais de administração e as máquinas virtuais IRP, o endereço de IP temporário deverá ser permitido através do firewall.

- Não desligue nenhum dos sistemas, nem desconecte-os da fonte de energia.
- Verifique se vSwitch não é usado nos organizadores ESXi como um switch distribuído. Os processos automáticos não suportam o Switch Distribuído vSwitch nos organizadores ESXi do CWMS. Altere para um switch padrão ou use um processo manual. (Consulte [Atualizando o sistema manualmente](#), na página 82, [Atualizando os centros de dados versão 2.5 e superior com inatividade do sistema](#), na página 71 ou [Expandindo o Tamanho do Sistema](#), na página 64.)

Etapa 1

Limpe o cachê do seu navegador.

Recursos estáticos são armazenados em cachê para melhorar o desempenho das páginas web; no entanto, o cachê de dados pode estar incorreto. Portanto, recomendamos que você limpe o cachê do navegador.

Etapa 2

Vá até o gerenciador de licenças no sistema original e gere uma solicitação de licença selecionando **Sistema > Ver mais > Gerenciar licenças**.

O gerenciador de licenças é aberto em uma nova aba.

Etapa 3

Selecione **Gerar Solicitação de Licença**.

Um pop-up é exibido com o texto de solicitação da licença. Copie o texto e salve a solicitação de licença em um local conveniente, pois ela pode ser necessária para o procedimento de reorganização manual para recuperar sua licenças.

Estas informações também podem ajudar a Cisco a encontrar suas licenças. Consulte [Solicitando Licenças utilizando o Gerenciador de Licenças](#), na página 249.)

Etapa 4

Usando o cliente vSphere, implemente a máquina virtual de Administração (usando o endereço de IP temporário) para o sistema atualizado selecionando a configuração com o sufixo **Atualização automática**, por exemplo **Atualização automática de administração de 250 usuários**. Use o mesmo organizador que a máquina virtual de administração do sistema original.

Etapa 5

Verifique se a máquina virtual de administração de atualização pode alcançar os discos do sistema original.

As máquinas virtuais de administração estão no mesmo organizador ESXi e têm acesso aos mesmos armazenamentos de dados, portanto, elas devem ser capazes de ver ambos os conjuntos de discos. O armazenamento de dados utilizado pelos arquivos de armazenamento de dados da máquina virtual de administração (vmdk) deve ser visível através do vCenter (usando as mesmas credenciais vCenter que o processo de atualização automática usa).

Etapa 6

Ligue a máquina virtual de Administração para o sistema atualizado e anote o URL de implantação exibido no console da máquina virtual.

Etapa 7

Insira a URL de implantação no campo de URL de um navegador da Internet.

Etapa 8

Insira as credenciais e URLs de administração e do vCenter para podermos implementar as máquinas virtuais para você. (Consulte [Fornecendo Credenciais Vmware vCenter](#), na página 23.)

Etapa 9

Para implementar qualquer máquina virtual adicional, selecione **Continuar**.

Até você iniciar a configuração do sistema atualizado e o sistema original for colocado em modo de manutenção, os usuários podem realizar reuniões, mas os administradores não devem modificar as máquinas virtuais do sistema original.

- Etapa 10** Anote os nomes das máquinas virtuais criadas automaticamente listadas no vCenter. O formato dos nomes de máquinas virtuais é `CWMS_hostname_MMDDH:mm` onde `mm`=minuto Quando a atualização estiver concluída, as máquinas virtuais não serão exibidas. Para encontrar as máquinas virtuais criadas como parte da atualização do CWMS, você pode pesquisar com este formato. O progresso da atualização é exibido na URL de implantação do sistema atualizado e no console VMware conectado à máquina virtual do Admin do sistema primário. O console VMware fornece a URL de implantação para ser utilizada caso a janela do navegador seja fechada inadvertidamente durante o processo.
- Etapa 11** Para colocar automaticamente o sistema em modo de manutenção e iniciar a configuração do sistema atualizado, selecione **Continuar**. Uma mensagem aparece quando o Modo de Manutenção é ativado, o que pode levar até 30 minutos.
- Etapa 12** Para iniciar o site de Administração atualizado do Cisco WebEx, selecione **Iniciar sessão no site de Administração** e inicie sessão.
- Etapa 13** Aguarde pelo sistema chegar a um bom estado, em seguida, desligue o modo de manutenção no sistema atualizado e selecione **Continuar**. Poderá levar alguns minutos até que o serviço de reuniões esteja novamente disponível. Seu sistema está pronto para que os usuários iniciem reuniões quando todas as máquinas virtuais listadas na página **Propriedades de Sistema** mostrem o estado de Bom (verde). Consulte [Ativando ou desativando o modo de manutenção para versão 2.0 e anterior](#), na página 110 para obter mais informações. O sistema se reinicia.
- Etapa 14** Teste o sistema atualizado. Consulte [Sobre o teste do sistema, na página 52](#). Quando seu sistema atualizado estiver em execução de modo satisfatório, você pode excluir o sistema original para liberar os recursos do sistema original. Mantenha o sistema atualizado em execução enquanto exclui o original para evitar a remoção acidental do arquivo base VMDK do disco rígido 4 que pode ser acessado pelo sistema atualizado. Se a atualização não foi bem sucedida, desligue o sistema atualizado e ligue o sistema original e entre em contato com Cisco TAC.
- Etapa 15** Reorganize e atualize a versão da licença conforme apropriado para o sistema atualizado. (Consulte [Sobre as licenças do organizador, na página 246](#) e [Reorganizando licenças após uma grande modificação do sistema, na página 253](#)). Se as Ferramentas de Produtividade ou o aplicativo Cisco WebEx Meetings anteriormente implementado são versões diferentes ou números de compilação a partir de uma versão recém implantada do aplicativo e a atualização não está bloqueada, você é notificado por uma caixa de diálogo de aviso de atualização. Pode ser necessário mover as Ferramentas de Produtividade ou o aplicativo Cisco WebEx Meetings para os usuários. Consulte a seção de *Matriz de compatibilidade das Ferramentas de Produtividade e do aplicativo Cisco WebEx Meetings* do Guia de Planejamento Cisco WebEx Meetings Server, encontrada em <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html>. No prazo de 180 dias ou menos, o período de licença gratuita expirará. Se o sistema original tinha licenças válidas, elas devem ser reorganizadas em 180 dias ou menos. Se o sistema original estava operando no prazo de carência sem licença, os dias restantes não vencidos são transferidos para o sistema atualizado.

Próximos passos

Se as Ferramentas de Produtividade ou o aplicativo Cisco WebEx Meetings anteriormente implementado são versões diferentes ou números de compilação a partir de uma versão recém implantada do aplicativo e a

atualização não está bloqueada, você é notificado por uma caixa de diálogo de aviso de atualização. Pode ser necessário mover as Ferramentas de Produtividade ou o aplicativo Cisco WebEx Meetings para os usuários. Consulte a seção de *Matriz de compatibilidade das Ferramentas de Produtividade e do aplicativo Cisco WebEx Meetings* dos Requisitos do Sistema e do Guia de Planejamento Cisco WebEx Meetings Server, encontrada em <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html>.

Atualizando o sistema manualmente

Este procedimento lista as tarefas de alto nível necessárias para concluir uma atualização manual. Ela inclui links para as seções do *Guia de Administração do Cisco WebEx Meetings Server* (em <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html>), que fornece detalhes sobre os passos necessários para completar cada tarefa.

Antes de iniciar

Em um ambiente de Vários centros de dados (MDC), os centros de dados não podem ser expandidos ou atualizados. Os centros de dados secundários devem ser removidos do MDC, tornando-os um ambiente de Centro de dados único (SDC). O ambiente MDC pode ser restaurado após os centros de dados serem modificados e verifica-se que a versão e os tamanhos dos centros de dados coincidem.

Certifique-se de que o sistema atualizado pode acessar os discos para a máquina virtual de administração do sistema existente. (O disco rígido 4 será copiado do original sistema para o sistema atualizado.)

Não ligue e execute ambos os sistemas ao mesmo tempo, pois os endereços IP do e os nomes originais das máquinas virtuais originais são utilizados no sistema atualizado.

Etapa 1

Limpe o cachê do seu navegador.

Recursos estáticos são armazenados em cachê para melhorar o desempenho das páginas web; no entanto, o cachê de dados pode estar incorreto. Portanto, recomendamos que você limpe o cachê do navegador.

Etapa 2

Vá até o gerenciador de licenças no sistema original e gere uma solicitação de licença selecionando **Sistema > Ver mais > Gerenciar licenças**.

O gerenciador de licenças é aberto em uma nova aba.

Etapa 3

Selecione **Gerar Solicitação de Licença**.

Um pop-up é exibido com o texto de solicitação da licença. Copie o texto e salve a solicitação de licença em um local conveniente, pois ela pode ser necessária para o procedimento de reorganização manual para recuperar sua licenças.

Estas informações também podem ajudar a Cisco a encontrar suas licenças. Consulte [Solicitando Licenças utilizando o Gerenciador de Licenças, na página 249](#).)

Etapa 4

Entre no site de Administração do sistema original.

Etapa 5

Vá para a guia de sistema e selecione **Atualizar**.

Etapa 6

Selecione **Atualização principal**.

Etapa 7

Selecione **Continuar** para arquivar os dados do sistema original e colocar o sistema no modo de manutenção.

Etapa 8

Usando o cliente VMware vSphere, selecione **Ligar > Desligar convidado** nas máquinas virtuais para o sistema original.

Etapa 9

Implante todas as máquinas virtuais do sistema atualizado, incluindo as máquinas virtuais de alta disponibilidade (HA) e de Proxy reverso da Internet (IRP).

Se você estiver implantando um Centro de multidados (MDC), não implante uma máquina de HA; O MDC não suporta HA.

Durante a implantação, há uma opção para **Ligar VM após a implantação**. Verifique se esta *não* está marcada ou se as VMs foram iniciadas manualmente antes da próxima etapa ser concluída; caso contrário, fará com que as VMs implantem como um novo sistema e criem uma nova implantação, em vez de migrarem os dados. Se as VMs estão ligadas, elas devem ser excluídas e redistribuídas antes de prosseguir.

- Etapa 10** Copie os dados de seu sistema original para a máquina virtual de Administração para o sistema atualizado. Consulte [Anexando um Arquivo VMDK Existente para uma Nova Máquina Virtual, na página 8.](#))
- Etapa 11** Ligue a máquina virtual Admin atualizada e anote o URL de implantação mostrada na consola da máquina virtual. Consulte [Configurando um Sistema de Alta Disponibilidade.](#))
Se o sistema incluir HA, não faça a configuração das máquinas virtuais HA a partir da Implantação de Admin HA; permita que o script de atualização descubra as máquinas virtuais HA.
- Etapa 12** Ligue as outras máquinas virtuais atualizadas.
- Etapa 13** Insira a URL de implantação em um navegador da web.
- Etapa 14** Selecione **Continuar** para iniciar a configuração do sistema.
O progresso da atualização é exibido na URL de implantação do sistema atualizado e no console VMware conectado à máquina virtual do Admin do sistema primário.
O console VMware fornece a URL de implantação para ser utilizada caso a janela do navegador seja fechada inadvertidamente durante o processo.
- Etapa 15** Aguarde até o sistema chegar a um bom estado, em seguida, desligue o modo de manutenção e selecione **Continuar**. Poderá levar alguns minutos até que o serviço de reuniões esteja novamente disponível. Seu sistema está pronto para que os usuários iniciem reuniões quando todas as máquinas virtuais listadas na página **Propriedades de Sistema** mostrem o estado de Bom (verde). Consulte [Ativando ou desativando o modo de manutenção para versão 2.0 e anterior, na página 110](#) para obter mais informações.
- Etapa 16** Teste o sistema atualizado. Consulte [Sobre o teste do sistema, na página 52.](#))
Quando seu sistema atualizado estiver em execução de modo satisfatório, você pode excluir o sistema original para liberar os recursos do sistema original. Mantenha o sistema atualizado em execução enquanto exclui o original para evitar a remoção acidental do arquivo base VMDK do disco rígido 4 que pode ser acessado pelo sistema atualizado.
Se a atualização não foi bem sucedida, desligue o sistema atualizado e ligue o sistema original e entre em contato com Cisco TAC.
- Etapa 17** Reorganize e atualize a versão da licença conforme apropriado para o sistema atualizado. (Consulte [Sobre as licenças do organizador, na página 246](#) e [Reorganizando licenças após uma grande modificação do sistema, na página 253.](#)). Se as Ferramentas de Produtividade ou o aplicativo Cisco WebEx Meetings anteriormente implementado são versões diferentes ou números de compilação a partir de uma versão recém implantada do aplicativo e a atualização não está bloqueada, você é notificado por uma caixa de diálogo de aviso de atualização. Pode ser necessário mover as Ferramentas de Produtividade ou o aplicativo Cisco WebEx Meetings para os usuários. Consulte a seção de *Matriz de compatibilidade das Ferramentas de Produtividade e do aplicativo Cisco WebEx Meetings* do Guia de Planejamento Cisco WebEx Meetings Server, encontrada em <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html>.
- No prazo de 180 dias ou menos, o período de licença gratuita expirará. Se o sistema original tinha licenças válidas, elas devem ser reorganizadas em 180 dias ou menos. Se o sistema original estava operando no prazo de carência sem licença, os dias restantes não vencidos são transferidos para o sistema atualizado.
- Etapa 18**

Próximos passos

Se as Ferramentas de Produtividade ou o aplicativo Cisco WebEx Meetings anteriormente implementado são versões diferentes ou números de compilação a partir de uma versão recém implantada do aplicativo e a atualização não está bloqueada, você é notificado por uma caixa de diálogo de aviso de atualização. Pode ser necessário mover as Ferramentas de Produtividade ou o aplicativo Cisco WebEx Meetings para os usuários. Consulte a seção de *Matriz de compatibilidade das Ferramentas de Produtividade e do aplicativo Cisco WebEx Meetings* dos Requisitos do Sistema e do Guia de Planejamento Cisco WebEx Meetings Server, encontrada em <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html>.



CAPÍTULO 11

Testando o Sistema

- Sobre o teste do sistema, página 85
- Usando o Teste de Reuniões, página 86
- Utilizar o teste de recursos do sistema, página 86

Sobre o teste do sistema

A maioria dos testes do sistema são realizados utilizando o sistema CWMS, por exemplo por [Usando o Teste de Reuniões, na página 86](#) e [Utilizar o teste de recursos do sistema, na página 86](#).

Ao testar um sistema atualizado, você pode manter o sistema original até que você tenha terminado de testar o sistema atualizado (mas como eles compartilham alguns parâmetros, tais como endereços de IP, você não pode ligar os dois sistemas ao mesmo tempo). Quando estiver satisfeito com os resultados dos testes no sistema atualizado, você pode remover (para sempre) o sistema original. Certifique-se de que seu sistema atualizado esteja em execução antes de remover o sistema original. Isso evita a remoção acidental do arquivo de disco da máquina virtual de base (VMDK), que pode ser acessado pelo sistema atualizado.

Alguns dos testes recomendados para executar no sistema são:

- Adicionar, editar, ativar e desativar usuários. Consulte [Gerenciando Usuários, na página 111.](#))
- Agende e realize uma reunião.
- Reagende uma reunião existente.
- Exclua uma série de reuniões agendadas.
- Adicione e abra um anexo de reunião a partir do convite de reunião.
- Grave uma reunião e reproduza a gravação.

O sistema também pode ser testado:

- [Confirmando que sua rede está configurada corretamente, na página 29](#)
- [Verificando o sistema, na página 29](#)
- [Verificando se o sistema primário e o sistema HA estão na mesma versão](#)

- Confirmando que o sistema primário irá ser transferido para o sistema HA, removendo a conexão física com o sistema primário e verificando se o Cisco WebEx está sendo executado no sistema HA.

Usando o Teste de Reuniões

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Suporte > Teste de Reuniões**.

Etapa 3 Selecione **Próximo**.

Seu sistema executa um teste de reuniões, verificando a sua capacidade agendar, iniciar e participar de uma reunião. Os resultados do teste aparecem dentro de alguns minutos.

Utilizar o teste de recursos do sistema

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Suporte > Teste de Recursos do Sistema**.

Etapa 4 Selecione **Próximo**.

Os resultados do teste são lançados para os seguintes:

- CPU, memória, rede e armazenamento para cada organizador em seu sistema
- Verificações de conectividade internas e externas para o seu site e URLs de administração

Etapa 5 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de

DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.



P A R T E



Guia de Configuração do Cisco WebEx Meetings Server

- [Usando o Seu Painel, página 91](#)
- [Gerenciando Usuários, página 111](#)
- [Configurando Seu Sistema, página 135](#)
- [Definindo as Configurações, página 161](#)
- [Gerenciando relatórios, página 237](#)
- [Gerenciando licenças, página 245](#)
- [Registrando centros de dados para criar um sistema de vários centros de dados \(MDC\), página 255](#)
- [Usando os Recursos de Suporte, página 265](#)



CAPÍTULO 12

Usando o Seu Painel

Este módulo descreve as funções em seu painel Cisco WebEx Server e como usá-las.

- [Sobre o Painel, página 91](#)
- [Visualizando e Editando Alarmes, página 94](#)
- [Visualizando Tendências de Reunião, página 96](#)
- [Agendando uma Janela de Manutenção, página 105](#)
- [Sobre o Modo de Manutenção, página 107](#)

Sobre o Painel

O painel é a página inicial do site de administração e fornece vários parâmetros e gráficos dos recursos de monitoramento principais.

O painel inclui as seguintes seções:

- Monitoramento de Sistema — Exibe a hora e estado do sistema, além de incluir as seguintes subseções:
 - Reuniões e Usuários — Estado das reuniões em andamento e em uso. Exibe o número de reuniões que estão em andamento e o número de participantes *distintos* (uso). O LED do estado indica se as reuniões em andamento e em uso estão abaixo ou acima do limite do alarme configurado. Um LED de estado verde indica abaixo do limite configurado, enquanto o vermelho indica acima do limite configurado. Consulte [Visualizando e Editando Alarmes, na página 94](#) para mais informações sobre configurar alarmes.
 - Ícone Alarme — Selecione o ícone Alarme para visualizar e editar as configurações de limite do alarme que você configurou. Os limites do alarme são exibidos na página **Alarmes** em forma numérica. Por padrão, os limites de alarme são exibidos como porcentagem. Consulte [Visualizando e Editando Alarmes, na página 94](#) para mais informações sobre configurar alarmes.

Você pode configurar alarmes para o seguinte:

- Reuniões em Andamento — Indica quando as reuniões atuais estão enfrentando problemas.
- Uso — Número total de usuários distintos que utilizam o sistema. Ocionalmente, os participantes estão em várias sessões, mas eles são contados apenas uma vez.

- Armazenamento — Espaço de armazenamento do backup do banco de dados e da gravação utilizado.

**Observação**

O alarme de armazenamento aparece se você tiver configurado um servidor de armazenamento. Consulte [Configurando um Servidor de Armazenamento, na página 146](#) para obter mais informações.

A gravação da reunião é desativada se o uso do armazenamento estiver acima do limite.

- Partição de registro — Quantidade de espaço usado para armazenar o Registro de Auditoria de Aplicativos.

**Observação**

Se um Auditor estiver configurado no sistema, este alarme só será visível para o Auditor.

- Utilização de licenças — Percentual de licenças permanentes designadas para organizar usuários.
- Licenças de carência — Indica se as licenças de carência são designadas para organizar usuários.

- Informações do centro de dados — Esta seção lista o nome de cada centro de dados, quer o modo de manutenção esteja ativado ou desativado, a quantidade de armazenamento utilizado para cada centro de dados e o status da replicação de dados. Consulte [Sobre as informações do centro de dados exibidas no painel, na página 93](#) para obter mais detalhes.
- Gráfico de Tendência da Reunião e Lista de Reuniões - Um gráfico do número de reuniões realizadas no seu sistema durante um período de tempo especificado. Use os campos **De** e **Para** para definir o período de tempo para as informações de tendência das reuniões e para as reuniões exibidas na lista Reuniões. Você pode selecionar um ponto no gráfico Tendência da Reunião para listar as reuniões na lista de Reuniões que ocorreram durante o horário especificado no gráfico. Para visualizar reuniões que ocorreram durante uma hora específica do dia, passe o mouse sobre o gráfico e selecione a hora desejada. A lista de Reuniões mostra o número total de reuniões que ocorreram durante o período de tempo selecionado, os organizadores, número de participantes, tópicos das reuniões, bem como o estado da reunião. Você pode classificar cada coluna de informações na lista de Reuniões, e as reuniões são exibidas em ordem por estado: Em andamento, terminada e não foi iniciada.
- Pesquisa de reuniões — Encontre uma reunião inserindo critérios de pesquisa específicos, como o número da reunião, tópico ou um intervalo de datas.
- Manutenção — Agenda uma janela de manutenção anunciando quando o modo de manutenção será ativado e desativado. Consulte [Agendando uma Janela de Manutenção, na página 105](#) e [Sobre o Modo de Manutenção, na página 107](#) para obter mais informações.
- Último Backup do Sistema — A hora e a data em que o último backup foi feito, o nome do arquivo, tamanho e localização do backup, e a data e hora do próximo backup. Ele também avisa se o backup falhou e a data da primeira tentativa de backup se uma não foi criada ainda. Um link de backup separado é fornecido para cada centro de dados.

**Observação**

Só aparece se você tiver configurado um servidor de armazenamento.

- Sistema — Exibe o número máximo de usuários que podem participar simultaneamente nas reuniões, o número da versão, URL do produto, se o acesso público é permitido, se é um sistema de alta disponibilidade, bem como o número de licenças do usuário. Selecione [Ver Mais](#) para ir para [Configurando Seu Sistema, na página 135](#).
- Usuários — Exibe o número de usuários ativos, se a Integração do Diretório está configurada, quando a próxima sincronização ocorrerá (se configurada) e o tipo de autenticação selecionada. Selecione [Ver Mais](#) para ir para [Editando Usuários, na página 122](#).
- Configurações — Mostra o número máximo de participantes permitidos em cada reunião, o tipo de áudio, e se o vídeo WebEx HQ está habilitado ou não. Selecione [Ver Mais](#) para ir para [Definindo as Configurações, na página 161](#).

Tópicos relacionados[Visualizando Seu Histórico de Recursos](#)[Usar as Reuniões no Gráfico de Progresso para Resolver os Problemas das Reuniões](#)[Agendando uma Janela de Manutenção, na página 105](#)[Ativando ou desativando o modo de manutenção para versão 2.0 e anterior, na página 110](#)**Sobre as informações do centro de dados exibidas no painel**

A seção de Monitor do Sistema do painel exibe informações de status para os centros de dados que compõem o sistema. Se você tiver um sistema de centro de dados único, o nome do centro de dados atribuído automaticamente pelo sistema será **Sistema CWMS**, mas as informações de status serão atualizadas dinamicamente para o único centro de dados. Em um sistema com vários centros de dados, cada centro de dados será listado em uma linha separada com o nome que você inseriu durante a participação no processo do centro de dados e as informações de status serão atualizadas dinamicamente, separadamente e exibidas para cada centro de dados.

- Status — Esta coluna exibe o status de cada centro de dados. O status pode ser bom, serviço parcial, bloqueado ou ruim.
 - Bom — Todos os componentes do centro de dados estão funcionando corretamente. Nenhuma mensagem de e-mail gerada pelo sistema foi enviada ao administrador.
 - Serviço parcial — Alguns dos componentes do centro de dados não estão funcionando adequadamente, mas o centro de dados está fornecendo serviço. O sistema envia um e-mail ao administrador, indicando que este centro de dados precisa de atenção.
 - Bloqueado — Alguns dos componentes em um centro de dados não têm trabalho adequadamente durante um período prolongado de tempo. O sistema bloqueou o serviço nestes centros de dados e está redirecionando toda a atividade para outro centro de dados. O sistema envia um e-mail ao administrador para indicar que o serviço está ruim, os dados estão sendo redirecionados para outro centro de dados e este centro de dados precisa de atenção.
 - Ruim — A operação de um centro de dados degradou ao ponto em que já não pode oferecer um serviço confiável e causou a falha de um centro de dados operacional em andamento. O sistema

envia um e-mail ao administrador para indicar que o serviço está ruim, os dados estão sendo redirecionados para outro centro de dados e este centro de dados precisa de atenção.

Em um ambiente com Vários centros de dados (MDC), alguns componentes são capazes de transferir, assim o serviço desativado neste centro de dados pode ser fornecido por um outro centro de dados. Esta não é uma indicação do estado geral do sistema; aplica-se apenas ao estado deste centro de dados.

- Bloqueado ou ruim e modo de manutenção está ativado — O status do centro de dados continua a mostrar que o centro de dados está bloqueado. Quando o Modo de Manutenção está desativado e todos os componentes estão novamente em funcionamento, o status muda.
- Inacessível — Outros centros de dados não podem se comunicar com este centro de dados. O sistema envia um e-mail ao administrador pedindo para verificar a conectividade de rede entre os centros de dados.
- Manutenção — Indica se um centro de dados possui o Modo de Manutenção ativado ou desativado.
- Armazenamento — A quantidade de armazenamento utilizado no servidor de armazenamento conectado a cada centro de dados. **Não configurado** é exibido se um servidor de armazenamento não está conectado ao sistema.
- Replicação de Dados — Indica se a replicação de dados está ocorrendo entre os centros de dados em um sistema MDC.

Quando um centro de dados está no estado Bloqueado ou Ruim, os usuários podem experimentar o seguinte:

- As reuniões em andamento são movidas automaticamente para um centro de dados operacional depois de alguns minutos; semelhante ao que acontece em uma situação de failover. Não há impacto nas reuniões de Discagem múltipla ou PCN.
- Reuniões agendadas anteriormente que ainda não foram movidas ao centro de dados operacional. Nenhuma outra ação é necessária para o organizador ou participantes.
- Os usuários iniciam sessão em uma URL do site WebEx da maneira usual, mas o sistema redireciona o início da sessão para o centro de dados operacional.
- Os administradores podem iniciar sessão no centro de dados bloqueado, bem como no centro de dados operacional.
- Os administradores recebem um e-mail gerado pelo sistema que explica qual centro de dados está no estado bloqueado, e informações explicando algumas das possíveis causas.

Visualizando e Editando Alarmes

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione o ícone de alarme.

A página **Alarmes** aparece exibindo os limites de alarme atuais.

Etapa 3 Selecione **Editar**.

A página **Editar Alarmes** aparece. Selecione **Porcentagem %** para visualizar o estado do alarme como uma porcentagem ou **Número #** para visualizar o estado do alarme como um número. A configuração padrão é **Porcentagem %**.

Etapa 4 Selecione as caixas de verificação para os alarmes que você deseja habilitar e selecione o intervalo para cada alarme habilitado.

Opção	Descrição
Reunião em Andamento	<p>Exibe as reuniões no limite do progresso.</p> <ul style="list-style-type: none"> Se definido para Percentagem %, mova a barra de seleção para definir de 2 a 99 por cento. Se definido para Número #, insira um número de 2 a 99 por cento. <p>Padrão: Selecionado com um intervalo de uma hora.</p>
Uso	<p>Exibe o estado atual do sistema.</p> <ul style="list-style-type: none"> Se definido para Percentagem %, mova a barra de seleção para definir de 2 a 99 por cento. Se definido para Número #, insira o número de usuários. <p>Padrão: Selecionado com um intervalo de 12 horas.</p>
Armazenamento	<p>Exibe o limite atual do armazenamento em GB. O limite máximo de armazenamento é calculado como (o espaço total - tamanho do buffer de gravação). O tamanho do buffer de gravação depende do tamanho do sistema do usuário [50 usuários (1 GB), 250 usuários (5 GB), 800 usuários (16 GB) ou 2000 usuários (40 GB)], do número de reuniões Cisco WebEx realizadas, bem como da duração das reuniões gravadas. Sistemas maiores de usuários (sistemas de 800 e 2000 usuários) requerem mais espaço de armazenamento para acomodar backups de bancos de dados maiores. Em geral, plano para fornecer espaço de armazenamento suficiente para três arquivos de backup. Consulte Armazenamento recomendado para arquivos de backup para obter detalhes.</p> <ul style="list-style-type: none"> Se definido para Percentagem %, mova a barra de seleção para definir de 2 a 99 por cento. Se definido para Número #, insira o número de gigabytes. <p>Padrão: Não selecionado. O intervalo é de uma hora.</p> <p>Observação Esta seção só aparece se você tiver configurado um servidor de armazenamento. A gravação é desativada se o uso de Armazenamento excede o limite configurado. Consulte Configurando um Servidor de Armazenamento, na página 146 para obter mais informações.</p>

Opção	Descrição
Uso de memória de registro	<p>Mostra a quantidade de espaço em disco usada para registros.</p> <p>Se um usuário é configurado como um Auditor durante a implantação do sistema, este alarme é visível e configurável apenas pelo Auditor na guia Auditoria. Se o sistema não tem um usuário com a função de Auditor, este alarme é visível e configurável por um Administrador, Administrador de SSO ou Administrador LDAP.</p> <ul style="list-style-type: none"> • Se definido para Percentagem %, move a barra de seleção para definir de 2 a 99 por cento. • Se definido para Número #, insira o número de gigabytes. <p>Defina o Intervalo para indicar quantas vezes o sistema verifica o uso de memória de registro.</p>
Uso da Licença	<p>Mostra o uso de licenças permanentes.</p> <ul style="list-style-type: none"> • Se definido para Percentagem %, move a barra de seleção para definir de 2 a 99 por cento. • Se definido para Número #, insira o número de gigabytes. <p>Defina o Intervalo para indicar quantas vezes o sistema verifica o número de licenças atribuídas.</p>
Licenças gratuitas	<p>Mostra o uso de licenças de carência.</p> <p>Selecione a caixa de seleção Enviar notificação por e-mail para enviar notificações aos usuários quando uma das seguintes condições selecionadas for atendida:</p> <ul style="list-style-type: none"> • É atribuído a um usuário uma licença de Carência • Uma licença de Carência atribuída a um usuário expirou • Todas as licenças de Carência estão atribuídas

Um e-mail é enviado para os administradores quando um alarme excede um limite. O intervalo é utilizado para suprimir vários alarmes dentro do tempo especificado para evitar o envio de muitos e-mails de alarme.

Etapa 5

Selecione **Salvar**.

As configurações do seu alarme são salvas e a página **Alarmes** é atualizada com suas alterações.

Visualizando Tendências de Reunião

Etapa 1

Inicie sessão no site da Administração.

Etapa 2

Acima do gráfico **Tendência da Reunião**, defina um período de tendência selecionando a data e hora **De** e **Para**.

- Você pode ver os dados de tendências de reuniões dos quatro meses anteriores, o mês atual e um mês no futuro.

- As reuniões agendadas antes do meia-noite e se estendendo até o dia seguinte são exibidas no gráfico pela data de inicio da reunião.
- Se uma reunião for desconectada devido a um problema de sistema e em seguida, reconectado, é contado duas vezes no gráfico Tendências de Reunião.
- Os dados de tendência da reunião para visualizações de um mês e seis meses são baseados pelo Greenwich Mean Time (GMT) e não são, portanto, precisamente exibidos ao longo de um período de 24 horas. Por exemplo, se o seu sistema hospeda 200 reuniões durante um determinado dia, o banco de dados registra a ocorrência dessas reuniões baseado no GMT e não no horário local. Os dados de tendência da reunião para visualizações de um dia e uma semana são baseados no fuso horário do usuário.
- Uma faixa verde indica as reuniões que estão em andamento ou que terminaram. Reuniões futuras são mostradas em amarelo.
- Se o intervalo de tempo selecionado é de 24 horas, os pontos dos dados das reuniões passadas ou em andamento estão em intervalos de cinco minutos e as reuniões futuras estão em intervalos de uma hora.
- Se o intervalo de tempo selecionado é maior do que um dia, mas menor do que ou igual a uma semana, os pontos dos dados para reuniões passadas, em andamento ou futuras são exibidos em intervalos de uma hora.
- Se o intervalo de tempo selecionado é maior do que uma semana, os pontos dos dados para reuniões passadas, em andamento ou futuras são exibidos em intervalos de um dia.

O gráfico **Tendência da Reunião** mostra o número total de reuniões que ocorreram durante o período de tempo selecionado. A lista de **Reuniões** abaixo do gráfico lista todas as reuniões durante o período de tendência selecionado.

Observação Algumas entradas de tendência de reuniões podem aparecer duplicadas, porque elas têm o mesmo nome. Uma entrada é criada cada vez que uma reunião é iniciada. Portanto, se uma reunião é iniciada, parada e reiniciada, várias entradas com o mesmo nome da reunião são mostradas.

Etapa 3 Para visualizar uma lista de reuniões que ocorreram em um determinado momento:

- Clique em um local específico no gráfico **Tendência da Reunião** para listar as reuniões que ocorreram no prazo de 5 minutos do tempo selecionado na lista **Reuniões** abaixo do gráfico. Consulte [Visualizando a Lista de Reuniões, na página 98](#) para obter mais informações.
- Selecione o símbolo do gráfico abaixo dos campos **De** e **Para** para exibir uma lista de datas e horários de quando as reuniões ocorreram entre o período De e Para. Em seguida, selecione uma data a partir da lista suspensa. Os pontos de dados mostrados no menu são os mesmos mostrados no gráfico. Eles se tornam acessíveis principalmente para o benefício de usuários com um teclado e leitor de tela.

Passe o mouse sobre o gráfico para ver o número total de reuniões que ocorreram nesse momento.

Próximos passos

- Consulte [Visualizando a Lista de Reuniões, na página 98](#) para ver mais informações sobre a reunião.
- Consulte [Localizando uma reunião, na página 100](#) para obter mais informações sobre como usar a guia **Pesquisa de reunião**.

Visualizando a Lista de Reuniões

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Acima do gráfico Tendência da Reunião, defina um período de tendência selecionando a data e hora **De** e **Para**.

Por padrão, a lista de Reuniões exibe as reuniões para o período de 24 horas atual. Consulte [Visualizando Tendências de Reunião, na página 96](#) para obter mais informações.

Por padrão, a lista de Reuniões exibe reuniões na ordem de hora de início agendada. As reuniões são exibidas em ordem de estado: Em Andamento, Terminada, Não Iniciada. As informações exibidas na lista de Reuniões incluem:

- Intervalo de tempo selecionado no gráfico de tendências
- Tópico da reunião
- Nome do organizador
- Número de participantes
- Estado da reunião: Em Andamento, Terminada, Não Iniciada

Observação Um ícone de status é exibido na primeira coluna para indicar o estado das reuniões que estão em andamento ou que já terminaram como *bom* (verde), *aceitável* (amarelo) ou *ruim* (vermelho).

- Razoável (amarelo) indica que o atraso de áudio/vídeo ou a instabilidade ocorrendo durante a reunião chegou a um limite menor e deve ser monitorado e investigado para determinar a causa.
- Ruim (vermelho) indica que o jitter ou o atraso de áudio/vídeo ocorrendo durante uma reunião chegou a um limite maior.
- Se a maioria das reuniões exibidas na lista de Reuniões indicar um estado ruim, entre em contato com o grupo de Assistência Técnica Cisco (TAC) para obter assistência.
- A tabela a seguir fornece mais detalhes para os diferentes indicadores de status da reunião.

Categoría	Bom	Aceitável	Insatisfatório
Round Trip Time de Dados	Menos de 3000 ms.	3000–5999 ms.	6000 ms. e superior
Round Trip Time de Áudio	Menos de 100 ms.	100–299 ms.	300 ms. e superior
Perda de Pacotes de Áudio	Menos de 5 por cento	5–9 por cento	10 por cento e superior
Jitter de Áudio	Menos de 100 ms.	100–499 ms.	500 ms. e superior
Round Trip Time de Vídeo	Menos de 100 ms.	100–499 ms.	500 ms. e superior
Perda de Pacotes de Vídeo	Menos de 20 por cento	20–49 por cento	50 por cento e superior
Jitter de Vídeo	Menos de 100 ms.	100–499 ms.	500 ms. e superior

Etapa 3 (Opcional) Selecione um título de coluna para classificar as reuniões.

Etapa 4 Use a função de paginação para visualizar a página seguinte ou anterior.

- Um máximo de 10 reuniões são exibidas em cada página.
- Talvez você visualize entradas de reuniões duplicadas na lista de Reuniões. Uma entrada de reunião é criada sempre que uma reunião é iniciada. Portanto, se uma reunião for iniciada, parada e reiniciada, várias entradas de reuniões com o mesmo nome serão exibidas na lista.

Etapa 5 Selecione um **tópico da reunião** na lista de Reuniões para exibir informações adicionais da reunião.

A lista é expandida para mostrar detalhes da reunião, como os nomes dos participantes, o horário de início e fim, bem como o estado da reunião

- Selecione **Carimbo de data/hora** para ir para a página **Relatório de análise da reunião**.

- Selecione **Baixar registro** para baixar o Registro de captura das informações do sistema (Infocap) para a unidade local.

Etapa 6 (Opcional) Para refinar sua pesquisa, selecione a guia **Pesquisa de reunião**.

Campos de pesquisa adicionais aparecem.

Próximos passos

- Consulte [Visualizando um relatório de análise de reunião, na página 101](#) para obter informações mais detalhadas sobre as reuniões.
- Consulte [Baixando registros de reuniões Cisco WebEx, na página 103](#) para baixar um arquivo compactado com vários registros de reuniões. Use esses registros para solucionar problemas que os participantes experimentaram durante uma reunião.
- Consulte [Localizando uma reunião, na página 100](#) para refinar os resultados da pesquisa ou encontrar reuniões específicas.

Localizando uma reunião

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Na seção Tendência da reunião, selecione a guia **Pesquisa de reunião**.

Etapa 3 Insira os critérios de pesquisa.

Pesquise reuniões utilizando alguns ou todos os seguintes campos:

- Número da reunião ou nome do organizador
- Estado — Selecione Tudo, Bom, Regular ou Ruim a partir do menu suspenso.
- Tópico da reunião — Você pode inserir as primeiras letras do tópico da reunião para encontrar todas as reuniões com tópicos semelhantes.
- A partir da data e hora — Utilize o ícone de calendário e o menu suspenso para selecionar a data e a hora.
- Para data e hora — Utilize o ícone de calendário e o menu suspenso para selecionar a data e a hora.

Etapa 4 Selecione **Pesquisar**.

Os **Resultados de pesquisa** listam as reuniões que correspondem aos critérios de pesquisa.

Etapa 5 Para iniciar uma nova pesquisa, selecione **Limpar**.

O sistema limpa os campos de pesquisa, mas os resultados da pesquisa anterior permanecem em **Resultados de pesquisa**.

Etapa 6 Selecione um **tópico da reunião** na lista de Reuniões para exibir informações adicionais da reunião.

A lista é expandida para mostrar detalhes da reunião, como os nomes dos participantes, o horário de início e fim, bem como o estado da reunião

- Selecione **Carimbo de data/hora** para ir para a página **Relatório de análise da reunião**.

- Selecione **Baixar registro** para baixar o Registro de captura das informações do sistema (Infocap) para a unidade local.
-

Próximos passos

Para visualizar informações adicionais sobre a reunião, consulte [Visualizando um relatório de análise de reunião, na página 101](#).

Para baixar um arquivo zipado com os registros da reunião, consulte [Baixando registros de reuniões Cisco WebEx, na página 103](#).

Visualizando um relatório de análise de reunião

Informações adicionais sobre a reunião do Cisco WebEx e seus participantes estão disponíveis na página [Relatório de análise de reuniões](#).

Antes de iniciar

Uma ou mais reuniões são exibidas na lista de Reuniões na guia **Tendência de reunião**. Consulte [Visualizando a Lista de Reuniões, na página 98](#) para obter detalhes.

Etapa 1 Selecione um **tópico de reunião** exibido na lista de reuniões na guia Tendência de Reunião.

Etapa 2 Na lista de reuniões, selecione **Analizar detalhes da reunião**.

Enquanto o sistema está processando as informações, a data e a hora que o sistema começou a gerar as informações são exibidas com um estado de Pendente. Quando o sistema for concluído gerando as informações, a data e a hora tornam-se um link ativo e o estado Pendente muda para um link ativo de Baixar registros.

Etapa 3 Selecione o link **data e hora** para visualizar a página **Relatório de análise de reuniões**.

As seguintes informações são exibidas:

- Tópico da reunião
- Endereço de e-mail do organizador
- Estado — Estado atual da reunião. Os valores podem ser Não iniciado, Em andamento ou Terminado.
- Hora de início — A data e a hora do início da reunião.
- Hora de término — Data e hora que a reunião terminou.
- ID de reunião on-line — A ID da reunião atribuída à parte on-line da reunião.
- Entrar antes do organizador — Indica se os participantes estão autorizados a participarem da reunião antes do organizador da reunião.
- Centro de dados — Mostra o nome do centro de dados utilizado para a reunião. Em um ambiente com centro de dados único, o nome é sempre Sistema CWMS.
- Número da reunião — Um número de 9 dígitos atribuído à reunião.
- Saúde — A saúde geral da reunião. Os valores podem ser Normal, Regular ou Insatisfatório.

- Hora de início agendada — A data e a hora que a reunião foi agendada para começar.
- Hora de término agendada — A data e a hora que a reunião foi agendada para terminar.
- ID de reunião de áudio — A ID da reunião atribuída à parte de áudio da reunião.
- Reunião de áudio começou primeiro — Indica se a parte de áudio da reunião foi iniciada antes da parte on-line da reunião.

Observação Quando o sistema atualiza a janela, os detalhes da reunião estão fechados. Selecione o tópico da reunião novamente para exibir a data e a hora ou os links para Baixar registros.

Etapa 4 Selecione a guia **Mensagens de reunião** para exibir a Função, Hora e Mensagens geradas durante uma reunião.

Etapa 5 Selecione a guia **Participantes** para exibir as seguintes informações para cada participante da reunião:

- Nome do participante
- Hora da entrada
- Navegador
- Endereço de IP do cliente — Endereço de IP do site WebEx.
- Hora de saída — Hora que o participante saiu da reunião.
- Razão da saída — Motivo para sair de uma reunião. Os valores são Normal ou Tempo limite.
- Número de telefone — Número de telefone que os participantes usam para participarem da reunião.
- Latência em VoIP
- QoS de Áudio — Qualidade do áudio durante a reunião. Os valores são Normal ou Ruim.
- QoS de vídeo — Qualidade do vídeo durante a reunião. Os valores podem ser Normal ou Ruim.
- Latência do cliente — Latência do cliente de reunião para o servidor de Reunião de Dados. Os valores podem ser Normal ou Ruim.
- Servidor de organização — Nome da máquina virtual que organizou a reunião. É parte do nome de domínio totalmente qualificado (FQDN) da máquina virtual que organizou a reunião. Por exemplo, se um FQDN da VM micro é susmicro-vm.orionqa.com, então susmicro-vm é exibida.

Próximos passos

Consulte [Baixando registros de reuniões Cisco WebEx, na página 103](#) para baixar um arquivo compactado com vários registros de reuniões.

Baixando registros de reuniões Cisco WebEx

Enquanto uma reunião Cisco WebEx está em andamento ou quando uma reunião terminar, você pode baixar os registros de reuniões gerados pelo sistema, que fornecem informações para a solução de um problema que os usuários experimentaram durante uma reunião.

-
- Etapa 1** Inicie sessão no site da Administração.
- Etapa 2** Selecione a guia Tendência da Reunião, então selecione um intervalo **De** e **Para** para exibir um gráfico de reuniões que ocorreram durante o período de tempo selecionado.
- Etapa 3** Clique em um local específico no gráfico **Tendência da Reunião** para listar as reuniões que ocorreram no prazo de 5 minutos do tempo selecionado na lista **Reuniões** abaixo do gráfico.
- Etapa 4** Selecione um **tópico da reunião** na lista **Reuniões**.
Informações sobre a reunião selecionada são exibidas abaixo do tópico da reunião.
- Etapa 5** Selecione **Baixar registros**.
-

Próximos passos

Consulte [Sobre os registros de reuniões, na página 103](#) para obter mais informações sobre os registros das reuniões baixadas.

Sobre os registros de reuniões

Seu arquivo compactado de Registros de reuniões baixado contém os seguintes registros:

Registro de conferência de dados

Este registro contém informações sobre a parte on-line de uma reunião.

- ID da conferência:
- ID da reunião
- Hora de início programada
- Hora de início
- Hora de término
- Endereço de e-mail do organizador
- URL do site
- Tipo de reunião — Cliente da reunião
- Nome da reunião — O tópico da reunião.
- Número de chamada de entrada primário
- Número de chamada de entrada secundário
- Excluir reunião ao terminar — Indica se esta reunião é excluída da página de detalhes das Reuniões quando a reunião for finalizada.

- Status da Reunião
- Compartilhamento de Aplicativos — Indica se o recurso de compartilhamento de aplicativo foi usado durante uma reunião.
- Telefonia regular — Indica se os participantes chamaram na reunião utilizando telefones.
- Telefonia híbrida
- Vídeo Eureka
- VoIP Eureka
- MMP VoIP
- VoIP híbrido
- Vídeo MMP
- NBR2
- Celular
- Difusão de áudio
- Difusão de áudio para celular

Registro de multimídia

Este registro fornece informações sobre streaming de áudio, comutação de áudio e adaptação de fluxo SVC para o cliente da reunião que se refere ao MMP.

- Nome da reunião
- ID da conferência:
- Tipo de sessão
- Participantes
- Total de participações
- Servidor MCS
- Hora de início
- Hora de término
- Duração

Registro da teleconferência

Este registro contém informações sobre uma reunião por teleconferência.

- ID de TeleConf.
- Servidor do app.
- Chamadores
- Retorno de chamada
- Chamada de entrada

- Hora de início
- Hora de término
- Duração
- Descrição
- Tipo de Conta

Registro de eventos de participação na Web

Este registro contém informações sobre os eventos de participação na Web.

- Nome da reunião — Exibe o tópico da reunião.
- ID de conferência — ID de instância da conferência de dados.
- ID do site — O nome do site Cisco WebEx.
- Participantes — Número total de participantes que participaram da reunião de um navegador da Web.



Observação

O organizador que inicia a reunião não está incluído neste total.

- Total de participações — O número total de pessoas que participaram da reunião.
- Hora de início — A data e hora de início da reunião.
- Hora do término — A data e hora de término da reunião.
- Duração — Quantidade de tempo, em minutos, que a reunião durou.
- Razão do término — Razão pela qual a reunião terminou.

Agendando uma Janela de Manutenção

Antes de realizar a manutenção do sistema, você deve agendar uma janela de manutenção. A única limitação que há quando a janela de manutenção está ativa é que os usuários não poderão agendar reuniões que estejam dentro ou se sobreponham à janela de manutenção. Por exemplo, um administrador deseja desligar o sistema por cerca de uma hora para manutenção, entre 5h-6h, momento em que nenhuma reunião parece estar agendada. Se houver reuniões agendadas, o administrador deve contatar cada organizador de reunião para dizer-lhes que uma janela de manutenção foi agendada durante o horário da reunião. Uma vez que uma janela de manutenção é definida, os usuários não podem agendar reuniões durante esse tempo. No entanto, os usuários podem iniciar uma reunião instantânea utilizando a função **Reunir-se Agora**.

Quando o modo de manutenção estiver ativo, todas as reuniões em curso serão encerradas e a função Reunir-se Agora não estará mais disponível. Suponha que você determine que as mudanças necessárias no sistema levariam aproximadamente duas horas para realizar-se. Uma das tarefas que você precisa levar a cabo é subir um novo certificado de Autoridade Certificadora (CA), o que pode exigir uma reinicialização do sistema assim que o modo de manutenção for desativado. Você pretende iniciar a manutenção do sistema em torno de 4h00. Você agenda uma janela de manutenção, especificando a hora de início para 15/04/2014 3h30 e uma duração de 3 horas e 30 min. Isso significa que a janela de manutenção estará em vigor a partir de 3h30 (permitindo que todas as reuniões sejam encerradas e nenhuma reunião agendada para 30 minutos antes do administrador iniciar a manutenção do sistema) até 7h00. Este período de tempo permite um tempo extra para que o sistema

se torne funcional após a reinicialização, que pode ocorrer depois de ligar o modo de manutenção, e o tempo para o administrador iniciar uma ou mais reuniões instantâneas para testar as configurações modificadas antes dos usuários agendarem ou organizarem reuniões.

Embora algumas tarefas de manutenção do sistema não requerem que você ative o modo de manutenção, esteja ciente de que as tarefas que exigem que o sistema esteja no modo de manutenção exigirão tempo extra para completar um reinício ou uma reinicialização após você desativar o modo de manutenção. O *reinício* do sistema leva apenas alguns minutos (cerca de 3-5 minutos), mas a *reinicialização* leva aproximadamente 30 minutos. Lembre-se de contar com este tempo extra que o seu sistema leva até estar totalmente operativo enquanto estiver agendando uma janela de manutenção. Consulte [Ativando ou desativando o modo de manutenção para versão 2.0 e anterior](#), na página 110 para obter mais detalhes.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Agendar Manutenção**.

A janela **Agendar Manutenção** é exibida.

Etapa 3 Selecione a data e a hora de início da janela de manutenção utilizando a ferramenta de calendário e o menu suspenso de hora.

Etapa 4 Insira a duração da janela de manutenção, especificando o número de horas e minutos.

Etapa 5 Selecione **Agendar**.

Quando a janela de manutenção tem início, os usuários recebem uma mensagem de erro se tentarem agendar uma reunião que se enquadra na janela de manutenção agendada.

A data da janela de manutenção agendada, a hora de início e a duração são exibidas no painel de manutenção.

Próximos passos

- Consulte [Enviando E-mails aos usuários](#), na página 133 para obter detalhes sobre notificar os usuários a respeito da manutenção do sistema.
- Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#) ou [Ativando ou desativando o modo de manutenção para versão 2.0 e anterior](#), na página 110 para obter informações sobre como ativar o modo de manutenção.

Alterando uma Janela de Manutenção Agendada

Depois de agendar uma janela de manutenção, você pode reagendar a data e a hora ou excluí-la.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Painel**.

Etapa 3 Selecione a data e a hora da manutenção do sistema exibido.

Etapa 4 Na **Janela de Manutenção Agendada**, você pode:

- Digitar uma data e hora de início diferentes.
- Modificar a hora e os minutos de duração.

- Selecione **Excluir** para remover a janela de manutenção.

Observação Se você terminar a sua manutenção do sistema mais cedo, você pode reduzir o tempo de duração ou selecionar **Excluir** na **Janela de Manutenção Agendada**.

Próximos passos

Lembre-se de desativar o modo de manutenção antes de modificar as propriedades do sistema. Consulte [Sobre o Modo de Manutenção, na página 107](#) para obter informações sobre quais propriedades do sistema não necessitam que o modo de manutenção seja ligado.

Sobre o Modo de Manutenção

Muitas alterações de configuração exigem que você coloque seu sistema no Modo de Manutenção. O Modo de Manutenção desliga toda a atividade de conferência em um centro de dados, então você deve alertar os usuários, agendando as janelas de manutenção (consulte [Agendando uma Janela de Manutenção, na página 105](#)).

Clique aqui para exibir [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Clique aqui para exibir [Ativando ou desativando o modo de manutenção para versão 2.0 e anterior, na página 110](#).

Ao colocar um centro de dados no Modo de Manutenção, o seguinte acontece:

- Desconecta os usuários e fecha todas as reuniões. Se você colocar um centro de dados que faz parte de um sistema de Vários centros de dados (MDC) em modo de manutenção, as reuniões em andamento falharão no centro de dados ativo.
- Os usuários são impedidos de entrarem em páginas da internet, plugin do Outlook e aplicativos móveis. Os e-mails são enviados automaticamente quando o sistema é retirado do modo de manutenção.
- Interrompe o acesso a gravações de reuniões.
- Usuários não poderão agendar ou organizar novas reuniões.
- O sistema continuará a mandar notificações automáticas de e-mail para usuários e administradores.

Uma *reinicialização* do sistema leva aproximadamente 30 minutos, dependendo do tamanho do seu sistema. Um *reinicio* pode levar de 3 a 5 minutos. O sistema monitora as modificações e faz a determinação automaticamente.

Utilize a seguinte tabela para ajudar a determinar quais tarefas requerem que você ative o modo de manutenção e a ação que seu sistema realiza depois de desativar o modo de manutenção, para que você possa planejar o tempo de inatividade. Quando o modo de manutenção é necessário, o sistema fornece mensagens de lembrete se você tentar executar uma tarefa sem ativar o modo de manutenção.

Tarefa	Referência	Modo de Manutenção Exigido	Reiniciar ou reiniciar
Adicionar ou remover Alta Disponibilidade	Configurando um Sistema de Alta Disponibilidade	S	Reiniciar

Tarefa	Referência	Modo de Manutenção Exigido	Reiniciar ou reiniciar
Adicionar ou remover acesso público	Adicionando acesso público ao seu sistema utilizando IRP, na página 138 OU Removendo o Acesso Público, na página 140	S	Reiniciar
Alterar o idioma padrão do sistema	Configurando as informações da empresa, na página 161	S	Reiniciar
Alterar as URLs da conta do organizador ou administrador	Alterando as Configurações do Seu Site, na página 142	S	Reiniciar
Alterar o seu servidor de e-mail	Configurando um servidor de e-mail (SMTP), na página 49	N	N/D
Alterar seu endereço de IP virtual	Alterando o endereço de IP virtual, na página 137	S	Reiniciar
Configurar e alterar as configurações de marca	Definindo as Configurações da Sua Marca, na página 163	N	N/D
Configurar e alterar muitas das configurações de áudio	Sobre Configurar Suas Definições de Áudio, na página 167	S	Reiniciar
Configurar e alterar os Números de acesso de chamadas, Nome de exibição e configurações de áudio do ID do chamador.	Definindo as configurações do áudio, na página 169	N	N/D
Configurar e alterar a qualidade das configurações de serviço	Configurando a Qualidade de Serviço (QoS), na página 183	N	N/D
Configurar e alterar configurações SNMP	Configurando as Suas Definições de SNMP, na página 151	S	Reiniciar
Configurar certificados	Gerenciando Certificados, na página 214	S	Reiniciar ou reinicializar
Definir configurações de recuperação de desastres	Recuperação de desastres usando o servidor de armazenamento, na página 148	S	Reiniciar
Configurar criptografia compatível a FIPS	Habilitar a Criptografia Compatível ao FIPS, na página 232	S	Reiniciar

Tarefa	Referência	Modo de Manutenção Exigido	Reiniciar ou reiniciar
Configurar servidores de armazenamento	Configurando um Servidor de Armazenamento, na página 146	S	Reiniciar
Configurando a Segurança da Máquina Virtual	Configurando a Segurança da Máquina Virtual, na página 230	S	Reiniciar
Expandindo o tamanho do sistema	Preparando para a Expansão do Sistema, na página 63	S	Reiniciar
Executando atualizações ou melhoramentos	Preparando-se para atualizar um sistema existente OU Preparando para atualizar um centro de dados, na página 77	S	Reiniciar
Atualizar chaves compartilhadas	Gerenciando Certificados, na página 214	S	Reiniciar
Utilizar o teste de Recursos do Sistema	Utilizar o teste de recursos do sistema, na página 86	S	Reiniciar

Cada uma das suas máquinas virtuais tem uma janela de console que indica quando está em modo de manutenção. Você pode abrir as janelas de console na barra de inventário do vCenter (para navegação). As janelas de console fornecem a URL do sistema, o tipo de sistema (primário, alta disponibilidade ou acesso público), o tipo da implantação (sistema com 50, 250, 800 ou 2.000 usuários) e o estado atual do sistema, incluindo se está ou não em modo de manutenção e a hora e a data da mudança do estado. A hora exibida é definida nas configurações de informações da sua Empresa. Consulte [Configurando as informações da empresa, na página 161](#) para obter mais informações.

Completando Tarefas de Manutenção de Sistema

Quando terminar de modificar a configuração do seu sistema, você pode desativar o modo de manutenção. Dependendo das tarefas realizadas, o seu sistema:

- Torna-se rapidamente operacional, porque o modo de manutenção não era necessário para as suas atualizações.
- Exibe uma mensagem para indicar que as alterações que você fez exigem um *reinício do sistema* que leva apenas alguns minutos.
- Exibe uma mensagem para indicar que as alterações que você fez exigem uma *reinicialização* do sistema que leva aproximadamente 30 minutos, dependendo do tamanho do seu sistema. Durante este tempo, a atividade de conferência não está disponível.

Quando o modo de manutenção está desativado, a página **Painel** é atualizada. Seu sistema está pronto para que os usuários iniciem reuniões com sucesso quando todas as máquinas virtuais listadas na página **Propriedades do Sistema** mostrem o estado de Bom (verde) e o Modo de Manutenção esteja desativado.

Consulte [Ativando ou desativando o modo de manutenção para versão 2.0 e anterior, na página 110](#) para obter mais informações.

Se o modo de manutenção estiver desativado e a janela de manutenção agendada ainda estiver ativa, os usuários poderão organizar e participar de reuniões previamente agendadas, mas não poderão agendar novas reuniões até que a janela de manutenção encerre.

Tópicos relacionados

[Agendando uma Janela de Manutenção, na página 105](#)

[Ativando ou desativando o modo de manutenção para versão 2.0 e anterior, na página 110](#)

Ativando ou desativando o modo de manutenção para versão 2.0 e anterior

Ao ativar o modo de manutenção se encerra a atividade de conferência e os usuários já não poderão iniciar sessão no site WebEx, agendar ou participar de reuniões, e reproduzir gravações de reuniões. As reuniões em andamento serão encerradas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Antes de iniciar

Agende uma janela de manutenção e notifique os usuários sobre o tempo de manutenção do sistema agendado. Consulte [Agendando uma Janela de Manutenção, na página 105](#) para obter detalhes.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione **Ativar o Modo de Manutenção**.

A caixa de diálogo **Ativar o Modo de Manutenção** é exibida. Não deixe de ler a respeito da condição do seu sistema enquanto o modo de manutenção está ligado.

Etapa 3

Selecione **Continuar** quando estiver pronto para iniciar a manutenção ou configuração do sistema.

Uma mensagem é exibida indicando que o sistema está em modo de manutenção. O botão **Desativar Modo de Manutenção** é exibido.

Etapa 4

(Opcional) Faça o backup das suas máquinas virtuais.

Etapa 5

Selecione **Desativar Modo de Manutenção** quando você terminar de configurar o seu sistema.

Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva.

Etapa 6

(Opcional) Para determinar se o sistema está totalmente operacional, selecione **Painel > Sistema > Ver mais** (na seção Sistema).

A atividade de conferência pode continuar quando o **Estado** para todas as máquinas virtuais listadas for **Bom** (verde).

Tópicos relacionados

[Agendando uma Janela de Manutenção, na página 105](#)

[Ativando ou desativando o modo de manutenção para versão 2.0 e anterior, na página 110](#)



CAPÍTULO 13

Gerenciando Usuários

Esta seção descreve como gerenciar usuários em seu sistema.

- [Sobre Gerenciar Usuários, página 111](#)
- [Criar arquivos delimitados por vírgula ou tabulações, página 113](#)
- [Exportando contas de usuários para um arquivo CSV, página 119](#)
- [Importando contas de usuários de um arquivo CSV, página 119](#)
- [Transferência de contas de usuários entre sistemas usando um arquivo CSV, página 120](#)
- [Adicionar usuários, página 121](#)
- [Editando Usuários, página 122](#)
- [Desbloquear uma conta de administrador, página 123](#)
- [Ativação ou desativação de usuários e administradores a partir da página Usuários, página 124](#)
- [Localizando usuários, página 124](#)
- [Configurando os Códigos de Rastreamento, página 124](#)
- [Configurando a integração de diretórios, página 126](#)
- [Sincronizando Grupos De Usuários, página 131](#)
- [Usando o CUCM para configurar o AXL Web Service e a sincronização de diretórios, página 132](#)
- [Usando o CUCM para configurar a integração e a autenticação LDAP, página 132](#)
- [Enviando E-mails aos usuários, página 133](#)

Sobre Gerenciar Usuários

Você pode adicionar usuários individualmente usando o GUI ou importar contas de usuários armazenadas em um arquivo separado por vírgulas ou delimitado por tabulações (CSV). Consulte [Criar arquivos delimitados por vírgula ou tabulações, na página 113](#).

O sistema suporta um tempo de vida máximo de 400 mil contas de usuários, a soma das duas contas de usuários ativos e desativados. (Este número máximo de vida útil de contas de usuários é grande o suficiente para acomodar o crescimento antecipado no banco de dados do usuário de qualquer organização.)

Você pode adicionar ou desativar as contas de usuário, mas você não pode excluí-las. Um usuário desativado pode ser reativado quando necessário. As contas de usuários reativados recuperam novamente o acesso às reuniões, gravações e outros dados que acessaram antes de serem desativados.

As contas de usuários são baseadas no endereço de e-mail do usuário. Se o endereço de e-mail de um usuário for alterado fora do sistema, o usuário pode não conseguir usar o sistema até que o endereço de e-mail seja reconciliado.

Para impedir o início de sessão não autorizado no sistema, desative quaisquer usuários que saiam da sua organização. Você pode desativar os usuários das seguintes formas:

- Se seu sistema não usa o SSO integrado, você pode desativar os usuários individualmente usando o GUI ou importar um arquivo CSV com o campo ATIVO definido para N para cada usuário que você deseja desativar. Consulte [Ativação ou desativação de usuários e administradores a partir da página Usuários, na página 124](#) para obter mais informações.
- Se o seu sistema usa o SSO integrado, você deve desativar os usuários removendo-os do diretório corporativo em seu SAML 2.0 iDP. Este procedimento não pode ser realizado através deste produto.
- Use o recurso de configuração de senha para desativar os usuários depois de um período específico. Consulte [Configurando as definições da senha geral, na página 185](#) para obter mais informações.

Para o Cisco WebEx Meetings Server Versão 2.5, há funções de usuário adicionais: Administrador SSO, administrador LDAP e auditor.

Função de auditor

A função de Auditor é uma função especial criada para ambientes que precisam auditar os inícios de sessão e as alterações de configuração feitas pelos administradores. Um auditor pode definir as configurações de registro e gerar registros de Auditoria de Aplicativos para atender aos requisitos de conformidade JITC e de segurança da empresa. A função do Auditor é uma função única, com os seguintes aspectos:

- Um único usuário Auditor pode ser criado durante o processo de implantação do sistema. Depois que o sistema é implantado, o primeiro administrador pode criar os números de auditores. Consulte [Adicionando uma função de auditor, na página 51](#).)
- Um auditor só pode iniciar sessão na URL do site de Administração.
- Um auditor só pode ver e configurar as definições na guia Auditor.
- Um auditor só pode participar de reuniões como um usuário convidado.
- Um auditor não pode agendar reuniões.



Observação

Se um Auditor não estiver configurado, todos os administradores terão acesso e poderão definir as configurações de Registro de Auditoria de Aplicativos em **Configurações > Segurança > Registro de Auditoria de Aplicativos** página e o alarme de Uso de Memória de Registro em **Painel > Alarmes > Editar alarmes** página. Se um auditor está configurado, os administradores podem visualizar essas páginas, mas não podem modificá-las.

Criar arquivos delimitados por vírgula ou tabulações

O sistema pode importar e exportar valores de contas de usuários contidos em um arquivo delimitado por vírgula ou tabulação (CSV). (Um aplicativo de planilha, como o Microsoft Excel, pode ser usado para gerenciar arquivos CSV.) Se uma conta em um arquivo CSV importado não existe, a conta é adicionada. Se a conta existe, os valores de contas CSV importados substituem os valores atuais.

O sistema pode exportar um arquivo CSV contendo valores de contas de usuários que podem ser modificados e importados de volta no sistema ou em um novo sistema.

Para importar com êxito um arquivo CSV, os seguintes critérios devem ser atendidos:

- Todos os campos listados na tabela são necessários, mas os valores dos campos podem estar vazios. Se um campo estiver faltando, uma mensagem de erro é exibida. Por exemplo, Formato de arquivo incorreto. É necessário o custom10.
- Os caracteres válidos no arquivo CSV são limitados aos contidos no Formato de Transformação UCS — 8 bits (UTF-8).
- Ao adicionar uma nova conta de usuário, o campo **UserId** pode ficar em branco se o campo **E-mail** contém um endereço de e-mail que não é usado por outra conta de usuário. Se o endereço de e-mail corresponde ao endereço de e-mail em outra conta de usuário, a conta de usuário no arquivo CSV não é adicionada.
- Ao editar uma conta de usuário, os valores **UserId** e **E-mail** devem corresponder a uma conta de usuário existente. Se eles não corresponderem a uma conta de usuário, nenhum dos valores atuais será alterado para os valores CSV.
- Até dez **Grupos de códigos de rastreamento** podem ser definidos. Os nomes dos grupos de códigos de rastreamento devem ser únicos. Não use nomes de campos predefinidos (USERID, ATIVO, NOME, SOBRENOME, E-MAIL, IDIOMA, HOSTPRIVILEGE, FUSO HORÁRIO e assim por diante) para códigos de rastreamento.

A tabela lista os nomes dos campos necessários, as descrições e os valores aceitáveis.

Nome do Campo	Descrição	Tamanho e Tipo de Valor
ID do usuário.	ID do usuário. Observação Este campo é gerado automaticamente pelo sistema e deve ser deixado em branco na importação de um arquivo CSV.	1 a 19 caracteres alfanuméricos
ATIVO	Indique se este usuário está ativo ou não.	S ou N
NOME	Primeiro nome do usuário.	sequência de 1 a 32 caracteres
SOBRENOME	Sobrenome do usuário.	sequência de 1 a 32 caracteres

Nome do Campo	Descrição	Tamanho e Tipo de Valor
E-MAIL	Endereço de e-mail do usuário	sequências de 1 a 192 caracteres alfanuméricos
IDIOMA	Idioma do usuário. Consulte Valores de campo de arquivos CSV, na página 115 para obter mais informações.	Sequência de 1 a 64 caracteres
PRIVILÉGIO DO ORGANIZADOR	Privilégios de Organizador.	ADMN ou ORGANIZADOR
FUSO HORÁRIO	Fuso horário no qual o usuário está localizado. Consulte Valores de campo de arquivos CSV, na página 115 para obter mais informações.	Nome do fuso horário
DIVISÃO	Divisão do usuário. Para o grupo de código de rastreamento 1. Este campo é configurável na página de Códigos de Rastreamento. Consulte Configurando os Códigos de Rastreamento, na página 124 para obter mais informações.	sequência de 1 a 128 caracteres
DEPARTAMENTO	Departamento do usuário. Para o grupo de código de rastreamento 2. Este campo é configurável na página de Códigos de Rastreamento. Consulte Configurando os Códigos de Rastreamento, na página 124 para obter mais informações.	sequência de 1 a 128 caracteres
PROJETO	Projeto do usuário. Para o grupo de código de rastreamento 3. Este campo é configurável na página de Códigos de Rastreamento. Consulte Configurando os Códigos de Rastreamento, na página 124 para obter mais informações.	sequência de 1 a 128 caracteres
OUTRAS	Outras informações. Para o grupo de código de rastreamento 4. Este campo é configurável na página de Códigos de Rastreamento. Consulte Configurando os Códigos de Rastreamento, na página 124 para obter mais informações.	sequência de 1 a 128 caracteres

Nome do Campo	Descrição	Tamanho e Tipo de Valor
CAMPO5	Campo 5 personalizado. Consulte Configurando os Códigos de Rastreamento, na página 124 para obter mais informações.	sequência de 1 a 128 caracteres
CAMPO6	Campo 6 personalizado.	sequência de 1 a 128 caracteres
CAMPO7	Campo 7 personalizado.	sequência de 1 a 128 caracteres
CAMPO8	Campo 8 personalizado.	sequência de 1 a 128 caracteres
CAMPO9	Campo 9 personalizado.	sequência de 1 a 128 caracteres
CAMPO10	Campo 10 personalizado.	sequência de 1 a 128 caracteres

Os tópicos a seguir fornecem informações adicionais:

- [Exportando contas de usuários para um arquivo CSV, na página 119](#)
- [Importando contas de usuários de um arquivo CSV, na página 119](#)
- [Transferência de contas de usuários entre sistemas usando um arquivo CSV, na página 120](#)
- [Configurando os Códigos de Rastreamento, na página 124](#)

Valores de campo de arquivos CSV

Valores do campo de idioma

A seguir estão os exemplos de valores dos códigos de países que você pode usar em um arquivo CSV.

Valor do campo	Idioma
en-us	EUA Inglês
zh-cn	Chinês Simplificado
zh-tw	Chinês Tradicional
jp	Japonês
ko	Coreano
fr	Francês
de	Alemão
it	Italiano
es-me	Espanhol castelhano

Valor do campo	Idioma
es	Espanhol da América Latina
nl	Holandês
pt-br	Português
ru	Russo

Valores do campo do fuso horário

A seguir, os valores do campo fuso horário (TIMEZONE) que você pode definir em um arquivo CSV.

Valor do campo	GMT
Ilhas Marshall	-12 horas
Samoa	-11 horas
Honolulu	-10 horas
Anchorage	-9 horas
San Francisco	-8 horas
Tijuana	-8 horas
Arizona	-7 horas
Denver	-7 horas
Chihuahua	-7 horas
Chicago	-6 horas
Cidade do México	-6 horas
Saskatchewan	-6 horas
Tegucigalpa	-6 horas
Bogotá	-5 horas
Panamá	-5 horas
Nova York	-5 horas
Indiana	-5 horas

Valor do campo	GMT
Caracas	-4,5 horas
Santiago	-4 horas
Halifax	-4 horas
Newfoundland	-3,5 horas
Brasília	-3 horas
Buenos Aires	-3 horas
Recife	-3 horas
Nuuk	-3 horas
Atlântico Médio	-2 horas
Açores	-1 hora
Reykjavik	0 hora
Londres	0 hora
Casablanca	0 hora
África Oeste	1 h
Amsterdã	1 h
Berlim	1 h
Madri	1 h
Paris	1 h
Roma	1 h
Estocolmo	1 h
Atenas	2 horas
Cairo	2 horas
Pretória	2 horas
Helsinki	2 horas

Valor do campo	GMT
Tel Aviv	2 horas
Amman	2 horas
Istambul	2 horas
Riyadh	3 horas
Nairobi	3 horas
Teerã	3,5 horas
Moscou	4 horas
Abu Dhabi	4 horas
Baku	4 horas
Kabul	4,5 horas
Islamabad	5 horas
Mumbai	5,5 horas
Colombo	5,5 horas
Ekaterinburg	6 horas
Almaty	6 horas
Katmandu	6,75 horas
Bangcoc	7 horas
Pequim	8 horas
Perth	8 horas
Cingapura	8 horas
Taipei	8 horas
Kuala Lumpur	8 horas
Tóquio	9 horas
Seul	9 horas

Valor do campo	GMT
Adelaide	9,5 horas
Darwin	9,5 horas
Yakutsk	10 horas
Brisbane	10 horas
Sydney	10 horas
Guam	10 horas
Hobart	10 horas
Vladivostok	11 horas
Ilhas Salomão	11 horas
Wellington	12 horas
Fiji	12 horas

Exportando contas de usuários para um arquivo CSV

Para exportar um arquivo CSV:

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Usuários > Importar/Exportar usuários**.

Etapa 3 Selecione **Exportar**.

Os seus dados de usuário está exportado como um arquivo CSV. O sistema envia ao administrador um link para o download do arquivo exportado.

Importando contas de usuários de um arquivo CSV

Para importar um arquivo CSV para o sistema:

Antes de iniciar

Prepare um arquivo delimitado por vírgula ou tabulação contendo informações das contas de usuários. Você pode exportar os valores das contas de usuários do sistema atual para um arquivo CSV, modificar o arquivo e importá-lo para adicionar ou alterar contas de usuários. Consulte [Exportando contas de usuários para um arquivo CSV, na página 119](#) e [Criar arquivos delimitados por vírgula ou tabulações, na página 113](#) para obter mais informações.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione **Usuários > Importar/Exportar usuários**.

A página **Importar/Exportar Usuários** é exibida.

Etapa 3

Selecione **Importar**.

A página **Importar Usuários** é exibida.

Etapa 4

Selecione **Navegar** e então selecione o arquivo CSV a ser importado.

Etapa 5

Selecione **Vírgula** ou **Tab** para indicar que tipo de arquivo CSV que você está importando, delimitado por vírgula ou delimitado por tabulações.

Etapa 6

Selecione **Importar**.

O arquivo é importado e o sistema envia um e-mail indicando quantas contas de usuários foram importadas com êxito e quantas contas não foram adicionadas ou modificadas.

Próximos passos

Selecione **Usuários** para visualizar as contas de usuários e verificar se os valores foram importados corretamente.

Transferência de contas de usuários entre sistemas usando um arquivo CSV

Para transferir contas de usuário de um sistema para outro usando um arquivo CSV:

Etapa 1

Inicie sessão no site da administração no sistema que contém o código fonte das contas de usuários a serem transferidas.

Etapa 2

Selecione **Usuários > Importar/Exportar usuários**.

Etapa 3

Selecione **Exportar**.

Os seus dados de usuário está exportado como um arquivo CSV. O sistema envia ao administrador um link para o download do arquivo exportado.

Etapa 4

Opcionalmente, abra o arquivo CSV exportado, modifique os valores das contas dos usuários, conforme necessário, e salve o arquivo CSV. (Consulte [Criar arquivos delimitados por vírgula ou tabulações, na página 113](#) para obter mais informações.)

Etapa 5

Inicie sessão no site de Administração do sistema alvo.

Etapa 6

Selecione **Usuários > Importar/Exportar usuários**.

A página **Importar/Exportar Usuários** é exibida.

- Etapa 7** Selecione **Importar**.
A página **Importar Usuários** é exibida.
- Etapa 8** Selecione **Navegar** e então selecione o arquivo CSV a ser importado.
- Etapa 9** Selecione **Vírgula** ou **Tab** para indicar que tipo de arquivo CSV que você está importando, delimitado por vírgula ou delimitado por tabulações.
- Etapa 10** Selecione **Importar**.
O arquivo é importado e o sistema envia um e-mail indicando quantas contas de usuários foram importadas com êxito e quantas contas não foram adicionadas ou modificadas.
-

Próximos passos

Selecione **Usuários** para visualizar as contas de usuários e verificar se os valores foram importados corretamente.

Adicionar usuários

- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Selecione **Usuários > Adicionar usuário**.
- Etapa 3** Selecione o tipo de conta (**Auditor**, **Organizador** ou **Administrador**).
A opção Auditor é visível, mas é uma opção disponível apenas para o Primeiro administrador.
- Etapa 4** Preencha as campos com informações do usuário. Os campos marcados com um asterisco são obrigatórios.
Importante Os usuários são identificados no sistema pelo endereço de e-mail. Se um endereço de e-mail do usuário é alterado e o usuário permanece ativo, o endereço de e-mail no CWMS também deve ser alterado ou esse usuário não receberá notificações.
- Etapa 5** Selecione **Salvar**.
O Cisco WebEx Meetings Server envia um e-mail ao usuário com o link **Criar senha**. Um usuário deve criar uma senha antes de iniciar a sessão no site WebEx comum.
O link Criar uma Senha expira após 72 horas. Se o link tiver expirado, o usuário pode selecionar o link **Esqueceu a senha** para receber uma nova mensagem de e-mail que dá outra oportunidade para criar uma senha.
O usuário é adicionado ao sistema.
-

Editando Usuários

Você pode alterar as informações de usuário e ativar ou desativar as contas de usuário com o recurso editar usuário.



Observação

Se uma conta de administrador estiver bloqueada devido a falhas nas tentativas para iniciar sessão, uma mensagem será exibida na página **Editar usuário** do administrador. Outro administrador pode usar o link fornecido na mensagem exibida na parte superior da página para desbloquear a conta do administrador. Consulte [Desbloquear uma conta de administrador](#), na página 123 para obter detalhes.

Etapas de Resumo

1. Inicie sessão no site da Administração.
2. Seleccionar **Usuários**.
3. Selecione um usuário para editar.
4. Faça alterações para campos editáveis. Os campos marcados com um asterisco são obrigatórios.
5. (Opcional) Selecione a caixa de seleção **Reservar licença** se este usuário for um organizador e essa pessoa requerer uma licença permanente para organizar reuniões regularmente.
6. (Opcional) Opcionalmente, selecione a caixa de seleção **Requerer que este usuário altere a senha na próxima vez que iniciar sessão**.
7. Opcionalmente, ative ou desative uma conta:
 - Selecione **Ativar** para reativar uma conta inativa.
 - Selecione **Desativar** para desativar uma conta.
8. Selecione **Salvar**. Isto salva as suas alterações sem mudar o estado da conta.

Etapas Detalhadas

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Seleccionar **Usuários**.

A lista de usuários aparece. O número padrão de usuários mostrado em cada página é 50. Você pode opcionalmente selecionar o menu suspenso **Usuários por Página** e alterar a configuração para **50** ou **100**.

Etapa 3 Selecione um usuário para editar.

Etapa 4 Faça alterações para campos editáveis. Os campos marcados com um asterisco são obrigatórios.

Etapa 5 (Opcional) Selecione a caixa de seleção **Reservar licença** se este usuário for um organizador e essa pessoa requerer uma licença permanente para organizar reuniões regularmente.

Consulte [Sobre as licenças do organizador](#), na página 246 para obter mais detalhes.

Etapa 6 (Opcional) Opcionalmente, selecione a caixa de seleção **Requerer que este usuário altere a senha na próxima vez que iniciar sessão**.

Observação Se SSO ou LDAP estiver ativado no seu sistema, esse recurso é desativado.

Etapa 7 Opcionalmente, ative ou desative uma conta:

- Selecione **Ativar** para reativar uma conta inativa.
- Selecione **Desativar** para desativar uma conta.

Observação Ativar ou desativar uma conta não salva quaisquer outras alterações que tenham sido feitas na conta. Você deve selecionar **Salvar** para salvar as alterações.

Etapa 8 Selecione **Salvar**. Isto salva as suas alterações sem mudar o estado da conta.

Desbloquear uma conta de administrador

Para impedir o acesso não autorizado a um site de administração, o sistema pode bloquear automaticamente uma conta de administrador. Esse recurso é desativado por padrão. Os parâmetros, tais como o número de falhas durante a quantidade de minutos e a duração de bloqueio, são configuráveis. Consulte [Configurando as definições da senha geral, na página 185.](#))

As seções seguintes descrevem como desbloquear uma conta.

O administrador desbloqueia sua própria conta a partir de um e-mail

O sistema envia ao administrador bloqueado um e-mail gerado automaticamente indicando que sua conta está bloqueada. No e-mail, o administrador pode selecionar o botão **Desbloquear conta** para desbloquear a conta. Essa opção é desativada por padrão.

Outro administrador desbloqueia a conta de um administrador a partir de um e-mail

Se houver várias contas de Administrador, cada administrador recebe um e-mail gerado automaticamente indicando que uma conta está bloqueada. Para desbloquear a conta, selecione o link **perfil do usuário** no e-mail para ir para a página **Editar usuário** daquele administrador. Em seguida, selecione o link **Desbloquear administrador** na mensagem exibida na parte superior da página e notifique o administrador que a conta foi desbloqueada. Esta opção está sempre habilitada.

Outro administrador desbloqueia a conta na página Editar Usuário

Quando uma conta de administrador está bloqueada, uma mensagem é exibida na parte superior da página **Editar usuário** do administrador bloqueado. Embora o administrador não possa acessar a página **Editar usuário**, outro administrador pode acessar a página e selecionar o link **Desbloquear administrador** na mensagem exibida e notificar o administrador que a conta está desbloqueada.

Aguarde até o temporizador expirar

Quando uma conta de administrador está bloqueada e se um temporizador está definido, uma mensagem é exibida na parte superior da página **Editar usuário** administrador bloqueado. O administrador pode novamente tentar efetuar logon quando o temporizador expirar.

Ativação ou desativação de usuários e administradores a partir da página Usuários

Utilize este recurso para ativar contas desativadas ou reativar contas inativas. As únicas contas que não podem ser desativadas são as contas de Auditores. Alternativamente, você pode ativar uma conta, definindo o parâmetro em um arquivo CSV e importando-o. Consulte [Editando Usuários](#), na página 122 para obter mais informações.

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Selecionar **Usuários**.
- Etapa 3** Selecione as caixas de verificação para quaisquer usuários inativos que você deseja ativar. Ou selecione as caixas de seleção para quaisquer usuários ativos que você deseja desativar.
- Etapa 4** Selecione **Ações > Ativar ou Desativar**.
As contas selecionadas são modificadas e o status de cada conta reflete o status atualizado.
-

Localizando usuários

Você pode classificar os usuários por tipo, por exemplo, ativo ou organizador, ou pelo tipo de licença atribuída aos organizadores. Além da classificação de usuários, você também pode pesquisá-los pelo nome, sobrenome ou nome completo e pelo endereço de e-mail. Os resultados da pesquisa exibem o perfil de usuário e as informações da licença.

-
- Etapa 1** Inicie sessão no site da Administração.
- Etapa 2** Selecionar **Usuários**.
- Etapa 3** Selecione uma categoria no menu suspenso para classificar os usuários.
- Etapa 4** (Opcional) Use o menu suspenso **Expirar em** para classificar os usuários com licenças temporárias pela expiração da licença (expirado, 1 mês, 3 meses, 6 meses).
- Etapa 5** Digite um nome de usuário (nome, sobrenome ou nome completo) ou o endereço de e-mail no campo de pesquisa e selecione **Procurar**.
-

Configurando os Códigos de Rastreamento

Você pode configurar os códigos de rastreamento para monitorar o uso do organizador em determinados grupos. Por exemplo, você pode configurar os códigos de rastreamento para projetos ou departamentos. Os códigos de rastreamento que você configura aparece como opções quando você adiciona ou edita usuários.

Você deve configurar o seguinte para cada código de rastreamento:

- Grupo de código de rastreamento – Configure os seus grupos de código de rastreamento. Os grupos de códigos de rastreamento são utilizados quando você adiciona e edita os usuários. Os padrões são Divisão, Departamento, Projeto, Outro e Personalizado5 através do Personalizado10.



Observação

Os nome dos grupos de código de rastreamento deveriam ser únicos e você não deveria utilizar campos de nome pré-definidos (IDDOUSUÁRIO, ATIVO, NOME, SOBRENOME, EMAIL, IDIOMA, PRIVILÉGIODEORGANIZADOR, FUSOHORÁRIO).

- Modo de entrada – Selecione **Campo de texto** ou **Menu suspenso**.
- Uso – Selecione **Não utilizado**, **Opcional** ou **Necessário**.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Usuários > Códigos de rastreamento**.

Etapa 3 Insira o nome de cada grupo de rastreamento que você deseja configurar na coluna **Grupo de código de rastreamento**.

Etapa 4 Selecione **Entrada de texto** ou **Menu suspenso** para cada código de rastreamento na coluna **Modo de entrada**.

- Selecione **Entrada de texto** e insira seu nome do código de rastreamento em um campo de texto.
- Selecione **Menu suspenso**. Um link **Editar lista** é exibido ao lado do campo **Modo de entrada**. Selecione o link **Editar lista** para configurar os valores deste código de rastreamento. Consulte [Editando Códigos de Rastreamento, na página 125](#) para obter mais informações.

Etapa 5 Selecione **Não utilizado**, **Opcional**, ou **Necessário** na coluna **Uso** para cada código de rastreamento.

Você deve apenas alterar o Uso para **Necessário** ou **Opcional** após você ter configurado uma lista do menu suspenso.

Etapa 6 Selecione **Salvar**.

As configurações do seu código de rastreamento são salvas.

Editando Códigos de Rastreamento

Por padrão, os códigos de rastreamento são exibidos como caixas de texto. Opcionalmente, você pode exibir as opções de código de rastreamento em um menu criando uma lista de Códigos de rastreamento. (Consulte também [Configurando os Códigos de Rastreamento, na página 124](#).)

Antes de iniciar

Para editar os códigos de rastreamento, você deve configurá-los. Consulte [Configurando os Códigos de Rastreamento, na página 124](#).

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione **Entrada de texto** ou **Menu suspenso** para cada código de rastreamento na coluna **Modo de entrada**.

- Se você selecionar **Entrada de texto**, insira o nome do código de rastreamento em um campo de texto.
- Se você selecionar **Menu suspenso**, um link **Editar lista** é exibido próximo ao campo **Modo de entrada**. Selecione o link **Editar lista** para configurar os valores deste código de rastreamento.

Etapa 3

Selecione o link **Editar lista**.

A caixa de diálogo **Editar Lista de Código de Rastreamento** aparece.

Etapa 4

Configure os campos em **Editar lista de códigos de rastreamento**:

- Selecione **Mostrar códigos ativos somente** para exibir apenas os códigos de rastreamento ativos quando você abre esta caixa de diálogo. Desmarque esta opção para mostrar todos os códigos de rastreamento. Você não pode selecionar esta opção a primeira vez que você configurar os códigos de rastreamento.
- Insira o nome do item do menu suspenso na caixa de texto **Código**. Limitar: 128 caracteres. Se não houver códigos de rastreamento vazios exibidos, selecione **Adicionar mais 20 linhas** para adicionar mais 20 códigos de rastreamento configuráveis. Limitar: 500 linhas (25 páginas).
- Selecione **Padrão** para fazer este item de menu a seleção padrão do menu suspenso.

Ativo é selecionada por padrão. Desmarque **Ativo** para tornar um código de rastreamento inativo. Códigos de rastreamento inativos não aparecem no menu suspenso deste grupo de código de rastreamento.

Etapa 5

Selecione **Atualizar** para salvar as suas configurações.

Suas configurações são salvas e a página **Editar lista de Código de Rastreamento** se fecha.

Configurando a integração de diretórios

A integração de diretórios permite que o seu sistema preencha e sincronize o banco de dados de usuários do seu Cisco WebEx Meetings Server com o banco de dados de usuários do Cisco Unified Communications Manager (CUCM) que é depois integrado com um diretório LDAP.

A integração de diretórios simplifica a administração do perfil de usuário das seguintes formas:

- Importando os perfis de usuários do CUCM para o Cisco WebEx Meetings Server.
- Periodicamente atualiza o banco de dados do Cisco WebEx Meetings Server com os atributos de usuários novos ou modificados no banco de dados do CUCM, incluindo o primeiro nome, o sobrenome, e o endereço de e-mail de cada usuário. O Cisco WebEx Meetings Server diferencia os usuários pelos seus

endereços de e-mail, por isso se os usuários tiverem o mesmo nome e sobrenome mas diferentes endereços de e-mail, o Cisco WebEx Meetings Server os trata como usuários diferentes.

- Periodicamente verifica a base de dados do CUCM para usuários inativos e desativa estes perfis de usuário no banco de dados do Cisco WebEx Meetings Server.
- Permite ao sistema usar a autenticação LDAP para autenticar os usuários de integração de diretórios no Cisco WebEx Meetings Server contra o diretório externo.
- Suporta a integração LDAP totalmente criptografada quando a LDAP Segura (SLDAP) estiver habilitada no CUCM e no servidor LDAP.
- Todos os usuários configurados no CUCM são sincronizados para o Cisco WebEx Meetings Server e suas contas são ativadas. Você pode opcionalmente desativar contas após a sincronização estar concluída. Todos os usuários ativos no CUCM são sincronizados dentro do Cisco WebEx Meetings Server. Usuários inativos não são importados para o Cisco WebEx Meetings Server. (Os usuários podem ser adicionados manualmente no CUCM em ambientes onde LDAP/AD não estão disponíveis ou configurados no CUCM.)

Antes de iniciar

Certifique-se que os seguintes pré-requisitos sejam atendidos antes de prosseguir com a integração de diretórios:

- Agende a sincronização para os horários fora do pico ou nos finais de semana para minimizar o impacto sobre seus usuários.
- Certifique-se de ter uma versão suportada do Cisco Unified Communications Manager (CUCM). Consulte <http://www.cisco.com/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html> para obter mais informações.
- Obtenha credenciais de usuário administrativo CUCM (necessário para adicionar um servidor CUCM para a integração de diretórios).
- Configure o serviço de diretório AXL e LDAP no CUCM. O CUCM é necessário para importar os usuários para o seu sistema Cisco WebEx Meetings Server. Use o CUCM para fazer o seguinte:
 - Ativar o Cisco AXL Web Service
 - Ativar a sincronização de diretórios Cisco
 - Configurar a integração LDAP
 - Configurar a autenticação LDAP

Consulte [Usando o CUCM para configurar o AXL Web Service e a sincronização de diretórios](#), na página 132 e [Usando o CUCM para configurar a integração e a autenticação LDAP](#), na página 132. Consulte http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html para obter informações adicionais.

- Certifique-se de que todos os usuários que exijam privilégios de organizador estejam disponíveis no CUCM. Qualquer usuário que não esteja no CUCM não será capaz de organizar reuniões (todos os usuários podem entrar como convidado). Se necessário, crie filtros ou grupos CUCM em que consistam apenas os usuários que você deseja importar do CUCM.

**Observação**

Se não utilizar grupos CUCM, todos os usuários ativos no CUCM são importados para o Cisco WebEx Meetings Server durante a sua primeira sincronização de diretório. Usuários inativos no CUCM não são importados. Somente os usuários ativos novos e modificados são importados durante as sincronizações subsequentes. Você deve desativar as contas de usuário do Cisco WebEx Meetings Server que você não deseja dar o acesso de organizador. Note que uma licença só é consumida pelo Cisco WebEx Meetings Server quando um usuário realmente organiza uma reunião. Contas que não organizam reuniões não consomem licenças. Consulte "Gerenciando Licenças" em [g_managingYourSystem.xml#topic_1213FB8D4C674F899219DF951AD6990B](#) para mais informações sobre o consumo de licenças.

- Usuários sem endereço de e-mail não são importados.
- Se os usuários possuem várias contas que utilizam o mesmo nome e sobrenome mas são atribuídos diferentes endereços de e-mail no CUCM, quando esses usuários são importados para o Cisco WebEx Meetings Server, estes endereços são tratados como usuários diferentes. Os usuários do CUCM são únicos por nome de usuário para que um administrador possa criar várias contas de usuário com o mesmo endereço de e-mail. Entretanto, as contas no Cisco WebEx Meeting Server são exclusivas pelo endereço de e-mail. Portanto, se várias contas de usuários do CUCM possuem o mesmo endereço de e-mail, o administrador do CUCM deve editar manualmente essas contas de usuários para tornar os endereços de e-mail exclusivos antes de importar essas contas para o Cisco WebEx Meetings Server.
- Quando a autenticação LDAP é habilitada, o Cisco WebEx Meetings Server usa a porta 8443 para se conectar ao CUCM quando você seleciona **Sincronizar Agora** ou marque a opção **Próxima sincronização** e digite uma data e hora.
- Cisco WebEx Meetings Server suporta senhas de até 64 caracteres. Ao criar um usuário no CUCM, garanta que a senha do usuário não tenha mais do que 64 caracteres. Usuários com senhas maiores que 64 caracteres não serão capazes de iniciar sessão no Cisco WebEx.

Etapa 1 Inicie a sessão no site da Administração do Cisco WebEx Meetings Server.

Etapa 2 (Opcional) **Aative o Modo de Manutenção.**

O modo de manutenção *não é necessário* para efetuar a integração de diretórios, porém grandes sincronizações podem afetar o desempenho do sistema. Você pode colocar o seu sistema em modo de manutenção para evitar que os usuários utilizem o sistema durante uma sincronização.

Etapa 3 Selecione **Usuários > Integração de diretórios**.

Etapa 4 (Opcional) Selecione o servidor (sob CUCM) para inserir as informações do servidor CUCM, se você não tiver feito isso:

- Endereço de IP ou o nome de domínio totalmente qualificado (FQDN)
- Nome de usuário
- Senha

O nome de usuário e senha poderão ser o seu nome de usuário e a senha de administrador do CUCM ou AXL. Após você configurar as suas informações no CUCM, o endereço de IP ou o FQDN do seu servidor CUCM aparecem sob o ícone do CUCM.

Observação Após você configurar as suas informações no CUCM, a alteração é um processo complexo que pode causar problemas na sincronização de usuários e não é recomendada.

Etapa 5 Selecione **Grupos de usuários CUCM para filtragem** para adicionar apenas aqueles usuários nos Grupos de Usuários CUCM selecionados para o Cisco WebEx Meeting Server.

Etapa 6 (Opcional) Selecione **Sincronização completa** para sincronizar todos os usuários ou desmarcá-los e o sistema sincroniza apenas os novos usuários. (Dependendo do tamanho do banco de dados do usuário, o desempenho do sistema pode ser afetado quando você optar por sincronizar o banco de dados.)

Etapa 7 Sincronize o seu sistema Cisco WebEx Meetings Server com o seu serviço de diretório LDAP. Você pode executar a sua sincronização das seguintes maneiras:

- Selecione **Sincronizar agora** para executar uma sincronização imediatamente. Você não pode cancelar a sincronização após ela iniciar. Você receberá um e-mail quando a sincronização estiver concluída. Os outros administradores no seu sistema não serão notificados após um **Sincronizar Agora**.
- Selecione **Próxima sincronização** e insira a data e a hora para agendar a sincronização. Você pode optar por **Repetir** a sincronização em intervalos regulares.

Se você selecionar **Sincronizar agora**, o seu sistema efetua imediatamente uma sincronização. Se você agendar uma sincronização, ela ocorre na data e hora indicadas. Todos os administradores recebem um e-mail depois que uma sincronização agendada estiver concluída. Se você deseja impedir futuras sincronizações, você poderá desmarcar a caixa de seleção **Próxima sincronização**.

Os seguintes atributos são mapeados durante o processo de sincronização:

Atributo CUCM	Atributo Cisco WebEx Meetings Server
Nome	Nome
Sobrenome	Sobrenome
ID da mensagem	Endereço de e-mail

Observação O nome e o sobrenome no Cisco WebEx Meetings Server são componentes do nome completo que é exibido para os usuários.

Os atributos mapeados no Cisco WebEx Meetings Server não podem ser atualizados por usuários finais.

Se a sincronização falhar, uma mensagem de erro é exibida na página e um e-mail com informações detalhadas sobre o erro é enviado ao administrador. Selecione **Exibir registros** para ver uma explicação detalhada do erro. Os registros fornecidos incluem um relatório dos usuários desativados, um relatório dos usuários com falhas, e um resumo.

Depois de você ter efetuado pelo menos uma sincronização, um resumo da sua última sincronização será exibido indicando se foi ou não concluída, a hora e a data em que foi concluída (usando a data e hora estabelecidas nas suas configurações das informações da Empresa), e a listagem das mudanças de usuários que incluem o seguinte:

- Adicionados — O número de usuários adicionados.
- Desativados — O número de usuários que foram desativados.

Etapa 8 Selecione **Salvar** se tiver configurado ou alterado o agendamento da sua sincronização ou suas configurações de notificação de administrador.

Etapa 9 Selecione a guia **Usuários** para ter certeza de que os usuários corretos foram sincronizados.

- a) Selecione **Usuários remotos** no menu suspenso para filtrar a lista de usuários. Certifique-se de que os usuários que você queria sincronizados estão presentes nesta lista. Usuários remotos são importados para o Cisco WebEx Meetings Server através de uma sincronização de diretório. Se um usuário for criado localmente primeiro e for sobreescrito por uma sincronização de diretório, este usuário irá tornar-se um usuário remoto, e não um usuário local.
- b) Selecione **Usuários locais** para ver quais os usuários não estavam incluídos na sincronização. Usuários locais são criados localmente por um administrador do Cisco WebEx Meetings Server. Os usuários locais podem ser adicionados manualmente ou importados usando um arquivo CSV.

Etapa 10 Certifique-se de os agendamentos de sincronização do seu CUCM e do Cisco WebEx Meetings Server são sequenciais. A sincronização deve ocorrer primeiro no CUCM e a sincronização do Cisco WebEx Meetings Server deve ocorrer imediatamente após.

Etapa 11 (Opcional) Marque ou desmarque **Notificar os administradores quando a sincronização completar** e depois selecione **Salvar**. Esta opção é selecionada por padrão e só informa os administradores depois de uma sincronização *agendada*.

Etapa 12 Selecione **Ativar a autenticação LDAP**.

Observação Se o seu sistema estiver configurado para usar o SSO, você deve primeiro desativar o SSO. Consulte [Desativando o SSO, na página 229](#) para obter mais informações. Se o seu sistema não estiver configurado para usar o SSO, ele usa a autenticação padrão até você habilitar a autenticação LDAP.

Após habilitar a LDAP, recomendamos que os administradores usem o servidor Active Directory para o gerenciamento de usuários incluindo a adição, a desativação, e a modificação de usuários. Após habilitar a autenticação LDAP, todos os participantes devem usar suas credenciais LDAP para iniciar a sessão no site WebEx. Os administradores, no entanto, ainda usam suas credenciais do Cisco WebEx Meetings Server para iniciarem sessão no site de Administração.

Etapa 13 Certifique-se que seus usuários possam iniciar sessão no sistema com suas credenciais de domínio AD.

Etapa 14 (Opcional) Se você colocou o sistema em modo de manutenção, selecione **Desativar modo de manutenção**.

Etapa 15 (Opcional) Se você tiver feito uma sincronização, você pode selecionar **Notificar agora** para notificar os usuários por e-mail que contas foram criadas para eles no sistema do Cisco WebEx Meetings Server ou quando suas contas forem alteradas. Você poderá, opcionalmente, selecionar **Automaticamente enviar notificações**, que automaticamente envia um e-mail para os seus usuários recém adicionados após cada sincronização. Após qualquer alteração nas configurações de autenticação (por exemplo, habilitando o LDAP), um e-mail com a alteração da senha de usuário é enviado para os usuários afetados.

Quando você seleciona **Notificar agora**

- Todos os usuários recebem apenas uma notificação durante toda a vida deles. As sincronizações subsequentes não causam o envio de e-mails adicionais.
- Os "Usuários que exigem notificação" indicam todos os usuários que estão ativos e ainda não foram notificados.
- Aos usuários inativos ou usuários locais não são enviadas quaisquer notificações.
- Adicionar um usuário local no Cisco WebEx Meetings Server envia um e-mail para este usuário. No entanto, esse usuário deve ser adicionado no seu servidor CUCM Active Directory antes de ele poder iniciar a sessão no site do WebEx.
- Você só pode enviar notificações aos usuários que foram adicionados com a funcionalidade da sincronização.
- Pode demorar alguns minutos para que as suas notificações por e-mail sejam enviadas para os seus usuários. Este atraso é causado por vários fatores alheios ao sistema do Cisco WebEx Meetings Server, incluindo o seu servidor de e-mail, problemas com a conexão de rede e detectores de spam em contas de e-mail individuais.

Seu sistema envia os seguintes e-mails:

- O e-mail de Ativação AD é enviado para cada usuário na primeira vez em que eles forem importados para o seu sistema em uma sincronização. Os usuários não recebem este e-mail nas sincronizações subsequentes.
- O e-mail com alteração da senha de usuário é enviado para os usuários que foram criados localmente no seu sistema.

Consulte [Sobre modelos de e-mail, na página 190](#) para obter informações sobre como personalizar esses modelos de e-mail.

Observação Se você está usando a Integração de Diretórios com a autenticação LDAP, os usuários configurados no CUCM são sincronizados no Cisco WebEx Meeting Server como organizadores e usam as suas credenciais LDAP para iniciarem sessão no site WebEx. Entretanto, se você alterar o tipo de conta de um usuário importado de **organizador** para **administrador**, o usuário recebe um e-mail com um link Criar Senha. Um usuário seleciona este link e digita uma nova senha no Cisco WebEx Meetings Server. O usuário utilizará esta senha recém criada para iniciar sessão no site de Administração, mas continuará a utilizar as credenciais LDAP para iniciar sessão no site WebEx.

Sincronizando Grupos De Usuários

Pode criar grupos de utilizadores administrador em cucm. Por exemplo, um administrador pode criar um grupo de usuários que consiste de usuários que terão permissão para utilizar o Cisco WebEx Meetings Server. De CWMS, o administrador pode filtrar e importar determinados usuários selecionando usuário específico grupos.

Antes de iniciar

Use para criar cucm grupos de utilizadores. Consulte a seção "Configuração de Gerenciamento de Usuário" no *Guia de Administração do Cisco Unified Communications Manager*http://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html para mais informações.

Etapa 1 Inicie a sessão no site da Administração do Cisco WebEx Meetings Server.

Etapa 2 Selecione **Usuários > Integração de diretórios**.

Etapa 3 Selecione o link **Grupos CUCM para Filtragem**.

Etapa 4 Verificar o usuário grupos para ser sincronizadas.

Observação Se não forem selecionados grupos, de integração usuário sincroniza todos os grupos.

Etapa 5 Selecione **Salvar**.

Etapa 6 Selecione Sincronizar Agora para executar uma sincronização imediatamente. O tempo que este processo demora varia de acordo com o número de usuários a serem sincronizados.

Observação O sistema se lembra que foram anteriormente sincronizados grupos de usuários. Se você não selecionar um usuário foi sincronizado anteriormente grupo, os usuários no grupo de usuários será desativado não selecionados durante o processo de sincronização.

Quando a sincronização estiver concluída, o sistema exibe o número de usuários adicionados e desativada.

Etapa 7 Selecione para resumo **Exibir Log** informações sobre os usuários que eram importadas ou desativada durante o processo de sincronização.

Usando o CUCM para configurar o AXL Web Service e a sincronização de diretórios

Use o CUCM para configurar o AXL Web Service e a sincronização de diretórios

Antes de iniciar

Execute este procedimento antes de usar a funcionalidade de integração de diretórios. Consulte [Configurando a integração de diretórios](#), na página 126 para obter mais informações.

Etapa 1 Inicie a sessão na sua conta CUCM.

Etapa 2 Selecione **Servicibilidade do Cisco Unified** do topo direito do menu suspenso e selecione **Ir**.

Etapa 3 Selecione **Ferramentas > Ativação de serviço**.

Etapa 4 Selecione **Cisco AXL Web Service** e **Cisco DirSync** e selecione **Salvar**.

Observação Se uma condição de failover do Cisco Unified Call Manager (CUCM) ocorre em um centro de dados que faz parte de um sistema com Vários centros de dados (MDC), as credenciais de administrador CUCM devem funcionar para todos os CUCMs nesse centro de dados.

Próximos passos

Use o CUCM para configurar a integração e a autenticação LDAP se ainda não tiver feito isso. Consulte [Usando o CUCM para configurar a integração e a autenticação LDAP](#), na página 132 para obter mais informações.

Usando o CUCM para configurar a integração e a autenticação LDAP

Use o CUCM para configurar a integração e a autenticação LDAP.



Importante

Os usuários são identificados no sistema pelo endereço de e-mail. Se um endereço de e-mail do usuário é alterado e o usuário permanece ativo, o endereço de e-mail no CWMS também deve ser alterado ou esse usuário não receberá notificações.



Observação

Se o CUCM é configurado para a Integração de Diretórios, você pode optar por usar a autenticação local, SSO ou LDAP.

Antes de iniciar

Execute este procedimento antes de usar a funcionalidade de integração de diretórios. Consulte [Configurando a integração de diretórios](#), na página 126 para obter mais informações.

-
- | | |
|----------------|--|
| Etapa 1 | Inicie sessão na sua conta do Cisco Unified Call Manager (CUCM). |
| Etapa 2 | Selecione Administração do Cisco Unified CM do menu suspenso no topo direito e selecione Ir . |
| Etapa 3 | Selecione Arquivo > LDAP > Sistema LDAP . |
| Etapa 4 | Selecione Ativar a sincronização a partir do servidor LDAP , selecione Microsoft Active Directory para o tipo de servidor LDAP, selecione Nome de conta sAM para o atributo LDAP para a ID de usuário e selecione Salvar . |
| Etapa 5 | Selecione a caixa de seleção para o servidor LDAP e então selecione Adicionar novo . |
| Etapa 6 | Complete os campos na página do Diretório LDAP e selecione Salvar . |
| Etapa 7 | Na página de autenticação LDAP, selecione a caixa de seleção Usar a autenticação LDAP para usuários finais , complete os campos na página, e então selecione Salvar . |
-

Próximos passos

Use o CUCM para configurar o Cisco AXL Web Service e o Cisco Directory Sync se ainda não tiver feito isso. Consulte [Usando o CUCM para configurar o AXL Web Service e a sincronização de diretórios](#), na página 132 para obter mais informações.

Enviando E-mails aos usuários

-
- | | |
|----------------|--|
| Etapa 1 | Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel. |
| Etapa 2 | Para enviar notificações por e-mail aos usuários, selecione Usuários > Enviar e-mail aos usuários . |
| Etapa 3 | Insira um endereço de e-mail de usuário alvo ou um apelido de e-mail no campo Para ou deixe o campo em branco para enviar e-mail para todos os usuários. |
| Etapa 4 | (Opcional) Insira os endereços de e-mail ou um apelido de e-mail no campo BCC . |
| Etapa 5 | Insira o assunto no campo Assunto . |
| Etapa 6 | Insira uma mensagem no campo Mensagem . |
| Etapa 7 | Clique em Enviar .
Pode demorar alguns minutos para que seus e-mails sejam recebidos pelos usuários. Este atraso pode ser causado por vários fatores alheios ao sistema do Cisco WebEx Meetings Server, incluindo o seu servidor de e-mail, velocidade de conexão de rede e detectores de spam em contas de e-mail individuais.
O seu e-mail foi enviado. |
-



Configurando Seu Sistema

Este módulo descreve como usar as páginas de administrador para configurar o seu sistema.

- [Configurando as Propriedades do Sistema, página 135](#)
- [Configurando Definições Gerais, página 142](#)
- [Configurando os Servidores, página 144](#)
- [Configurando as Suas Definições de SNMP, página 151](#)

Configurando as Propriedades do Sistema

Configure as propriedades do sistema, selecionando o Sistema e Exibir Mais na seção do Sistema.

Alterando as configurações da máquina virtual

Use este recurso para alterar as configurações da máquina virtual. Não utilize o VMware vCenter para alterar as configurações da máquina virtual.

Durante a implantação, você só pode definir as configurações de IPv4. Após a implantação, você pode configurar as definições IPv6 se você tiver uma conexão IPv6 entre o proxy reverso da Internet na rede DMZ e suas máquinas virtuais internas.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões.

ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Sistema** e selecione **Ver Mais** na seção de Sistema.

Etapa 4 Para modificar as configurações de uma máquina virtual, selecione o nome da máquina virtual na seção do Sistema Primário ou do Sistema de Alta Disponibilidade.

Etapa 5 Você pode modificar as seguintes configurações da máquina virtual:

- Nome de domínio totalmente qualificado (FQDN) em caracteres minúsculos
- Servidor primário DNS
- Servidor secundário DNS
- Prefixo/Máscara de Sub-rede
- Entrada

O campo de Máquina Virtual fica acinzentado (indisponível). O sistema recupera automaticamente o endereço de IP solucionando o nome do organizador para o endereço de IP de uma máquina virtual no servidor DNS. Consulte [Alterando o endereço de IP de uma máquina virtual, na página 137](#) para obter mais informações sobre como alterar o endereço de IP de uma máquina virtual.

Etapa 6 Selecione **Salvar**.
Suas alterações são salvas e a máquina virtual é reiniciada.

Etapa 7 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Próximos passos

Se você fizer alterações em qualquer uma das máquinas virtuais, você deve implantar um novo certificado em todas as máquinas virtuais em cada centro de dados, a menos que você esteja usando certificados curinga para os sistemas no mesmo domínio. Para obter mais informações, consulte [Gerenciando Certificados, na página 214](#).

Alterando o endereço de IP de uma máquina virtual

Se você alterar o nome do organizador de uma máquina virtual que faz parte da sua implantação, o endereço de IP correspondente é captado automaticamente do DNS. Este procedimento explica como alterar o endereço de IP de uma máquina virtual e manter o mesmo nome de organizador.

-
- Etapa 1** Configure um nome de organizador temporário no servidor DNS.
 - Etapa 2** Complete o procedimento [Alterando as configurações da máquina virtual, na página 135](#) para alterar o nome do organizador da máquina virtual para o nome do organizador temporário que você inseriu no servidor DNS.
Quando você tirar o sistema do modo de manutenção, o novo nome de organizador temporário entrará em vigor.
O nome de organizador original não será mais parte da implantação depois de fazer esta mudança.
 - Etapa 3** Altere o endereço de IP do nome do organizador original no DNS para o novo endereço de IP.
 - Etapa 4** Usando o procedimento [Alterando as configurações da máquina virtual, na página 135](#), altere o nome do organizador temporário da máquina virtual para o nome do organizador original.
Quando você tirar o sistema do modo de manutenção, o nome do organizador original entrará em vigor.
Agora o nome do organizador original com o novo endereço de IP está configurado.
-

Alterando o endereço de IP virtual

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
 - Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#))
 - Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.
 - Etapa 3** Selecione **Sistema**, selecione o *centro de dados*, e selecione **Ver mais** na seção Sistemas.
A página **Propriedades** é exibida.
 - Etapa 4** Para modificar os endereços de IP, na seção Endereço de IP Virtual, selecione um link na coluna Tipo.
 - Etapa 5** Insira os endereços de IP virtuais.
 - Etapa 6** Insira o endereço de IP virtual, a máscara de sub-rede e um gateway na coluna Endereço IPv6 se você tiver habilitado IPv6 para conexões de clientes.

Os endereços de IP virtuais públicos e privados devem estar em sub-redes IPv6 separadas.

Etapa 7 Selecione **Salvar**.

Etapa 8 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Configurando o Acesso Público

O acesso público possibilita que pessoas externas à sua rede organizem e participem de reuniões online através da Internet ou dispositivos móveis. Remover o acesso público removerá as configurações do endereço de IP virtual público para a URL do seu site WebEx e encerrará o acesso externo ao seu site.

Adicionando acesso público ao seu sistema utilizando IRP

Os requisitos para o Proxy reverso de Internet (IRP) são:

- O processo de adição ou remoção de IRP é o mesmo para um sistema de centro de dados único, pois ele é para um sistema de MDC.
- Ao adicionar um centro de dados para um sistema de MDC, todos os centros de dados ou nenhum dos centros de dados deve ser configurado para usar o IRP.
- Um nó IRP é usado por centro de dados.
- Modificar o IRP exige que o sistema seja colocado no modo de manutenção. Em um sistema de MDC, o IRP pode ser adicionado ou removido de um sistema de cada vez para evitar a interrupção do serviço.
- Em um ambiente de MDC, adicionar ou remover um VIP público local em um centro de dados não afeta os outros centros de dados.

Para uma descrição de topologia de proxy reverso da Internet interna, consulte [Topologia de rede do proxy reverso da internet \(IRP\) interna](#).

Antes de iniciar

Para permitir o acesso público, você deve primeiro configurar uma máquina virtual do proxy reverso da Internet para servir como o sistema de acesso público. Inicie o VMware vCenter e realize o seguinte:

- Faça backup de suas máquinas virtuais usando o VMware Data Recovery (vSphere 5.0) ou o VMware vSphere Data Protection (vSphere 5.1). Isso permite que você reverta as alterações, se necessário. Consulte [Criando um Backup Usando o VMware vCenter](#), na página 6 para obter mais informações.
- Implemente uma máquina virtual de proxy reverso da internet usando o mesmo arquivo OVA que você usou para implantar a máquina virtual do administrador. A máquina virtual de proxy reverso da internet deve estar na mesma sub-rede que o endereço de IP virtual público.

**Observação**

Se você tem um sistema de alta disponibilidade, você também deve implantar uma máquina virtual de proxy reverso da internet para o sistema de alta disponibilidade.

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#))
- Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.
- Etapa 3** Selecione **Sistema > Ver mais**.
- Etapa 4** Selecione **Adicionar Acesso Público**.
- Etapa 5** Insira sua máquina virtual de proxy reverso da internet no campo **FQDN**.
Há dois campos de nomes de domínios totalmente qualificados (FQDN) se o seu sistema está configurado para alta disponibilidade. Insira o FQDN de alta disponibilidade no segundo campo.
- Etapa 6** Selecione **Detectar máquinas virtuais**.
Se o sistema não está configurado para alta disponibilidade, aparece uma tabela mostrando a máquina virtual de proxy reverso da internet.
Se o sistema está configurado para alta disponibilidade, aparece uma tabela mostrando a máquina virtual do proxy reverso da internet do sistema primário e a máquina virtual do proxy reverso da internet de alta disponibilidade.
Se o sistema tem qualquer atualização incompatível com a versão OVA que você usou para criar a máquina virtual de proxy reverso da Internet, você receberá uma mensagem de erro e não poderá continuar até depois de reimplantar a máquina virtual de proxy reverso da Internet utilizando um arquivo OVA apropriado.
- Etapa 7** Selecione **Continuar**.
- Etapa 8** Insira o endereço de IP da mesma sub-rede que você usou para configurar a máquina virtual de proxy reverso da internet no campo **Endereço de IPv4 Virtual Público (VIP)** e selecione **Salvar**.
Seu sistema está atualizado e o acesso público está configurado. Mantenha a janela do navegador aberta durante todo o processo.
Se o sistema requer pequenas atualizações compatíveis com a versão OVA que você usou para criar a máquina virtual de proxy reverso da internet, elas serão aplicadas automaticamente na sua máquina virtual de proxy reverso da internet.
- Etapa 9** Se o seu sistema requer pequenas atualizações, você será solicitado a selecionar **Reiniciar** depois que as atualizações forem concluídas.

Após a reinicialização do sistema, você receberá uma mensagem de confirmação indicando que você adicionou o acesso público.

- Etapa 10** Verifique a sua configuração. Se você estiver satisfeito, você pode apagar o backup da máquina virtual que você configurou antes de realizar este procedimento.
- Etapa 11** Selecione **Concluído**.
- Etapa 12** Verifique se os seus certificados de segurança ainda são válidos. Pelo fato deste procedimento alterar as suas máquinas virtuais, ele pode afetar os seus certificados. Se necessário, o sistema fornece um certificado autoassinado para manter o funcionamento do sistema até que você possa reconfigurar os seus certificados. Consulte [Gerenciando Certificados, na página 214](#) para obter mais informações.
- Etapa 13** Faça as alterações necessárias para os seus servidores DNS.
- Etapa 14** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.
O serviço de reuniões para usuários neste centro de dados é restaurado.

Removendo o Acesso Público

Antes de iniciar

Faça backup das suas máquinas virtuais usando o VMware Data Recovery ou o VMware vSphere Data Protection. Consulte [Criando um Backup Usando o VMware vCenter, na página 6](#) para obter mais informações. Verifique se você ligou as suas máquinas virtuais após o backup estar completo.

- Etapa 1** Inicie sessão no site da Administração. Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#). Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.
- Etapa 3** Selecione **Sistema** e então selecione o link **Ver Mais** na seção de Sistema.

A página **Propriedades** é exibida.

Etapa 4 Selecione o site desejado, selecione **Remover Acesso Público** e selecione **Continuar**.

Depois de remover o acesso público do seu site, você não pode adicionar a mesma máquina virtual proxy da internet neste site. Para reconfigurar o acesso público, você precisa começar novamente através da reimplantação de uma máquina virtual proxy reverso da Internet do arquivo OVA. Consulte [Adicionando acesso público ao seu sistema utilizando IRP, na página 138](#) para obter mais informações.

O acesso público é removido do site.

Etapa 5 Selecione **Concluído**.

Etapa 6 Abra o VMware vCenter. Desligue e exclua a máquina de Proxy Reverso da Internet (e a máquina de proxy reverso da Internet de alta disponibilidade, se implantada) do seu sistema.

Etapa 7 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Configurando IPv6 para conexões de clientes

Quando você tem uma topologia de rede sem split-horizon, todos os usuários (internos e externos) com uma conexão de cliente IPv6 podem acessar a URL do site WebEx usando o endereço VIP público para organizar e acessar reuniões on-line. Quando as informações sobre o endereço de IP virtual IPv6 privado estão configuradas, os administradores com uma conexão de cliente IPv6 podem iniciar sessão no site da Administração.



Observação

- O endereço de IP virtual privado IPv6 deve estar na mesma sub-rede IPv6 que a máquina virtual de Administração.
- O endereço de IP virtual público IPv6 deve estar na mesma sub-rede IPv6 que a máquina virtual de Proxy Reverso da Internet.

Antes de iniciar

Considere o seguinte ao configurar uma conexão de cliente IPv6:

- Configurando uma conexão IPv6 apenas para topologias de rede sem split-horizon.
- As informações de endereço IPv4 já devem estar configuradas para máquinas virtuais internas e proxy reverso da Internet.
- O endereço de IP virtual privado e público IPv4 já deverá estar configurado antes de configurar um endereço de IP virtual público IPv6.
- O endereço de IP virtual privado e público para conexões de clientes IPv6 estão em sub-redes separadas.

- Configure os servidores DNS para que a URL de Administração local aponte para os endereços de IP virtuais IPv4 privado e IPv6 privado.
- Configure os servidores DNS para que a URL do site WebEx aponte para os endereços de IP virtuais IPv4 público e IPv6 público.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Ativar modo de manutenção > Continuar**.

Etapa 3 Selecione **Sistema** e então selecione o link **Ver Mais** na seção de Sistema.

Etapa 4 Na seção de Endereço de IP Virtual, selecione um link na coluna **Tipo**.

- Selezione o link *Público* para configurar o endereço IPv6 para acessar a URL do site WebEx.
- Selezione o link *Privado* para configurar o endereço IPv6 para acessar a URL de Administração.

A página Endereço de IP Virtual Privado ou Público exibe o endereço de IP IPv4, a máscara de sub-rede e um endereço de IP do gateway inseridos anteriormente da URL do site WebEx e da URL de Administração.

Etapa 5 Na coluna **Endereço IPv6**, insira o endereço de IP IPv6, a máscara de sub-rede e o endereço de IP do gateway da URL do site WebEx e da URL de Administração.

Etapa 6 Selecione **Salvar**.

Etapa 7 Selecione **Desativar modo de manutenção > Continuar**.

O sistema reinicia após desligar o modo de manutenção. Você pode iniciar sessão novamente no site de Administração, após a reinicialização.

Configurando Definições Gerais

Definições gerais incluem os seguintes parâmetros:

- Configurações do site — Gerencia a URL do site.
- Configurações do site de administração — Gerencia a URL do site de administração.

Endereços de IP virtuais são mostrados no bloco de informação e podem ser gerenciados no **Sistema > Propriedades**.

Alterando as Configurações do Seu Site

Use este recurso para configurar ou alterar a URL do site de administração e a URL do site da administração local, se você tiver um sistema com Vários centros de dados (MDC). Você configurou as URLs do site original durante a implantação. Em um sistema de MDC, a URL do site local é configurada durante o processo de registro dos centros de dados. Para obter maiores informações sobre a configuração da URL do site e nomear convenções, consulte [URLs do Site WebEx e da Administração WebEx, na página 27](#).

Antes de iniciar

Certifique-se de manter a URL do site original no servidor DNS e redirecionar a URL do site original para a URL do site atualizado. Se os usuários tentarem usar a URL original e você não tiver redirecionado para a nova URL, eles não serão capazes de organizar ou participar de reuniões ou efetuar logon em páginas da internet, ferramentas de produtividade e aplicativos móveis.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter](#), na página 7.)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Sistema > (Configuração/Configurações gerais)** [Ver mais](#).

A janela Configurações Gerais é exibida.

Etapa 4 Selecione o centro de dados, se este for um sistema de MDC.

Etapa 5 Na seção Configurações do site a ser modificada, selecione **Editar**.

Etapa 6 Insira as URLs e selecione **Salvar**.

Etapa 7 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Próximos passos

Atualize o certificado do seu site para garantir acesso seguro. Consulte [Gerenciando Certificados](#), na página 214 para obter mais informações.

Alterando Suas Configurações de Administração

Você configura a definição da URL do seu site de administração original durante a implantação. Em um sistema de MDC, a URL do site de Administração Local é configurada durante o processo de registro dos centros de dados. Para obter maiores informações sobre a configuração do site de administração e nomenclatura de convenções, consulte [URLs do Site WebEx e da Administração WebEx](#), na página 27.

Antes de iniciar

Certifique-se de manter a URL original do seu site de administração no servidor DNS. Redirecione a URL do seu site original de administração para a URL do site de administração atualizado. Se os usuários tentarem usar a URL original e você não tiver redirecionado para a nova URL, eles não serão capazes de organizar ou participar de reuniões ou efetuar logon em páginas da internet, ferramentas de produtividade e aplicativos móveis.

-
- Etapa 1** Inicie sessão no site da Administração.
- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).)
- Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.
- Etapa 3** Selecione **Sistema**.
- Etapa 4** Na seção Configuração, selecione **Ver mais**.
- Etapa 5** Na seção Configurações de Administração, selecione **Editar**.
- Etapa 6** Insira as novas URLs do site de administração na caixa de diálogo e selecione **Salvar**.
- Etapa 7** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.
- O serviço de reuniões para usuários neste centro de dados é restaurado.
-

Próximos passos

Atualize o certificado do seu site para garantir acesso seguro. Consulte [Gerenciando Certificados, na página 214](#) para obter mais informações.

Configurando os Servidores

Use estes recursos para configurar os seus servidores:

- Servidor SMTP — O servidor SMTP cuida do envio de e-mails do Cisco WebEx Meetings Server para o destino.
- Servidor de Armazenamento — O servidor NFS é o servidor de armazenamento onde todas as gravações de reunião são armazenadas.

Configurando um servidor de e-mail (SMTP)

Configure um Servidor de e-mail para habilitar o sistema para enviar convites de reuniões e outras comunicações aos usuários.

É importante que o Servidor de e-mail esteja sempre operacional. O e-mail é o principal método de comunicação com os seus usuários, incluindo notificações de gravação, alterações de informações de reuniões, estado da conta e muitos outros anúncios importantes. (Consulte também [Adicionar usuários](#), na página 121).



Importante

Os usuários são identificados no sistema pelo endereço de e-mail. Se um endereço de e-mail do usuário é alterado e o usuário permanece ativo, o endereço de e-mail no CWMS também deve ser alterado ou esse usuário não receberá notificações.



Observação

Não é necessário desativar o modo de manutenção para modificar estas propriedades.

Etapa 1 Inicie sessão no site de Administração.

Etapa 2 Selecione **Sistema** e selecione **Exibir Mais** na seção Servidores.

Etapa 3 Na seção **Servidor SMTP**, selecione **Editar**.

Etapa 4 Insira o nome de domínio totalmente qualificado (FQDN) de um servidor de e-mail que o sistema usará para enviar e-mails.

Etapa 5 (Opcional) Selecione **TLS habilitado** para ativar o Transport Layer Security (TLS). (A autenticação básica está habilitada por padrão.)

Etapa 6 (Opcional) Edite o campo **Porta** para alterar o valor padrão.

Os números de porta padrão SMTP são 25 ou 465 (porta SMTP segura).

Observação O nó da Web e o nó da Administração enviam solicitações SMTP para o servidor de e-mail configurado. Se houver um firewall entre as máquinas virtuais internas da Web e de Administração e o servidor de e-mail, o tráfego SMTP pode ser bloqueado. Para garantir que a configuração do servidor de e-mail e a notificação de e-mail funcionem corretamente, a porta 25 ou 465 (número de porta SMTP segura) deve estar aberta entre o servidor de e-mail e as máquinas virtuais da Web e de Administração.

Etapa 7 (Opcional) Ative a autenticação do servidor de e-mail, selecione **Autenticação do servidor habilitada**. Se você ativar a autenticação, insira as credenciais **Nome de usuário** e **Senha** necessárias para o sistema acessar o servidor de e-mail corporativo.

Os e-mails do sistema são enviados pelo admin@<WebEx-site-URL>. Verifique se o servidor do e-mail pode reconhecer este usuário.

Para sistemas micro, pequenos ou médios, as notificações de e-mail vêm das máquinas virtuais de administração (sistema primário ou de alta disponibilidade).

Para sistemas grandes, as notificações de e-mail vêm das máquinas virtuais da web (sistema primário ou de alta disponibilidade). Em um sistema grande, existem três máquinas virtuais da web no sistema primário e uma máquina virtual da web no sistema de alta disponibilidade.

Etapa 8 Selecione **Salvar**.

Próximos passos

Consulte também [Ativação ou desativação de usuários e administradores a partir da página Usuários](#), na página 124, [Adicionar usuários](#), na página 121 e [Editando Usuários](#), na página 122.

Configurando um Servidor de Armazenamento

Use o seu servidor de armazenamento para fazer backup do sistema e armazenar as gravações das reuniões. Durante uma Recuperação de Desastres (consulte [Recuperação de desastres usando o servidor de armazenamento](#), na página 148), esses backups podem ser usados para restaurar o sistema. (O método de armazenamento suportado é o Network File System (NFS). Certifique-se de que o servidor de armazenamento seja acessível a partir de todas as máquinas virtuais internas. (Também há um recurso de Recuperação de Dados VMware fornecido pela VMware para fazer o backup das máquinas virtuais. Consulte http://www.vmware.com/pdf/vdr_11_admin.pdf para obter mais informações.)

Você não precisa conectar seu servidor de armazenamento para as máquinas virtuais externas, tais como servidores externos do proxy reverso da Internet (IRP).



Restrição

Não crie manualmente os arquivos ou diretórios no compartilhamento NFS usado pelo Cisco WebEx Meetings Server, uma vez que ele executa vários scripts em arquivos e diretórios NFS. O servidor de armazenamento NFS deve ser de uso exclusivo do Cisco WebEx Meetings Server.

O servidor de armazenamento apoia o seguinte em uma base diária:

- Algumas configurações do sistema
- Informações do usuário
- Informações sobre a reunião
- Certificados SSL carregados no sistema
- URL do site

Os backups são realizados diariamente e são inicialmente definidos para 04h20, horário local. O Cisco WebEx Meetings Server é executado durante o processo de backup, sem qualquer interrupção de reuniões, gravações ou outras funções. O sistema não elimina o backup anterior até o próximo backup diário estar completo para garantir que um backup esteja disponível.

O sistema leva cerca de cinco minutos para fazer o backup de 500 MB. O tempo que leva para fazer o backup do sistema depende da velocidade de armazenamento, velocidade de NFS e de outros fatores. Um banco de dados de 70 GB leva aproximadamente uma hora para fazer backup e 10 minutos para transferi-lo para o NFS. O tempo de transferência é de 12 MB/seg, a fim de permitir outra comunicação de rede e garantir o funcionamento contínuo do produto.

Antes de iniciar

Certifique-se de configurar os privilégios do seu acesso Unix para que o seu sistema possa armazenar o conteúdo gerado pelos usuários e os backups de sistema.

Nos sistemas de armazenamento baseados em Linux, isto depende da configuração das suas permissões de leitura/gravação para os usuários anônimos em um diretório específico a ser utilizado no seu sistema de arquivos de rede (NFS).

Nos sistemas de armazenamento baseados em Windows, isto depende do **Acesso à Rede: Deixe que as permissões de Todos se apliquem às configurações dos usuários anônimos**. Além disso, você deve fornecer ao grupo de usuários Todos as permissões de leitura e gravação para o NFS.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Na seção Servidores, selecione **Servidores > (Servidores) Ver mais**.

Se um servidor de armazenamento está presente no seu sistema, ele é exibido nesta página. Se não há nenhum servidor de armazenamento no seu sistema, você terá a opção de configurar um.

Etapa 4 Na sessão Servidor de Armazenamento, selecione **Adicionar um Servidor de Armazenamento agora**.

Etapa 5 Insira ponto de montagem NFS e selecione **Salvar**.

O sistema confirma o seu ponto de montagem NFS.

Etapa 6 Selecione **Continuar**.

Você recebe uma mensagem de confirmação que o seu servidor de armazenamento foi adicionado.

Etapa 7 Selecione **Concluído**.

Etapa 8 (Opcional) Você pode alterar a hora padrão para o backup diário. Na seção Servidor de Armazenamento, clique na **hora** do Horário de Backup do Sistema e selecione outra hora no menu. Depois selecione **Salvar**. Um backup diário ocorre na hora selecionada.

Etapa 9 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Próximos passos

Configure o seu sistema para usar o servidor de armazenamento para o seguinte:

- Gravações de reunião.

- Recuperação de desastre. Consulte [Recuperação de desastres usando o servidor de armazenamento, na página 148](#) para obter mais informações.

Para garantir o bom funcionamento do seu servidor de armazenamento, certifique-se de que

- Seu servidor de armazenamento possa ser acessado de fora do Cisco WebEx Meetings Server.
- Seu servidor de armazenamento esteja ligado.
- Existe conectividade de rede para o seu servidor de armazenamento.
- A montagem/acesso é possível a partir de uma máquina sem o Cisco WebEx Meetings Server.
- Seu servidor de armazenamento não está cheio.



Observação

Se um usuário inadvertidamente apaga uma gravação da página **gravações de reunião Cisco WebEx** mas a gravação está salva no servidor de armazenamento do sistema de arquivos de rede (NFS), contate o centro de assistência técnica Cisco (CAT) para assistência na recuperação da gravação.

Recuperação de desastres usando o servidor de armazenamento

Um desastre pode ser uma falha de rede, falha do servidor, queda do centro de dados ou outro evento que faz com que o seu sistema seja inutilizável. Existem dois tipos de recuperação de desastres:

- Recuperação de desastres do Centro de dados único (SDC) — Você pode reinstalar o sistema SDC no mesmo centro de dados e restaurá-lo para o mesmo estado, utilizando backups do servidor de armazenamento.
- Recuperação de desastres de Vários centros de dados (SDC) — Se um centro de dados falhar, você pode acessar o sistema MDC através do segundo centro de dados, restaurar o centro de dados danificado e unir os centros de dados para restaurar o sistema MDC.

Depois de configurar um servidor de armazenamento, é feito o backup do sistema em uma base diária. Um aviso de backup do sistema aparece no seu painel que inclui informações sobre o backup mais recente. Apenas um sistema de cópia de segurança é mantido em armazenamento de cada vez. Depois de executar um aprimoramento ou atualização, o backup da versão do Cisco WebEx Meetings Server anterior é mantido. Nós recomendamos que você não use o mesmo diretório de armazenamento para diferentes instalações do Cisco WebEx Meetings Server.

Note que a recuperação de desastres

- Demora mais de 30 minutos.
- Substitui as suas configurações com as configurações do backup mais recente.
- Requer que você execute as etapas adicionais para restaurar o serviço aos seus usuários (detalhado em *O que fazer a seguir* na seção)

Este procedimento faz a cópia de segurança de algumas configurações do sistema, informações do usuário, informações de reuniões, certificados SSL carregados no sistema e a URL do site. O processo da cópia de segurança não armazena as credenciais do VMware ou as informações do endereço de IP nas máquinas virtuais individuais. (Também há um recurso de Recuperação de Dados VMware fornecido pela VMware para fazer o backup das máquinas virtuais. Consulte http://www.vmware.com/pdf/vdr_11_admin.pdf para obter mais

informações.) Na eventualidade de você executar uma recuperação de desastres, você deve reaplicar manualmente certas configurações, incluindo as seguintes:

- Conexões para determinados componentes externos, por exemplo o Cisco Unified Communications Manager (CUCM).
- Certificados SSL (caso os nomes dos organizadores do sistema de recuperação de desastres diferir daqueles no sistema original).
- Em sistemas SDC, você pode usar, opcionalmente, o mesmo endereço de IP ou o nome de organizador. Em sistemas com vários centros de dados, você pode, opcionalmente, usar os endereços de IP ou os nomes de organizadores originais para o sistema primário.

Execute o procedimento abaixo depois que um desastre ocorreu e você perdeu a capacidade de utilizar o sistema.

Antes de iniciar

Procedimentos para efetuar a recuperação de desastres:

- Um servidor de armazenamento deve ter sido configurado. Se você não tiver um servidor de armazenamento configurado, a opção **Recuperação de Desastres** não estará disponível e nenhuma cópia de segurança estará disponível. Consulte [Configurando um Servidor de Armazenamento, na página 146](#) para obter mais informações.
- Você deve ter acesso a um sistema no qual você pode restaurar a sua implantação. Consulte as informações na recuperação de desastres do Centro de dados único (SDC) e Vários centros de dados (MDC), abaixo.
- O seu sistema de recuperação deve ser do mesmo tamanho da implantação e da versão do software que o seu sistema original.

Para um sistema de alta disponibilidade (HA), você deve primeiro configurar a recuperação de desastres, e depois configurar a HA no sistema. Se você tem um sistema HA que exige a recuperação de desastres, você deve primeiro restaurar o sistema e depois reconfigurar a HA no sistema restaurado. Para obter mais informações sobre a HA, consulte [Adicionar um Sistema de Alta Disponibilidade, na página 57.](#)

Etapa 1 Inicie a sessão no site da Administração em um sistema onde você pode restaurar a sua implantação.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior.](#) Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.\)](#)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Sistema > > Servidores > Adicionar servidor de armazenamento.**

Etapa 4 Insira o nome do seu servidor de armazenamento no campo **Ponto de montagem NFS** e selecione **Salvar**.

Exemplo:

192.168.10.10:/CWMS/backup.

Etapa 5

Selecione **Continuar** para prosseguir com a recuperação de desastres.

Se o tamanho da implantação do sistema de recuperação e da versão do software correspondem ao seu sistema original, você pode prosseguir com a recuperação de desastres. Se o sistema tem um tamanho diferente de implantação ou versão de software, você não pode continuar até que você a reimplantação aplicativo no seu sistema para que a implantação de tamanho e software corresponde a versão original implantação. O endereço de IP ou nome do organizador não precisam corresponder à sua implantação original.

Etapa 6

Selecione uma das seguintes opções para continuar:

- **Cancelar** — Faça backup do seu sistema pré-existente antes de adicionar um servidor de armazenamento. Depois de fazer o backup do seu sistema, você retorna para esta página e pode selecionar **Continuar** para prosseguir.
- **Continuar** — Substitua seu sistema pré-existente e continue com a recuperação de desastres.

O processo de recuperação de desastre inicia. Se você fechar o navegador, você não poderá iniciar sessão novamente no sistema até que o processo seja concluído.

Etapa 7

Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Próximos passos

É necessário executar os seguintes procedimentos para restaurar o serviço para os usuários:

- Reconfigurar suas definições de teleconferência. Consulte Configurar CUCM no Guia de Planejamento para obter mais informações.
- Reconfigurar suas configurações SSO. Consulte [Configurando as Definições de Registro Único Federado \(SSO\)](#), na página 226 para obter mais informações.
- Reconfigure suas configurações SNMP. Consulte [Configurando as Suas Definições de SNMP](#), na página 151 para obter mais informações.
- Reconfigure os seus certificados. Você pode ter que recarregar os seus certificados SSL se eles não coincidem com os certificados SSL que estão configurados no sistema de recuperação. Consulte [Restaurar um Certificado SSL](#), na página 221 para obter mais informações.
- O sistema de recuperação é configurado inicialmente para o Modo de Licença Gratuita, que expira em 180 dias. Reorganize as licenças do seu sistema anterior no sistema de recuperação. Consulte [Reorganizando licenças após uma grande modificação do sistema](#), na página 253 e [Sobre Licenças](#) para obter mais informações.
- Defina as configurações DNS para que a URL do seu site aponte para o VIP atual. O VIP no sistema restaurado pode ser diferente do qual você tinha no sistema original. Você deve completar a configuração DNS para usuários finais para que utilizem os links originais para iniciarem sessão ou participarem de

reuniões no sistema restaurado. Consulte [Alterando o endereço de IP virtual, na página 137](#) para obter mais informações.

- Se você configurou o seu sistema para a integração de diretórios e habilitou a autenticação LDAP, verifique se as suas credenciais do CUCM estejam funcionando. Depois de tirar o seu sistema do modo de manutenção e o reinício do sistema estiver concluído, inicie a sessão no site de Administração, selecione **Usuários > Integração de Diretórios**, e então selecione **Salvar**. Se as suas credenciais do CUCM estiverem erradas, você receberá uma mensagem de erro **Credenciais Inválidas**. Se você receber esta mensagem de erro, digite as credenciais corretas e selecione **Salvar** novamente. Consulte [Configurando a integração de diretórios, na página 126](#) para obter mais informações.

Configurando as Suas Definições de SNMP

Você pode configurar as seguintes definições SNMP

- Sequências de comunidade — Autenticar acesso das sequências de comunidade SNMP aos objetos MIB e funções como senhas embutidas.
- Usuários USM — Configura a segurança com base no usuário (USM) para fornecer segurança de nível de mensagem adicional. Seleccione uma configuração USM existente para editá-la ou adicionar configurações USM adicionais. Além do usuário USM padrão, serveradmin, que tem privilégios para ler e escrever as informações MIB, todos os novos usuários USM que você configurar terão apenas privilégios somente leitura das informações MIB.
- Destinos de notificação — Use este recurso para configurar a armadilha/informação do receptor.

Configurando as Sequências de Comunidade

Você pode adicionar e editar sequências de comunidade e privilégios de acesso a sequência de comunidade.

Adicionar Sequências de Comunidade

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões

ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Sistema** e selecione o link **Exibir mais** na seção **SNMP**.

Etapa 4 Selecione **Adicionar** na seção **Sequências de Comunidade**.

Etapa 5 Complete os campos na página **Adicionar Sequência de Comunidade**.

Opção	Descrição
Nome da String da Comunidade	Insira o nome da sua sequência de comunidade. Comprimento máximo: 256 caracteres.
Privilégios de Acesso	Defina os privilégios de acesso para a sequência de comunidade. As opções incluem: <ul style="list-style-type: none"> • ApenasLeitura • LeituraEscrita • NotificarLeituraEscrita • ApenasNotificar • Nenhum Padrão: ApenasLeitura
Informações do Endereço de IP do Organizador	Selecione o tipo de informação do endereço de IP do organizador. (Padrão: Aceitar Pacotes SNMP de quaisquer Organizadores) Se você selecionar Aceitar Pacotes SNMP destes Organizadores , uma caixa de diálogo aparece abaixo da seleção. Insira os nomes de organizadores e endereços de IP separados por vírgulas.

Selecione **Adicionar**.

A sequência de comunidade é adicionada em seu sistema.

Etapa 6 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Editando Sequências de Comunidade

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#))

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

- Etapa 3** Selecione **Sistema** e selecione o link **Exibir mais** na seção **SNMP**.

- Etapa 4** Selecione um link do nome da sequência de comunidade na seção **Sequências de Comunidade**.

- Etapa 5** Altere os campos desejados na página **Editar Sequência de Comunidade**.

Opção	Descrição
Nome da String da Comunidade	Altere o nome da sua sequência de comunidade. Comprimento máximo: 256 caracteres.
Privilégios de Acesso	Defina os privilégios de acesso para a sequência de comunidade: <ul style="list-style-type: none"> • ApenasLeitura • LeituraEscrita • NotificarLeituraEscrita • ApenasNotificar • Nenhum Padrão: ApenasLeitura
Informações do Endereço de IP do Organizador	Selecione o tipo do endereço de IP do seu organizador. Padrão: Aceitar Pacotes SNMP de qualquer Organizador Aceite pacotes SNMP desses organizadores: uma caixa de diálogo é exibida abaixo da seleção. Insira os nomes de organizadores e endereços de IP separados por vírgulas.

Selecione **Editar**.

As informações da sua sequência de comunidade são alteradas.

- Etapa 6** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Configurando os Usuários de USM

Você pode adicionar e editar os seus usuários USM.

Adicionar Usuários USM

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).)

Ativar o modo de manutenção em todos os centros ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Sistema** e então selecione **Exibir mais** na seção SNMP.

Etapa 4 Selecione **Adicionar** na seção de Usuários USM.

Etapa 5 Conclua os campos na página **Adicionar Usuário USM**.

Opção	Descrição
Nome de Usuário USM	Insira o nome de usuário USM que você deseja configurar. Máximo de 256 caracteres.
Nível de Segurança	<p>Selecione o nível de segurança. O nível de segurança que você seleciona, determina quais algoritmos e senhas você pode definir para o usuário. As opções incluem:</p> <ul style="list-style-type: none"> • noAuthNoPriv — Nenhum algoritmo de autenticação e senha e nenhum algoritmo de privacidade e senha para o usuário. • authPriv — Permite que você configure o algoritmo de autenticação e senha e algoritmo de privacidade e senha para o usuário. • authNoPriv — Permite que você configure o algoritmo de autenticação e a senha para o usuário. <p>Padrão: noAuthNoPriv</p>

Opção	Descrição
Algoritmo de Autenticação	Selecione o algoritmo de autenticação para o usuário. Observação Esta opção aparece apenas se o nível de segurança é definido para authPriv ou authNoPriv . Padrão: SHA
Autenticação de Senha	Insira a autenticação de senha para o usuário. Observação Esta opção aparece apenas se o nível de segurança é definido para authPriv ou authNoPriv .
Algoritmo de Privacidade	Selecione o algoritmo de privacidade para o usuário. Observação Esta opção aparece apenas se o nível de segurança é definido para authPriv . Padrão: AES128
Privacidade de Senha	Insira a senha de privacidade para o usuário. Observação Esta opção aparece apenas se o nível de segurança é definido para authPriv .

Etapa 6 Selecione **Adicionar**.

O usuário USM é adicionado em seu sistema.

Etapa 7 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Editando os Usuários USM**Observação**

O usuário USM padrão, serveradmin, é usado internamente. Um administrador pode alterar o nome de usuário USM e a senha de privacidade do usuário serveradmin, mas não pode alterar o nível de segurança, o algoritmo de autenticação ou o algoritmo de privacidade deste usuário.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

- Etapa 3** Selecione **Sistema** e então selecione **Exibir mais** na seção SNMP.

- Etapa 4** Selecione um usuário USM na seção de Usuários USM.

- Etapa 5** Altere os campos desejados na página **Editar Usuário USM**.

Opção	Descrição
Nome de Usuário USM	Alterar o nome do usuário USM. Máximo de 256 caracteres.
Nível de Segurança	<p>Selecione o nível de segurança. O nível de segurança que você seleciona, determina quais algoritmos e senhas você pode definir para o usuário. As opções incluem:</p> <ul style="list-style-type: none"> • noAuthNoPriv — Nenhum algoritmo de autenticação e senha e nenhum algoritmo de privacidade e senha para o usuário. • authPriv — Permite que você configure o algoritmo de autenticação e senha e algoritmo de privacidade e senha para o usuário. • authNoPriv — Permite que você configure o algoritmo de autenticação e a senha para o usuário. <p>Padrão: noAuthNoPriv</p>
Algoritmo de Autenticação	<p>Selecione o algoritmo de autenticação para o usuário.</p> <p>Observação Esta opção aparece apenas se o nível de segurança é definido para authPriv ou authNoPriv.</p> <p>Padrão: SHA</p>
Autenticação de Senha	<p>Altera a autenticação de senha para o usuário.</p> <p>Observação Esta opção aparece apenas se o nível de segurança é definido para authPriv ou authNoPriv.</p>
Algoritmo de Privacidade	<p>Selecione o algoritmo de privacidade para o usuário.</p> <p>Observação Esta opção aparece apenas se o nível de segurança é definido para authPriv.</p> <p>Padrão: AES128</p>

Opção	Descrição
Privacidade de Senha	Altere a senha de privacidade para o usuário.
Observação	Esta opção aparece apenas se o nível de segurança é definido para authPriv .

- Etapa 6** Selecione **Editar**.
As informações do usuário USM estão alteradas.
- Etapa 7** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.
O serviço de reuniões para usuários neste centro de dados é restaurado.

Configurando os Destinos de Notificação

Você pode configurar suas máquinas virtuais no seu sistema para gerar notificações SNMP ou armadilhas para:

- Inicialização da máquina virtual (armadilha para arranque a frio)
- Todas as condições de alarme

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#))
- Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.
- Etapa 3** Selecione **Sistema** e selecione o link **Exibir mais** na seção SNMP.
- Etapa 4** Selecione **Adicionar novo Destino de Notificação** em **Destinos de Notificação**.
- Etapa 5** Configure os seguintes campos para o seu destino de notificação:

Opção	Descrição
Endereço de IP / Hostname de Destino	O hostname ou endereço de IP da máquina virtual que você deseja configurar como um destino de notificação.
Número da Porta	O número da porta para a sua máquina virtual. Padrão: 162
Versão SNMP	Sua versão SNMP. Padrão: V3
Tipo de Notificação	Selecione Informe ou Armadilhas . Padrão: Armadilha
Usuário USM	Selecione os usuários USM. Consulte Configurando os Usuários de USM, na página 154 para obter mais informações.
Observação Esta opção só aparece quando a versão SNMP está definida para V3.	
Sequência de Comunidade	Selecione sequências de comunidade. Consulte Configurando as Sequências de Comunidade, na página 151 para obter mais informações.
Observação Esta opção só aparece quando a versão SNMP não está definida para V3.	

- Etapa 6** Selecione **Adicionar**.
Seu destino de notificação está adicionado.
- Etapa 7** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.
O serviço de reuniões para usuários neste centro de dados é restaurado.

Editar um Destino de Notificação

Configurando os Destinos de Notificação

- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, à la page 7.](#))

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

- Etapa 3** Selecione **Sistema** e selecione o link **Exibir mais** na seção **SNMP**.
Etapa 4 Selecione um link de destino da notificação da lista **Destinos da notificação**.
Etapa 5 Você pode editar os seguintes campos para o seu destino de notificação:

Opção	Descrição
Endereço de IP / Hostname de Destino	O hostname ou endereço de IP da máquina virtual que você deseja configurar como um destino de notificação.
Número da Porta	O número da porta para a sua máquina virtual. Padrão: 162
Versão SNMP	Sua versão SNMP. Padrão: V3
Tipo de Notificação	Selecione Informe ou Armadilhas . Padrão: Informar
Usuário USM	Selecione os usuários USM. Consulte Configurando os Usuários de USM, na página 154 para obter mais informações.
Observação Esta opção só aparece quando a versão SNMP está definida para V3.	
Sequência de Comunidade	Selecione sequências de comunidade. Consulte Configurando as Sequências de Comunidade, na página 151 para obter mais informações.
Observação Esta opção só aparece quando a versão SNMP não está definida para V3.	

- Etapa 6** Selecione **Salvar**. Suas mudanças de destino de notificação são salvas.
- Etapa 7** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.
- O serviço de reuniões para usuários neste centro de dados é restaurado.



CAPÍTULO 15

Definindo as Configurações

Este módulo descreve como definir as suas configurações.

- [Configurando as informações da empresa, página 161](#)
- [Definindo as Configurações da Sua Marca, página 163](#)
- [Definindo as configurações de reunião, página 164](#)
- [Sobre Configurar Suas Definições de Áudio, página 167](#)
- [Definindo as configurações de vídeo, página 182](#)
- [Definindo suas configurações de dispositivos móveis, página 182](#)
- [Configurando a Qualidade de Serviço \(QoS\), página 183](#)
- [Configurando Senhas, página 185](#)
- [Configurando as Configurações do Seu E-mail, página 189](#)
- [Sobre os downloads de aplicativos, página 212](#)
- [Gerenciando Certificados, página 214](#)
- [Carregando a mensagem de aviso de segurança de início de sessão, página 233](#)
- [Configurando o registro de auditoria do aplicativo, página 234](#)
- [Configurando um aviso de segurança ao iniciar sessão, página 235](#)

Configurando as informações da empresa

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 (Opcional) Para alterar a configuração de Idioma, selecione **Ativar o modo de manutenção**.

Você não precisa desativar o modo de manutenção enquanto modifica outras configurações na página **Informação da Empresa**.

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Configurações**. Se você está visualizando uma das outras páginas de configuração, você também pode selecionar **Informações da Empresa** na seção Configurações.

Etapa 4 Complete os campos na página e selecione **Salvar**.

Opção	Descrição
Nome da empresa	O nome da sua empresa ou organização.
Endereço 1	Linha de endereço 1.
Endereço 2	Linha de endereço 2.
Cidade	Sua cidade.
Estado/Província	Nome do seu estado ou província.
CEP	CEP ou outro código postal.
País/Região	Nome do seu país ou região.
Telefone comercial	Menu suspenso com código de país e campo para telefone comercial com código de área.
Fuso horário	Seu fuso horário.
Idioma	Seu idioma. A configuração de idioma afeta: <ul style="list-style-type: none"> A página de iniciar sessão vista pelos administradores quando eles ativam suas contas de administrador pela primeira vez Idioma dos relatórios. (Consulte Gerenciando relatórios, na página 237)
Localidade	Sua localidade. O configuração de localidade afeta a exibição de horas, datas, moedas e números.

Etapa 5 (Opcional) Se você modificar o idioma, selecione **Desativar modo de manutenção** e **Continuar** para confirmar. Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de

DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

Definindo as Configurações da Sua Marca

Antes de iniciar

Prepare o seguinte antes de definir as configurações da sua marca:

- Uma imagem de 120x32 PNG, GIF ou JPEG contendo o logotipo da sua empresa
- URL da declaração de privacidade da sua empresa
- URL da declaração dos termos de serviço da sua empresa
- URL de suporte da sua empresa

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Identificação de marca**.

Etapa 3 Complete os campos na página e selecione **Salvar**.

Opção	Descrição
Logomarca da empresa	Seu arquivo de logotipo. Seu logotipo deve ser no formato PNG, JPEG ou GIF. As dimensões máximas são 120x32 pixéis e o tamanho máximo do arquivo é 5MB.
Declaração de Privacidade	URL para a declaração de privacidade da sua empresa.
Termos do serviço	URL para os termos de serviço da sua empresa.
Texto de Rodapé Personalizado	O texto inserido é exibido no rodapé dos e-mails e das páginas web de todos os usuários finais e administradores que são enviados pelo sistema.
Cor do plano de fundo do cabeçalho	Seleciona esta opção para desativar a cor de fundo padrão, incluindo todos os e-mails e barras de navegadores.
Ajuda on-line	Seleciona a opção de ajuda on-line que se aplica ao seu ambiente. Se os usuários são impedidos de acessar a Internet, selecione a opção de ajuda personalizada e insira as URLs dos vídeos da empresa, os manuais do usuário e as perguntas frequentes.

Opção	Descrição
URL do Contato de Suporte	URL para a página web de suporte da empresa.

Removendo um Logotipo da Empresa

Antes de iniciar

Criar um arquivo transparente de 120x32 em GIF ou PNG.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione **Configurações > Identificação de marca**.

Etapa 3

Para o campo Logotipo da Empresa, selecione **Procurar** e escolha o arquivo transparente de 120x32 em GIF ou PNG.

Etapa 4

Selecione **Salvar**.

O seu logotipo da empresa anterior é substituído por arquivo PNG ou GIF em branco. Confirme se o logotipo original foi removido.

Definindo as configurações de reunião

Defina as configurações de reunião para controlar quais recursos os participantes podem usar:

- Participe das configurações da reunião
- Máximo de participantes por reunião (tamanho reunião)
- Privilégios do Participante

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione **Configurações > Reuniões**.

Etapa 3

Na seção Participar de configurações de reunião, selecione as suas opções.

As configurações padrão são **Permitir que os participantes entrem na reunião antes que o organizador**, **Permitir que os participantes entrem na teleconferência antes que o organizador**, e **Primeiro participante a entrar será o apresentador**.

Se você desmarcar **Permitir que os participantes participem em reuniões antes do organizador**, o recurso **O primeiro participante que participar será o organizador** é automaticamente desmarcado.

Os participantes podem entrar nas reuniões até 15 minutos antes da hora de início se estiverem selecionados **Permitir que os participantes entrem na reunião antes que o organizador** e **Permitir que os participantes entrem na teleconferência antes que o organizador**. Opcionalmente selecione **Qualquer pessoa pode apresentar na reunião**.

Etapa 4 Selecione o máximo de participantes por reunião, arrastando o controle deslizante:

Configuração do número de participantes	Tamanho do sistema
50	Sistema de 50 usuários com ou sem HA (centro de dados único)
250	Sistema de 250 usuários com ou sem HA (centro de dados único) Sistema de 50 usuários sem HA (vários centros de dados)
500	Sistema de 800 ou 2000 usuários com ou sem HA (centro de dados único) Sistema de 800 ou 2000 usuários sem HA (vários centros de dados) 5

Esta configuração é limitada pelo tamanho do sistema configurado durante a implantação. Consulte [Confirmando o Tamanho do Seu Sistema, na página 22](#) para obter mais informações.

Etapa 5 Na seção **Privilégios de participante**, selecione suas opções.

Bate-papo, Sondagem, Apresentação e revisão de documento e Compartilhamento e controle remoto são selecionados por padrão. Os privilégios de participante selecionado aparece nos controles do usuário.

Etapa 6 Selecione **Gravar** para gravar e armazenar reuniões em seu servidor de armazenamento.

- Selecionar **Enviar notificação por e-mail para o organizador e convidados quando a gravação da reunião estiver pronta** para permitir que o sistema envie a notificação por e-mail ao organizador e a todos os usuários que receberam um convite de reunião.
- Selecionar **Restringir a visualização e o download da gravação para os usuários que iniciaram sessão** para permitir que apenas os usuários do sistema, e não os convidados, visualizem ou baixem uma gravação da reunião.

A gravação está desativada por padrão.

Você deve configurar um servidor de armazenamento para habilitar a gravação. Consulte [Configurando um Servidor de Armazenamento, na página 146](#) para obter mais informações.

Etapa 7 Selecione **Transferência de arquivos** para permitir que os usuários compartilhem arquivos durante uma reunião.

Etapa 8 Selecione **Salvar**.

Sobre Segurança de Reuniões

O Cisco WebEx Meetings Server permite diferentes recursos de segurança de reunião, dependendo dos seguintes fatores:

- Tipo de usuário: organizador, organizador alternativo, usuário (registrado) e o convidado.
- A reunião tem ou não uma senha.

- A senha está oculta ou visível no convite da reunião.
- A senha está oculta ou visível no convite da reunião do e-mail.
- Comportamento exibido na página para entrar na reunião (consulte as tabelas a seguir).

Tabela 1: A senha é excluída ao agendar a reunião

Tipo de usuário	A senha é exibida no lembrete e no convite por email	Página de Detalhes da Reunião
Organizador	Sim	Sim
Organizador substituto	Sim	Sim
convidado	Não	Não
Convidado encaminhado	Não	Não

Tabela 2: A senha é incluída ao agendar a reunião

Tipo de usuário	A senha é exibida no lembrete e no convite por email	Página de Detalhes da Reunião
Organizador	Sim	Sim
Organizador substituto	Sim	Sim
convidado	Sim	Sim
Convidado encaminhado	Sim	Sim

- O recurso Participar antes do Organizador está ativado ou desativado:
 - Ativado: Os convidados ou visitantes podem participar da reunião a partir de 15 minutos antes do horário de início até o final do horário da reunião.
 - Desativado: Os convidados ou visitantes não podem participar da reunião antes do organizador. O organizador ou o organizador alternativo pode iniciar a reunião, então os convidados podem entrar.
- O recurso Entrar na teleconferência antes do organizador está ativado ou desativado:
 - Ativado: Se o organizador não iniciar a teleconferência no cliente de reunião, então os convidados podem entrar na teleconferência antes do organizador.
 - Desativado: Se o organizador não iniciar a teleconferência no cliente de reunião, então os convidados não podem entrar na teleconferência antes do organizador.
- O recurso O primeiro participante pode apresentar está ativado ou desativado:
 - Ativado: Quando Participar antes do organizador estiver configurado, o primeiro convidado será o apresentador.
 - Desativado: O organizador sempre tem a bola.

Sobre Configurar Suas Definições de Áudio

A primeira vez que configurar as suas definições de áudio, você é guiado através do processo por um assistente que lhe ajuda a definir sua configuração CUCM SIP e o números de acesso de chamada de entrada. Depois de ter concluído o assistente e configurado as configurações iniciais de áudio, você pode configurar todas as outras configurações de áudio.

Você deve habilitar a teleconferência e configurar o CUCM antes de prosseguir com a configuração do seu áudio. Você deve configurar o CUCM em dois sistemas se você pretende fornecer teleconferência de alta disponibilidade. Consulte o *Guia de Planejamento* para obter mais informações. Para prosseguir, você deve obter a seguinte informação:

- Uma lista de números de acesso de chamada de entrada que os participantes usam para chamar as reuniões.
- O endereço de IP CUCM.
- (Opcional) Um certificado de conferência seguro válido se você planeja usar a criptografia de teleconferência TLS/SRTP. Consulte [Importar Certificados de Teleconferência Segura](#), na página 224 para obter mais informações.



Observação

Este recurso não está disponível na Rússia ou na Turquia.

Configurando as Configurações de Seu Áudio pela Primeira Vez

A primeira vez que você configurar as definições de áudio, um assistente orienta você durante o processo de instalação. Você deve configurar o Cisco Unified Communications Manager (CUCM) como parte deste processo.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter](#), na página 7.)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3

Selecione **Configurações > Áudio**.

A página **Áudio** é exibida e inclui os Recursos de áudio atuais.

Etapa 4

Selecione **Próximo**.

A página **Configuração SIP** aparece. Esta página exibe os parâmetros de configuração SIP que você precisa configurar o CUCM, incluindo o endereço de IP e número de porta para cada tipo de servidor.

Etapa 5 Selecione **Próximo**.

A página **Habilitar Teleconferência: Configuração do CUCM** é exibida, exibindo as suas configurações atuais.

Etapa 6 Selecione **Editar** para alterar as suas configurações.

A caixa de diálogo **CUCM (Cisco Unified Communication Manager)** aparece.

Etapa 7 Complete os campos na caixa de diálogo do **CUCM (Cisco Unified Communication Manager)** como segue:

- Insira um endereço de IP para o endereço de IP CUCM 1 e opcionalmente para o endereço de IP CUCM 2.

Estes endereços de IP precisam corresponder ao nó CUCM primário e secundário, opcionalmente, que fazem parte do Grupo Cisco Unified Communications Manager, como definido no pool do dispositivo que está configurado nos Troncos SIP do Ponto de Aplicação no CUCM. Consulte "Configurando um tronco SIP em um ponto de aplicação" no *Guia de Planejamento* em <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html> para mais detalhes.

Observação O CUCM 2 não é exigido, mas recomenda-se para a teleconferência de alta disponibilidade.

- Insira o número da porta para o seu sistema. O número da porta deve coincidir com o número da porta designada no CUCM. (**Padrão:** 5062)

- Use o menu suspenso **Transporte** para selecionar o tipo de transporte para seu sistema. (**Padrão:** TCP)

Se você selecionar TLS como seu tipo de transporte, você deve importar um certificado de conferência seguro válido para cada um dos seus servidores CUCM, exportar o certificado SSL e carregá-lo no CUCM e configurar o nome de domínio totalmente qualificado (FQDN) do sistema, assim como o nome de domínio SIP em cada servidor CUCM. Consulte **Importar Certificados de Teleconferência Segura**, na página 224 para obter mais informações sobre como importar os certificados, e "Configurando o Cisco Unified Communications Manager (CUCM)" no *Guia de Planejamento* para obter mais informações sobre como gerenciar o controle de chamadas no CUCM.

- Selecione **Continuar**.

As configurações atualizadas ou novas do CUCM aparecem na página **Habilitar Teleconferência: Configuração do CUCM**.

Etapa 8 Selecione **Próximo**.

A página **Habilitar Teleconferência: Configuração do Número de Acesso** é exibida.

Etapa 9 Selecione **Editar**.

A caixa de diálogo **Números de Acesso de Chamada de Entrada** aparece.

Etapa 10 Selecione **Adicionar** para adicionar um número de acesso de chamada de entrada.

Uma linha é adicionada na caixa de diálogo para a etiqueta do telefone e número. Cada hora que você selecionar **Adicionar**, uma linha adicional aparece na caixa de diálogo.

Etapa 11 Insira a **Etiqueta do Telefone** e **Número de Telefone** para cada número acesso que você adicionar e selecionar **Continuar** após você ter finalizado a adição de números.

Certifique-se que somente você adiciona números que você configurou no CUCM. Os números que você adicionar aparecem em convites de e-mail e no seu cliente Cisco WebEx Meetings.

Exemplo:

Insira "Sede" para a **Etiqueta do Telefone** e 888-555-1212 para o **Número de Telefone**.

Os números de acesso que você inseriu estão adicionados no seu sistema e você retorna para a página **Habilitar Teleconferência: Configuração do Número de Acesso**. A página agora indica quantos números de acesso foram configurados.

Etapa 12 Selecione **Salvar**.

O assistente informa que você configurou com sucesso as suas funcionalidades de teleconferência.

Etapa 13 (Opcional) Insira um número de exibição na caixa de diálogo **Nome de exibição**.

Etapa 14 (Opcional) Insira um ID de chamada válido na caixa de diálogo **ID do Chamador**.

O ID de chamadas está limitado aos caracteres e traços (-) numéricos e possui um comprimento máximo de 32 caracteres.

Etapa 15 (Opcional) Defina a configuração do seu Chamar-me WebEx (**Padrão**: Pressione 1 para conectar à reunião). Selecione esta opção para ignorar a exigência de pressionar 1 para conectar a uma reunião.

Observação Não recomendamos que você selecione esta opção a menos que seu sistema telefônico seja incapaz de enviar um dígito 1.

Etapa 16 (Opcional) Selecione a sua **Entrada de telefone e tom de saída**.

- Beep (padrão)
- Sem som
- Anunciar nome

Etapa 17 (Opcional) Se o IPv6 é suportado e está configurado no seu sistema, defina a configuração **Teleconferência IPv6** para **Ativado** ou **Desativado**. (**Padrão**: Desativado. Uma configuração de **Desativado** indica que o IPv4 é a configuração.)

Etapa 18 Selecione o **Idioma do sistema de áudio** que os usuários ouvirão quando eles discarem para a parte de áudio de uma reunião WebEx ou quando usarem o serviço Chamar-me.

Etapa 19 Selecione **Salvar**.

Etapa 20 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Definindo as configurações do áudio

Antes de iniciar

Se você estiver configurando as definições de áudio pela primeira vez, consulte [Configurando as Configurações de Seu Áudio pela Primeira Vez](#), na página 167.

**Observação**

Ativar o Modo de Manutenção não é necessário para configurar ou alterar a Discagem Múltipla, idiomas de serviço da chamada de entrada, nome de exibição ou configurações de áudio da ID do chamador.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).

Ativar o modo de manutenção em todos os centros ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3

Selecione **Configurações > Áudio**.

Etapa 4

Selecione **Configurações globais**. Configure as configurações de recursos de áudio.

Para a configuração de áudio, existem configurações globais e cada centro de dados possui configurações locais. As configurações globais são aplicadas à todos os centros de dados. As configurações locais aplicam-se a centros de dados individuais.

Opção	Descrição
Áudio WebEx	<ul style="list-style-type: none"> • Serviço de chamada de entrada do usuário e Chamar-me – Permitem que os usuários participem de uma teleconferência, ligando de números de telefone específicos ou recebendo um chamada Chamar-me do sistema. • Chamada de entrada – Permite que os usuários participam de uma teleconferência, ligando de números de telefone específicos. Um organizador de reuniões não pode iniciar uma reunião de Discagem Múltipla. • DESATIVADO–Desativa todas as funcionalidades da chamada. Um organizador de reuniões não pode iniciar uma reunião de áudio WebEx, Discagem Múltipla ou de Conferência Pessoal.
Conferência Pessoal	<ul style="list-style-type: none"> • Selecione a caixa de seleção Ativar Conferência Pessoal para permitir que os usuários iniciem e disquem para as reuniões de conferência pessoal. • Selecione Permitir que os participantes participem das reuniões de Conferência Pessoal antes do organizador para permitir que os participantes iniciem a parte de áudio de uma reunião de Conferência Pessoal inserindo apenas o código de acesso do participante; a senha do organizador não é necessária.

Opção	Descrição
Conexão de voz usando o computador	<ul style="list-style-type: none"> Ligado permite uma conexão de voz pelo computador. Desligado nega uma conexão de voz pelo computador.

Etapa 5 Configure a Discagem Múltipla, conforme descrito em [Sobre a discagem múltipla WebEx, na página 174](#).

Etapa 6 Na seção Editar Configurações de Teleconferência, selecione o link **Editar** no CUCM (Cisco Unified Communication Manager) para alterar as suas configurações.

Em um sistema MDC, cada centro de dados deve estar conectado a um Cisco Unified Call Manager (CUCM). Vários centros de dados podem compartilhar um CUCM ou cada um deles pode estar associado a um CUCM. As configurações do CUCM em um sistema MDC são as mesmas como se fosse um sistema com Centro de dados único (SDC).

Opção	Descrição
Endereço de IP CUCM 1	Insira o hostname ou um endereço de IP para o seu sistema CUCM 1.
Endereço de IP CUCM 2	(Opcional) Insira o nome do organizador ou um endereço de IP para o seu sistema CUCM 2 (serviço de平衡amento de carga). Observação O CUCM 2 não é exigido, mas recomenda-se para a teleconferência de alta disponibilidade.
Número da Porta	Insira um número de porta válido. Certifique-se que o número da porta corresponde a configuração no CUCM. Padrão: 5062
Transporte	Selecione o tipo de transporte. Se você selecionar TLS como seu tipo de transporte, importe um certificado de conferência seguro válido para cada um dos seus servidores CUCM, exporte o certificado SSL, carregue-o no CUCM e configure o nome de domínio totalmente qualificado (FQDN) do sistema, assim como o nome de domínio SIP em cada servidor CUCM. Consulte Importar Certificados de Teleconferência Segura, na página 224 para obter mais informações sobre a importação dos seus certificados e a "configuração do CUCM" no <i>Guia de Planejamento</i> para mais informações sobre o CUCM. Padrão: TCP

A caixa de diálogo **CUCM (Cisco Unified Communication Manager)** aparece. Complete os campos e selecione **Continuar**.

Etapa 7 Selecione **Editar** na seção Números de acesso das chamadas de entrada para adicionar, alterar ou excluir os números de acesso.

- Seleciona **Adicionar** e insira uma etiqueta de telefone e número de telefone para cada novo número de acesso que você deseja adicionar. Para excluir um número, selecione o link **Excluir** no final da linha.
- Insira informações atualizadas nos campos etiqueta de telefone e número de telefone para qualquer número de acesso que você deseja alterar.
- Seleciona **Continuar**.

As alterações não serão salvas até que você selecione **Salvar** na página principal.

Certifique-se que somente você adiciona números que você configurou no CUCM. Os números que você adicionar aparecem em convites de e-mail e no seu cliente Cisco WebEx Meetings.

Etapa 8 Selecione **Editar** na seção Idiomas de serviços de chamada de entrada para adicionar, alterar ou excluir idiomas disponíveis para os usuários que ligam para a parte de áudio de uma reunião.

- a) Selecione **Adicionar** e insira um padrão de rota associado a cada número de chamada de entrada que você deseja fornecer opções de idioma para os usuários que ligam para a parte de áudio de uma reunião.
Todos os usuários que ligam para os números de chamada de entrada associados ao padrão de rota podem escolher entre as seleções de idiomas configurados. Por exemplo, se você configurar inglês, espanhol, francês como as seleções de idiomas, quando um usuário ligar para o número de chamada de entrada associado ao padrão de rota, o chamador ouvirá a saudação em inglês, mas será dada a opção de selecionar espanhol ou francês. Se um usuário seleciona espanhol, os prompts de áudio iniciais são falados em espanhol.

Observação O idioma padrão é definido como o idioma configurado para **Configurações > Áudio > Configurações globais > Idioma de áudio do sistema**.

- b) Para excluir uma entrada, selecione **X** no final da linha.
- c) Para alterar uma entrada, digite um padrão de rota diferente e selecione diferentes configurações de idioma.
- d) Selecione **Continuar**.

Suas alterações não são salvas até você selecionar **Salvar** na parte inferior da página.

Certifique-se de adicionar somente padrões de rota que foram configurados no CUCM.

Etapa 9 Use o menu suspenso **Transporte** para selecionar o tipo de transporte para seu sistema e o número de porta para cada servidor. (**Padrão:** TCP)

Se você selecionar TLS como seu tipo de transporte, você deve importar um certificado de conferência seguro válido para cada um dos seus servidores CUCM, exportar o certificado SSL e carregá-lo no CUCM e configurar o nome de domínio totalmente qualificado (FQDN) do seu sistema, assim como o nome de domínio SIP em cada servidor CUCM. Consulte [Importar Certificados de Teleconferência Segura](#), na página 224 para obter mais informações sobre como importar os certificados, e "Configurando o Cisco Unified Communications Manager (CUCM)" no *Guia de Planejamento* para obter mais informações sobre como gerenciar o controle de chamadas no CUCM.

Certifique-se que o número da porta corresponde a configuração no CUCM.

Etapa 10 Insira um número de exibição na caixa de diálogo **Nome de exibição**.

Este é o nome exibido no telefone de IP de um participante da reunião ao usar o serviço Chamar-me ou ao chamar o Cisco WebEx Meeting Server (CWMS).

Etapa 11 Insira um ID de chamada válido na caixa de diálogo **ID do Chamador**.

O ID do chamador está limitado aos caracteres e traços (-) numéricos e possui um comprimento máximo de 32 caracteres.

Etapa 12 Defina a configuração do seu Chamar-me WebEx (**Padrão:** Pressione 1 para conectar à reunião). Opcionalmente, selecione esta opção para ignorar a exigência de pressionar 1 para conectar a uma reunião.

Não recomendamos que você selecione esta opção a menos que seu sistema telefônico seja incapaz de enviar um dígito 1.

Etapa 13 Selecione a sua **Entrada de telefone e tom de saída**.

- Beep (padrão)
- Sem som

- Anunciar nome

Etapa 14 Se o IPv6 é suportado e está configurado no seu sistema, defina a configuração **Teleconferência IPv6** para **Ativado** ou **Desativado**. (**Padrão: Desativado** indica que o IPv4 é a configuração.)

Etapa 15 Selecione o **Idioma do sistema de áudio** que os usuários ouvirão quando eles discarem para a porção de áudio de uma reunião Cisco WebEx ou quando usarem o serviço Chamar-me.

Esta configuração aparece como o idioma padrão para os Idiomas de serviços de chamadas de entrada.

Etapa 16 Selecione **Salvar**.

Etapa 17 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Configurando o Áudio CUCM

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Configurações > Áudio > CUCM centro de dados**.

Etapa 4 Selecione **Editar CUCM** (Cisco Unified Communications Manager) para alterar as configurações.

- No **Endereço de IP CUCM 1**, insira o nome do organizador ou um endereço de IP no seu sistema CUCM 1.
- (Opcional) Insira o nome do organizador ou um endereço de IP para o seu sistema CUCM 2 (serviço de平衡amento de carga).

O CUCM 2 não é exigido, mas recomenda-se para a teleconferência de alta disponibilidade.

Etapa 5 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este

centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Sobre a discagem múltipla WebEx

O recurso de Discagem múltipla WebEx permite que os usuários, designados como organizadores de reuniões, chamem a um número de telefone e insiram uma senha de organizador (se necessário) para iniciar imediatamente a parte de áudio de uma reunião. Ao mesmo tempo, o sistema coloca automaticamente as chamadas em uma lista de participantes definidos para o grupo de Discagem múltipla. Dentro de minutos, o organizador pode começar a discutir um assunto urgente ou fornecer instruções detalhadas para lidar com uma questão importante com as pessoas que têm autoridade de homologação ou são treinadas para situações de emergência. Além de iniciar a parte de áudio da reunião, o organizador pode acessar um e-mail gerado automaticamente para iniciar a parte on-line da reunião para compartilhar imagens, vídeo ou informações eletrônicas com os participantes da reunião.

Quando o sistema liga para uma pessoa em uma lista de participantes, essa pessoa atende a chamada e inseri um PIN de participante (se necessário) para participar da parte de áudio da reunião. Uma vez que a parte de áudio da reunião estiver em andamento, o organizador pressiona *# para ouvir os nomes das pessoas que entraram na reunião ou olha a lista de Participantes na parte on-line da reunião. Qualquer participante pode optar por não atender a chamada ou retirar-se de um grupo de Discagem múltipla. Um administrador pode excluir uma pessoa de um grupo de Discagem múltipla a qualquer momento.

Cada grupo de Discagem múltipla pode ter o número máximo de participantes suportados por cada sistema de usuários (consulte a seção "Matriz da capacidade do sistema" nos *Requisitos do sistema e no guia de planejamento do Cisco WebEx Meetings Server* para obter detalhes). Um administrador configura o grupo de Discagem múltipla e seus participantes, mas depende do organizador da reunião para fornecer as configurações do grupo e as informações para a lista de Participantes. Um administrador pode adicionar participantes a um grupo de Discagem múltipla inserindo-os manualmente na página de Discagem múltipla ou importando um arquivo de Modelo de Participantes concluído por um organizador.

Baixando o modelo de grupo

Use o link fornecido para baixar um Modelo de grupo para enviar à pessoa que organizará reuniões para um grupo de Discagem Múltipla.

-
- | | |
|----------------|---|
| Etapa 1 | Inicie sessão no site da Administração. |
| Etapa 2 | Selecione Configurações > Áudio . |
| Etapa 3 | Selecione o link Modelo de grupo para baixar o modelo que um organizador utiliza para fornecer as configurações gerais, como o nome do grupo e a senha do organizador, para o novo grupo de Discagem Múltipla. |
| Etapa 4 | Envie um e-mail com o Modelo de Grupo para o organizador do grupo de Discagem Múltipla. Peça ao organizador para completar o modelo e devolvê-lo a você. |
-

Próximos passos

Se você possui as informações para criar um novo grupo, vá para [Adicionando um grupo de discagem múltipla, na página 175.](#)

Para importar os participantes, exclua as instruções e as linhas com o texto de exemplo no arquivo de modelo Participantes e vá para [Importando uma lista de participantes, na página 182.](#)

Para adicionar participantes à um grupo manualmente, vá para [Adicionando participantes de discagem múltipla, na página 178.](#)

Adicionando um grupo de discagem múltipla

Para cada grupo de Discagem Múltipla, especifique um nome de grupo, um padrão de rota e um número de chamada de entrada. O padrão de rota e o número de chamada de entrada devem ser definidos no CUCM e copiados para a página de Discagem Múltipla. Para fornecer um nível de segurança para as reuniões, configure uma senha de organizador e um PIN de participante. Para cada grupo, selecione a caixa de seleção **Organizador** para, pelo menos, um dos participantes internos para tornar esse usuário um organizador. Deve haver pelo menos um organizador para cada grupo de Discagem Múltipla. Você pode designar vários participantes internos como organizadores de um grupo de Discagem Múltipla e todos os organizadores podem começar a parte de áudio de uma reunião de Discagem Múltipla. No entanto, um organizador de reuniões requer que uma licença inicie a parte on-line de uma reunião de Discagem Múltipla.

Quando o grupo de Discagem Múltipla está configurado, o sistema envia um e-mail para o organizador com o senha do organizador e o número da chamada de entrada. Todos os participantes recebem um e-mail com o PIN de participante e o número de Chamada de entrada. Um organizador liga para o número de chamada de entrada e inseri a senha do organizador para começar uma reunião. Os participantes atendem a chamada de Discagem Múltipla (ou ligam para o número de chamada de entrada se eles não atenderem a chamada) e inserem um PIN de participante (se necessário). Ao contrário de outros tipos de reuniões do Cisco WebEx que terminam automaticamente após 24 horas, uma reunião de Discagem Múltipla continua até que a última pessoa termina a chamada ou deixa a parte on-line da reunião.



Observação

Quando um organizador inicia a parte on-line de uma reunião de Discagem Múltipla, os tons DTMF são desativados.

Antes de iniciar

Configure um padrão de rota e o número de chamada de entrada correspondente no Cisco Unified Communications Manager para cada grupo de Discagem Múltipla. Cada grupo de Discagem Múltipla requer seu próprio número de chamada de entrada específico. Consulte "Configuração de roteamento de chamada" no *Guia de Administração do Cisco Unified Communications Manager* para obter detalhes sobre os padrões de rota.

Baixe o arquivo de **Modelo de grupo** e envie-o para o organizador do grupo de discagem múltipla. O organizador deve concluir o modelo e devolvê-lo. Use as informações no modelo para criar o grupo de Discagem Múltipla.

-
- Etapa 1** Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Áudio > Configurações globais**.

Etapa 3 Na seção de Discagem Múltipla, selecione **Adicionar grupo**.

Etapa 4 Insira um **Nome de grupo**.

Etapa 5 Insira um **Padrão de rota**.

Um padrão de rota deve ser configurado no Cisco Unified Communications Manager para cada grupo de Discagem Múltipla.

Etapa 6 Digite o **Número de chamada de entrada** associado ao padrão de rota configurado para este grupo de Discagem Múltipla. Cada grupo de Discagem Múltipla precisa de um número de chamada de entrada específico. Um organizador discia o número de chamada de entrada para iniciar uma reunião de Discagem Múltipla.

Observação Este número de chamada de entrada deve ser redirecionado para o padrão de rota selecionado para este grupo no Cisco Unified Communications Manager. Consulte <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> para obter detalhes.

Etapa 7 (Opcional) Digite uma senha alfanumérica no campo **Senha da Reunião**.

Se configurado, os participantes inserem esta senha para entrar na parte on-line de uma reunião de Discagem Múltipla.

Observação As regras que governam a senha da reunião estão definidas em **Configurações > Gerenciamento de senha > Senha da reunião**. Consulte [Definindo as configurações de reunião](#), na página 164 para obter detalhes.

Etapa 8 Escolha uma das opções de **Senha do organizador**:

- (Padrão) Selecione **Gerar automaticamente um senha de organizador** e move o controle deslizante para o nível de segurança desejado. Conforme você move o controle deslizante, o PIN e o nível de segurança mudam. Selecione **Atualizar** para gerar outro número.

- Selecione **Digite uma senha de organizador** e digite um PIN numérico. Quando esta opção for selecionada, um PIN será necessário.

Um PIN de 3 dígitos tem baixa segurança, um PIN de 4 a 7 dígitos tem segurança média e um PIN de 8 a 10 dígitos tem um alto nível de segurança.

Observação Uma senha de organizador não pode ter uma sequência de um único número ou número sequencial, como 11111 ou 1234567.

- Selecione **Nenhum** se você não quiser exigir que um organizador insira um PIN para iniciar uma reunião de Discagem Múltipla.

Observação Quando esta opção for selecionada, qualquer usuário que souber o número da chamada de entrada poderá iniciar uma reunião de Discagem Múltipla.

Etapa 9 Escolha uma das opções de **PIN de participante**:

- (Padrão) Selecione **Nenhum** se você não quiser exigir que um participante insira um PIN para participar de uma reunião de Discagem Múltipla.

- Selecione **Digite um PIN de participante** e digite um PIN numérico. Quando esta opção for selecionada, um PIN será necessário.

Um PIN de 3 dígitos tem baixa segurança, um PIN de 4 a 7 dígitos tem segurança média e um PIN de 8 a 10 dígitos tem um alto nível de segurança.

Observação Um PIN de participante não pode ter uma sequência de um único número ou número sequencial, como 11111 ou 1234567.

- Etapa 10** Selecione o número de **Tentativas de chamada** que o sistema deve fazer para ligar para um participante. O sistema liga para cada participante o número de vezes selecionado de tentativas de Chamada. Se um usuário lista quatro números de telefone na página **Minhas contas** (para usuários internos) ou um administrador insere quatro números de telefone no arquivo CSV importado no sistema, o sistema discará o primeiro número do número de vezes selecionado de Tentativas de chamada, em seguida, liga para o segundo número do número de vezes selecionado de Tentativas de chamada, e assim por diante. Depois que o sistema discará cada número de telefone o número de vezes selecionado de tentativas de chamada, o sistema deixa de chamar o participante. Se **Ilimitado** é selecionado para este campo, o sistema continua a chamar os participantes até atenderem a chamada ou até a reunião de Discagem Múltipla terminar.
- 1 (O sistema chama cada participante uma vez.)
 - 3 (padrão)
 - 5
 - 10
 - Ilimitado (Selecione esta opção quando a política da empresa determinar que o sistema continua a chamar os participantes até que eles participem da reunião.)
- Etapa 11** Selecione o link **Adicionar participantes** na seção **Lista interna**.
- Etapa 12** Na **Lista interna**, insira um endereço de e-mail para pelo menos um organizador e selecione + para adicionar cada pessoa à lista de Participantes.
- Etapa 13** Marque a caixa de seleção **Organizador** para designar o usuário interno como o organizador da reunião.
- Etapa 14** (Opcional) Selecione o link **Adicionar participantes** na seção **Lista externa**.
- Etapa 15** (Opcional) Para usuários externos, insira um nome, endereço de e-mail e um número de telefone e, em seguida, selecione **Adicionar** para adicionar a pessoa à lista de Participantes. Consulte [Adicionando participantes de discagem múltipla, na página 178](#) para obter detalhes sobre os usuários externos.
- Etapa 16** Selecione **Salvar** para salvar suas alterações.
O grupo de Discagem Múltipla é adicionado ao sistema.

Próximos passos

Para importar uma lista de participantes, exporte um arquivo CSV com títulos de colunas pré-configurados. Consulte [Exportando uma lista de participantes, na página 180](#) e [Importando uma lista de participantes, na página 182](#) para obter detalhes.

Para criar uma lista de discagem múltipla pequena ou adicionar algumas novas pessoas para uma lista existente, consulte [Adicionando participantes de discagem múltipla, na página 178](#).

Para excluir um grupo de discagem múltipla, consulte [Excluindo um grupo de Discagem Múltipla, na página 178](#).

Editando as configurações do grupo de discagem múltipla

Você pode alterar as configurações do grupo de discagem múltipla, incluindo a lista de participantes.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Configurações > Áudio**.

Etapa 3 Na seção Discagem Múltipla , selecione um link **Nome do grupo**.

Etapa 4 Faça alterações para campos editáveis. Os campos marcados com um asterisco são obrigatórios.

Etapa 5 Para fazer alterações em uma entrada na lista de participantes, selecione X para excluir uma entrada, e em seguida, adicione a entrada novamente com os dados atualizados.

Etapa 6 Selecione **Atualizar** para salvar suas alterações.

Excluindo um grupo de Discagem Múltipla

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Áudio**.

Etapa 3 Na seção Discagem Múltipla, selecione X ao lado do grupo que você deseja excluir.

Etapa 4 Selecione **OK** para confirmar.

O grupo de Discagem Múltipla e as listas de participantes relacionados são excluídos do sistema.

Adicionando participantes de discagem múltipla

Depois de configurar as definições para um grupo de Discagem Múltipla, crie a lista de Participantes internos e externos. O sistema chama os membros das listas de participantes internos e externos quando um organizador inicia uma reunião de Discagem Múltipla WebEx, discando os membros da lista interna primeiro, seguido pelos membros da lista externa.

Os participantes internos possuem um endereço de e-mail da empresa. Um administrador inseri apenas um endereço de e-mail para usuários internos e o sistema localiza os nomes e números de telefone dos usuários nas suas páginas **Minha Conta**. O sistema chama os números de telefone dos participantes internos listados na página **Minha Conta** em ordem consecutiva, ou seja, se um usuário inseri um número do escritório, o sistema discia esse número, mas se um usuário inseri um número de celular, mas nenhum número do escritório, o sistema discia para o número de celular primeiro. Consulte "Atualizando suas informações da conta" no *Manual do usuário Cisco WebEx Meetings Server* para obter detalhes.

Os participantes externos podem participar de reuniões Discagem Múltipla como convidados, mas eles não têm endereços de e-mail da empresa. Um administrador insere um nome, endereço de e-mail e um número

de telefone na caixa de diálogo **Discagem Múltipla** para os participantes externos. O sistema disca os números de telefone em ordem consecutiva.

Há duas formas de adicionar participantes.

- Insira as informações de um participante nos campos fornecidos nas seções da Lista interna ou Lista externa.
- Peça à pessoa que organizará as reuniões de Discagem Múltipla para selecionar o link **Modelo de participantes** na página **Minha conta** para baixar um arquivo de modelo. O organizador deve inserir as informações dos participantes e enviar o modelo completo para o administrador importar para o sistema.
- Exporte um arquivo CSV da lista de participantes, insira as informações necessárias e importe o arquivo CSV atualizado.



Observação

Os participantes externos não podem organizar uma reunião de Discagem Múltipla WebEx.

O sistema verifica todas as entradas de participantes e move automaticamente as entradas entre as listas de participantes se o endereço de e-mail de um usuário interno é inserido na lista de participantes externos ou se o sistema não pode localizar o endereço de e-mail para uma entrada na lista de participantes internos no banco de dados. Se a entrada de um participante interno é movida para a lista externa, insira um nome de usuário e número de telefone para tornar a entrada válida.

Antes de iniciar

Contate a pessoa que organizará as reuniões de Discagem Múltipla e peça ao organizador para selecionar o link **Modelo de participantes** na página **Minha conta** para baixar um arquivo de modelo. O organizador deve inserir as informações dos participantes e enviar o modelo completo para um administrador. Consulte a seção "Baixar os modelos de grupo e participantes" no *Manual do usuário Cisco WebEx Meetings Server Versão 2.5*.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Configurações > Áudio**.

Etapa 3 Na seção Discagem Múltipla , selecione um link **Nome do grupo**.

Etapa 4 Você pode exportar a lista de Participantes existentes, modificar o arquivo CSV e importar o arquivo para adicionar ou alterar as informações dos participantes.

Observação A primeira vez que você selecionar **Exportar lista**, o sistema exportará um arquivo CSV vazio, com os títulos das colunas apropriadas.

Etapa 5 Para importar participantes:

- Selecione **Guia** ou **Vírgula** para indicar qual tipo de arquivo CSV você está importando, delimitado por guia ou por vírgulas.
- Selecione **Navegar** e então selecione o arquivo CSV a ser importado.
- Selecione **Importar**.

Etapa 6 Para adicionar entradas individuais nos campos fornecidos:

- Para os participantes internos, digite um endereço de e-mail e selecione + para adicionar a entrada.
- Para os participantes externos, digite o nome de um participante, um endereço de e-mail e um número de telefone, incluindo o código do país. Depois selecione **Adicionar**.

Os participantes recém adicionados aparecem na Lista interna ou na Lista externa.

- Etapa 7** (Opcional) Marque a caixa de seleção **Organizador** para designar uma pessoa como o organizador.
Observação O sistema requer que pelo menos um participante interno seja designado como o organizador para cada grupo de discagem múltipla.

- Etapa 8** Selecione **Salvar** para salvar as configurações do grupo de discagem múltipla e as entradas recém adicionadas na lista de participantes.
A pessoa designada como o organizador recebe uma notificação por e-mail que inclui a senha do organizador, o PIN de um participante, a senha da reunião (se configurada) e o número de chamada de entrada de discagem múltipla. Todos os outros participantes recebem uma notificação por e-mail que inclui o PIN do participante e a senha da reunião (se configurada).

Próximos passos

Para modificar uma entrada em uma lista de participantes, consulte [Editando as configurações do grupo de discagem múltipla, na página 178](#).

Para importar uma lista de participantes, consulte [Importando uma lista de participantes, na página 182](#).

Para exportar uma lista de participantes, consulte [Exportando uma lista de participantes, na página 180](#).

Exportando uma lista de participantes

Antes de criar uma lista de participantes, selecione **Exportar lista** para exportar um arquivo CSV em branco com os títulos das colunas adequadas. Caso contrário, o sistema exporta todas as informações dos participantes para este grupo de Discagem Múltipla. A lista exportada que contém os participantes internos e externos contém: NOME, E-MAIL, NÚMERO DE TELEFONE 1, NÚMERO DE TELEFONE 2, NÚMERO DE TELEFONE 3, NÚMERO DE TELEFONE 4 e ISHOST.

-
- Etapa 1** Inicie sessão no site da Administração.
- Etapa 2** Selecione **Configurações > Áudio**.
- Etapa 3** Selecione um **Nome do grupo** na seção de Discagem Múltipla.
- Etapa 4** Selecione **Exportar lista** na seção de Participantes.
Os dados dos participantes são exportados como um arquivo CSV.
- Etapa 5** Na caixa de diálogo de exportação, selecione para abrir o arquivo com um aplicativo específico ou salve o arquivo e baixe-o.
- Etapa 6** Acesse o arquivo CSV exportado e adicione, altere ou exclua os dados dos participantes.
Para os participantes externos, o sistema requer um **nome, e-mail e um número de telefone**. Para os participantes internos, o sistema requer apenas um **e-mail** da empresa do usuário. Pelo menos para um usuário interno deve ser atribuído uma função de organizador.

Observação Se você inserir informações de participantes que não são necessárias, por exemplo, o nome de um usuário interno, o sistema não salva essas informações quando o arquivo CSV é importado. No entanto, se as informações estiverem incompletas, por exemplo, você se esqueceu de inserir o nome de um participante externo, o sistema importa as informações, mas exibe uma mensagem de erro. Entradas incorretas são consideradas inválidas e não são salvas no banco de dados.

- **Nome** (requerido para os participantes externos) — Insira o primeiro e o último nome de uma pessoa em qualquer formato desejado. Todos os símbolos são permitidos, mas < and > não é recomendado. Este nome é exibido na Lista externa e nas mensagens de e-mail que o sistema envia aos participantes com informações sobre como participar de uma reunião de Discagem Múltipla. Se o nome for muito longo para uma Lista externa, ele será truncado. (Os nomes em e-mails nunca serão truncados.) Para os usuários internos, o nome é recuperado da página **Minha conta** WebEx do usuário.
- **E-mail** (requerido para todos os participantes) — O sistema usa esse endereço para enviar as informações de chamada de entrada e PIN, enviar links para a parte on-line de uma reunião de Discagem Múltipla e para determinar se uma pessoa é um participante interno ou externo. Se um endereço de e-mail está armazenado no Cisco WebEx Meetings Server, a pessoa é uma participante interno e o sistema detecta automaticamente as informações de nome e telefone da página **Minha conta** WebEx do usuário. Se o endereço de e-mail for externo, o sistema usa o nome e os números de telefone inseridos no arquivo CSV.
- **Número de telefone** (requerido para participantes externos) — Insira até quatro números de telefone, incluindo o código do país, para os participantes externos. O sistema discia os números de telefone em ordem, ou seja, Número de telefone 1, então Número de telefone 2, e assim por diante. Insira pelo menos um número de telefone de cada participante externo. Os caracteres: 0 a 9, (,), - são permitidos. O sistema CWMS não identifica, verifica o formato ou converte o número do telefone; ele apenas encaminha a entrada para o CUCM.
- **Função** (para participantes internos somente) — Insira **organizador** para todos os usuários internos que serão organizadores de reuniões. Os organizadores recebem um e-mail com a senha do organizador, PIN de participante e o número da chamada de entrada. Mais do que uma pessoa pode ser designada como um organizador.

Próximos passos

Vá até [Importando uma lista de participantes](#), na página 182.

Importando uma lista de participantes

Antes de iniciar

Prepare um arquivo delimitado por vírgula ou delimitado por tabulações (CSV) que contenha as informações do participante. Você pode exportar os atuais valores da lista de participantes para um arquivo CSV, modificar o arquivo e importá-lo para adicionar ou alterar as informações do participante.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Configurações > Áudio**.

Etapa 3 Selecione um **Nome do grupo** na seção de Discagem Múltipla.

Etapa 4 Selecione **Tab ou Vírgula** para indicar o tipo de arquivo CSV que você está importando.

Etapa 5 Selecione **Navegar** e então selecione o arquivo CSV a ser importado.

Etapa 6 Selecione **Importar**.

O arquivo é importado para o sistema.

Etapa 7 Selecione **Atualizar** para salvar as informações do participante.

As informações dos participantes importados são salvas no banco de dados.

Próximos passos

Percorra as listas de participantes para visualizar as informações dos participantes e verificar se os valores foram importados corretamente.

Vá para [Exportando uma lista de participantes](#), na página 180 para exportar uma lista de participantes.

Definindo as configurações de vídeo

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Vídeo**.

Etapa 3 Selecione **360p, 180p** ou **Desativado** e então selecione **Salvar**.

Consulte a seção "Sobre gravações da reunião" no Guia de Planejamento CWMS para os requisitos de armazenamento aproximados.

Definindo suas configurações de dispositivos móveis

Se seu sistema está configurado pra permitir mais de um número de acesso de chamada de entrada, o sistema assume que o primeiro número é um número de acesso gratuito e tenta ligar primeiramente para este número.

O aplicativo não conectará se o número não for acessível a partir de uma rede móvel. Certifique-se que este número seja acessível por uma rede celular.

Ao usar um dispositivo móvel iOS e os certificados dos centros de dados não forem de uma autoridade de certificação bem conhecida, é necessário importar os dois certificados SSL dos centros de dados no dispositivo móvel iOS. Caso contrário, o dispositivo móvel iOS exibe um erro ao tentar iniciar uma reunião.

Recomendamos que os usuários de dispositivos móveis Android importem os dois certificados dos centros de dados antes de tentarem iniciar uma reunião. Depois de importar certificados no dispositivo Android, o dispositivo deve confiar nos sites WebEx e não mostrar uma mensagem de aviso ao iniciar uma reunião a partir deste site.



Observação

O Android é compatível com o Cisco WebEx Meetings Server 2.0 e superior. Ambos os aplicativos WebEx iOS e Android são ativados por padrão.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Celular**.

Etapa 3 Defina as suas configurações móveis, selecionando quais plataformas móveis o seu sistema suporta e então selecione **Salvar**.

Padrão: O aplicativo WebEx iOS e os aplicativos WebEx Android.

Os aplicativos WebEx iOS e Android funcionam da mesma forma como o aplicativo de desktop Cisco WebEx, a partir de uma intranet interna ou internet externa.

Próximos passos

Para o Cisco WebEx Meetings Server Versão 2.0 e posterior, consulte [Exportando um Certificado SSL para Dispositivos Móveis](#), na página 219 para obter informações sobre como exportar certificados para enviar por e-mail aos usuários de dispositivos móveis.

Configurando a Qualidade de Serviço (QoS)

As configurações do ponto de código (DSCP) dos Serviços Diferenciados (DiffServ) determinam o QoS para a sinalização de mídia de áudio e vídeo, conforme definido na RFC 2475. A Cisco recomenda que você guarde o valor padrão. Os outros valores estão disponíveis para os casos raros quando a rede requer uma configuração DSCP diferente. Para obter mais informações, consulte o capítulo "Infraestrutura de Rede" do Cisco Unified Communications Solution Reference Network Design (SRND) que se aplica à sua versão do Cisco Unified Communications Manager em http://www.cisco.com/en/us/products/sw/voicesw/ps556/products_implementation_design_guides_list.html.

A seguir estão os valores padrão:

- Áudio WebEx (Mídia)
 - IPv4 QoS Marcação: **EF DSCP 101110**

- IPv4 QoS Marcação: **EF DSCP 101110**
- Áudio WebEx (Sinalização)
 - IPv4 QoS Marcação: **CS3 (precedência 3) DSCP 011000**

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione **Configurações > Qualidade de Serviço**.

Etapa 3

Selecione as configurações de marcação QoS usando os menus suspensos apropriados e então selecione **Salvar**.

Sobre a Marcação QoS

Veja as tabelas abaixo para informações sobre Marcação QoS para instalações que possuem tráfego fluindo através de um servidor Proxy Internet Reverso em comparação a instalações sem tráfego fluindo através de um servidor Proxy Internet Reverso.

Marcação QoS no Sistema de Servidor de Reuniões Cisco Webex Sem Tráfego Movendo-se Através de um Servidor Proxy Internet Reverso

Tráfego	Marcação QoS
Áudio SIP — mídia — CWMS para o Endpoint	Sim
Áudio SIP — sinalização — CWMS para Endpoint	Sim
Áudio do PC — mídia — CWMS para o Cliente	Não
Áudio do PC — sinalização — CWMS para o Cliente	Não
Áudio do PC — mídia — Cliente para o CWMS	Não
Áudio do PC — sinalização — Cliente para o CWMS	Não
Vídeo do PC — mídia — CWMS para o Cliente	Não
Vídeo do PC — sinalização — CWMS para o Cliente	Não
Vídeo do PC — mídia — Cliente para o CWMS	Não
Vídeo do PC — sinalização — Cliente para o CWMS	Não

Marcação QoS no Sistema de Servidor de Reuniões Cisco Webex Sem Tráfego Movendo-se Através de um Servidor Proxy Internet Reverso

Tráfego	Marcação QoS
Áudio SIP — mídia — CWMS para o Endpoint	Sim
Áudio SIP — sinalização — CWMS para Endpoint	Sim
Áudio do PC — mídia — CWMS para o Cliente	Sim
Áudio do PC — sinalização — CWMS para o Cliente	Sim
Áudio do PC — mídia — Cliente para o CWMS	Não
Áudio do PC — sinalização — Cliente para o CWMS	Não
Vídeo do PC — mídia — CWMS para o Cliente	Sim
Vídeo do PC — sinalização — CWMS para o Cliente	Sim
Vídeo do PC — mídia — Cliente para o CWMS	Não
Vídeo do PC — sinalização — Cliente para o CWMS	Não

Configurando Senhas

Você pode configurar as definições de senha para o seguinte:

- Senhas Gerais — Controla o período de expiração da senha e permite que você force os usuários a alterar suas senhas imediatamente ou em intervalos específicos.
- Senhas de Usuário — Permite que você configure a força das senhas para contas de usuário incluindo maiúsculas e minúsculas, comprimento, tipos de caractere e uso, controles de texto da página dinâmica da internet e definição de uma lista de senhas inaceitáveis.
- Senhas da Reunião — Permite que você force o uso da senha para reuniões e configure a força da senha para reuniões incluindo maiúsculas e minúsculas, comprimento, tipos de caractere e uso, controles de texto da página dinâmica da internet e definição de uma lista de senhas inaceitáveis.



Observação

Se o SSO for habilitado em seu sistema, as definições nas páginas **Senha Geral** e **Senha do Usuário** e o controle de alteração de senha na página **Editar Usuário** não mais se aplicam às contas do organizador.

Configurando as definições da senha geral

Todas as configurações de senha nesta página são opcionais e podem ser ativadas (marcadas) ou desativadas (desmarcadas).

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Gerenciamento de Senha > Senha Geral**.

Etapa 3 (Opcional) Selecione **Desativar a conta de organizador após [número] dia(s) de inatividade** e insira o número de dias no campo de texto. (**Padrão:** Desmarcada (desativada) e definida para 90 dias.)
Se você ativar a configuração padrão, um usuário é desativado se ele não organizou ou agendou uma reunião por 90 dias consecutivos.

Este recurso apenas se aplica as contas de organizador. Você não pode desativar uma conta de administrador usando este recurso. Para desativar uma conta de administrador, consulte [Ativação ou desativação de usuários e administradores a partir da página Usuários, na página 124](#).

Etapa 4 (Opcional) Selecione **Forçar todos os usuários a alterar a senha a cada número dia(s)** e insira o número de dias no campo de texto. (**Padrão:** Desmarcado)

Etapa 5 (Opcional) Selecione **Forçar todos os usuários a alterar a senha no próximo logon**. (**Padrão:** Desmarcado)

Etapa 6 (Opcional) Selecione **Ativar o bloqueio da conta do usuário**. (**Padrão:** Desmarcado)
Os administradores podem desbloquear a conta (consulte [Desbloquear uma conta de administrador, na página 123](#)). Os parâmetros adicionais exibem:

- Número de falhas consecutivas de início de sessão [*número*].
- Esqueça a tentativa de início de sessão que falhou depois de [*número*] minutos.
- Remova o bloqueio da conta do usuário após [*número*] minutos.
- Envie notificações por e-mail aos usuários bloqueados.

Etapa 7 Selecione **Salvar**.

Configurando as exigências e limitações da senha do usuário

Essas configurações se aplicam para o administrador e os usuários finais quando o sistema utiliza autenticação padrão. Essas configurações se aplicam apenas para o administrador quando o sistema usa autenticação LDAP (Protocolo de Acesso Diretivo Inconsequente) ou autenticação SSO (Registro Único); as senhas de usuários finais são gerenciadas por um servidor AD ou um servidor IdP.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Gerenciamento de senha > Senha de usuário**.

Etapa 3 Altere as configurações da sua senha de usuário, configurando os campos na página.

Opção	Descrição
Requer senhas fortes para contas do usuário	Selecionar esta opção para ativar as opções restantes. Padrão: Selecionado

Opção	Descrição
Extensão mínima de caracteres	Exigência de caractere mínimo. Padrão: Selecionados e 6 caracteres
Número mínimo de caracteres alfabéticos	Alfabético mínimo (caracteres não numéricos, não especiais). Padrão: Selecionado e 1 caractere
Número mínimo de caracteres numéricos	Numérico mínimo (caracteres não alfabéticos, não especiais). Padrão: Selecionado e 1 número
Número mínimo de caracteres especiais	Especial mínimo (caracteres não alfabéticos, não numéricos). Padrão: Não selecionado e 1 caractere
Deve incluir letras maiúsculas e minúsculas misturadas	A senha deve conter caracteres alfabéticos maiúsculos e minúsculos. Padrão: Selecionado
Não permita que qualquer caractere seja repetido 3 vezes ou mais	Nenhum caractere (alfabético, numérico ou especial) podem ser repetidos mais que três vezes. Padrão: Selecionado
Lista de senhas inaceitáveis	A lista de senhas inutilizáveis especificadas pelo administrador . Padrão: Não selecionado
Nome da empresa, nome do site, endereço de e-mail do usuário e nome do organizador são sempre inaceitáveis	Não use esses nomes específicos. Padrão: Selecionado
Não deve incluir senhas <i>n</i> anteriores	Não use senhas utilizadas anteriormente. Selecione um número no menu suspenso para especificar o número de senhas anteriores que você não pode usar. Padrão: Selecionado Número padrão: 5

Etapa 4 Selecione **Salvar**.

Configurando as Suas Senhas de Reunião

Use esse recurso para configurar os parâmetros da senha da reunião. A tabela descreve quando os usuários devem inserir uma senha para participar de uma reunião.

Senha configurada	Senha excluída do convite do e-mail	O criador da reunião iniciou sessão	O organizador iniciou sessão	O convidado iniciou sessão	O convidado iniciou sessão	O convidado não iniciou sessão
Não	N/D	A senha não é necessária.	A senha não é necessária.	A senha não é necessária.	A senha não é necessária.	A senha não é necessária.
Sim	Sim	A senha não é necessária.	A senha não é necessária.	A senha não é necessária.	Senha necessária.	Senha necessária.
Sim	Não	A senha não é necessária.	A senha não é necessária.	A senha não é necessária.	Senha necessária. A senha é pré-preenchida.	Senha necessária. A senha é pré-preenchida.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Configurações > Gerenciamento de senha > Senha da reunião**.

Etapa 3 Altere as configurações da senha de reunião, configurando os campos na página.

Opção	Descrição
Todas as reuniões devem ter senhas	Exige que todas as reuniões tenham senhas.
Requer senhas fortes para reuniões	Habilita as opções restantes.
Extensão mínima de caracteres	Número mínimo de caracteres. Padrão: 6
Número mínimo de caracteres alfabéticos	Número mínimo de caracteres alfabéticos (não numéricos, não especiais). Padrão: 15
Número mínimo de caracteres numéricos	Caracteres numéricos mínimos (não alfabéticos, não especiais). Padrão: 15
Número mínimo de caracteres especiais	Caracteres especiais mínimos (não alfabéticos, não numéricos). Padrão: 15

Opção	Descrição
Não deve conter estes caracteres especiais (espaço, \, ', ", /, &, <, >, =, [,])	Selecione esta opção para proibir o uso desses caracteres.
Deve incluir letras maiúsculas e minúsculas misturadas	A senha deve conter caracteres alfabéticos maiúsculos e minúsculos.
Lista de senhas inaceitáveis	Lista de senhas inutilizáveis especificada pelo administrador.
Nome da empresa, nome do site, endereço de e-mail do usuário, nome do organizador e tópico de reunião são sempre inaceitáveis	Selecione esta opção para proibir o uso das sequências destas palavras ou caracteres.

Etapa 4 Selecione **Salvar**.

Configurando as Configurações do Seu E-mail

Você pode configurar as configurações do seu e-mail e modelos. Os modelos do seu e-mail tem configurações padrão que você pode opcionalmente alterar.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > E-mail**.

A página **Variáveis** abre.

Etapa 3 Insira o seu **Nome do remetente**, o seu **Endereço de e-mail do remetente**, o seu endereço de e-mail **Responder para**, e então selecione **Salvar**.

Se você inserir o nome de uma pessoa no De Nome na página Variáveis, exceto os convites de reuniões refletirão o endereço de e-mail do organizador.

Etapa 4 Selecione **Modelos**. Consulte [Sobre modelos de e-mail, na página 190](#) para obter descrições de cada tipo de modelo. A página **Modelos** aparece. Selecione a guia **Comum** ou **Reuniões**. **Comum** é o padrão.

Etapa 5 Para configurar os modelos de e-mail, selecione o link de modelo desejado na guia **Comum** e **Reuniões**.

Etapa 6 Faça alterações (se houver) no modelo de e-mail que você selecionou e selecione **Salvar**.

Exemplo:

Selecione o link de modelo **Conta Reativada** na guia **Comum**. Faça alterações nos campos na caixa de diálogo **Conta Reativada** e selecione **Salvar**.

Os valores padrão para **Nome do remetente**, **Endereço de e-mail do remetente**, e **Responder para** são retirados das configurações que você inseriu na página **Variáveis**.

Observação Se você inserir o nome de uma pessoa no **De Nome** na página **Variáveis**, o sistema substitui automaticamente o nome da pessoa pela URL do site WebEx em todos os convites de reuniões.

Sobre modelos de e-mail

Use os modelos de e-mail para comunicar eventos importantes aos usuários. Cada modelo de e-mail tem variáveis que você deve configurar. Consulte a tabela abaixo para obter as descrições das variáveis em cada modelo.

Há dois tipos de modelos de e-mail:

- Comum - Incluindo senha perdida, notificações de organizador e convidados, disponibilidade de gravação e outros avisos gerais.
- Reuniões - Incluindo convites de reunião, cancelamentos, atualizações, lembretes e avisos de informação.

Tabela 3: Modelos de E-mail Comum

Cargo	Descrição	Variáveis
Ativação AD	Enviada a um usuário depois que uma conta AD foi ativada.	<ul style="list-style-type: none"> • %SiteURL% • %DisplayName% • %SSOSignINLink% • %OrgLogo% • %Participants% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
A Sincronização AD falhou	Enviado para um administrador após uma falha na sincronização.	<ul style="list-style-type: none"> • %FullName% • %Failure_Reason% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Sucesso na Sincronização AD	Enviado para um administrador após uma sincronização com sucesso.	<ul style="list-style-type: none"> • %FullName% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Conta Reativada	Enviado para um usuário após um administrador reativar a conta do usuário.	<ul style="list-style-type: none"> • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Esqueceu a Senha-Senha Alterada	Enviado para um usuário após ele ter redefinido sua senha no site do usuário final.	<ul style="list-style-type: none"> • %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Esqueceu a Senha – Redefinir Senha	Enviado para um usuário após ele ter redefinido sua senha no site do usuário final. Este e-mail solicita que o usuário crie uma nova senha.	<ul style="list-style-type: none"> • %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Convite de Reunião PT — Convidado	Enviado para os convidados da reunião após uma reunião ser agendada usando as Ferramentas de Produtividade através de uma conta de Conferência Pessoal.	<ul style="list-style-type: none"> • %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %Meeting Space% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Notificação de Reunião PT — Organizador	Enviado para um organizador de reunião após uma reunião ser agendada usando as Ferramentas de Produtividade através de uma conta de Conferência Pessoal.	<ul style="list-style-type: none"> • %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %Meeting Space% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Convite de reunião PT — Organizador	Enviado para um organizador de reunião após uma reunião ser agendada usando as Ferramentas de Produtividade.	<ul style="list-style-type: none"> • %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%
Convite de reunião PT - Convidado	Enviado para os convidados da reunião após uma reunião ser agendada usando as Ferramentas de Produtividade.	<ul style="list-style-type: none"> • %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%

Cargo	Descrição	Variáveis
Gravação Disponível para o Organizador	Envia um link ao organizador para uma gravação de reunião.	<ul style="list-style-type: none"> • %SiteURL% • %OrgLogo% • %DisplayName% • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
E-mail de Ativação do SSO	Enviado após o registro único (SSO) ser habilitado.	<ul style="list-style-type: none"> • %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Enviar E-mail Para Todos os Usuários	Envia um e-mail para todos os usuários no sistema.	<ul style="list-style-type: none"> • %SiteURL% • %Subject% • %OrgLogo% • %AttendeeName% • %Body% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Configurar o Cisco WebEx — Dispositivo móvel	Informa aos usuários sobre o aplicativo Cisco WebEx para dispositivos móveis e fornece um link de download para o aplicativo.	<ul style="list-style-type: none"> • %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Compartilhar Gravação	Envia aos convidados da reunião selecionados um link com a gravação da reunião.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %OrgLogo% • %AttendeeName% • %HostName% • %Topic Name% • %Duration% • %Recording Time% • %Personalized Message% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Compartilha Gravação do MC	Envia aos convidados da reunião selecionados um link com a gravação da reunião. Os participantes selecionados pelo organizador no Meeting Center após selecionar Sair da reunião .	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %OrgLogo% • %AttendeeName% • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Usuários—Senha Alterada	Envia um e-mail aos usuários quando a senha foi alterada.	<ul style="list-style-type: none"> • %SiteURL% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
E-mail de boas-vindas	Enviado a um novo administrador após sua conta ser criada.	<ul style="list-style-type: none"> • %SiteURL% • %DisplayName% • %SiteURL% • %Support% • %participants% • %CustomFooterText% • %Year%

Tabela 4: Modelos de E-mail de Reuniões

Cargo	Descrição	Variáveis
Convite de reunião Blast Dial para o organizador	Enviado ao organizador quando um organizador disca um número de chamada de entrada de Discagem múltipla para iniciar uma reunião.	<ul style="list-style-type: none"> • %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %HostPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText% • %Year%
Convite de reunião Blast Dial para o convidado	Enviado aos participantes quando um organizador disca um número de chamada de entrada de Discagem múltipla para iniciar uma reunião.	<ul style="list-style-type: none"> • %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText% • %Year%
O grupo de reunião de Discagem Blast foi excluído	Enviado aos membros do grupo de Discagem múltipla quando um administrador exclui o grupo.	<ul style="list-style-type: none"> • %SiteURL% • %BlastDialGroupName% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Convite de reunião Blast Dial em andamento para o organizador	Enviado a outros organizadores quando um organizador os convida para uma reunião enquanto a reunião está em andamento.	<ul style="list-style-type: none"> • %SiteURL% • %BlastDialGroupName% • %HostName% • %MeetingInfoURL% • %AccessNumber% • %HostPin% • %MeetingPassword% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText% • %Year%
Convite de reunião Blast Dial em andamento para o convidado	Enviado aos usuários quando um organizador os convida para uma reunião enquanto a reunião está em andamento.	<ul style="list-style-type: none"> • %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %MeetingPassword% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
As informações da reunião de Discagem Blast foram atualizadas para o organizador	Fornece informações da reunião para um organizador quando as definições da reunião foram alteradas.	<ul style="list-style-type: none"> • %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %HostPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText% • %Year%
As informações da reunião de Discagem múltipla foram atualizadas para o convidado	Fornece informações da reunião aos participantes quando as definições da reunião foram alteradas.	<ul style="list-style-type: none"> • %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Convite de Reunião em Andamento para o Convidado	Enviado aos usuários quando um organizador os convida para uma reunião enquanto a reunião está em andamento.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %AttendeeName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Convite de Reunião Instantânea para o Organizador	Enviado ao organizador e convidados quando o organizador seleciona Reunir-se agora .	<ul style="list-style-type: none"> • %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Reunião Cancelada para o Convidado	Informa ao usuário que uma reunião agendada foi cancelada.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %AttendeeName% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Year%
Reunião Cancelada para o Organizador	Enviado ao organizador da reunião para confirmar o cancelamento de uma reunião.	<ul style="list-style-type: none"> • %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Informações Atualizadas da Reunião para o Organizador Alternativo	Fornece informações da reunião para o organizador alternativo quando as definições da reunião foram alteradas.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Informações Atualizadas da Reunião para o Convidado	Fornece informações da reunião para um participante da reunião quando as definições da reunião foram alteradas.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Informações Atualizadas da Reunião para o Organizador	Fornece informações da reunião para o organizador quando as definições da reunião foram alteradas.	<ul style="list-style-type: none"> • %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Lembrete de Reunião para o Organizador Alternativo	Envia um lembrete de reunião para o organizador alternativo da reunião.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Lembrete de Reunião para o Organizador	Envia um lembrete de reunião para o organizador da reunião.	<ul style="list-style-type: none"> • %SiteURL% • %Topic% • %OrgLogo% • %HostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Reunião Remarcada para o Organizador Alternativo	Envia informações atualizadas da reunião para o organizador alternativo.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Reunião Remarcada para o Convidado	Envia informações atualizadas da reunião para os convidados.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Informações de Reunião para o Organizador Alternativo	Envia uma confirmação de reunião para o organizador alternativo.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Informações de Reunião para o Convidado	Envia um convite de reunião para os convidados.	<ul style="list-style-type: none"> • %HostName% • %Hoste-mail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Informações de Reunião para o Organizador	Envia uma confirmação de reunião para o organizador.	<ul style="list-style-type: none"> • %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Cargo	Descrição	Variáveis
Lembrete de Reunião Automático PCN—Organizador	Envia um lembrete de reunião automático para o organizador da reunião (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Convite de Reunião PCN—Convidado	Envia um convite de reunião para os convidados (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Cargo	Descrição	Variáveis
Lembrete de Reunião Manual PCN—Organizador	Envia um lembrete de reunião manual para o organizador da reunião (apenas contas PCN).	<ul style="list-style-type: none"> • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Lembrete de Reunião Manual PCN—Convidado	Envia um lembrete manual de reunião para os convidados (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Cargo	Descrição	Variáveis
Notificação de Reunião PCN—Organizador	Envia uma notificação de reunião para o organizador (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
Convite Instantâneo de Reunião PCN — Organizador	Envia uma notificação de reunião instantânea para o organizador (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %SiteURL% • %Support%

Cargo	Descrição	Variáveis
Convite de Reunião PCN em Andamento — Convidado	Envia uma notificação de reunião instantânea para um convidado (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
Alteração do Agendamento da Reunião PCN — Organizador	Envia uma notificação de alteração do agendamento para o organizador (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%

Cargo	Descrição	Variáveis
Alteração do Agendamento da Reunião PCN — Convidado	Envia uma notificação de alteração do agendamento para um convidado (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
Remarcação da Reunião PCN — Convidado	Envia uma notificação de reagendamento da reunião para um convidado (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Cargo	Descrição	Variáveis
Cancelamento da Reunião PCN — Organizador	Envia uma notificação de cancelamento da reunião para o organizador (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%
Cancelamento da Reunião PCN — Convidado	Envia uma notificação de cancelamento da reunião para um convidado (apenas contas de Conferência Pessoal).	<ul style="list-style-type: none"> • %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%

Sobre os downloads de aplicativos

Você pode implantar esses aplicativos CWMS em massa usando as ferramentas disponíveis para você no site de Administração. Os aplicativos disponíveis para download incluem o seguinte:

- Aplicativo WebEx Meetings



Observação

A execução do aplicativo WebEx Meetings em um sistema operacional virtualizado não é suportada.

- Ferramentas de produtividade WebEx

Depois de uma atualização para um sistema, os usuários devem desinstalar quaisquer versões antigas das Ferramentas de Produtividade WebEx. Após a atualização, você pode usar o site de Administração para mover as Ferramentas de Produtividade WebEx aos seus usuários ou pedir que os usuários baixem as Ferramentas de Produtividade WebEx da página **Downloads** do usuário final.

- Reprodutor de Gravações de Rede WebEx

Você pode usar o site de Administração para permitir que os usuários baixem aplicativos eles mesmos, para mover aplicativos aos computadores dos usuários ou baixar os arquivos de instalação e pedir aos usuários para que instalem os aplicativos manualmente eles mesmos.

Você pode adquirir os instaladores .MSI para cada um dos aplicativos a partir da página **Admin > Configurações > Downloads**. Consulte [Baixar aplicativos a partir do site de administração](#) para obter mais informações.

Se os usuários têm privilégios de administrador em seus computadores, você pode distribuir os aplicativos usando os downloads automáticos, a instalação e o download habilitado pelo usuário ou movendo os aplicativos para os computadores dos usuários. Se sua empresa não dá privilégios de administrador aos usuários, você deve usar uma abordagem alternativa para instalar os aplicativos nos computadores.

Recomendamos que você move os aplicativos aos computadores dos usuários off-line, antes de informar a esses usuários finais que as contas foram criadas a eles. Isso garante que os usuários podem iniciar e participar de reuniões e reproduzir gravações de rede na primeira vez que iniciarem sessão.

Se um usuário não tiver os aplicativos instalados, a primeira vez que um usuário participar de uma reunião, o aplicativo WebEx Meetings será baixado no PC. Isso pode ser configurado para ser feito sob demanda ou em silêncio. O usuário tem a opção de usar o aplicativo Cisco WebEx Meetings durante a duração da reunião e tê-lo removido quando a reunião terminar ou executar uma instalação do aplicativo para acelerar o processo de iniciar ou participar de reuniões futuras. Isso pode falhar porque o usuário não tem privilégios de administrador.

Em PCs onde os usuários possuem privilégios de administrador, os usuários podem baixar e instalar o aplicativo Cisco WebEx Meetings, as Ferramentas de Produtividade e o Reprodutor de gravações de rede a partir das páginas de download do usuário final. Nenhuma ação adicional do administrador é necessária.

Ao **atualizar** para o Cisco WebEx Meetings Server Versão 1.5MR3 ou superior em um ambiente bloqueado onde os PCs dos usuários não têm privilégios de administrador, antes de iniciar o procedimento de atualização, move a nova versão do aplicativo WebEx Meetings a todos os PCs dos usuários. Ter as novas e antigas versões do aplicativo Meetings armazenadas nos PCs dos usuários permite que eles participem das reuniões organizadas pelos usuários executando as versões mais recentes ou anteriores do aplicativo Meetings. Os usuários podem ter várias versões do aplicativo WebEx Meetings armazenadas nos PCs, desde que os arquivos estejam armazenados nas pastas corretas.



Observação

Para sites que implantaram o Cisco WebEx Meetings Server Versão 1.5 MR3 (build 1.5.1.386) ou anterior e usam o WebEx Meeting Services baseado em nuvem, desinstale o aplicativo Meetings do WebEx Meetings Server e WebEx Meeting Services e então reinstale o aplicativo Meetings nas pastas corretas nos PCs dos usuários. Caso contrário, os usuários não podem participar de reuniões organizadas pelos usuários WebEx baseados em nuvem. Consulte "Usuários com PCs sem privilégios de administrador não podem entrar em reuniões organizadas pelos usuários WebEx baseados em nuvem" no *Guia de solução de problemas do Cisco WebEx Meeting Server* para obter mais detalhes.

Definição das Configurações de Download

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Downloads**.

Etapa 3 Selecione a caixa de seleção **Atualização automática das ferramentas de produtividade WebEx** para configurar as atualizações automáticas periódicas. (**Padrão:** Marcado.)

Observação Se você planeja mover manualmente as ferramentas de produtividade WebEx para seus usuários, recomendamos que você desmarque esta opção.

Observação Quando esta opção for selecionada, depois que os usuários instalam uma versão atualizada das Ferramentas de Produtividade Cisco WebEx, a versão das Ferramentas de Produtividade WebEx exibida nos **Programas e Recursos** no Painel de Controle do Windows mostra um número de versão mais antigo. No entanto, a versão exibida em **Sobre as Ferramentas de Produtividade WebEx** no Assistente WebEx mostra a versão correta. Este é um problema conhecido e será corrigido em uma versão posterior.

Etapa 4 Selecione os seus métodos de download:

- Permitir que usuários baixem aplicativos do desktop WebEx
- Mova manualmente o WebEx Meetings e as Ferramentas de Produtividade para o desktop do usuário

Se você selecionar **Permitir que usuários baixem aplicativos do desktop WebEx**, você pode selecionar **Salvar** para finalizar a sua configuração de download. Nenhuma ação é necessária.

Se você selecionar **Mover manualmente o WebEx Meetings e as Ferramentas de Produtividade para o desktop do usuário**, o aplicativo WebEx Meetings, as ferramentas de produtividade e as seções de reproduutor de gravações de rede WebEx aparecem na página. Prossiga para a próxima etapa.

Etapa 5 Para cada aplicativo que você deseja baixar e instalar, selecione **Baixar** e selecione **Salvar** para salvar um arquivo ZIP para seu sistema que contém instaladores para o aplicativo correspondente.

Cada arquivo ZIP contém instaladores de aplicativos para todas as plataformas e idiomas suportados.

Etapa 6 Selecione **Salvar** para salvar as suas configurações de Download.

Gerenciando Certificados

Os certificados garantem a comunicação segura entre os componentes de seu sistema. Quando o sistema estiver implantado, é configurado com um certificado autoassinado. Embora um certificado autoassinado pode durar até cinco anos, nós recomendamos que você configure certificados que são validados por uma autoridade certificadora. Uma autoridade certificadora garante que a comunicação entre suas máquinas virtuais seja autenticada. Um sistema pode ter várias máquinas virtuais. Apenas um certificado é necessário para um centro de dados. Exceto para a máquina virtual IRP, o certificado do sistema inclui os nomes de domínio totalmente qualificado (FQDN) para todas as outras máquinas virtuais, URLs de sites e URLs de administração.

Os seguintes tipos de certificado são suportados:

- SSL — Necessário em todos os sistemas. Consulte [Importando os Certificados IdP de SSO, na página 222.](#)
- SSO IdP — Para o SSO com certificados de provedor de identidade (IdP).
- Teleconferência Segura — Necessário para teleconferência TLS. Você pode configurar até dois certificados de teleconferência segura, um para cada sistema CUCM que você escolher configurar.
- SMTP — Necessário se o servidor de e-mail tem TLS habilitado.

Este produto suporta os seguintes certificados SSL:

- Autoassinado
- Certificado de autoridade assinado
- Certificado de autoridade assinado externo

Você não pode atualizar os certificados ou a Solicitação de Assinatura de Certificado (CSR), mas você pode gerar um certificado ou um CSR a qualquer momento. Se você adicionar máquinas virtuais em seu sistema ou alterar qualquer uma das máquinas virtuais existentes, você deve gerar novos certificados para cada máquina virtual em seu sistema.

Os certificados SSL podem se tornar inválidos, pelas seguintes razões:

- Um centro de dados está associado ao sistema.
- O tamanho do sistema foi expandido, resultando na implantação de novas máquinas virtuais. As FQDNs dessas novas máquinas virtuais não existem em seus certificados SSL originais.
- Um sistema de alta disponibilidade foi adicionado, resultando na implantação de novas máquinas virtuais. As FQDNs dessas novas máquinas virtuais não existem em seus certificados SSL originais.
- A URL do site da Cisco WebEx mudou. Esta URL não está presente em seu certificado SSL original.
- A URL do site de Administração mudou. Esta URL não está presente em seu certificado SSL original.
- O FQDN da máquina virtual de administração mudou. Esta FQDN não está presente em seu certificado SSL original.
- Seu certificado SSL atual expirou.

Se o seu certificado SSL tornar-se inválido por qualquer motivo, o sistema irá gerar automaticamente novos certificados autoassinados e você será informado da mudança através de uma mensagem de alerta global no topo da página do site de Administração indicando que o SSL tornou-se invalidado.

Gerando Certificados SSL

Seu sistema deve ter os seguintes certificados SSL configurados: Este produto suporta os seguintes tipos de certificados SSL:

- Autoassinado
- Certificado de autoridade assinado
- Certificado de autoridade assinado externo

Gerando um Certificado de Solicitação de Entrada (CSR)

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

- Etapa 2** Selecione **Configurações > Segurança > Certificados > centro de dados > Gerar CSR.**
- Etapa 3** Complete estes campos na página **Gerar CSR (Certificado de Solicitação de Entrada).**

Opção	Descrição
Nome comum	Selecione o certificado da URL do site local , certificado da URL do site global ou certificado Curinga .
Nomes Alternativos do Assunto Esta opção só aparece se você selecionar Nome alternativo do assunto para o seu tipo de Nome Comum.	Seu site de administração e nomes da máquina virtual. Nenhum nome alternativo de assunto são necessários se você selecionou um nome comum para o curinga.
Organização	Insira o nome da sua organização.
Departamento	Insira o nome do seu departamento.
Cidade	Digite sua cidade.
Estado/Província	Insira seu Estado ou província.
País	Selecione o seu país.
Tamanho da Chave	Selecione o tamanho de chave. Padrão: 2048 (Recomendado)

- Etapa 4** Selecione **Gerar CSR.**
A caixa de diálogo **Baixar CSR** aparece.
- Etapa 5** Selecione **Baixar.**
Você recebe um arquivo ZIP que contém a CSR e a chave privada associada. O arquivo CSR é chamado de `csr.pem` e o arquivo de chave privada é chamado `csr_private_key.pem`.
- Etapa 6** Faça backup do sistema usando o VMware Data Recovery ou o VMware vSphere Data Protection. Consulte [Criando um Backup Usando o VMware vCenter](#), na página 6.
O backup do sistema preserva a chave privada, no caso em que seja necessário restaurá-lo.

Importando um Certificado SSL

O Cisco WebEx Meetings Server suporta certificados X.509 com codificação PEM e DER e arquivos PKCS12.

Os usuários podem ter problemas ao participarem de reuniões se o sistema usar um certificado autoassinado. Para evitar isso, configure o lado do cliente para usar certificados autoassinados.

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

- Etapa 3** Selecione **Configurações > Segurança > centro de dados > Certificados > Mais opções > Importar certificado SSL/chave privada.**

Se você já tem um certificado instalado, o sistema avisa que importando um novo certificado irá substituí-lo.

- Etapa 4** Selecione **Continuar.**

- Etapa 5** Selecione **Procurar** e escolha seu certificado.

Você deve escolher um certificado compatível com o X.509 ou cadeia de certificação. Os tipos válidos incluem:

- Certificado codificado PEM/DER: .CER / .CRT / .PEM / .KEY
- Certificado criptografado PKCS12: .P12 / .PFX

Você pode importar uma cadeia de certificado usando um arquivo PKCS#12 ou um único arquivo de blocos PEM. Se usar um arquivo PEM, ele deve ser formatado da seguinte maneira:

- (Opcional) Para carregar uma chave privada, a chave privada deve ser o primeiro bloco no arquivo. Ele pode ser criptografado ou não criptografado. Ele deve estar codificado PEM em formato PKCS#8.. Se ele for criptografado, você deve inserir uma senha para decifrá-lo.
- O próximo elemento deve ser o certificado da autoridade de certificação intermediária que emitiu o certificado em formato PEM X.509 codificado.
- Você pode incluir tantos certificados intermediários como você usa em sua infraestrutura. O certificado da autoridade de certificado raiz não deve ser incluído. Se você estiver usando uma autoridade de certificação privada, você deve se certificar de que o certificado raiz seja distribuído para todos os clientes.

Todos os certificados devem ser carregados juntos em um arquivo; você não pode carregar um certificado e, em seguida, adicionar os certificados intermediários mais tarde. Você pode carregar os certificados intermediários para evitar avisos de certificados se você estiver usando uma autoridade de certificação que utiliza certificados intermediários e os certificados intermediários não são distribuídos em seus clientes.

Se os certificados vêm com uma cadeia de certificados, você deve combinar um certificado intermediário e um certificado de usuário final em um arquivo. A sequência é que o certificado intermediário seja o primeiro, e o certificado de usuário final o próximo. Os dois certificados estão juntos; não há espaço entre eles.

Os arquivos PKCS#12 devem ter a extensão .p12. Eles só devem conter os certificados e a chave privada (opcional).

- Etapa 6** Selecione **Carregar.**

O sistema determina se o certificado é válido. Um certificado pode estar inválido pelas seguintes razões:

- O arquivo certificado não é um arquivo certificado válido.
- O arquivo de certificado expirou.
- Sua chave pública é inferior a 2048 bits.

- Os domínios do servidor no certificado não correspondem a URL do site.
- A chave privada que foi auto gerada pelo sistema não é compatível com o certificado.
- Ele não contém todos os nomes de organizadores do sistema (exceto nomes de organizadores DMZ) ou as URLs do site e de administração. Em um sistema MDC, ele deve conter as URLs do site global, do site local e de administração.

Etapa 7 (Opcional) Insira a **Frase secreta**.

Uma frase secreta é necessária para descriptografar os arquivos PKCS12 ou uma chave privada criptografada (se os arquivos PEM carregados contêm a chave privada).

Etapa 8 Selecione **Continuar**.

O seu sistema importa o seu certificado SSL e o exibe em uma caixa de diálogo de rolagem o arquivo certificado.

Etapa 9 Selecione **Concluído**.**Etapa 10** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Exportando o Certificado SSL

Baixando o certificado Secure Socket Layer (SSL):

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Segurança > Certificados > centro de dados > Mais opções > Exportar certificado SSL**.

Uma opção para abrir ou salvar o certificado é exibida.

Etapa 3 Salvar o arquivo de certificado.

Isso proporciona apenas o certificado da entidade final CWMS do Cisco WebEx Meeting Server. Se você carregou certificados intermediários adicionais, eles não estão incluídos.

Próximos passos

Garanta que os administradores e os usuários finais sejam capazes de iniciar sessão na administração ou nas páginas web comuns sem deixar de visualizar avisos de *sites não confiáveis*.

Exportando um Certificado SSL para Dispositivos Móveis

Os iPhones ou iPads da Apple que executam o iOS 5.0 ou posterior da Apple possuem um certificado raiz confiável integrado. Se sua empresa usa um certificado autoassinado, ou se o certificado raiz instalado no Cisco WebEx Meetings Server não está na lista da Autoridade Certificadora Confiável da Apple, você deve exportar um certificado SSL e enviá-lo aos seus usuários que devem instalar nos seus dispositivos móveis antes de participarem de uma reunião WebEx.

É necessário exportar um certificado SSL somente se você estiver utilizando um certificado autoassinado. Se você estiver utilizando um Certificado confiável assinado por Autoridade, a exportação do certificado SSL não é necessária.

Antes de iniciar

Verifique se o certificado raiz confiável pré-instalado no iPhone ou iPad da Apple de um usuário está na lista da Autoridade Certificadora Confiável da Apple. Consulte <http://support.apple.com/kb/ht5012> para obter detalhes.

Verifique se os usuários possuem uma conexão de Internet de alta velocidade ativa para seus dispositivos móveis.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Segurança > Certificados > centro de dados > Mais opções > Exportar certificado SSL**.

Etapa 3 Salve o arquivo do certificado para o disco rígido local.

Etapa 4 Anexe o arquivo de certificado salvo em um e-mail e envie-o para a conta de e-mail do iOS de cada usuário autorizado.

Etapa 5 Os usuários abrem o e-mail nos seus dispositivos móveis, salvam o arquivo e instalam o arquivo de certificado nos seus dispositivos móveis:

- a) Toque em **Instalar** na página **Instalar Perfil**.
 - b) Toque em **Instalar agora** na caixa de diálogo Perfil Sem Assinatura.
 - c) Insira uma senha do iOS.
 - d) Toque **Próxima**.
 - e) Toque **Concluído**.
-

Baixando um CSR e a chave privada

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Segurança > Certificados > centro de dados > Mais opções > Baixar o CSR**.

Uma caixa de diálogo aparece pedindo para você salvar o arquivo CSR.zip, que contém o CSR e a chave privada.

Etapa 3 Selecione um local em seu sistema para salvar o arquivo e selecione **OK**.

Etapa 4 Faça backup do arquivo de chave privada, csr-private-key.pem, no caso de você precisar dele mais tarde.

Gerar um Certificado Auto Assinado

Um certificado autoassinado é automaticamente gerado após você implementar o seu sistema. Recomendamos que você instale um certificado que é assinado por uma autoridade de certificado. Você pode gerar um novo certificado autoassinado a qualquer momento, usando este recurso.



Observação

Os usuários podem ter problemas ao participar de reuniões se o sistema usar um certificado autoassinado, a menos que o administrador no lado do cliente configurou o sistema para usar certificados autoassinados.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Segurança > Certificados > centro de dados > Mais opções > Gerar certificado auto assinado.**

Etapa 3 Complete os campos na página **Certificado Auto Assinado Geral**.

Opção	Descrição
Nome do Certificado	Insira um nome para o seu certificado autoassinado. (Necessário)
Nome do assunto X.509	O nome do organizador do seu sistema é a URL do site. Em um sistema MDC, você pode escolher entre a URL do site local e a URL do site global.
Organização	Insira o nome da sua organização.
Departamento	Insira o nome do seu departamento.
Cidade	Insira o nome da sua cidade.
Estado/Província	Insira o nome do seu estado ou província.
País	Selecione o nome do seu país.

Etapa 4 Selecione **Gerar Certificado e Chave Privada**.

Se você precisar usar o mesmo certificado SSL depois de uma grande atualização, você deve carregar a chave privada gerada com o CSR que é usado para obter o certificado. A chave privada deve ser o primeiro bloco no arquivo de certificado.

Seu arquivo de certificado é gerado e exibido.

Etapa 5 Seleione **Concluído**.

Restaurar um Certificado SSL

No caso do seu certificado tornar-se inválido ou você tiver executado uma recuperação de desastres em seu sistema, você pode restaurar um certificado SSL usando este recurso. O Cisco WebEx Meetings Server suporta certificados X.509 com codificação PEM e DER e arquivos PKCS12.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Configurações > Segurança > Certificados > centro de dados > Mais opções > Importar certificado SSL/chave privada**.

Se você já tem um certificado instalado, o sistema avisa que importando um novo certificado irá substituí-lo.

Etapa 4 Selecione **Continuar**.

Etapa 5 Selecione **Procurar** e escolha seu arquivo de certificado.

Você deve escolher um certificado compatível com o X.509 ou cadeia de certificação. Os tipos válidos incluem:

- Certificado codificado PEM/DER: .CER / .CRT / .PEM / .KEY
- Certificado criptografado PKCS12: .P12 / .PFX

Você pode importar uma cadeia de certificado usando um arquivo PKCS#12 ou um único arquivo de blocos PEM. Se usar um arquivo PEM, ele deve ser formatado da seguinte maneira:

- (Opcional) Se você quiser reaplicar um par de chaves pública/privada antes para a recuperação de desastres, combine o arquivo de chave pública (csr_private_key.pem) e o certificado recebido da sua autoridade de certificação (CA) em um arquivo. A chave privada deve ser o primeiro bloco no arquivo seguido pela chave pública. Ele pode ser criptografado ou não criptografado. Ele deve estar codificado PEM em formato PKCS#8. Se ele é criptografado, você deve digitar a senha para decifrá-lo no campo senha.
- O próximo elemento deve ser o certificado da autoridade de certificação intermediária que emitiu o certificado em formato PEM X.509 codificado.

- Você pode incluir tantos certificados intermediários como você usa em sua infraestrutura. O certificado da autoridade de certificado raiz não deve ser incluído. Se você estiver usando uma autoridade de certificação privada, você deve se certificar de que o certificado raiz seja distribuído para todos os clientes.

Todos os certificados devem ser carregados juntos em um arquivo. Você não pode carregar um certificado e, em seguida, adicionar os certificados intermediários mais tarde. Você pode querer fazer o upload dos certificados intermediários se você estiver usando uma autoridade de certificação que utiliza certificados intermediários e os certificados intermediários não são distribuídos em seus clientes. Carregá-los irá evitar avisos de certificados.

Os arquivos PKCS#12 devem ter a extensão .p12. Eles só devem conter os certificados e a chave privada (opcional).

Etapa 6 Seleione **Carregar**.

Após selecionar **Carregar**, o sistema vai determinar se o seu certificado é válido. Um certificado pode ser inválido pelas seguintes razões:

- O arquivo certificado não é um arquivo certificado válido.
- O arquivo certificado que você selecionou expirou.
- A chave pública deve ter pelo menos 2048 bits.
- Os domínios do servidor no certificado não correspondem a URL do site.
- A chave privada que foi auto gerada pelo sistema não é compatível com o certificado.

Se o certificado for válido, proceda até o próximo passo. Se o certificado for inválido, você não pode carregá-lo. Você deve selecionar um certificado válido antes de continuar.

Etapa 7 (Opcional) Insira uma **Frase secreta**.

Uma senha é necessária para descriptografar os arquivos PKCS12 ou uma chave privada criptografada (se carregados, os arquivos .pem contêm a chave privada).

Etapa 8 Seleione **Continuar**.

O seu sistema importa o seu certificado SSL e o exibe em uma caixa de diálogo de rolagem o arquivo certificado.

Etapa 9 Seleione **Continuar** na página **Certificados SSL** para concluir a importação.

Etapa 10 Seleione **Concluído**.

Etapa 11 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Importando os Certificados IdP de SSO

Para Registro Único (SSO) de provedor de serviço iniciado com uma solicitação de autenticação assinada em um sistema com Vários centros de dados (MDC), você deve importar o certificado de cada centro de dados

para o Provedor de Identidade (IdP). (O Cisco WebEx Meeting Server não pode usar sua chave privada para descriptografar a afirmação.)

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
 - Etapa 2** Selecione **Configurações > Segurança > Certificados IdP de SSO**.
 - Etapa 3** Selecione **Navegar** e escolha o seu certificado IdP de SSO.
 - Etapa 4** Selecione **Carregar**.
Seu arquivo de certificado é exibido.
 - Etapa 5** Selecione **Concluído** para submeter o seu certificado.
-

Importando certificados SMTP

Importando certificados SMTP de um computador local para o sistema CWMS.

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
 - Etapa 2** Selecione **Configurações > Segurança > Certificados > centro de dados > Certificado SMTP > Importar certificado**.
 - Etapa 3** Selecione **Procurar** e escolha o certificado SMTP.
 - Etapa 4** Selecione **Carregar**.
Seu arquivo de certificado é exibido.
 - Etapa 5** Se o sistema não está em modo de manutenção, selecione **Continuar** para entrar no modo de manutenção.
 - Etapa 6** Selecione **Concluído** para submeter o seu certificado.
 - Etapa 7** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).
Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.
O serviço de reuniões para usuários neste centro de dados é restaurado.
 - Etapa 8** Selecione **Continuar**.
O sistema reinicia.
-

Importar Certificados de Teleconferência Segura

Os certificados de teleconferência segura só são necessários se a conferência TLS for habilitada. Se a conferência TLS não for habilitada, esta opção não estará disponível.

Antes de iniciar

Os certificados de teleconferência segura são necessários para os seus servidores CUCM quando o TLS é selecionado como o tipo de transporte em suas configurações de áudio. Consulte [Sobre Configurar Suas Definições de Áudio, na página 167](#) para obter mais informações.

- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).)
- Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.
- Etapa 3** Selecione **Configurações > Segurança > Certificados**.
A seção Certificado de Teleconferência Segura exibe uma das duas seguintes mensagens:
- Este sistema não exige certificados de teleconferência segura porque a teleconferência TLS não está habilitada.
 - Os certificados de conferência segura CUCM são necessários para teleconferência TLS que está habilitada em seu sistema.
- Se os certificados de teleconferência segura são necessários, um botão **Importar certificado** é exibido para cada servidor CUCM que deve ser configurado.
- Etapa 4** Selecione **Importar certificado** para CUCM *n*.
A página **Certificado de Teleconferência Segura** é exibida.
- Etapa 5** Digite um nome do certificado.
- Etapa 6** Selecione **Procurar** e escolha seu arquivo de certificado.
Observação Se o CUCM utiliza certificados autoassinados, então use o arquivo CallManager.pem. Se o CUCM utiliza certificados de terceiros, então use o certificado de Autoridade de Certificação Raiz (CA). Veja "Baixando Certificados CUCM" no *Guia de Planejamento* para mais detalhes sobre como baixar um certificado CUCM no seu disco rígido local.
- Etapa 7** Selecione **Carregar**.
Após selecionar **Carregar**, o sistema vai determinar se o seu certificado é válido.

Se o certificado for válido, proceda até o próximo passo. Se o certificado for inválido, você não pode carregá-lo. Você deve selecionar um certificado válido antes de continuar.

Etapa 8 Selecione **Continuar**.

O seu sistema importa o seu certificado SSL e o exibe em uma caixa de diálogo de rolagem o arquivo certificado. Você será notificado de que você importou um certificado SSL.

Etapa 9 Selecione **Concluído**.

Etapa 10 Retorne ao passo 4 e repita o processo para o próximo servidor CUCM.

Etapa 11 Selecione **Desativar modo de manutenção > Continuar**.

O sistema reinicia após desligar o modo de manutenção. Você pode iniciar sessão novamente no site de Administração, após a reinicialização.

Configurando a Segurança da Sessão de Usuário

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Segurança > Sessões de Usuário**.

Etapa 3 Complete os campos na página **Sessões de Usuário** para definir o tempo de expiração da página da internet.

Opção	Descrição
Vencimento da página da web	Configure os dias, horas e minutos antes que os usuários fiquem automaticamente desconectados. Padrão: Uma hora e 30 minutos.
Expiração das Ferramentas de Produtividade ou Móveis (SSO)	Configure os dias, horas e minutos antes que os usuários fiquem automaticamente desconectados. Padrão: 14 dias Observação Este campo apenas aparece se o SSO é configurado.
Sessões de usuários simultâneos	Configure o número de sessões de usuário (do mesmo tipo) que um usuário pode começar a qualquer momento ou selecione Ilimitado .
Sessões simultâneas de administrador	Configure o número máximo de sessões de administrador que um usuário pode abrir a qualquer momento ou selecione Ilimitado .

Opção	Descrição
Exibir informações importantes de registro	Selecione esta opção para exibir o endereço de IP a partir do qual o usuário iniciou sessão e o número de tentativas que falharam para iniciar sessão. Padrão: selecionado.

Etapa 4 Selecione Salvar.

Configurando as Definições de Registro Único Federado (SSO)

O sistema CWMS suporta sistemas de registro único (SSO) com base no protocolo Security Assertion Markup Language (SAML) 2.0 padrão da indústria.

O SSO permite que os clientes usem seus sistemas SSO no local para simplificar o gerenciamento do sistema CWMS. Com o SSO, os usuários efetuam logon de modo seguro no sistema usando suas credenciais de logon corporativo. Você também pode configurar o SSO para criar ou gerenciar contas de usuários em tempo real, quando os usuários tentam iniciar a sessão. As credenciais de logon dos usuários não são enviadas para Cisco, protegendo as informações de logon corporativas.

**Observação**

Permitindo que o SSO substitua as configurações de logon de usuários. Certifique-se de informar os usuários antes de habilitar o SSO.

Configurar o SSO pode ser uma operação complexa e nós recomendamos que você entre em contato com o seu Parceiro de Canal Cisco ou Serviços Avançados Cisco antes de continuar.

Antes de iniciar

- Gere um conjunto de chaves públicas e privadas e um certificado X.509 que contenha a chave pública, e carregue-os como descrito em [Gerenciando Certificados](#), na página 214.

**Observação**

Após você ter habilitado o SSO, as credenciais de usuário são gerenciadas pelo seu sistema de autenticação corporativo. Recursos de gerenciamento de determinada senha não mais se aplica aos seus usuários. Consulte [Configurando Senhas](#), na página 185 e [Editando Usuários](#), na página 122 para obter mais informações. Embora os administradores também são usuários finais, os administradores não iniciam sessão usando o SSO; os administradores iniciam sessão usando suas credenciais de administrador para este produto.

- Configure um certificado SSO IdP para o usuário deste recurso. Consulte [Importando os Certificados IdP de SSO](#), na página 222 para obter mais informações.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Selecione **Configurações > Segurança > Certificados > SSO federado**.

Etapa 3 Após você ter gerado chaves públicas e privadas e um certificado X.509, como descrito nos pré-requisitos, selecione **Continuar**.

Etapa 4 Selecione o seu método de iniciação:

- SP (Provedor de Serviço) Iniciado, os usuários selecionam um link para o provedor de serviço e são temporariamente redirecionados para o provedor de identidade para autenticação. Os usuários são retornados ao link, que inicialmente solicitaram.
- IdP (Provedor de Identidade) Iniciado, os usuários iniciam em seu provedor de identidade, registra-se e depois é redirecionado para uma página de destino no provedor de serviços.

Etapa 5 Complete os campos e selecione as suas opções na página **Configuração SSO**:

Observação Consulte o arquivo de configuração do seu IdP para completar os campos de IdP. Selecione o link **Certificado IdP**.

Campo	Descrição
SP (Provedor Serviço) Iniciado	Selecione esta opção para o início de sessão iniciado do provedor de serviço.
AuthnRequest assinado	Selecione esta opção para exigir que a mensagem AuthnRequest deve ser assinada pela chave privada do provedor de serviço. Observação Você deve selecionar esta opção se desejar que o arquivo de metadados SAML exportado inclua o certificado SSL do seu site.
Destino	A URL da implantação SAML 2.0 do IdP que recebe solicitações de autenticação para o processamento. Observação Este campo aparece apenas quando AuthnRequest assinado é selecionada.
IdP (Identidade Provedor) Iniciado	Selecione esta opção para identificar o início de sessão iniciado do provedor.
Nome do parâmetro de URL da página de destino:	Seu sistema redireciona para esta URL quando o SSO estiver com sucesso. Padrão: TARGET Observação Em um sistema de IdP iniciado, a URL deve ser uma URL combinada no seguinte formato: sua URL de logon de serviço, "?" ou "&", o parâmetro da URL da página de destino, "=" (se não estiver presente), e a URL de destino.

Campo	Descrição
Emissor de SAML (ID SP)	Insira a mesma ID SP configurada para o IdP. Referencie o protocolo SAML2.
Emissora para SAML (IdP ID)	Insira o mesmo ID configurado para o IdP. Referencie o protocolo SAML2.
URL de logon de serviço SSO do Cliente	A URL de consumo de afirmação para o SAML2 no IdP.
Formato IDNome	<p>Selecione o mesmo formato IDNome que você definiu no IdP. O IDNome é o formato em que você envia a ID do usuário na afirmação e o pedido de logoff único do Cisco WebEx. Consulte o protocolo SAML para orientação.</p> <p>Recomendamos que você defina o endereço de e-mail como o seu NameID. Isso fará com que o processo de utilizar o SSO facilite para os usuários finais que já criaram suas contas com base no seu endereço de e-mail no sistema.</p> <p>Utilizar outros formatos de NameID é suportado, mas não é recomendado. Se você utilizar um formato que não seja o endereço e-mail, os usuários já não mais poderão iniciar a sessão num site WebEx se o SSO estiver desabilitado.</p> <p>Padrão: Não especificado</p>
AuthnContextClassRef	<p>Insira o valor que está configurado no IdP. AuthnContextClassRef é o valor que aparece na mensagem de AuthnRequest.</p> <p>Padrão: urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</p>
Padrão URL WebEx da Página de Destino	Seu sistema redireciona para esta URL quando o SSO estiver com sucesso. A página padrão é a página de reunião Cisco WebEx que é a mesma que um logon normal.
URL de erro SSO do Cliente	Seu sistema redireciona para esta URL quando o SSO não estiver com sucesso. Por padrão, a página de erro é uma página de erro comum do Cisco WebEx.
Logoff único	<p>Esta opção permite o logoff único que é definido pelo protocolo de SAML2. Se você escolheu a opção SSO, mas NÃO selecionou a opção logoff único, a opção desconectar não aparecerá nas páginas do usuário final.</p> <p>Desmarque esta opção para o ADFS 2.0.</p> <p>Observação O SLO de Idp iniciado não é suportado nesta versão.</p>

Campo	Descrição
URL de logoff de serviço SSO do Cliente Observação Esta opção aparece apenas quando logoff único é selecionado.	Insira a URL de consumo de afirmação para o SAML2 no IdP.
Criação automática de conta	Os usuários sem uma conta Cisco WebEx não conseguem iniciar sessão. Se você selecionar esta opção, uma conta é criada automaticamente para novos usuários quando eles tentam iniciar sessão.
Atualização automática da conta	Se você selecionar esta opção, as informações de usuário é atualizada quando há um "updateTimeStamp" na afirmação SAML2 com mais informações recentes do usuário do que os dados atuais no Cisco WebEx.
Remova o Sufixo de Domínio UID para o Active Directory UPN	Selecione esta opção para autenticar os usuários sem um sufixo de domínio. A opção Remova o Sufixo de Domínio UID para o Active Directory UPN funciona nos seguintes casos: <ul style="list-style-type: none"> O formato NomeID é e-mail, e o formato UID é o nome do assunto X509 ou o Nome do Principal Usuário (UPN). O formato NomeId é o nome do assunto X509 ou UPN.

Etapa 6

Selecione **Ativar SSO**.

A página **Revisão de Configurações do SSO** aparece. Revise as suas configurações e selecione **Salvar**.

Desativando o SSO

Antes de iniciar

Desativando o SSO irá desativar a capacidade dos seus usuários de iniciarem sessão com suas credenciais da empresa. Certifique-se de informar seus usuários que você está desativando o SSO e que eles ainda podem iniciar sessão com suas credenciais Cisco WebEx.

Etapa 1

Inicie sessão no site da Administração.

Etapa 2

Selecione **Configurações > Segurança > SSO Federado**.

Etapa 3

Encontre a frase, "Se você quiser desativar SSO, por favor clique aqui." Selecione o link **Clique aqui**.

Etapa 4

Selecione **Desabilitar SSO** para confirmar.

A página **União SSO** aparece com uma bandeira que confirma que você desativou o SSO.

Configurar seus recursos de nuvem

Você pode configurar o sistema para que os usuários possam usar uma única versão das ferramentas de produtividade Cisco WebEx que pode ser usada nas suas contas Cisco WebEx Meetings Server e SaaS WebEx ou para visualizar vídeos de treinamento on-line organizados pela Cisco WebEx.



Observação

O sistema suporta as versões Cisco WebEx SaaS WBS27 e superior e Cisco WebEx Meetings 1.2.

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Selecione **Configurações > Segurança > Recursos Cloud**.
- Etapa 3** (Opcional) Selecione **Permitir que usuários iniciem sessão nas contas SaaS WebEx a partir das Ferramentas de Produtividade WebEx**.
- Etapa 4** Selecione **Salvar**.
-

Configurando a Segurança da Máquina Virtual

Seus recursos de segurança de máquinas virtuais incluem a capacidade de atualizar suas chaves de criptografia e ativar ou desativar a criptografia compatível com os FIPS.

Atualizar as suas chaves de criptografia

O Cisco WebEx Meetings Server utiliza chaves de criptografia geradas internamente, para assegurar todas as comunicações entre as máquinas virtuais no seu sistema. Utilize este recurso para atualizar periodicamente as chaves de criptografia.

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Configurações > Segurança > Máquinas Virtuais**.

Etapa 4 Selecione **Atualizar Chaves de Criptografia**.

Etapa 5 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Sobre o FIPS

O Federal Information Processing Standard (FIPS) 140 é uma norma do governo dos EUA e Canadá que especifica requisitos de segurança para módulos criptográficos. Um módulo criptográfico é um "conjunto de hardware, software e/ou firmware que implementa funções de segurança aprovadas (incluindo algoritmos criptográficos e geração de chaves) e está contido dentro do limite de criptografia". O módulo criptográfico é o que está sendo validado.

Requerimentos FIPS 140

A um nível muito elevado, os requisitos do FIPS 140 se aplicam às seguintes características do módulo:

- Implantação de algoritmos aprovados pelo FIPS
- Gestão específica do ciclo de vida fundamental
- Geração aprovada de números aleatórios
- Testes automáticos de algoritmos de criptografia, integridade da imagem e geradores de números aleatórios (GNAs)

O Cisco WebEx Meetings Server usa o CiscoSSL 2.0 para atingir o cumprimento do Nível 2 do FIPS 140-2.

Com o FIPS Ativado

Ativar o FIPS pode resultar em compatibilidade reduzida com os navegadores da web populares e com os sistemas operacionais. Os sintomas podem incluir, mas não estão limitados a, problemas para iniciar sessão no sistema, erros 404 e iniciar e participar de reuniões.

A Cisco recomenda que você tome as seguintes ações:

- Certifique-se que os seus computadores Windows estão em execução, pelo menos o Windows XP SP3 ou acima.

- Atualize todos os computadores Windows para o Microsoft Internet Explorer 8 ou superior, independentemente se o navegador que o seu usuário deseja é o Internet Explorer, o Mozilla Firefox ou o Google Chrome. Seus usuários devem fornecer o Internet Explorer 8 em todos os computadores porque os nossos clientes habilitados do FIPS (Cisco WebEx Meetings, Ferramentas de Produtividade e reproduutor de gravações WebEx) usam bibliotecas de sistemas habilitados do FIPS que só estão disponíveis no Internet Explorer 8 e acima.
- Configure **Configurações da Internet** em todos os computadores de usuários para criptografia TLS. Na área de trabalho do computador, selecione **Painel de Controle > Opções da Internet > Avançado > Segurança > Usar TLS 1.0 e Usar TLS 1.2**. É recomendável selecionar as duas opções para o máximo de compatibilidade, mas você deve selecionar pelo menos **Usar TLS 1.0**.
- Se os seus usuários planejam organizar reuniões para os convidados (por exemplo, pessoas que não trabalham para a sua empresa), você deve informar seus usuários convidados para atualizar manualmente seus sistemas operacionais e navegadores, como descrito acima, antes de participar das suas reuniões. Se eles não executarem os passos acima, podem enfrentar problemas de compatibilidade. É recomendável que você inclua as instruções acima em seus convites para reuniões. Você pode fazer isso editando os convites adequados para reuniões, disponíveis no site de Administração em **Configurações > E-mail > Modelos**.

Habilitar a Criptografia Compatível ao FIPS

Utilize este recurso para permitir que o Processamento Padrão de Informações Federais (FIPS) configure a criptografia compatível.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7](#).)

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3

Selecione **Configurações > Segurança > Máquinas Virtuais**.

Etapa 4

Selecione **Habilitar** para permitir a criptografia compatível do FIPS e **Continuar** para confirmar.

A criptografia compatível do FIPS é configurada no seu sistema.

Etapa 5

Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).

Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Desativar a Criptografia Compatível ao FIPS

Utilize este recurso para desabilitar a criptografia compatível do Processamento Padrão de Informações Federais (FIPS) no seu sistema.

Etapa 1 Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2 Ative o Modo de Manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Recomendamos que você tire uma foto instantânea de cada máquina virtual. Consulte [Tirando uma Foto Instantânea utilizando o VMware vCenter, na página 7.](#))

Ativar o modo de manutenção em todos os centros de dados ativos desativa a atividade de conferência e impede que os usuários iniciem sessão no site WebEx, agendem reuniões, participem de reuniões ou reproduzam gravações de reuniões. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC) e outro centro de dados está ativo, as reuniões em andamento irão falhar para o centro de dados ativo. Isso pode causar uma breve interrupção em reuniões ativas. Consulte [Sobre o Modo de Manutenção](#) para obter informações sobre quais tarefas do sistema necessitam que o modo de manutenção seja ligado.

Etapa 3 Selecione **Configurações > Segurança > Máquinas Virtuais**.

Etapa 4 Selecione **Desabilitar** para desativar a criptografia compatível do FIPS e **Continuar** para confirmar. A criptografia compatível do FIPS está desabilitada no seu sistema.

Etapa 5 Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#). Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.

O serviço de reuniões para usuários neste centro de dados é restaurado.

Carregando a mensagem de aviso de segurança de início de sessão

Para sites seguros que exigem que os usuários leiam uma mensagem de segurança e aceitem um acordo antes de iniciarem sessão no site, carregue um arquivo que contenha um texto de advertência.

Para remover a mensagem de aviso de início de sessão, vá para [Configurando um aviso de segurança ao iniciar sessão, na página 235](#).

Antes de iniciar

Crie um arquivo de texto (.txt) com o aviso a ser exibido antes de um usuário iniciar sessão em um site comum WebEx ou em um site de administração. O arquivo de texto deve usar caracteres e codificação UTF-8.

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Selecione **Configurações > Segurança > Aviso para Iniciar sessão**.
- Etapa 3** Selecione **Procurar** e o arquivo de texto a ser carregado.
- Etapa 4** Selecione **Carregar**.
O arquivo é carregado e imediatamente aparece em todas as páginas de início de sessão.
-

Configurando o registro de auditoria do aplicativo

Se for requerido que seu site armazene informações de auditoria sobre as mudanças do sistema, configure as definições de Registro de Auditoria do Aplicativo.

Se um usuário é configurado como um Auditor, a opção **Registro de auditoria do aplicativo** fica visível e configurável apenas pelo Auditor. Se o sistema não possui um usuário com a função de Auditor, a opção **Registro de auditoria do aplicativo** fica visível e configurável por um Administrador, Administrador SSO ou Administrador LDAP.

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Selecione **Configurações > Segurança > Registro de auditoria do aplicativo**.
- Etapa 3** Selecione **Habilitar registro de auditoria** para gerar um registro.
- Etapa 4** Para registrar as informações de auditoria do aplicativo em um servidor syslog remoto, insira os parâmetros no **Servidor syslog remoto primário**.
Os eventos no menu Nível do Evento de Auditoria Syslog Remoto são organizados em ordem de importância.
- Insira o **Endereço IPv4** e o **Número da porta** se você quiser que o sistema registre as informações de auditoria do aplicativo em um servidor syslog remoto.
 - Selezione o protocolo.
 - Selezione o **Nível do Evento de Auditoria Syslog Remoto**.
Quando você selecionar um nível de evento, os níveis anteriores também serão selecionados. Por exemplo, se você selecionar o nível de evento **Erro**, o sistema recupera os eventos de Erro, Crítico, Alerta e de Emergência.
- O nível afeta apenas os registros do sistema operacional e a gravidade de tais mensagens.
- O nível do evento de emergência é o padrão. Na visão do Auditor, o alarme para a partição de registro também é exibido.

- Etapa 5** (Opcional) Para registrar as informações de auditoria do aplicativo em um servidor syslog remoto secundário, insira os parâmetros para o Servidor syslog remoto secundário.
- Etapa 6** (Opcional) Para excluir os arquivos de registros antigos, selecione a data para purgar os arquivos de registros anteriores em **Configurações de purga de registros** e selecione **Purgar arquivo de registro**.
- Etapa 7** Configure a **Porcentagem mínima de espaço livre na partição de registro** movendo a barra deslizante. O parâmetro para o serviço de registro garante que o percentual de espaço livre selecionado na partição de registro esteja disponível. O padrão é 20 por cento.
- Quando um Auditor acessa esta janela a partir da guia Auditor, a configuração para o Alarme da partição de registro é exibida.
- Etapa 8** Consulte **Manter os arquivos de registro por não mais do que o número de dias selecionado**. O padrão é 40 dias.
- Etapa 9** Selecione **Salvar**.
-

Próximos passos

Consulte [Visualizando e Editando Alarmes, na página 94](#) para obter detalhes sobre a configuração dos limites do alarme.

Configurando um aviso de segurança ao iniciar sessão

O Aviso de Segurança ao Iniciar Sessão exibe a mensagem de aviso nas páginas para iniciar sessão do site WebEx comum, site WebEx de Administração e CLI.

-
- Etapa 1** Inicie sessão no site da Administração. Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Selecione **Configurações > Segurança > Aviso para Iniciar sessão**.
- Etapa 3** Navegue na mensagem e selecione **Carregar** ou selecione **Remover mensagem**. A mensagem é adicionada ao sistema e será exibida nas páginas de início de sessão ou o arquivo é removido do sistema e não aparecerá nas páginas de início de sessão.
-



CAPÍTULO 16

Gerenciando relatórios

Você pode visualizar os relatórios mensais e personalizar os relatórios para intervalos de data específicos. Seus relatórios usam o idioma, a localidade e as definições de fuso horário configuradas na página **Informações sobre a empresa**. Consulte [Configurando as informações da empresa](#), na página 161 para obter mais informações.



Importante

Quando o sistema está implantado ou atualizado, não há dados disponíveis para os relatórios, exceto o Relatório de Detalhes Personalizados, até o final do primeiro mês. Nesse caso, os links de **Downloads** e todos os outros relatórios descritos nesta seção não estarão disponíveis até depois do final do primeiro mês.

- [Baixar os relatórios mensais](#), página 237
- [Sobre os relatórios mensais](#), página 238
- [Gerando Relatórios de Detalhes Personalizados](#), página 240
- [Sobre Relatórios de Detalhes Personalizados](#), página 240

Baixar os relatórios mensais

Você pode visualizar e baixar relatórios mensalmente em formato PDF.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione **Relatórios**.

Etapa 3

Selecione o link **Baixar** para o relatório mensal que você deseja visualizar.

Sobre os relatórios mensais

Seu relatório de resumo mensal contém as seguintes seções:

Relatório Resumido do Sistema

Seu relatório de resumo do sistema contém os seguintes relatórios:

- Conclusão do serviço — Este relatório exibe um gráfico que mostra o número de organizadores e participantes exclusivos sobre os três meses anteriores e a taxa de crescimento previsto para os próximos três meses.
- Licenças do usuário — Este relatório exibe a porcentagem de licenças adquiridas que você está usando e um gráfico que mostra o número de licenças usadas ao longo dos últimos três meses e a taxa de crescimento esperada para os próximos três meses. Você pode usar esses números para prever o uso da licença futura e ajustar suas compras de licenças. Consulte [Solicitando Licenças utilizando o Gerenciador de Licenças](#) para obter mais informações.
- Tamanho do sistema — Este relatório exibe o pico de participantes da reunião e a porcentagem do tamanho do sistema que o uso máximo consome. O gráfico mostra o pico de participantes da reunião ao longo dos últimos três meses e a taxa de crescimento prevista para os próximos três meses.
- Armazenamento — Este relatório mostra o uso do armazenamento do seu arquivo de dados e as gravações, tanto como uma porcentagem do espaço total de armazenamento e em total de gigabytes (GB). O gráfico mostra o total de armazenamento ao longo dos últimos três meses e a taxa de crescimento esperada para os próximos três meses. Utilize este relatório para monitorar o uso do armazenamento. Se você precisar adicionar espaço de armazenamento adicional você deve copiar manualmente o seu arquivo de dados de armazenamento existente e as gravações para o seu novo servidor de armazenamento antes de ativá-lo.



Observação

Este relatório só aparece se você tiver configurado um servidor de armazenamento. Consulte [Configurando um Servidor de Armazenamento](#), na página 146 para obter mais informações.

- Rede — Este relatório exibe o seguinte:

- O pico do consumo de largura de banda da rede em Mbps.
- Um gráfico que descreve o pico de consumo de banda de rede em Mbps nos últimos três meses e a taxa de crescimento prevista para os próximos três meses (a barra vermelha indica a banda máxima da rede).
- Um gráfico circular indicando a porcentagem da banda consumida por cada um dos recursos do sistema.

Os relatórios extraem seus dados a partir da base de dados. O módulo de monitoramento escreve 0 para o banco de dados se o consumo de largura de banda é inferior a 1 Mbps. Portanto, um 0 no relatório significa que o recurso não está usando a largura de banda de rede significativa.

- O tempo de inatividade planejado do sistema e interrupção não planejada — Este relatório apresenta o seguinte:
 - O tempo de atividade média do sistema dos últimos três meses.

- O tempo médio de interrupções do sistema não planejadas ao longo dos últimos três meses.
- O número médio de reuniões interrompidas devido a falhas nos últimos três meses.
- Um gráfico que descreve o tempo de inatividade planejado e as interrupções não planejadas ao longo dos últimos três meses e a taxa de crescimento prevista para os próximos três meses.



Observação

O tempo de inatividade aumentado é às vezes um reflexo do aumento do uso. Certifique-se de comparar as estatísticas de tempo de inatividade com as estatísticas de uso exibidas em outros relatórios.

Relatório de Resumo de Reunião

O relatório de resumo da reunião contém os seguintes relatórios:

- Estado da reunião — Este relatório exibe um gráfico que mostra o estado da reunião no mês anterior o percentual de reuniões que tiveram problemas e o número total de reuniões realizadas durante o mês. Para o estado de reunião em tempo real, visualize o Painel. Consulte [Sobre o Seu Painel](#) para obter mais informações. Para mais informações sobre o estado da reunião, consulte [Visualizando a Lista de Reuniões, na página 98](#).
- Tamanho da reunião — Este relatório exibe um gráfico que mostra os tamanhos das reuniões realizadas em seu sistema ao longo do mês anterior, a repartição dos tamanhos de reuniões e informações detalhadas sobre a maior reunião realizada durante o mês.
- Uso de recurso da reunião — Este relatório apresenta o seguinte:
 - O recurso mais utilizado ao longo do mês anterior, incluindo o número total de minutos que o recurso foi usado.
 - O recurso que mais cresceu em seu sistema durante o mês anterior, incluindo a taxa de crescimento.
 - Um gráfico que descreve o uso em minutos para cada recurso em seu sistema.
 - Um gráfico que descreve a taxa de crescimento do recurso de crescimento mais rápido no sistema.
- Principais domínios de e-mail de participantes ativos — Este relatório apresenta o seguinte:
 - Um gráfico que descreve os principais domínios de e-mail de participantes ativos.
 - A repartição dos domínios de e-mail dos participantes.
 - Uma lista dos três principais domínios de e-mail utilizados por participantes da reunião no sistema.
- Dia e hora de pico — Este relatório apresenta dois gráficos. O primeiro gráfico mostra o dia mais movimentado da semana durante o mês anterior. O segundo gráfico mostra o período mais movimentado do dia em seu sistema durante o mês anterior.

Gerando Relatórios de Detalhes Personalizados

-
- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Selecione **Relatórios > Personalizar seu relatório**.
- Etapa 3** Selecione o intervalo de data dos relatórios que você deseja visualizar e selecione **Enviar**.
O padrão é o mês mais recente. Você pode selecionar um intervalo de data que se estende até seis meses atrás.
A página **Solicitação de relatório submetido personalizado** aparece exibindo as datas de seu relatório personalizado. Um e-mail é enviado para você com um link para o seu relatório personalizado no formato CSV.
- Etapa 4** Selecione **Concluído**.
-

Sobre Relatórios de Detalhes Personalizados

Quando você gera relatórios de detalhes personalizados, você recebe um e-mail contendo um arquivo com os seguintes relatórios em formato CSV:

- **Relatório de tentativas de fraude** — exibe qualquer tentativa sem sucesso de acesso telefônico onde o chamador inseriu os códigos de acesso do organizador ou do participante errados ou a senha do organizador por três vezes enquanto tenta iniciar ou entrar em uma reunião de Conferência Pessoal:
 - Número de acesso chamado — O número da chamada de entrada Cisco WebEx discado para iniciar ou entrar em uma reunião de Conferência Pessoal.
 - Número da chamada — O número do telefone usado para fazer a chamada.
 - Hora de início da chamada — A data e a hora da chamada.
 - Primeiro código de acesso tentado — O primeiro código de acesso inválido inserido pelo chamador.
 - E-mail do proprietário do primeiro código de acesso (se disponível) — O endereço de e-mail do usuário associado ao primeiro código de acesso inválido, se o código de acesso for associado a uma conta do Cisco WebEx Meetings Server válida.
 - Segundo código de acesso tentado — O segundo código de acesso inválido inserido pelo chamador.
 - E-mail do proprietário do segundo código de acesso (se disponível) — O endereço de e-mail do usuário associado ao segundo código de acesso inválido, se o código de acesso for associado a uma conta do Cisco WebEx Meetings Server válida.
 - Terceiro código de acesso tentado — O terceiro código de acesso inválido inserido pelo chamador.
 - E-mail do proprietário do terceiro código de acesso (se disponível) — O endereço de e-mail do usuário associado ao terceiro código de acesso inválido, se o código de acesso for associado a uma conta do Cisco WebEx Meetings Server válida.

- **Relatório de reunião** — Contém informações sobre todas as reuniões que ocorreram durante o período especificado:

- ID da reunião — ID da conferência exclusiva gerado pelo seu sistema quando a reunião foi agendada.
- Número da reunião — Número da reunião Cisco WebEx.
- Assunto — Nome da reunião configurado pelo organizador.
- Nome do organizador — Nome do organizador da reunião.
- Hora de início — Hora de início e data da reunião.
- Duração — Duração da reunião em minutos.
- Número de participantes — Número de participantes incluindo os organizadores.



Observação

Se um convidado ou organizador participa de uma reunião duas vezes, o sistema adiciona as participações para o convidado duas vezes, mas uma única participação para o organizador na contagem do participante.

- Status de cada reunião.
- Número de Minutos de Áudio de Chamada de Entrada
- Número de Minutos de Áudio de Retorno de Chamada
- Número dos Minutos da VoIP
- Número de Minutos dos Vídeos
- Número dos Minutos da Gravações
- Intervalo de Gravação — Hora de início e de parada de cada gravação criada durante a reunião.
- Número de minutos WebSharing — O número total de minutos que todos os participantes gastaram na reunião da web (por exemplo, se três participantes entrarem na parte Web de uma reunião que dura 10 minutos, o número de minutos compartilhados na web é de 30).
- Participantes — Uma lista de participantes da reunião.
- Plataforma/navegador do organizador — A versão do sistema operacional e do navegador que o organizador estava utilizando quando o organizador iniciou uma reunião Cisco WebEx.
- Endereço de IP do organizador — O endereço de IP utilizado pelo organizador quando o organizador iniciou uma reunião Cisco WebEx.
- TrackingCodes — Os códigos de controle aplicados pelo organizador ao agendar a reunião.

- **Relatório de utilização da largura de banda de rede** — O consumo de largura de banda de rede para cada dia no período especificado para cada uma das seguintes características:

- Máximo Consumo da Banda Larga para Áudio (mbps)
- Máximo consumo da largura de banda para áudio VoIP (mbps)
- Máximo Consumo da Banda Larga para Vídeo (mbps)
- Máximo Consumo da Banda Larga para Compartilhamento da Web (mbps)

Um consumo de 0 (zero) indica que o recurso não foi utilizado nessa data. Um consumo de menos de 1 é exibido se menos de 1 Mbps foi consumido na data especificada.

O consumo de largura de banda de rede para o vídeo inclui vídeo de compartilhamento de arquivos de vídeo e câmeras a partir de reuniões da web. Se o vídeo está desativado para o seu site, você não pode ligar uma câmera para o vídeo, mas você ainda pode compartilhar arquivos de vídeo. Isto resulta em algum consumo de largura de banda de rede para o vídeo, que é incluído nos relatórios. Esta é a única situação que causa o consumo de largura de banda de rede para o vídeo quando o vídeo é desativado de um site.

- Relatório de utilização de capacidade de armazenamento — Exibe o espaço total em disco utilizado a partir da data listada e o número de reuniões gravadas que ocorreram para cada data.



Observação

Este relatório só é incluído se você tiver configurado um servidor de armazenamento. Consulte [Configurando um Servidor de Armazenamento](#), na página 146 para obter mais informações.

- **Relatório dos participantes** — O histórico das reuniões, a hora que cada reunião iniciou e o código de rastreamento aplicado em cada reunião.

- ID da reunião — O ID da conferência exclusiva gerado pelo seu sistema quando a reunião foi agendada.
- Nome da Conferência — Nome da reunião que o organizador inseriu no campo **Qual** durante o agendamento de uma reunião.
- Nome de Usuário — Nome de usuário do organizador.
- Hora de Participação — Hora e data quando um usuário participou de uma reunião Cisco WebEx.
- Hora de Saída — Hora e data quando um usuário saiu de uma reunião Cisco WebEx.
- Duração — Período de tempo, em minutos, que um usuário participou de uma reunião Cisco WebEx.
- Plataforma/Navegador — A versão do sistema operacional e do navegador utilizada por um organizador quando o organizador iniciou uma reunião Cisco WebEx.
- Endereço de IP do Cliente — Endereço de IP do cliente WebEx utilizado por um organizador ou participante para iniciar ou participar de uma reunião Cisco WebEx.
- Hora de Início da Sessão — Hora que a sessão iniciou.
- Hora de Término da Sessão — Hora que a sessão terminou.
- Tipo de Sessão — O tipo de sessão pode ser por vídeo (compartilhamento web), VoIP (conexão telefônica), chamada de entrada ou retorno de chamada.
- Duração da Sessão - Tempo que a sessão durou.
- Número de Telefone - Número de telefone do telefone utilizado para fazer a chamada de entrada para a reunião WebEx.
- Servidor do tel. — Servidor do telefone.

- **Relatório do tempo de inatividade do sistema** — Informações do tempo de inatividade do sistema durante o período especificado e inclui os seguintes campos:

- Categoria — Fora de serviço ou manutenção. Fora de serviço indica uma queda de energia. A manutenção indica uma janela de manutenção planejada.
 - Serviço — Os recursos afetados.
 - Início do tempo de inatividade — A data e a hora que o tempo de inatividade iniciou.
 - Fim do tempo de inatividade — A data e a hora que o tempo de inatividade terminou.
 - Número de reuniões interrompidas — O número das reuniões interrompidas. Este campo está em branco para paradas de Manutenção, porque são planejadas. Se nenhuma reunião foi agendada durante um tempo de inatividade de Fora de Serviço (Out Of Service), o número é 0.
- **Relatório de utilização de licença do usuário** — Existem duas versões deste relatório. Uma versão exibe o uso de licenças dos últimos 30 dias e é intitulado UserLicenseUtilizationReportForLastMonth.csv e a outra versão exibe o uso de licenças do mês atual (o primeiro dia do mês até o dia atual) e é intitulado UserLicenseUtilizationForThisMonth.csv. Cada um desses relatórios inclui os seguintes campos:
 - Nome do usuário — O nome de usuário do organizador da reunião.
 - Endereço de e-mail — Endereço de e-mail do organizador da reunião.
 - ID da reunião — O ID da conferência exclusiva gerado pelo seu sistema quando a reunião foi agendada.
 - Número da reunião — Número da reunião Cisco WebEx.
 - Hora de início — A data e a hora do início da reunião.
 - Reunião simultânea — Número de reuniões simultâneas agendadas pelo mesmo usuário. Cada reunião simultânea registrada resulta em uma linha adicional adicionada a este relatório para o usuário que agendou a reunião simultânea.



CAPÍTULO 17

Gerenciando licenças

- Gerenciando licenças, página 245
- Reorganizando licenças do organizador, página 252

Gerenciando licenças

Um sistema suportado por um único centro de dados não requer uma licença do sistema. Quando você inicialmente implantar este produto, você terá um período de teste de 180 dias, que permite um número ilimitado de licenças de Organizador. Após o período de teste gratuito expirar, você é obrigado a comprar licenças de Organizador Permanente assim como todos os usuários que organizam reuniões. As licenças não são necessárias para os usuários que agendam ou participam de reuniões, mas para os que organizam reuniões.

Se você implantar um sistema suportado por vários centros de dados, você deve adquirir licenças de recursos de Vários centros de dados (MDC). Não há período de carência ou período de teste para as licenças MDC. As licenças MDC devem ser organizadas no centro de dados primário antes de tentar registrar nos centros de dados em um sistema MDC. Para implantar um sistema MDC, consulte [Registrando centros de dados para criar um sistema de vários centros de dados \(MDC\)](#), na página 255.

Sobre licenças MDC

Não há período de teste para um novo MDC (Vários centros de dados). As licenças de recursos do MDC são compradas para o tamanho do sistema antes dos centros de dados serem unidos. As licenças MDC estão hospedadas no centro de dados primário; o centro de dados que um outro centro de dados está unido para formar um sistema, normalmente o centro de dados que está executando o gerenciador de licenças. Se você atualizar ou expandir um sistema MDC existente, você deve adquirir as licenças da versão e tamanho corretos em 90 dias ou menos.

- Licenças MDC permanentes — Compradas para permitir que os centros de dados sejam unidos em um único sistema MDC.
- Licenças de carência MDC — Limitadas a 90 dias, você pode atualizar ou expandir os centros de dados em um sistema MDC antes de comprar as licenças necessárias. Após esta modificação do sistema, você tem 90 dias para resolver quaisquer problemas com as licenças, tais como a aquisição de licenças MDC para um sistema maior. Se as licenças do tamanho e da versão apropriados não forem instaladas antes do período de carência MDC expirar, o centro de dados que não está hospedando o Gerenciador de Licença será desativado.

- Licenças MDC de demonstração — Suporte de licença temporária para um sistema MDC. A emissão de licenças MDC de demonstração é determinada pelo fornecedor em uma base de caso a caso e a duração de validade das licenças é determinada quando as licenças são emitidas.

Para implantar um sistema MDC, consulte [Registrando centros de dados para criar um sistema de vários centros de dados \(MDC\), na página 255](#).

Sobre as licenças do organizador

Este produto tem **Licenciamento baseado em organizador** que requer que você compre uma licença para cada usuário que **organiza** reuniões ou é atribuído manualmente uma licença. Um usuário não consome uma licença de Organizador participando ou agendando uma reunião em nome de terceiros. O cálculo do uso da licença para fins de relatório ocorre uma vez por mês, por exemplo, uma vez a partir de 1º a 31 de janeiro, e uma vez a partir de 1º a 28 de fevereiro, etc.



Observação

Ao atualizar de uma versão anterior para a versão 2.5 ou superior, todas as licenças que estavam no sistema original são lançadas a partir da sua designação para os usuários. Os usuários podem readquirir licenças organizando reuniões ou atribuindo licenças manualmente. Isto também é verdade ao instalar um sistema de Vários centros de dados (MDC). As licenças do organizador são perdidas no centro de dados que está no sistema MDC. Essas licenças podem ser reorganizadas no sistema MDC após o Registro.

Na página **Relatórios**, você pode pedir um relatório que fornece o número total de licenças consumidas. Além disso, recomendamos que você veja o Relatório de Resumo em PDF que mostra as tendências de consumo de licença. Ao ver a tendência geral da licença, você pode planejar futuras aquisições de licenças de forma mais eficaz, para coincidir com a crescente adoção desse sistema na sua empresa.

Tipos de licenças de organizador

Uma licença de Organizador é necessária para organizar uma reunião. Uma licença não é necessária para agendar ou participar de uma reunião. Os tipos de licenças de organizador são:

- **Licença de Organizador Permanente** — Uma licença de Organizador instalada é comprada para permitir que um usuário organize reuniões que são atribuídas a esse usuário na primeira vez que ele organiza uma reunião. Uma licença de Organizador pode ser atribuída manualmente a um usuário por um administrador; um usuário não precisa esperar para organizar uma reunião para ser atribuída uma licença. Se houver um usuário com uma licença de Carência e uma licença de Organizador Permanente tornar-se disponível, pela remoção de um organizador ou pela compra de licenças adicionais de Organizadores permanentes, a licença permanente será atribuída ao organizador com uma licença de Carência.

Na versão 2.5, um usuário nunca usa mais de uma licença de Organizador Permanente e pode organizar um máximo de duas reuniões ao mesmo tempo. Além disso, uma licença de Organizador Permanente é lançada para uso por outro organizador somente quando o usuário dessa licença é desativado (em oposição à versão 2.0, onde as licenças dos organizadores que não organizam reuniões por um período de tempo são lançadas). Se alguém tenta organizar uma reunião e:

- Não há licenças disponíveis.
- A licença do organizador expirou desde que a reunião foi agendada ou o organizador da reunião foi desativado.

Uma mensagem de erro é exibida e a reunião não pode ser iniciada. Consulte [Excedendo o número de licenças disponíveis, na página 248.](#))

- **Licença de teste do organizador** — A licença de Organizador Temporário atribuída automaticamente em um sistema que está em período de teste.
- **Licença de carência do organizador** — Uma licença temporária usada por um organizador de reuniões em um *ambiente de licença permanente*, onde todas as licenças permanentes foram usadas. Um número limitado de Licenças de Carência de Organizador estará temporariamente disponível para um sistema com Licenças de Organizadores Permanentes (um sistema que não está em um período de teste) se o número de licenças instaladas for ultrapassado brevemente. Avisos sobre as licenças em excesso são exibidos para o administrador. As licenças de carência temporárias de organizador neste cenário são associadas a um usuário por 180 dias. Quando uma licença de Organizador Permanente torna-se disponível, ela é associada com o usuário e a licença de carência é lançada. Se após 180 dias o usuário não tiver adquirido uma licença de Organizador Permanente, ele não poderá mais organizar reuniões. (Consulte [Excedendo o número de licenças disponíveis, na página 248](#) para obter mais informações sobre o comportamento do sistema quando o número de licenças de organizadores permanentes é excedido.)
- **Licença de Demonstração** — Licenças de organizadores temporários, com durações variáveis válidas, fornecidas por um fornecedor em uma base de caso a caso. (Elas são utilizadas principalmente para testes.) Quando essas licenças expirarem, o sistema retornará ao seu estado da licença anterior. A licença de Organizador de Demonstração expira se foi ou não atribuída a um usuário.
- **Licenças de Organizador Local** — Licenças gerenciadas no centro de dados local.
- **Licenças de Organizador Remoto** — Licenças gerenciadas usando o Diretório Ativo.
- **Licenças de Organizador Expirado** — Uma licença de organizador temporário que foi invalidada porque o tempo designado foi excedido. Um usuário com uma licença de Organizador Expirado ainda pode participar de reuniões e agendar reuniões para outros.

Status da licença dos usuários

Esta seção descreve a relação entre o status dos usuários e como as licenças dos organizadores são contadas.

- **Participante** — Uma pessoa que participa de reuniões, mas não organiza reuniões, e não possui controle sobre os recursos do organizador, tais como apresentação de conteúdo, a menos que o participante seja designado por um organizador para ser o apresentador. Nenhuma licença de organizador foi consumida pelos participantes da reunião. Este usuário também pode agendar reuniões em nome de outros, sem consumir uma licença de organizador.
- **Organizador da reunião** — Agenda e participa de reuniões na qualidade do organizador da reunião, e está autorizado a controlar os recursos selecionados, tais como identificar um apresentador ou desativar o som de outro participante. Organizar uma reunião consome uma licença e essa licença é mantida por esse usuário até que o usuário é desativado. A licença de Organizador pode assumir diversas formas. (Consulte [Tipos de licenças de organizador, na página 246](#) para obter mais informações sobre as formas das licenças do Organizador.)
- **Organizador alternativo** - Identificado quando a reunião é agendada como alguém que pode assumir o papel do organizador na ausência do organizador da reunião. Se o organizador da reunião que agendou a reunião não comparecer, o organizador alternativo recebe o controle sobre a maior parte dos mesmos recursos que o organizador da reunião. A licença necessária para organizar a reunião é validada contra o status do usuário que agendou a reunião. Em outras palavras, o usuário que agendou a reunião deve ter uma licença válida no momento da reunião, mesmo se o usuário não participar da reunião.

- Participar antes do organizador (EAO) - Permite que os participantes participem de uma reunião antes da chegada do organizador ou do organizador alternativo.
- Reuniões sobrepostas - Duas ou mais reuniões que foram agendadas durante o mesmo período do dia com o mesmo organizador. A partir da versão 2.5, o usuário pode organizar um máximo de duas reuniões simultâneas, usando apenas uma licença.; nenhum usuário pode organizar mais de duas reuniões ao mesmo tempo.

Excedendo o número de licenças disponíveis

Durante o período de teste gratuito, o número de licenças disponíveis em qualquer tamanho de sistema é ilimitado. Depois de ter comprado e instalado as licenças no sistema, você deve se certificar de que tem licenças o suficiente instaladas para acomodar todos os organizadores no sistema.

Se o número de licenças instaladas for ultrapassado brevemente, uma licença de carência pode ser adquirida por um novo organizador. (Licenças de carência são descritas em detalhe em [Tipos de licenças de organizador, na página 246.](#))

Se o número de organizadores ativos no seu sistema excede regularmente o número de licenças instaladas, um e-mail é enviado ao administrador indicando que o número de licenças instaladas foi excedido e é recomendada a compra de licenças adicionais. Você deve reduzir o uso de licenças ou aumentar o número de licenças no sistema para que ele atenda ou exceda o número de organizadores ativos.

O gerente de auditoria executa uma vez por dia (às 2:00) para ajustar o número de licenças usadas, conforme necessário. Se o número de organizadores caiu abaixo do número de licenças instaladas, a condição das licenças excedidas termina. Se o número de organizadores ativos ainda excede o número de licenças, um e-mail é enviado ao administrador a cada mês, indicando que a condição de licenças excedidas ainda existe.

A partir da versão 2.5, os usuários com licenças podem continuar a usar o sistema, mas os usuários sem licenças não podem organizar reuniões. Se não há licenças disponíveis quando um usuário não licenciado agenda uma reunião, o usuário é notificado de que ele pode não ser capaz de organizar essa reunião, devido à falta de licenças.

Em todas as versões, o site de Administração continua a estar disponível, assim um administrador pode iniciar sessão, adicionar licenças e restabelecer a capacidade dos usuários de sediar reuniões e acessar gravações.

Obtenção de licenças

Durante o período de testes do sistema, use o painel para visualizar o uso, o histórico dos recursos e as tendências das reuniões para determinar quantos usuários estão organizando e participando das reuniões no seu sistema. Depois de ter usado o produto por alguns meses, você pode usar os relatórios de resumo mensais e os relatórios de detalhes personalizados para ajudar a determinar quantas licenças de Organizador Permanente você precisa. Os seus relatórios de resumo mensais exibem as estatísticas sobre a adoção do serviço e o uso de licença do usuário. As estatísticas de adoção de serviços exibem a velocidade com que novos *usuários* estão adotando o sistema, apresentando a taxa de adoção dos três meses anteriores e prevendo a taxa de crescimento ao longo dos próximos três meses. As estatísticas de Licença do Organizador exibem o uso da licença do *organizador* ao longo dos três meses anteriores e o crescimento esperado para os próximos três meses.

Não há período de testes para licenças de Vários centros de dados (MDC); é necessário obter licenças MDC antes de criar um sistema MDC. Você deve comprar um mínimo de duas licenças MDC, um para cada centro de dados no sistema. (Todas as licenças estão instaladas no centro de dados que hospeda o Gerenciador de Licenças.)

Obtenha licenças de Organizador ou MDC:

- Usando e-cumprimento (consulte [Usando Licenças ao utilizar o eFulfilment, na página 250](#)).
- Usando cumprimento baseado em arquivo (consulte [Solicitando Licenças utilizando o Gerenciador de Licenças, na página 249](#)).
- Contatando o TAC para abrir um processo para solicitar licenças (consulte [Solicitando Licenças Contatando o CAT, na página 252](#)).

Consulte a seção [Gerenciando licenças, na página 245](#) do *Guia de administração do Cisco WebEx Meetings Server* para obter mais informações sobre o gerenciamento de suas licenças.

Conexão do gerenciador de licenças

Quando você compra licenças, você usa uma ferramenta de gerenciamento de licenças incorporada para inserir sua PAK e registrar as licenças. O gerenciador de licenças executa a sincronização a cada 12 horas para atualizar o estado da licença e o último tempo de conformidade. Se dois dias se passaram sem conexão com um gerenciador de licenças, um e-mail é enviado ao administrador para informá-lo que o gerenciador de licenças não pode sincronizar com o sistema. Foi dado a você um período de carência de 180 dias para se reconectar a um gerenciador de licenças.

Um novo e-mail é enviado ao administrador, no final de cada mês, que o sistema não consegue se conectar com o gerenciador de licenças, informando-o a data em que o sistema será desativado. Se o sistema se reconectar com o gerenciador de licenças antes do período gratuito de seis meses passar, esta condição termina.

Se o sistema não se reconectar com o gerenciador de licenças no prazo de 180 dias, o sistema será definido para o modo de manutenção e não poderá ser ativado até que o problema seja resolvido. A mensagem de e-mail informa ao administrador a data de quando isso irá ocorrer. Quando o sistema está no modo de manutenção, os usuários não podem agendar, organizar ou participar de reuniões ou acessar gravações no sistema. O site da Administração funciona normalmente para que um administrador possa iniciar a sessão no sistema, mas o sistema deve reconectar com o gerenciador de licenças para acabar com essa condição e restaurar a capacidade dos usuários de agendar, organizar e participar de reuniões e acessar gravações.

Solicitando Licenças utilizando o Gerenciador de Licenças

Obtenha as licenças de Organizador e do Centro multidados (MDC) usando o Enterprise License Manager incorporado da Cisco:

Antes de iniciar

Contate seu representante de vendas para pedir as licenças de Organizador e do Centro multidados (MDC) para seu sistema. O representante de vendas irá enviar a você um e-mail que contém a Chave de Autorização do Produto (PAK).

- | | |
|----------------|--|
| Etapa 1 | Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel. |
| Etapa 2 | Selecione Sistema e então selecione o link Exibir mais na seção de Licenças . |
| Etapa 3 | Selecione Gerenciar Licenças |

Seu navegador abre uma nova guia ou janela contendo um gerenciador de licenças. (O gerenciador de licenças está incorporado no Cisco WebEx Meetings Server; ele não é um site externo.)

- Etapa 4** Selecione **Gerenciador de Licenças > Licenças**.
- Etapa 5** Selecione **Gerar Solicitação de Licença**.
A caixa de diálogo **Pedido de Licenças e Próximos Passos** aparece.
- Etapa 6** Copie o texto selecionado no campo e selecione **Registro de Licença Cisco**.
- Etapa 7** Efetue logon na sua conta Cisco e exiba **Registro de Licença do Produto**.
- Etapa 8** Insira a Chave de Autorização do Produto (PAK) que você recebeu do seu representante de vendas da Cisco no campo **Chave de Autorização do Produto** e selecione **Próximo**.
A página **Completar PAK** ou a guia **Atribuir SKUs para dispositivos** é exibida.
- Etapa 9** Insira a quantidade de licenças de cada PAK que você está ativando no campo **Quantidade para atribuir**.
- Etapa 10** Cole o conteúdo da Solicitação de Licença que você gerou e copie no campo **Colar o conteúdo...** e selecione **Próximo**.
A guia **Revisão** é exibida.
- Etapa 11** Verifique se o endereço de e-mail do contato está correto. Opcionalmente, altere o endereço de e-mail do contato no campo **Enviar para**.
- Etapa 12** Reveja a página e selecione **Eu concordo com os termos da Licença**.
- Etapa 13** Selecione **Obter Licença**
A caixa de diálogo **Estado da Solicitação de Licença** aparece.
- Etapa 14** Obtenha o arquivo de licença em uma das seguintes formas:
 - Selecione **Baixar** para baixar o arquivo de licença (.bin).
 - Extraia o seu arquivo de licença (.bin) do arquivo ZIP que lhe foi enviado por e-mail.
- Etapa 15** Retorne para o site da Administração e selecione **Sistema** e então selecione o link **Exibir mais** na seção **Licenças**.
- Etapa 16** Selecione **Gerenciar Licenças**.
Seu navegador abre uma janela de **Licenças**.
- Etapa 17** Selecione **Preencher licenças a partir do arquivo** no menu Outras opções de cumprimento.
- Etapa 18** Selecione **Procurar** e selecione o arquivo de licença (.bin) que você baixou ou extraiu do arquivo ZIP no seu e-mail.
- Etapa 19** Selecione **Instalar**.
Seu arquivo de licença está instalado. Verifique as informações da licença que são exibidas para garantir que ela está correta.
- Etapa 20** Selecione **Atual** na coluna Completar a Data.
A página **Completar a Licença** é exibida. Verifique se as informações exibidas na seção **Licenças Concluídas** estão corretas.

Usando Licenças ao utilizar o eFulfilment

Complete o pedido de licença, inserindo a Chave de Autorização do Produto (PAK) no gerenciador de licenças sem usar o site.

Antes de iniciar

Contate seu representante de vendas da Cisco para pedir as licenças de Organizador e do Centro multidados (MDC) para seu sistema. O representante de vendas irá enviar a você um e-mail que contém a Chave de Autorização do Produto (PAK).

O e-Fulfilment requer que uma conexão de rede entre o sistema e a Cisco Systems, Inc. possa ser estabelecida. Verifique se o seu sistema não está protegido por um firewall que não permite o acesso. Se o acesso não é permitido, use o cumprimento baseado em arquivo (consulte [Solicitando Licenças utilizando o Gerenciador de Licenças, na página 249](#)) ou entre em contato com o TAC para abrir um processo para solicitar licenças (consulte [Solicitando Licenças Contatando o CAT, na página 252](#)).

- Etapa 1** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 2** Selecione **Sistema** e então selecione o link **Exibir Mais** na seção de Licenças.
- Etapa 3** Selecione **Gerenciar Licenças**
O navegador abre uma nova guia ou janela contendo o gerenciador de licenças incorporado no Cisco WebEx Meetings Server. (O site do gerenciador de licenças não é um site externo.)
- Etapa 4** Selecione **Completar Licenças da PAK**.
O assistente **Completar Licenças da PAK** é exibido.
- Etapa 5** Digite a PAK que você recebeu do seu representante de vendas da Cisco no campo **Chave de Autorização do Produto** e selecione **Seguinte**.
A página **Completar a PAK** é exibida.
- Etapa 6** Selecione **Adicionar licenças de uma nova PAK**.
- Etapa 7** Insira o código da PAK na caixa * **código PAK** e selecione **Próximo**.
- Etapa 8** Faça logon usando o seu ID de usuário e senha cisco.com.
A janela **Completar Licenças** é exibida indicando o número de licenças disponíveis.
- Etapa 9** Selecione **Completar** na coluna **Ações**.
- Etapa 10** Clique na coluna **Instalar** para editar os valores.
- Etapa 11** Insira o número de licenças que deseja completar neste sistema. Se a PAK suporta o preenchimento parcial, o intervalo é de 1 para o número de licenças remanescentes na PAK.
- Etapa 12** Selecione **Salvar**.
- Etapa 13** Selecione **OK**.
A janela **Completar Licenças** é exibida. O valor na coluna **Instalar** exibe o número de licenças que você elegerá para serem preenchidas.
- Etapa 14** Selecione **Próximo**.
A janela **Revisar Conteúdo** é exibida. A coluna **Valores Atuais** exibe o número de licenças ativas. A coluna **Após o preenchimento** exibe quantas licenças você terá quando o e-Fulfilment estiver completo.
- Etapa 15** Selecione **Próximo**.
- Etapa 16** Selecione **Ao verificar esta caixa, eu reconheço que li, entendi e concordo em ficar vinculado aos termos e condições do Contrato de Licença do Usuário Final**.
- Etapa 17** Selecione **Finalizar**.
Uma barra de progresso **Conectando ao servidor da licença** é exibida enquanto o gerenciador de licenças se conecta à Cisco para completar as suas licenças. Quando o e-Fulfilment está concluído, uma nova linha é adicionada na janela

Licenças. A coluna **Completar a Data** exibe a data atual seguida por - **Atual**. Você pode selecionar este link para exibir os detalhes das suas licenças, incluindo o tipo e o número de licenças que estão instaladas no sistema.

Solicitando Licenças Contatando o CAT

Antes de iniciar

Obtenha o seu número ID de registro. Você pode encontrar seu número ID de registro, abrindo a sua ferramenta de Gerenciamento de Licença Empresarial e selecionando **Sobre**.

Etapa 1

Inicie sessão no site da Administração.

Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.

Etapa 2

Selecione **Suporte** e chame o CAT no número listado.

Etapa 3

Abra um processo, solicitando o número da licença de Organizador e do Centro multidados (MDC) que você deseja. Processamos sua solicitação e permitimos as licenças adicionais no seu sistema.

Etapa 4

Selecione **Sistema**.

Etapa 5

Verifique a seção de licença para confirmar que as licenças adicionais foram adicionadas.

Reorganizando licenças do organizador

A reorganização move as licenças do organizador em um sistema que está sendo unido a um sistema MDC, atualizado, ampliado ou substituído para o sistema sobrevivente por um período de tempo limitado. Se as licenças não forem reorganizadas, não podem ser atualizadas. Por exemplo, quando um sistema é atualizado a partir da versão 1.5MR3 para a versão 2.0, as licenças do organizador originalmente organizadas no sistema 1.5MR3 podem ser reorganizadas no sistema 2.0 por 180 dias antes de serem substituídas por licenças válidas para a versão 2.0. Se as licenças do organizador 1.5 em execução no sistema 2.0 não forem substituídas no prazo de 180 dias, o sistema será desligado até o problema das licenças ser resolvido. (A única tarefa permitida é a adição de licenças do organizador no sistema. Consulte [Reorganizando licenças após uma grande modificação do sistema, na página 253](#).)

Se o sistema original estava operando sem licenças e dentro de um período de licença de teste, o número restante de dias gratuitos da licença do organizador é transferido para o sistema atualizado.

Acessando o Formulário de Solicitação GLO

Para exibir o formulário de solicitação de Operações de Licenciamento Globais (GLO), selecione **Fale Conosco** na página de Registro de Licença do Produto (<https://tools.cisco.com/SWIFT/LicensingUI/Quickstart>). Na página Informação de Contato do Suporte GLO, selecione **solicitação**.

Antes de iniciar

Esteja preparado para fornecer as seguintes informações:

- Informações de contato
- Descrição do problema
- Nome do produto e atividade de licenciamento (tal como reenviar as informações de licença ou atualizar a licença)
- Informação de autorização (tal como um número de série do produto)

Reorganizando licenças após uma grande modificação do sistema

Depois que o sistema foi modificado como o resultado de uma ação, como uma atualização ou expansão, e os testes concluídos, o próximo passo é a reorganizar suas licenças.

Se você tem um sistema de Vários centros de dados (MDC) e esse sistema foi ampliado, é necessário adquirir licenças MDC maiores. Se ele foi atualizado, você tem 90 dias para atualizar as licenças MDC. Licenças reorganizadas são automaticamente invalidadas no sistema original. Antes de começar a reorganizar, preserve uma *solicitação de licença* do sistema original, caso seja necessário para reorganizar as licenças no sistema original, devido a algum erro na modificação desse sistema.

Ao reorganizar licenças, o número de licenças que você pode reorganizar está limitado ao número de licenças do sistema original. O método preferido de reorganizar licenças é através do portal do Registro de Licenças do Produto.

Se o sistema original tem licenças de Organizador, o sistema modificado permite um período de 180 dias antes que as licenças de Organizador atualizadas sejam solicitadas, permitindo que você teste o sistema atualizado antes de reorganizar as licenças originais no sistema atualizado. Uma vez que as licenças são reorganizadas, o período de testes termina. A reorganização pode ser feita usando o Portal de Registro de Licenças do Produto em <http://tools.cisco.com/SWIFT/LicensingUI/Home>. (Consulte [Acessando o Formulário de Solicitação GLO](#), na página 252.)

Gerar uma solicitação de licença

Para adquirir um pedido de licença para o sistema original:

-
- | | |
|----------------|---|
| Etapa 1 | A partir da janela de Administração do sistema original, selecione Sistema . |
| Etapa 2 | Selecione (em Licenças) ver mais > Gerenciar licenças . |
| Etapa 3 | Selecione Outras opções de cumprimento > Gerar solicitação de licença . |
| Etapa 4 | Copie o conteúdo e salve a solicitação de licença em um arquivo no PC. |
-

Próximos passos

Registre as licenças. Consulte [Registre Licenças para serem Reorganizadas](#), na página 254 para obter instruções.

Registre Licenças para serem Reorganizadas

Para usar o portal de Registro de Licenças do Produto, efetue logon em <https://tools.cisco.com/SWIFT/LicensingUI/Quickstart>. É enviado a você um e-mail contendo as licenças reorganizadas. Note que se você está fazendo a reorganização como parte de uma atualização de software, você deve reorganizar (consulte [Reorganizando licenças após uma grande modificação do sistema, na página 253](#)) e atualizar a versão antiga das licenças em seu sistema atualizado. Uma mensagem de erro, como **Você está usando um arquivo de licença inválida com a sua implantação atual**, pode ser exibida no site de administração do seu sistema atualizado. Isso é esperado. A mensagem inclui uma data de validade que indica quando o sistema será encerrado se você não atualizar as licenças de Organizador antes desta data. A única tarefa que você pode realizar após esta data é a instalação de licenças.

Próximos passos

Depois de reorganizar as licenças, conclua a atualização da licença antes da data indicada para assegurar o uso ininterrupto do sistema. Consulte [Solicitando Licenças utilizando o Gerenciador de Licenças, na página 249](#) para obter mais informações.

Atualizando licenças depois de uma modificação de software

Após uma modificação do software, as licenças instaladas são reorganizadas do sistema original para o sistema atualizado. (Consulte [Reorganizando licenças após uma grande modificação do sistema, na página 253](#) para obter mais informações.) Após as licenças serem reorganizadas, elas podem ser atualizadas para uso no sistema atualizado.

A associação de usuários para licenças é excluída. Os usuários são associados a licenças na primeira vez que organizam uma reunião.

Para atualizar suas licenças instaladas usando o eFulfilment:

- 1 Obtenha um código da Chave de Autorização do Produto (PAK) do seu fornecedor.
- 2 A partir da janela **Sistema**, selecione **(em licenças) exibir mais>Gerenciar licenças> Licenças> Preencher licenças a partir do PAK**. A janela **Preencher licenças do PAK** é exibida.
- 3 Insira o código PAK e selecione **Próximo**.
- 4 Faça logon usando suas credenciais de conta cisco.com. A janela **Preencher licenças do PAK** é exibida.
- 5 Clique na coluna **Instalar** para selecionar o número de licenças que você deseja instalar.
- 6 Indique o número de licenças a serem instaladas e selecione **Salvar**. As licenças são instaladas no sistema como parte do eFulfilment da PAK.



Observação

O número de licenças que você pode instalar é limitado ao número de licenças disponíveis da PAK atualizada e não pode exceder o número de licenças que foram reorganizadas a partir do sistema original.

Para atualizar a versão de suas licenças instaladas a partir de um arquivo de licença:

- 1 Obtenha um arquivo de licença do seu fornecedor usando cisco.com/go/license.
- 2 Da janela **Sistema**, selecione **(em Licenças) exibir mais>Gerenciar licenças>Licenças>Preencher licenças a partir do arquivo**. A janela **Instalar arquivo de licença** é exibida.
- 3 Procure no arquivo de licença. O arquivo é exibido na janela **Licenças**.

As licenças são atualizadas.



CAPÍTULO 18

Registrando centros de dados para criar um sistema de vários centros de dados (MDC)

- Registrando centros de dados para criar um sistema de vários centros de dados (MDC), página 255

Registrando centros de dados para criar um sistema de vários centros de dados (MDC)

Sobre os vários centros de dados

O recurso licenciado dos vários centros de dados (MDC) está disponível na versão 2.5 e superior. A versão 2.5 permite que dois sistemas CWMS sejam unidos em um único sistema MDC. Uma licença deve ser adquirida para cada centro de dados CWMS em um sistema MDC. As licenças MDC devem ser compradas antes de tentar implantar o MDC. Um sistema com um único centro de dados não precisa de uma licença do recurso. As licenças MDC são ainda descritas em [Sobre licenças MDC, na página 245](#).

As vantagens de um sistema de vários centros de dados incluem:

- O usuário final acessa todos os centros de dados usando uma URL e um conjunto de números de telefone; a existência do MDC é transparente para os usuários finais.
- Os dados de gerenciamento relacionados, as gravações e as licenças do organizador migram livremente entre os centros de dados unidos.
- Os usuários podem discar para reuniões, sem restrições geográficas; participar de reuniões discando números de telefones locais.
- Os centros de dados podem (opcionalmente) ser localizados em diferentes áreas geográficas.
- Tempo de inatividade zero durante alguns eventos de manutenção planejada, quando os centros de dados podem estar executando diferentes versões de *atualização* CWMS 2.5. Consulte as notas de versão no <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-release-notes-list.html> para determinar quais versões do CWMS podem ser executadas simultaneamente.

Ocasionalmente, os centros de dados em um sistema MDC podem estar executando versões de *atualização* diferentes. Consulte as notas de versão no <http://www.cisco.com/c/en/us/support/conferencing/>

[webex-meetings-server/products-release-notes-list.html](#) para determinar quais versões do CWMS podem ser executadas simultaneamente.

- Um ambiente de recuperação de desastres que é transparente para os usuários. Se um centro de dados falhar por qualquer motivo, o outro centro de dados suportará usuários.

Embora em um ambiente MDC os centros de dados estão todos executando o CWMS e pares considerados, com a finalidade de unir os centros de dados em um sistema, a relação entre os centros de dados é considerada *primária* e *secundária*. Antes da União, o centro de dados primário suporta o *sistema* que você deseja manter. O centro de dados secundário torna-se parte do sistema MDC. A distinção é importante, especialmente se você está unindo centros de dados que têm apoiadoativamente usuários.



Observação

Não há aumento da capacidade quando um centro de dados é adicionado a um sistema MDC. Se um centro de dados de 2.000 portas for adicionado a um sistema MDC suportado por um centro de dados de 2.000 portas, o sistema resultante será um MDC de 2.000 portas.

Se você está se registrando em um centro de dados do sistema CWMS secundário recém criado que não tem os dados do usuário para um sistema MDC, continue a [Preparando um sistema MDC para receber solicitações de registro de centros de dados, na página 258](#).

Se você está participando de um centro de dados do sistema CWMS secundário ativo que inclui os dados do usuário para um sistema MDC, continue a [Preparando-se para registrar um centro de dados CWMS ativo para um sistema MDC, na página 256](#).

Preparando-se para registrar um centro de dados CWMS ativo para um sistema MDC

Quando você se registrar em um centro de dados do sistema CWMS secundário que tem estado em serviço aos usuários, ele foi adquirido ou configurado com os dados do usuário que podem ser perdidos quando unido à Vários centros de dados (MDC). Em um ambiente de Centro de dados único, um centro de dados CWMS serve a comunidade de usuários. Quando um sistema MDC é desejado, tipicamente um novo centro de dados CWMS é criado e registrado ao sistema MDC antes que o centro de dados é colocado em serviço e, portanto, não há nenhuma informação do usuário, licenças ou informações de configuração de valor a reter sobre o que se tornará o centro de dados secundário durante o Registro. No entanto, se você está se registrando em dois centros de dados ativos, o conteúdo do usuário é substituído ou inacessível:

- Todos os dados globais são substituídos. (Parâmetros de configuração local para os centros de dados são preservados.)
- Informações do usuário, reuniões agendadas, relatórios e e-mails relacionados que estavam no centro de dados secundário são excluídos.
- As gravações de reunião são inacessíveis para os usuários. As gravações permanecem intactas no NAS, mas elas não podem ser acessadas ou recuperadas pelos usuários. Consulte [Preservando gravações antes de registrar um sistema MDC, na página 257](#).)
- As licenças de Organizador se perdem, mas as licenças de Organizador Permanente que foram registradas no centro de dados secundário podem ser recuperadas registrando-as novamente no sistema MDC. (Se o centro de dados primário é removido do sistema, as licenças devem ser registradas novamente em outro centro de dados.

Se o centro de dados primário desligar por algum motivo, ele deve ser ligado novamente antes das licenças do organizador serem modificadas. Se o centro de dados de gestão não puder ser recuperado, os centros de dados sobreviventes entrarão em um modo de carência por 180 dias. Para recuperar, as

licenças de Organizador Permanente devem ser registradas novamente antes do término do período de carência. (Consulte [Reorganizando licenças do organizador, na página 252](#)). Se as licenças não forem registradas novamente antes do término do período de carência, o sistema será colocado em modo de manutenção até as licenças serem registradas novamente.

- As associações de licença de usuário para organizador em um centro de dados secundário ativo são perdidas quando os centros de dados são registrados. Usuários que foram organizadores em um centro de dados secundário ativo podem recuperar as licenças simplesmente organizando reuniões no sistema registrado ou um administrador pode atribuir manualmente licenças de organizador a partir do centro de dados, gerenciando as licenças.

As seguintes informações sobre os centros de dados secundários são mantidas após o Registro:

- Configurações específicas do sistema, tais como Cisco Unified Call Manager (CUCM).
- Definições de idioma, tais como configurações de idioma IVR.
- Configuração de áudio.
- Informações sobre a Discagem múltipla

Preservação dos dados CWMS em um centro de dados secundário antes um registro

Os dados CWMS em um centro de dados secundário que está sendo registrado em um sistema MDC são substituídos ou ficam inacessíveis. Se você está registrando um centro de dados CWMS que não foi colocado em serviço, não há dados significativos para preservar e você pode continuar a [Preparando um sistema MDC para receber solicitações de registro de centros de dados, na página 258](#). Caso contrário, considere a preservação de dados críticos.

Quando um centro de dados secundário é registrado a um sistema MDC, esse centro de dados perde:

- Associações de licença de usuário-organizador
- Licenças de organizador (que podem ser recuperadas registrando-as novamente no sistema MDC [Reorganizando licenças após uma grande modificação do sistema, na página 253](#))
- Reuniões agendadas (que devem ser reagendadas manualmente no sistema MDC)
- As gravações de reuniões que podem ser preservadas:
 - Pedindo aos usuários para baixarem e reterem gravações localmente.
 - Arquivadas para recuperação por um administrador do sistema.
 - Ambos. (Recomendado)

Gravações de reuniões "ao vivo" no NFS, para que não sejam perdidas; elas não são acessíveis aos usuários a partir do CWMS.

Preservando gravações antes de registrar um sistema MDC

No diretório `NFS:/nbr` estão os diretórios de Gravação, `nfskeepalive` e Foto instantânea. Para arquivar os arquivos, copie `NFS1:/nbr/1/*` para `NFS2:/nbr/1`.



Observação

Este procedimento é fornecido como um exemplo. O processo do sistema pode variar.

Para os efeitos das medidas de exemplo, suponha que o NFS está em DC1 e nomeado `sanjose-nfs:/cisco/cwms` e o NFS em DC2 é nomeado `rtp-nfs:/cisco/cwms`.

Antes de iniciar

- Acesse uma máquina Linux com acesso raiz para o NFS. (Qualquer variante fará, Redhat, CentOS, e assim por diante.)
- Se o NFS tem uma filtragem ou controle de acesso baseado em IP para a montagem, adicione o IP do organizador Linux à lista de acesso.

Etapa 1 `cd/tmp`

Etapa 2 Crie um novo diretório temporário que será usado para montar o NFS do DC1. `mkdir nfs-dc1`.

Etapa 3 Crie um novo diretório temporário que será usado para montar o NFS do DC2: `mkdir nfs-dc2`.

Etapa 4 Monte o DC1 NFS para `/tmp/nfs-dc1 : mount -t nfs -o vers=3,rw,soft,timeo=400 sanjose-nfs:/cisco/cwms/tmp/nfs-dc1/`

Etapa 5 Monte o DC2 NFS para `/tmp/nfs-dc2 : mount -t nfs -o vers=3,rw,soft,timeo=400 rtp-nfs:/cisco/cwms/tmp/nfs-dc2/`.

Etapa 6 Sincronize as gravações: `rsync -av --exclude='*Snapshot*' nfs-dc1/ nfs-dc2.`

Etapa 7 Desmonte o DC1 NFS: `umount nfs-dc1`.

Etapa 8 Desmonte o DC2 NFS: `umount nfs-dc2`.

Etapa 9 Exclua o diretório de montagem temporário DC1 NFS: `rm -r nfs-dc1`.

Etapa 10 Exclua o diretório de montagem temporário DC2 NFS: `rm -r nfs-dc2`.

Preparando um sistema MDC para receber solicitações de registro de centros de dados

Os centros de dados podem ser unidos e gerenciados como um único sistema. Este procedimento descreve como preparar o centro de dados *primário* que já está atendendo o *sistema* para receber solicitações de Registro do centro de dados *secundário*:

Antes de iniciar

O seguinte é uma lista de tarefas que o administrador de um sistema deve concluir para garantir que a união de um centro de dados para um sistema seja bem sucedida.

- 1 Verifique se todos os centros de dados estão executando a mesma versão do software CWMS.
- 2 Verifique se todos os centros de dados estão executando os mesmos tipos de software. Por exemplo, verifique para que todos os centros de dados sejam Áudio Criptografado -AE ou Áudio não Criptografado -AU.
- 3 Verifique se todos os centros de dados são do mesmo tamanho de sistema.
- 4 Network Time Protocol (NTP) é necessário para todos os centros de dados e todos os centros de dados devem estar no mesmo tempo do NTP.
- 5 Todos os organizadores de máquinas virtuais devem ser configurados com servidores NTP.
- 6 Os servidores NTP devem ser acessíveis a partir dos organizadores de máquinas virtuais. (Erros podem ocorrer se o DNS ou o firewall não passarem pelo NTP ou se o servidor NTP errado for configurado.)

- 7 Instale licenças de Vários centros de dados (MDC) (duas no mínimo) no centro de dados primário que está executando o gerenciador de licenças.
- 8 Todos os centros de dados possuem o Proxy Reverso da Internet (IRP) ativado ou desativado. Não pode haver uma incompatibilidade, mas após o Registro, o IRP pode ser adicionado ou removido de qualquer centro de dados.
- 9 Nenhum dos centros de dados está executando Alta Disponibilidade (HA). (Consulte [Removendo a alta disponibilidade de um sistema, na página 62](#)).
- 10 Verifique se o armazenamento está configurado em ambos os centros de dados ou em nenhum deles. Se o armazenamento estiver configurado, os centros de dados devem estar usando o armazenamento em servidores diferentes ou pelo menos em pastas diferentes.
- 11 Verifique se todos os centros de dados estão usando o mesmo modo de autenticação. O modo de autenticação pode ser LDAP, SSO ou modo padrão.
- 12 Verifique se o DNS tem entradas para todas as URLs locais, todas as URLs comuns e todos os nomes de organizadores. A URL comum de administração deve ser associada a apenas um endereço de IP quando o Registro é executado. A URL comum WebEx deve ser associada a apenas um endereço de IP quando o Registro é executado. Depois que o centro de dados é unido a um sistema, a URL comum deve retornar dois endereços de IP.
- 13 Verifique se o transporte CUCM em ambos os centros de dados usa o mesmo protocolo. O protocolo de transporte pode ser TCP, UDP ou TLS.

Etapa 1 Notifique os usuários no sistema secundário do Registro. Se o centro de dados secundário não tem sido uma parte de algum sistema ativo, pule esta etapa. Se este centro de dados está suportando um sistema ativo, consulte [Preparando-se para registrar um centro de dados CWMS ativo para um sistema MDC, na página 256](#). Os dados do usuário, as reuniões agendadas e o acesso a gravações de reuniões no centro de dados secundário se perdem como resultado de um Registro. Antes de enviar uma solicitação de Registro do centro de dados secundário, recomendamos que você envie uma notificação aos usuários que querem preservar alguma gravação de reunião, eles devem baixar as gravações para seus computadores locais.

Etapa 2 Selecione **Centros de dados > Adicionar centros de dados > Preparar sistema para Participação**

Etapa 3 Inserir:

- URL do site local — URL do site do usuário que permite aos usuários agendarem, participarem ou organizarem reuniões.
- URL de administração comum — URL de administração do sistema que resolve para o endereço VIP privado do sistema.
- E-mail de administração remoto — Dircione o endereço de e-mail para onde o sistema pode enviar informações e alertas.
- Nome do centro de dados local — Identifica o centro de dados secundário no sistema local.

Etapa 4 Baixe o certificado que será usado para unir os sistemas.

O certificado do centro de dados primário deve ser carregado em um centro de dados secundário antes do registro. Os certificados são modificados pelo sistema, por isso é melhor não tentar reutilizar os certificados antigos para realizar um registro.

Observação Ao usar o Safari, o certificado baixado é salvo como `CAcert.pem.txt`. Este é o comportamento padrão do navegador Safari. Para restaurar a extensão `.pem` (antes de carregar o certificado), exclua a sequência `.txt`.

Etapa 5 Selecione **Concluído**.

Etapa 6 Inicie sessão no centro de dados secundário e envie uma solicitação de Registro a partir desse centro de dados. Consulte [Unindo um centro de dados a um sistema MDC](#), na página 260 para obter instruções.

Unindo um centro de dados a um sistema MDC

A solicitação de Registro é enviada de um centro de dados *secundário* para o centro de dados *primário* (o centro de dados que suporta o sistema com Vários centros de dados (MDC) CWMS que irá reter seus dados e acesso a gravações de reuniões após o Registro). As licenças de recursos do MDC e as licenças de Organizador Permanente são normalmente hospedadas e gerenciadas no centro de dados primário. Não há período de teste para um sistema MDC; As licenças MDC devem ser carregadas no centro de dados primário antes do Registro. Sem uma licença MDC disponível no centro de dados primário, um centro de dados secundário não pode ser registrado em um sistema.



Observação

Ao registrar centros de dados, os certificados do centro de dados primário são atualizados. Os novos certificados são autoassinados e automaticamente regenerados para pegar as novas URLs a partir do centro de dados secundário. Isso provoca um aviso de certificado no navegador quando você acessa o centro de dados primário ou o site de Administração MDC. Aceite os avisos e siga o procedimento padrão para atualizar os certificados do sistema. Consulte [Gerenciando Certificados](#), na página 214.)

**Observação**

Ao registrar centros de dados que usam outros idiomas além do inglês, sempre haverá um breve período durante a operação de Registro quando a lista de tarefas aparecer em inglês. As mensagens de erro também podem aparecer em vários idiomas durante o Registro. (O equilíbrio do texto na página é exibido no idioma original.)

Quando a tarefa **As tabelas do banco de dados são sincronizadas** é lançada, o comportamento esperado do idioma na lista de tarefas é:

- Se a conta de Administrador está hospedada no centro de dados primário e secundário com as mesmas configurações de idioma, a lista de tarefas é exibida em inglês durante a tarefa **As tabelas do banco de dados são sincronizadas**. Após as tabelas serem sincronizadas, os nomes das tarefas voltam para o idioma do Administrador.
- Se a conta de Administrador está hospedada no centro de dados primário que permanecerá após o Registro e há outra conta de Administrador no centro de dados secundário unindo o sistema que está definido para um idioma diferente do que a conta de Administrador no centro de dados primário, a lista de tarefas é exibida em inglês, enquanto as tabelas do banco de dados são sincronizadas. Após a sincronização, a lista de tarefas muda para o idioma que o administrador definiu no centro de dados primário.
- Se a conta de Administrador está hospedada apenas no centro de dados secundário que une o sistema e o Administrador não tem uma conta no centro de dados primário que permanecerá após o Registro, a lista de tarefas é exibida em inglês enquanto as tabelas do banco de dados são sincronizadas. Uma vez que o sistema terminar a sincronização, não haverá mais alterações de idioma e nenhum botão de **Concluído**. Para continuar, o administrador deve fechar a janela do navegador atual e abrir uma nova janela usando a URL de administração local do centro de dados secundário, iniciar sessão usando uma conta de administrador no centro de dados primário, selecionar **Centros de dados > Adicionar centros de dados** e verificar o estado.

Antes de iniciar

O Network Time Protocol (NTP) deve ser configurado da seguinte forma:

- O NTP é necessário para todos os centros de dados e todos os centros de dados devem estar no mesmo tempo do NTP.
- Todos os organizadores de máquinas virtuais devem ser configurados com servidores NTP.
- Os servidores NTP devem ser acessíveis a partir dos organizadores de máquinas virtuais. (Erros podem ocorrer se o DNS ou o firewall não passarem pelo NTP ou se o servidor NTP errado for configurado.)

Se este centro de dados estiver suportando um sistema ativo, as licenças de Organizador suportado neste centro de dados serão removidas. Estas licenças de Organizadores podem ser reorganizadas no centro de dados que hospeda o Gerenciador de Licenças. (Consulte [Reorganizando licenças do organizador, na página 252](#)). Recomendamos que você salve uma solicitação de licença deste centro de dados antes de iniciar o registro, no caso de você precisar de ajuda do TAC para localizar suas licenças.

Etapa 1 Para enviar uma solicitação para participar de um sistema MDC de um centro de dados secundário, selecione **Centros de dados > Adicionar centros de dados > Participar de sistemas**.

Etapa 2 Inserir:

- **Certificado do sistema remoto** — O certificado que corresponde a um no centro de dados primário.

Observação Ao usar o Safari, o certificado baixado é salvo como CAcert.pem.txt. Este é o comportamento padrão do navegador Safari. Para restaurar a extensão .pem (antes de carregar o certificado), exclua a sequência .txt.

- **URL de administração comum remota** — URL de administração do sistema remoto que resolve para o endereço VIP privado do sistema secundário.
- **E-mail de administração remoto** — Direcione o endereço de e-mail para onde o sistema pode enviar informações e alertas.
- **Senha de administrador remoto** — Senha que permite o acesso administrativo ao sistema secundário.
- **Nome do centro de dados local** — Cadeia de caracteres que identifica o centro de dados secundário no sistema local.

Etapa 3 Selezione Continuar.

A lista de tarefas do centro de dados de registro é exibida.

Observação Durante a tarefa **As tabelas do banco de dados são sincronizadas**, todos os usuários no centro de dados secundário são excluídos e os usuários listados no centro de dados primário são replicados para o centro de dados secundário. O sistema não pode obter o idioma do administrador (como não há usuários no DC2) e os padrões de interface para exibição em inglês.

Se o administrador do centro de dados secundário também existe no centro de dados primário, então após o administrador iniciar sessão no centro de dados secundário, o sistema exibirá o idioma do administrador (a menos que o idioma configurado no centro de dados primário para esse administrador é um idioma diferente do que está configurado no centro de dados secundário).

Se o administrador do centro de dados secundário também existe no centro de dados primário (ou há um erro na sincronização do banco de dados), então o sistema é exibido em inglês.

Etapa 4 Tire todos os centros de dados no sistema MDC do modo de manutenção.

Próximos passos

Adicionar os ponteiros para o servidor DNS

- **URL do site comum** — Endereço VIP público para cada centro de dados.
- **URL de administração comum** — Endereço VIP privado de ambos os centros de dados.
- **URL do site local** (de um centro de dados) — Endereço VIP público desse centro de dados.
- **URL do site local** (do outro centro de dados) — Endereço VIP público desse centro de dados.
- **URL do site de administração local** (de um centro de dados) — Endereço VIP privado desse centro de dados.
- **URL do site de administração local** (do outro centro de dados) — Endereço VIP privado desse centro de dados.

Modificar os números de acesso de áudio e serviços linguísticos

O número de acesso de áudio e os serviços linguísticos configurados no centro de dados primário são configurados como o número de acesso global e serviços linguísticos, substituindo a configuração do número

de acesso original e dos serviços linguísticos. Se necessário, vá para a configuração global e ajuste os números de acesso e os serviços linguísticos de forma adequada. (Consulte [Definindo as configurações do áudio](#), na página 169).

Recuperação de desastres em um ambiente com vários centros de dados

Em um ambiente com Vários centros de dados (MDC), onde um centro de dados falhou devido a um problema de hardware ou de centro de dados, recomendamos substituir o centro de dados através da criação de um novo centro de dados e unindo esse centro de dados ao sistema. (Consulte também [Recuperação de desastres usando o servidor de armazenamento](#), na página 148).

-
- Etapa 1** Cadastre-se no site da Administração do centro de dados sobrevivente.
 - Etapa 2** Remova o centro de dados com falha do sistema.
(Consulte [Removendo um centro de dados](#), na página 263).
 - Etapa 3** Crie um novo centro de dados para substituir o centro de dados que falhou.
A versão do centro de dados de substituição deve corresponder à versão do centro de dados sobrevivente.
 - Etapa 4** Conclua as configurações locais, como CUCM, SNMP, e assim por diante, combinando com o centro de dados que falhou.
 - Etapa 5** Prepare o centro de dados sobrevivente no sistema para receber as solicitações de Registro.
(Consulte [Preparando um sistema MDC para receber solicitações de registro de centros de dados](#), na página 258).
 - Etapa 6** Una o novo centro de dados ao sistema.
(Consulte [Unindo um centro de dados a um sistema MDC](#), na página 260).
Os dados do centro de dados sobrevivente são replicados no novo centro de dados.
 - Etapa 7** Atualize o DNS com a nova URL e as informações do endereço de IP.
-

Removendo um centro de dados

Quando um centro de dados é removido de um sistema com Vários centros de dados (MDC), todas as configurações CWMS são removidas. Os parâmetros que são aplicados ao centro de dados removido são excluídos do centro de dados sobrevivente.



Observação

Em um ambiente com Vários centros de dados (MDC), o Gerenciador de Licenças está sendo executado em apenas um centro de dados; ele não pode ser executado em mais de um centro de dados. Se você remover o centro de dados que hospeda o Gerenciador de Licenças, você tem 90 dias para configurar o Gerenciador de Licenças em outro centro de dados e reorganizar as licenças. Consulte [Registre Licenças para serem Reorganizadas](#), na página 254.)

Antes de iniciar

Faça um backup do sistema e do centro de dados a ser removido.

Remova todas as entradas do Communications Manager e DNS.

-
- Etapa 1** Desligue as máquinas virtuais do centro de dados que está sendo removido.
- Etapa 2** Inicie sessão no site da Administração.
Em um sistema com Vários centros de dados, o DNS determina qual Painel do centro de dados é exibido. Todos os centros de dados podem ser gerenciados a partir deste Painel.
- Etapa 3** Selecione **Centros de dados**.
A janela **Centro de dados** é exibida.
- Etapa 4** (Opcional) Verifique se o centro de dados está inacessível.
Você pode verificar isso manualmente ou você pode começar o processo de remoção do centro de dados e deixar a seleção do CWMS disponível. Se o centro de dados pode executar um ping, o processo de remoção não procede, e uma mensagem de erro é exibida.
- Etapa 5** Para enviar uma solicitação para excluir um centro de dados de um sistema MDC , selecione **Remover** na coluna **Ação**. Se o centro de dados a ser removido está hospedando o Gerenciador de Licenças, um aviso é exibido. Há também um aviso de que são necessárias mudanças de DNS.
O centro de dados primário é colocado em modo de manutenção e a janela **Remover centro de dados** é exibida mostrando o andamento da ação.
- Etapa 6** Selecione **Continuar**
- Etapa 7** Quando todas as tarefas estiverem verde, selecione **Concluído**.
O centro de dados é removido e você volta à janela do **Centro de dados**.
- Etapa 8** Verifique se o centro de dados foi removido.
As URLs para o acesso ao sistema mudam e o sistema retém apenas as URLs globais.
- Etapa 9** Remova todas as entradas DNS do centro de dados removido e mapeie os endereços de IP virtuais privados e públicos do centro de dados sobrevivente para as URLs globais.
- Etapa 10** Desative o modo de manutenção. Consulte [Ativar ou desativar o modo de manutenção para a versão 2.5 e posterior](#).
Quando o modo de manutenção for desativado, o sistema determina se é necessário um *reinicio* (leva aproximadamente 3-5 minutos) ou uma *reinicialização* (leva aproximadamente 30 minutos) e mostra a mensagem respectiva. Se este centro de dados faz parte de um sistema com Vários centros de dados (MDC), o administrador é redirecionado para a URL de administração global. O centro de dados que o administrador vê é determinado pela política de resolução de DNS. Se o Key Regeneration for habilitado, tirar um centro de dados do modo de manutenção automaticamente tira todos os centros de dados do sistema do modo de manutenção.
O serviço de reuniões para usuários neste centro de dados é restaurado.
- Etapa 11** (Opcional) Se você removeu o centro de dados que hospeda o Gerenciador de Licenças, reorganize o Gerenciador de Licenças e as licenças no centro de dados sobrevivente.
-



CAPÍTULO 19

Usando os Recursos de Suporte

- Personalizar Seu Registro, página 265
- Configure uma Conta de Suporte Remoto, página 266
- Desativar uma Conta de Suporte Remoto, página 267

Personalizar Seu Registro

Você pode gerar arquivos de registro que mostram atividades em todo o seu sistema ou para especificar reuniões. Use os arquivos de registro para solução de problemas ou para submeter ao Centro de Assistência Técnica Cisco (CAT) quando você precisar de assistência.



Observação

Recomendamos que você gere arquivos de registro durante horários fora do expediente. O tamanho grande do arquivo de registro pode afetar o desempenho do sistema.



Observação

Dados de registro retidos por 40 dias. No entanto, se você atualizar a implantação do Cisco WebEx Meetings Server versão 2.0 para a versão 2.5, os dados de registro da versão 2.0 não serão transferidos para o sistema do Cisco WebEx Meetings Server 2.5 e portanto não estarão disponíveis depois que a atualização para a versão 2.5 estiver completa.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Suporte > Logs**.

Etapa 3 Complete os campos na página **Personalizar Seu Log** e selecione **Enviar**.

Campo	Descrição
(Opcional) ID do Caso	Insira a ID do caso do TAC da Cisco. As IDs de caso são obtidas a partir do TAC da Cisco quando ele está ajudando você com um caso. Usando este recurso permite que você associe os registros que você gerou com a ID de caso.

Campo	Descrição
Tipo	<p>Selecione o tipo de registro. Você pode selecionar Registro do Sistema Total ou Registro de Reunião Particular. Um Registro do Sistema Geral contém todas as informações do registro especificado para o seu sistema e o Registro de Reunião Particular coleta registros e dados do banco de dados para o processamento de MATS.</p> <p>Padrão: Registro do Sistema Total</p>
Intervalo	<p>Seleciona o intervalo para o seu registro. Você deve especificar a data e hora de inicio e fim do seu registro. O limite é 24 horas. Os dados de registro estão disponíveis apenas para os últimos 40 dias.</p> <p>Observação Para gerar registros com mais de 24 horas, você deve repetir esta operação, selecionando intervalos de data e hora consecutivas. Cada operação resulta na criação de um arquivo de registro separado. Por exemplo: Para gerar registros a partir de 1º de janeiro a 3 de janeiro, primeiro selecione um intervalo de data de 1º de janeiro a 2 de janeiro, selecione Enviar e baixe o arquivo de registro criado. Em seguida, selecione um intervalo de data de 2 de janeiro a 3 de janeiro. Seleccione Enviar e baixe o arquivo de registro criado.</p>
Inclui	<p>Especifica os dados que você deseja incluir em seu registro.</p> <p>Padrão: Todas as Atividades</p>

O seu registro é gerado e um e-mail é enviado para você contendo um link para baixar o registro.

Configure uma Conta de Suporte Remoto

Se você está tendo problemas técnicos e de contato com o CAT da Cisco para obter assistência, você pode configurar uma conta de suporte remoto para conceder um acesso temporário do representante do CAT para

o seu sistema. Este produto não oferece acesso de CLI para os administradores e, portanto, requer um representante do CAT para solucionar alguns problemas.

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Suporte > Conta de Remote Support**.

Etapa 3 Selecione **Ativar Remote Support**.

Etapa 4 Complete os campos na página **Conta de Remote Support** e selecione **Criar conta**.

Campo	Descrição
Nome da Conta de Suporte Remoto	Insira um nome para a sua conta de suporte remoto (6 a 30 caracteres).
Vida da Conta	Especifique a duração da conta em horas. O máximo é de 720 horas (30 dias).
Decodificador da Versão	Selecione 2- WebEx Meetings Server . Observação Se você tiver uma conta de suporte remoto que foi ativa antes do lançamento da versão do Cisco WebEx Meetings Server Version 1.5, você não terá de configurar esta opção.

A caixa de diálogo **Criação da Conta de Suporte Remoto** aparece, exibindo o código de acesso. Contate o CAT da Cisco e forneça o Nome da Conta de Suporte Remoto e o código de acesso para permitir que o pessoal de Suporte da Cisco tenha acesso ao seu sistema.

Desativar uma Conta de Suporte Remoto

Etapa 1 Inicie sessão no site da Administração.

Etapa 2 Selecione **Suporte > Conta de Remote Support**.

Etapa 3 Próximo à mensagem de estado, "Suporte Remoto é habilitado", selecione link **Desativá-lo**.
A sua conta de suporte remoto está desativada.

