



I'm not robot



Continue

Cwms 4.0 administration guide

Do you have an account? Personal content You products and support Sign in Forgot your user ID and/or password? Manage Account page 2 Cisco Webex Meetings Server Guides provides detailed procedures that plan, deploy, and manage your system: These include installation and network checklists to help you gather information and make decisions before deployment. In addition, we cover post-deployment, system-changing procedures, for example: Adding a high availability (HA) Extending the system to a larger system size Update or upgrade your system to the latest version in the Cisco Webex Meetings Server Administration Guide describes how to use the features available to you on the administration site and includes the following sections: Dashboard—Your dashboard displays your system monitor and contains links to your alarm settings, the Meeting Trends page, the Resource History page, system pages, and settings pages. User management—Add, import, enable, and disable users, configure tracking codes, and email users on the system with these features. See Manage users for more information. System—Configure system properties, site and administration site URLs, servers, SNMP settings, and licenses with these features. See Set up your system for more information. Settings—Configure your settings including business information, brand protection features, meeting settings, audio, video, mobility, quality of service, passwords, email settings, downloads, and security settings with these features. See Configure settings for more information. Report management—Set up and view your monthly reports. See Manage reports for more information. Support access and information—Open and view support requests, configure troubleshooting features, and conduct system resource and meeting tests using these features. See Use support features for more information. Page 3 Delete all VMware snapshots. Do not take snapshots during the expansion process. To delete snapshots, see Delete a snapshot. Obtain the base 4.0 Open Virtualization Archive (OVA) file. This requirement applies to systems that are initially distributed with 4.0 and systems that are deployed with 3.0 and updated (less) to 4.0. Table 1. Expansion Checklist Field Name Current Value For Your System Webex Site URL Administration Site URL Private VIP Address Public VIP Address When expanding a Multi-data center (MDC) system, it is necessary to remove any secondary datacenters. (Typically, the data center that is not running License Manager See Delete a datacenter.) Note Upgrading from an unencrypted version to an encrypted version or upgrading from an unencrypted version to an encrypted version is not supported. Get based on your existing system deployment. Step 1 Sign in to Webex Site Administration. In a Multidata Center system, DNS determines which datacenter Dashboard Dashboard Use this Dashboard to manage all datacenters in this system. Step 2 If you are extending an MDC system, delete the secondary datacenter, leaving only the primary datacenter. See Delete a data center. Step 3 If you are extending an MDC system, create a new datacenter running Cisco Webex Meeting Server to go to after the primary system is expanded. See Create a Multi-data center (MDC) system. Step 4 Create a backup copy of the original system. () Step 5 Enable Maintenance Mode. See Turning maintenance mode on or off. If the datacenter is part of a Multidata Center (MDC) system, the in-progress meetings fail over to an active datacenter. Failover can cause a brief interruption in active meetings. See About maintenance mode for details. If you turn on Maintenance Mode for all active datacenters, all conferencing functions are turned off. No one can log on to the Webex site, schedule meetings, join meetings, or play meeting recordings. Step 6 Select Continue. Step 7 Select . The Manage System Specifications page appears. Step 8 Select Expand System Size. Step 9 Select Continue. Your system checks connectivity to the VMs. If there are connectivity issues with one or more VMs, you must fix the issues before you can continue. If there are no connectivity issues, your system performs an automatic backup. When the backup is complete, you'll be notified that you can continue with your expansion. Step 10 Using the VMware vSphere client, select the VMs for the original system. Step 11 Using the vSphere client, deploy the virtual admin for the new system size. If you perform an automatic expansion, we create the other virtual machines for your system. If you perform a manual expansion, you can create the other VMs for your system. (See Deploying the OVA file from the VMware vSphere client.) Step 12 Attach Hard Drive 4 from the original System Admin VM to Admin virtual machine for the expanded system. (See Attaching an existing VMDK file to a new VM.) Step 13 Power on the extended system virtual admin and write down the deployment URL. If you perform an automatic expansion, we power on the other virtual machines for your system. If you perform a manual expansion, power on the other virtual machines for your system. Step 14 Enter the deployment URL in a web browser and continue deploying your extended system. Step 15 Select the preferred language for deploying the extended system. (See Choosing the language of setup.) Step 16 Select . Step 17 Confirm system size. (See Confirm the size of your system.) This system size must be greater than or equal to the original system. Step 18 Select Install a primary system. Step 19 automatic or manual deployment. (See See type of deployment.) If you selected manual deployment, continue to the next step. If you selected automatic deployment: Use the same OVA file that you first used to install the system. Deploy an administrator vm for the new system size. Your system will notify you when the expansion is complete. Step 20 If you want public access for your expanded system, then make sure there is a control in the Create an Internet Reverse Proxy VM check box. Otherwise, clear this check box. (See Add public access to your system using IIRP.) If you have chosen to add public access: Step 21 Enter the public VIP address for the Webex site URL. (See Enter the public VIP address.) You can enter the same public VIP address that you use for your original system, or change it to a new IP address. If you change it, then make the necessary updates in the DNS server. Step 22 Enter the private VIP address for the Webex site URL. (See Enter the private VIP address.) You can enter the same private VIP address that you use for your original system, or change it to a new IP address. If you change it, then make the necessary updates in the DNS server. Step 23 Enter the URL for the Webex Common site. (See Specify Webex common site url and administration site.) Participants will have access to this URL to host and participate in meetings. This URL resolves the private VIP address or public VIP address, depending on whether you are using a shared-horizon DNS or not. You can specify the same Webex Common site URL that you used for your original system, or change to a new one. If you do change it, then make the necessary updates in the DNS server. Note! If users try to use the original URL, these users cannot. Once this change is made, system traffic that comes from host names is released, other than those currently configured. Host or attend meetings Sign in from web pages, Desktop Application for Web order meetings, or mobile applications Play recordings Step 24 Enter the webex administration site URL for administrators to access the Cisco Webex Administration site. (See Specify Webex common site url and administration site.) This URL resolves the private VIP address. You can specify the same Webex Administration Site URL that you use for the original system, or change to a new one. If you do change it, then make the necessary updates in the DNS server. Step 25 Make sure that you have made all the configuration changes for the network, DNS server, and firewall that are required for the system. (See Confirm that your network is configured correctly.) Step 26 Once your virtual machines have been deployed successfully, select Next to continue to (See manually deploying VMs.) Along with the system control, we update the extended system with any necessary maintenance release updates to match the software version of the original system. (These updates may address the one hour.) When this is done, the system restarts. (See Check the system.) Step 27 Select Restart. Step 28 Sign in to Webex Site Administration. In a Multidata Center system, the DNS determines which datacenter Dashboard is displayed. Use this Dashboard to manage all datacenters in this system. Step 29 If you are extending an MDC system, go with it to the MDC system. (See Connecting a datacenter to a Multi-Datacenter System.) Step 30 Turn off Maintenance Mode. When you turn off Maintenance Mode, the system determines whether a restart or restart is required, and displays the appropriate message. A restart takes about 3 to 5 minutes and a restart takes about 30 minutes. If the datacenter is part of a Multidata Center (MDC) system, you'll be redirected to the Global Admin URL. The DNS resolution policy determines which datacenter you see. If Key Regeneration is enabled, a datacenter automatically exits all datacenters in the system from maintenance mode. See Turning the maintenance mode on or off. Meeting service on the data center is restored. Step 31 Select Continue. The system restarts. You can log on to Webex Site Administration after the restart is complete. Step 32 Test the expanded system. See about system testing. If the expansion fails, stream the expanded system and power on the original system. Contact Cisco TAC if necessary for further assistance. Updating the system to the desired MR. Page 4 Session types defines the features and options available for scheduled meetings. There is a predefined session type that can be set by default for new users. You can create up to four custom session types (Pro1 through Pro4) based on the predefined session type. Custom session types can be assigned to specific users to manage meeting security, bandwidth, and the conference options available to a user. For example, you can use session types to prevent specific users from using screen sharing. This is done by creating a custom session type that does not include the desktop sharing option, and then assigning this session type to specific users by editing their accounts. The audio privileges enabled in the meeting are listed under the Audio section. The audio permission can be edited from the scheduling page only by changing the meeting type. The audio privileges depend on: Site settings User Permission Permission Session Type Privileges To enable a privilege, it must be enabled on site, user, and session type. All three must be true. If there is no common option between these three audio options, the system searches for common audio options between the website and the user. If there are no common options between the website and the user, the system uses the settings for the website's When you use the Meet Now feature. There is no option to change session type. The session type used for the meeting is first in the list of assigned session types for values, sorted by alphabetical order by session code. The selected session type appears on the meeting details page. When you schedule a meeting using Webex Meetings Desktop Application, the host can select a session type from the list of session types allowed for that user. The predefined session type cannot be disabled; only custom session types can be enabled or disabled. You can select the default session types that are assigned when a new user ID is created. The default session types are applied to new users who are added to the system by: Synchronization with LDAP server. Import a csv file that does not have the session types field configured for a new user. Add users to the system through SSO login. Add new user to admin console. The Default session type for new users is selected by default. Page 5 An upgrade is defined as a replacement of the system to distribute major changes we have made to the system. For example, a system currently running version 2.8MR1 replaces Patch 2 or later to version 4.0, which includes new features. An update is defined as overwriting an existing (original) system to take advantage of changes we made to improve the system. For example, you might update a system from version 2.8MR1 to 2.8MR1 Patch 2 or to 2.8MR2. An expansion is defined as enlarging an existing system, but not modifying the application version. For example, you can extend a system from 800 users to 2,000 users. In all cases, the processes include transferring all data from the original system to the updated, upgraded, or expanded system. The complete update procedure, including backing up your virtual machines, can take up to an hour depending on: System Size Database Size Speed and load on vCenter Node CWMS System is the default name of the data center after an upgrade; it is not translated from English into other languages. Use the following table to determine your upgrade path to Cisco Webex Meetings Server Release 4.0. Installed Release Path to Release 4.0.1 2.8.2 Update to the latest available 2.8MR3 patch. Install Webex Productivity Tools, or push it to your desktops. Upgrade to 4.0 FCS. Update to the latest available 4.0MR release and patch. Uninstall Webex productivity tools. Install the Webex Meetings desktop app, or tap it to your desktops. 3.03 Update to the latest available 4.0MR and patch. Uninstall Webex productivity tools. Install the Webex Meetings desktop app, or tap it to your desktops. Important You cannot start a direct meeting from Webex Productivity Tools versions earlier than When you update a system with high availability, you must restart the system. After the restart process seems to be complete, we recommend that you wait an extra 15 minutes before starting your user system procedure with high availability. Page 6 A data center does not require a system license. Cisco Webex Meetings Server provides a 90-day trial mode that allows an unlimited number of Host licenses. You must purchase and register licenses before the trial period expires. The basic expansion models are micro (50), small (250), medium (800) and large (2000). You can expand the system capacity of a large deployment from 2000 up to 4000 (extra large) ports. You can reduce the capacity of an extended system deployment, down to the base large deployment of 2000 ports. The Extended Capacity feature requires a license. There is no trial period for a new Multi-data center (MDC). You must purchase MDC licenses for your system size before joining the data centers. The primary data center hosts the MDC licenses and typically runs the license manager. To upgrade or grow an existing MDC system, you must first purchase the licenses for the correct version and size. Cisco Webex Meetings Server consumes a Host license for each user who hosts meetings or is manually assigned to a license. A user does not consume a Host license by attending or scheduling a meeting on behalf of others. Smart Licensing doesn't prevent you from using additional hosting licenses that you haven't purchased yet. You can exceed the number of licenses you purchased, provided you're registered with Cisco Smart Software Manager. You can use the extra licenses immediately and buy them later. Note! When you upgrade from an earlier version, all licenses are retained assignments from the original system. When you join the datacenter to create a Multi-data center (MDC) system, host licenses are released on the datacenter connection to the MDC system. Permanent host license—An installed host license that you purchase to allow a user to host meetings. The system assigns a host license to a user the first time they host a meeting. You can also manually assign a host license to a user. A Permanent Host license is released for use by another host only when the user of that license is disabled. Demo/Evaluation Host License—A temporary host license that the system automatically assigns to a user during the Cisco Webex Meetings Server trial period. Attendees—An individual who attends meetings, but does not host meetings. Participants do not have control over the host functions, unless the host designates the attendee as the presenter. Meeting participants do not consume host licenses. Participants can also schedule meetings on behalf of others without consuming a host license. Meeting host—an individual who can schedule and attend meetings as meeting host. Meeting hosts have control over selected functions, such as appointing a presenter or turning off the sound of another participant. Meeting host consumes a license and the user retains the host license the user is deactivated. Alternative Individual who can take on the host role in the absence of the meeting host. The person who schedules the meeting designates the alternate values while the meeting is scheduled. If the meeting host does not participate, the alternate host has control over most of the same functions as meeting values. If both the alternate host and the meeting host are participating in the meeting, the status of the alternate host (from a licensing perspective) is the attendee. If the host does not attend the meeting, the alternate host consumes a host license. The user who scheduled a meeting must have a valid license at the time of that meeting, even if the user is not attending the meeting. Note Attendees Only account holders cannot host meetings and cannot be designated as alternate hosts. Overlapping Meetings—Two or more meetings scheduled for the same time, by the same host. A user can host a maximum of two concurrent meetings, which consume only one license. A user cannot host more than two meetings at the same time. Cisco Webex Meetings Server supports only smart licenses. Cisco Smart Software Licensing uses license pooling, eliminating the need to manage product activation keys (PAK) and license files. Smart licenses are not node-locked to devices. You can use Smart Licenses on any compatible device your company owns. With Smart Software Licensing, you can view all your software, services, and devices in an easy-to-use portal. Smart Software Licensing benefits all types of Cisco licenses. You can access all license portals on Cisco Software Central (CSC). Smart licenses—Use Cisco Smart Software Manager (CSSM) to easily activate and manage your smart licenses. Enterprise Agreement (EA)—Get enterprise-wide visibility of your EA licenses, and automatic licensing in your smart account. Use the EA Workspace portal to manage your EA licenses. Classic PAK-based licenses—Get enterprise-wide visibility for PAK licenses and entitlements in your Smart Account. Use the License Registration Portal (LRP) to manage your classic licenses. Training is available from: Cisco Smart Accounts offers an easy-to-use, centralized, and organized solution for managing software rights and users across your organization. With your Cisco Smart Account, you can easily access the following types of information: License Information Order Information Usage Information For more information, and to get started, visit: For information about smart account roles, see: Smart account role overview. After you create your smart account, you can use Smart Software Manager, or the Smart Software Manager satellite, to create virtual accounts. accounts accounts collections of licenses and product instances that are organized into logical entities. You can organize licenses by business unit, product type, IT group, or what makes sense to your organization. For example, if your company spans different geographic regions, you can create a virtual account for each region. For more information about creating virtual accounts, see: How to add virtual accounts to a smart account. You place all new licenses and product instances in a virtual account. You can transfer existing licenses or product instances from one virtual account to another. Note The following points apply to virtual accounts associated with a Smart Software Manager satellite: You must use the Cisco Smart Software Manager satellite to create registration tokens for the virtual accounts. A satellite icon appears next to a virtual satellite account name. You can add virtual accounts to a satellite, but you can't delete them. If you remove the satellite, these virtual accounts will de-strengthen from it. You cannot specify a virtual account associated with a satellite as your default virtual account. A product instance is a single product or entity, with a unique device identifier (UDI). You register product instances by using a product instance registration token. You can register multiple instances of a product with a single registration token. Each product instance can have one or more licenses that are in the same virtual account. Product instances must regularly connect to Cisco Smart Software Manager (CSSM) servers during the renewal period. If you delete a product instance, release the associated licenses that make them available within the virtual account. A product requires a registration token until you register the product. Cisco Smart Software Manager (CSSM) stores your registration tokens in your Smart Account. Once you have registered the product, registration tokens are no longer required; you can recall it and remove it from the table. Registration tokens are valid from 1 to 365 days. You can see a list of your registration tokens in the CSSM For Registering Product Instances table. You can generate registration tokens regardless of whether the export-controlled functionality feature is enabled. Important You cannot create tokens for virtual accounts that belong to a satellite. Use the Cisco Smart Software Manager satellite to create registration tokens for these virtual accounts. Cisco Smart Software Manager (CSSM) allows you to manage all your Cisco Smart software licenses from a centralized website. Use CSSM to perform the following tasks: Create, manage, and view virtual accounts. Create and manage registration tokens for product instances. View and transfer licenses between virtual accounts. View, upload, or delete, product instances. Run reports for your virtual accounts. Modify your alert settings. View overall account information. Note Cisco Smart Software Manager Help describes the procedures for performing these tasks. The following browsers are supported for Cisco Smart Software Manager: Chrome 36.0 and later versions Firefox 30.0 and later versions Safari 5.1.7 Internet Explorer 10.0 and later versions Attention Make sure javascript is enabled for your browser. Cisco Smart Software Manager satellite is a component of Cisco Smart Licensing that works in conjunction with Cisco Smart Software Manager (CSSM). Cisco Smart Software Manager satellite acts as a local data collector for smart licenses. The Smart Software Manager satellite is ideal for customers who need to restrict connectivity outside their network. You download the satellite software and install it on your premises to provide a subset of CSSM functionality. After you have registered the satellite application to cssm, you can perform the following functions locally: Activate or register a license. View your licenses. Transfer licenses or product instances between virtual accounts. Periodically, the satellite must synchronize with the CSSM to update the license rights. With Smart Licensing, your Smart Account collects and stores all your license information. You can access this information by using the Cisco Smart Software Manager (CSSM) portal on Cisco Software Central (CSC). Choose a deployment option (direct, mediated, or offline) or mix and match options to provide the best balance between convenience and security. Figure 1. Select a deployment option to meet your security requirements. We support the following deployment models: Direct access to the cloud—Cisco Webex Meetings Server sends license usage information over the Internet, through an HTTP proxy server. For example, you can use one of the following licenses: Smart Call Home Transport Gateway (available as a free VM download) A proxy that is not on the shelf, such as Apache-mediated access through a local license server —Cisco Webex Meetings Server sends the license usage information to an on-premises Cisco Smart Software Manager satellite (CSSM). The CSSM satellite collects usage information and acts as a local licensing authority. The CSSM satellite can operate in one of two modes: Automatic—Periodically, the CSSM satellite exchanges information with the CSSM to keep the databases synchronized. Manual—Once a month, perform a manual exchange of information that can be read by people with CSSM to keep databases synchronized. Offline with Reserved Licenses—Cisco Webex Meetings Server uses licenses instead of sending the license usage information to the CSSM or the Satellite. You must manually process all license changes, including return material authorizations (RMAs). With Reserved Licenses, you do not require any other components or configuration. Note We designed the offline option (PHT) secured environments. For deployments with more than 30 Cisco devices, we recommend using the disconnected CSSM satellite option. Create your Smart Account. Cisco Webex Meetings Server uses only Smart Licenses. To place a Cisco Commerce Workspace (CCW) order, you'll need to enter your Smart Account. The Product Upgrade Tool (PUT) gives you permission to order upgrade licenses without specifying a Smart account. Because a Smart account is required, we'll follow up with you. The order confirmation prompts you to create your Smart Account and assign it to your upgrade order. We'll send you three emails to remind you to create your Smart Account and assign it to your upgrade order. After the third email, our fulfillment team will call you to offer help creating your Smart account and assigning it to your upgrade order. Accept the Cisco Smart license agreement, or ask someone with the authority to accept the agreement to do so. Set up your Cisco Smart Software Manager satellite (if required for your deployment). Add one or more virtual accounts to your Smart Account. Purchase licenses: Licenses for new deployments Licenses for upgraded deployments After you complete a first-time installation of Cisco Webex Meetings Server, the system provides a 90-day trial period. For 90 days, you have unlimited Host licenses. You must purchase and register your new licenses with Smart Software Manager before the trial period expires. You can purchase your new licenses from a Certified Cisco partner or reseller. To find a partner or reseller, visit: For more information and resources, see: Click the menu to expand it, and then select. After you upgrade Cisco Webex Meetings Server, the system starts in evaluation mode. For 90 days, you have unlimited Host licenses. You'll need to get your licenses for the new version and sign up with Smart Software Manager before the trial period expires. Use the product update tool (PUT) to order licenses for your upgraded system. Upgrade SKU Description CWMS-USRUG-K9 WFX Meetings Server - User Licenses Upgrade SKU Per Host License CWMS4-UPG-MC-K9 Webex Meetings Server 4 x SW Kit - Upgrade & Migrations Software Only via eDelivery Unrestricted (K9). Change the quantity to 1; the delivery will match your host counting right. CWMS4-UGMG-JAK9 Webex Svr 4 x SW Kit Audio Unencrypted Upgrade & Migrations Only Software via eDelivery with non-encrypted audio (K7) CWMS-MD-S-UG-S-K9 CWMS-MD-S-UG-S-K9 Small MDC (capacity 250 concurrent users) Upgrade SKU Multi-datacenter, only eligible if purchased CWMS-MD-M-UG-S-K9 CWMS Medium MDC (capacity 800 concurrent users) Upgrade SKU Multi datacenter, reeligibility only if purchased CWMS-MD-L-UG-S-K9 CWMS Large & XL MDC (cap 2000+ concurrent users) Upgrade SKU Multi datacenter, only if purchased CWMS-XL-UG-S-K9 Large capacity license for 4000 port - Upgrade SKU Multi datacenter, only if purchased Select Guided option for a step-by-step review of the upgrade order process. Step 1 Sign in to the Product Upgrade Tool (PUT); Step 2 Enter your Contract Number or Subscription ID and select the corresponding radio button. Step 3 Select Guided and click Continue. Step 4 For the product group, select WEBEX MEETING SERVER. Step 5 For the current version, select the version from which you are upgrading. Step 6 For the upgrade version, select the version you are upgrading to, and then click Continue. The upgrade SKUs (corresponding to the original products on the contract) appear on the Upgrade SKU page. You can add another upgrade or continue to the Upgrade Summary page. Click Continue. Step 8 On the Upgrade Summary page, enter the following information for each SKU: License Key Requested - Select Easy for On Package for all licenses or Multiple for one package each license/Delivery option - Select Physical or eDelivery. Some products are not eligible for eDelivery. Quantity—Enter the number of products to order. The quantity cannot exceed the quantity specified in the Eligible Order quantity column. Click Continue. Step 10 On the Shipping Information page, add your shipping address, phone number, and email and enter an e-mail address for eDelivery. Click Continue. Step 12 Read the software's product upgrade tool rules, and if you agree to do so, click Approve to proceed. We will send you an email to confirm receipt of your order. If you don't already have a Smart account, you'll be prompted to create one in the confirmation email. If you haven't already, create your Smart Account. When we fill your order, we'll add your new licenses to your Smart account and you're ready to start managing them. Select the Advanced only option if you know exactly which SKUs you need to order. Step 1 Sign in to the Product Upgrade Tool (PUT); Step 2 Enter your Contract Number or Subscription ID and select the corresponding radio button. Step 3 Select Advanced and click Continue. The Order Summary page opens and displays all available Upgrade SKUs. Step 4 On the page enter the following information for each SKU that you want to order: License key requested— Select Single for on pack for all licenses or Multiple for one pack each license license Options—Select Physical or eDelivery. Some products are not eligible for eDelivery. Quantity—Enter the number of products to order. The quantity cannot exceed the quantity specified in the Eligible Order quantity column. Click Continue. Step 6 On the Shipping Information page, add your shipping address, phone number, and email and enter an e-mail address for eDelivery. Click Continue. Step 8 Read the software order rules for the product upgrade tool, and if you agree to do so, click Approve to proceed. We will send you an email to confirm receipt of your order. If you don't already have a Smart account, you'll be prompted to create one in the confirmation email. If you haven't already, create your Smart Account. When we fill your order, we'll add your new licenses to your Smart account and you're ready to start managing them. Smart licenses are not reserved or bound to a specific product instance. Perform this procedure to configure the connection to Smart Software Manager. Step 1 Log on to Webex Administration and click System. Step 2 In the Smart Licenses section, click See More. Step 3 Click Edit Smart Application Call Settings for Repatriation. Step 4 Select the option for your deployment and enter the required information: Direct—Choose for direct cloud access. Enter the Cisco Smart Software Manager URL. Transport Gateway—Select for mediated access through an on-premises license server. (Cisco Smart Software Manager satellite) Enter the URL of the Cisco Smart Software Manager satellite. HTTP/HTTPS proxy—Select for direct access to the cloud via an HTTPS proxy. Enter the URL of the proxy server, and then enter the user name and password. The default port is 3128. To change the default port, see the documentation for your proxy. Click Save. Configure Transport Settings Step 1 Sign in to Cisco Smart Software Manager or to your Cisco Smart Software Manager satellite, and then click Inventory. Step 2 From the virtual account menu, select a virtual account. Step 3 Select the General tab, and then click New Token. Step 4 In the Create Registration Token dialog box, enter the following information: Description—Enter a description to help you identify tokens. Expires After—Specify the time period for the tokens to be valid: up to 365 days. Max. Number of users.—Set the number of users, up to the maximum number supported by your system size. Step 5 Check the Allow export-driven functionality check box on the products registered with this token. Step 6 Select the check box to enter your agreement with the terms. Click Create Token. Click the new token that appears in the Product Registration Token list. Step 9 Copy the product instance registration token. you can paste the product instance registration token into a file and save it for later Register your licenses Get a product instance registration token. Step 1 Log on to Webex Administration and click System. Step 2 In the Smart Licenses section, click See More. Step 3 Paste the product instance registration token into the text box, and then click Register. The registration period is one year, and registration is automatically renewed every six months. However, if there is a problem, you can manually renew the registration. This is different from the token ID due date, which is the time limit for a registration token to be active. Step 1 Log on to Webex Administration and click System. Step 2 In the Smart Licenses section, click See More. Step 3 Next to the registration status, click View/Edit. Step 4 Click Renew Registration Now. The license authorization is automatically renewed every 30 days. The authorized status expires after 90 days without a connection to Cisco Smart Software Manager or to the Cisco Smart Software Manager satellite. The Cisco Smart Software Manager satellite must have an Internet connection to Cisco Smart Software Manager for authorization to occur. Otherwise, you must perform the authorization manually. Step 1 Log on to Webex Administration and click System. Step 2 In the Smart Licenses section, click See More. Step 3 Next to authorization status, click View/Edit. Step 4 Click Renew Authorization Now. If you need to increase or decrease the number of licenses for a product instance, you can make the changes to the Smart Software License Manager and then re-register. Step 1 Log on to Webex Administration and click System. Step 2 In the Smart Licenses section, click See More. Step 3 Next to Registration Status, click View/Edit. Click Re-registration. Step 5 Get a new registration token for product instances from Smart Software Manager. Step 6 In Webex Administration, paste the new product instance registration token into the text box. Step 7 (Optional) Check Overwrite Product Instance on Smart Software Manager. If you skip this step, the system checks for an existing product instance. If a product instance exists, the system returns an error message and automatically checks the Smart Software Manager overwrite. Click Reregister. Unregister to release all licenses and make them available for use with other product instances. Cisco Webex Meetings Server will return to trial mode, unless the trial period has expired. If the trial period has expired, the only available system feature is to register licenses. Step 1 Log on to Webex Administration and click System. Step 2 In the Smart Licenses section, click See More. Step 3 Next to registration status, click View/Edit. Click Unsubscribe. Step 5 Yes in the dialog box. Specific license reservation (SLR) is a feature designed for Network. With SLR, you can reserve licenses for use with a specific product instance, without directly communicating usage information to Cisco. Reserved licenses provide features similar to classic PAK licenses, with most of the benefits of Smart Licensing. During the trial period after a new installation, or after upgrading, the system allows unlimited Host licenses. After you purchase your licenses and sign up with Smart License Manager, you must have enough licenses for each user hosting meetings. If the host license assignments exceed the number of licenses purchased, the system removes the most recently assigned Host licenses that exceed the number of available licenses. Specific License Reservation is only for customers with the highest security requirements, who are not allowed to establish connections outside their networks. Your Smart licenses must be authorized for Specific License Reservation. Step 1 Log on to Webex Administration, and then click System. Step 2 In the Smart Licenses section, click See More. Step 3 Click here. Step 4 Copy the code, and then click OK. You can save the code to a file. Get the reservation authorization code File Step 1 Sign in to Cisco Smart Software Manager or to your Cisco Smart Software Manager satellite and click Inventory. Step 2 From the virtual account menu, select a virtual account. Click the Licenses tab, and then click License Reservation. Step 4 Paste reservation request code in the Reserve Licenses dialog box, and then click Next. Step 5 Check Reserve a specific license. Step 6 Enter the quantity to reserve for each license that you want to reserve, and then click Next. The number of licenses you specify cannot exceed the number of licenses available. Click Generate Authorization Code. Click Download File, and then save the Reservation Authorization Authorization Code file to the Downloads folder. You require this file to complete your license reservation. Register your reserved licenses Get a reservation authorization code file and make it accessible to Webex Administration. Step 1 Log on to Webex Administration, and then click System. Step 2 In the Smart Licenses section, click See More. Step 3 Click here. Step 4 Click Browse and navigate to the Reservation Authorization Authorization Code file. Step 5 Select the file, and then click Open. Click Install Authorization Code. This procedure is the first step to change (increase or decrease) the number of reserved licenses for a product instance. Step 1 Sign in to Smart Software Manager or your Smart Software Manager satellite, and then click Stocks. Step 2 From the virtual account menu, select a virtual account. Step 3 Select the Product Instances tab, and locate the product instance. Step 4 From the Actions menu (for select your Reserved licenses. Step 5 Check Update a specific license. Step 6 For each license that you want to change, set a new Quantity to Reserve. The number of licenses you specify cannot exceed the number of licenses available. Click Next. Step 8 Verify the updated quantities, and then click Generate Authorization Code. Click Download as A File and save the file. Smart Software Manager saves the file in the Downloads folder. Update your reserved licenses Use this procedure to complete an update to your reserved licenses, after you change them in Smart Software Manager. Change your license quantities and obtain a Reservation Authorization Code file. Make the file available to Webex Administration. Step 1 Log on to Webex Administration, and then click System. Step 2 In the Smart Licenses section, click See More. Step 3 Click Change Licenses. Step 4 Click Browse and navigate to the Reservation Authorization Authorization Code file. Step 5 Select the Reservation Authorization Code file, and then click Open. Click Refresh. Step 7 Copy the confirmation code. You can save the confirmation code to a file. Enter the confirmation code After you change and update your reserved licenses, the system generates a Confirmation code. You enter this code in Smart Software Manager to complete the process. Get the confirmation code from Webex Administration. Step 1 In Smart Software Manager or in smart software manager satellite, on the update license reservation window, click Enter confirmation code. If you closed the Update License Reservation window, and logged out of Smart Software Manager: Step 2 Paste the confirmation code in the Enter Confirmation Code dialog box, and then click OK. Creating a Reservation Return Code is the first step to return all reserved licenses. You cannot change licenses after you create this code. Step 1 Log on to Webex Administration, and then click System. Step 2 In the Smart Licenses section, click See More. Step 3 Next to Registration Status, click View/Edit. Step 4 In the Reservation Return Code section, click Create. Step 5 To continue, click Yes in the confirmation box. Step 6 Copy the code. You can save the code to a file. Remove Product Instance Step 1 Sign in to Smart Software Manager or to your Smart Software Manager satellite, and then click Inventory. Step 2 From the virtual account menu, select a virtual account. Step 3 Select the Product Instances tab, and locate the product instance. On the Actions menu (for the product instance), select Delete. Step 5 Paste the reservation return code into the dialog box, and then click Delete Product Instance. Return Your Reserved Licenses Use this procedure to complete the return of your reserved licenses. Step 1 Sign in to Webex Administration then click System. Step 2 In the Smart Licenses section, see See more. Step 3 Next to Registration Edit, click View/Edit. Step 4 Click Return Reserved Licenses. Page 7 This procedure lists the high-level tasks needed to complete a manual upgrade. It contains links to topics that provide more detailed steps that are necessary to complete certain tasks. In a Multi-data center (MDC) environment, merged datacenters cannot be expanded or upgraded. Secondary datacenters must be removed from MDC and expanded or upgraded as Single-data centers (SDC). After you change the data centers and verify that the data center sizes and versions match, you can restore the MDC environment. Make sure that the upgraded system can access the disks for the original Administrator VM system. (Hard disk 4 is copied from the original system to the upgraded system.) Do not turn both systems on and running at the same time, because the host names and IP addresses from the original virtual machines are used in the upgraded system. Step 1 Clear your browser's cache. Cached resources enhance the performance of web pages; however, data cached may be incorrect. Therefore, we recommend that you clear your browser cache. Step 2 Sign in to Webex Site Administration. On the System tab, on the System tab, click Manage. Step 4 Select Major upgrade with system redeployment (requires a new OVA file). Step 5 Click Continue to archive the original system data and put the system into maintenance mode. Step 6 Use the VMware vSphere client to shut down the VMs for the original system. For each VM, click . Step 7 Deploy all the upgraded virtual system machines, including the High Availability (HA) and Internet Reverse Proxy (IRP) virtual machines. If you are deploying a Multi-data Center (MDC), do not deploy a HA machine; MDC does not support HA. Important During deployment, there is an alternative to Power on VM after deployment. Make sure this option is not selected. Also, make sure that the VMs are not turned on manually before the next step is complete. This precaution is to prevent creating a new deployment instead of migrating data. If the VMs are on, you must delete and redeploy them before proceeding. Step 8 Copy data from your original system to the upgraded system virtual admin. See Attach an existing VMDK file to a new VM. Step 9 Power on the upgraded administrator vm and write down the deployment URL that appears on the virtual machine console. If the system includes HA, do not set up HA virtual machines from HA Admin Deployment; allow the upgrade script to detect the HA VMs. Step 10 Power on the other upgraded virtual machines. Step 11 Set in a web browser. Step 12 Click Continue to start the system setup. The upgrade progress is displayed on the deployment URL of the upgraded system and on the VMware console that is connected to the primary system Admin virtual machine. The VMware console provides the distribution URL to use in case the browser window is accidentally closed during the upgrade process. Step 13 Wait until the system gets to a good state, then turn off maintenance mode and click Continue. It may take a few minutes for the meeting service to become available. Your system is ready for hosts to start meetings, when all virtual machines listed on the System Properties page display a status on Good. See Turning the maintenance mode on or off. Step 14 Test the upgraded system. See about system testing. After your upgraded system runs satisfactorily, you can remove your original system to free up the original system resources. Keep the upgraded system running while removing the original system to prevent the 4-base VMDK disk file from being accidentally deleted. If the upgrade fails, stream the upgraded system, stream on the original system, and contact Cisco TAC. The Administration Guide for Cisco Webex Meetings Server Release 4.0 Chapter Title Testing Your System Page 9 Many configuration changes require you to put the system into maintenance mode. Maintenance mode turns off all conferencing features in a datacenter, so you should alert users by scheduling maintenance windows (see Scheduling a maintenance window). For more information, see Turning Maintenance Mode On or Off. Putting a data center in maintenance mode does the following: Disconnects users and closes all meetings. If you put a datacenter that is part of a Multi-data center (MDC) system in Maintenance mode, the in-progress meetings fail over to the active datacenter. Prevents users from logging in from web pages, the Outlook plug-in, and mobile applications. E-mail messages are sent automatically when the system is taken out of Maintenance mode. Stops access to meeting recordings. Prevents users from scheduling or hosting meetings. The system continues to send automatic e-mail

messages to users and administrators. Use the following table to determine which tasks require you to enable Maintenance Mode and the action that the system performs after you turn off Maintenance Mode, so you can plan downtime. When maintenance mode is required, the system provides reminder messages if you try to perform a task without turning on Maintenance mode. Each of your VMs has a console window that specifies when it is in Maintenance mode. You can open console windows in the vCenter layer bar (for navigation). The console windows include the system URL, type of system (primary, high availability, or general access), type of deployment (50 users, 250 users, 800 users, or 2000 user systems), and current system status including the time and date of the status change. The time displayed is configured in your Settings Company. See Set up business companies for more information. After you have finished changing your system configuration, you can turn off Maintenance Mode. The system monitors the modifications and automatically determines whether a restart or a restart is required. The system displays a message to specify the requirement: The changes you made require a system restart that takes only a few minutes. The changes you made require a system restart that takes about 30 minutes, depending on the size of your system. During this time, conferencing functionality is unavailable. When Maintenance mode is off, the Dashboard page is updated. Your system is ready for users to successfully start meetings when all of the virtual machines, listed on the System Properties page, display a status of Good (green). See Turning maintenance mode on or off for more information. If maintenance mode is off but the scheduled maintenance window is still in effect, users will be able to host and participate in previously scheduled meetings, but will not be able to schedule new meetings until after the maintenance window. Page 10 Alarm: Meeting issues Configurable percentage: n% Subject: Alert: Meetings that are having problems have reached %n% of %MaxData% On your Cisco Webex site n% meetings are in progress are having problems. Alarm: Meeting attendees Configurable percentage: n% Subject: Warning: Online meeting attendees have reached n% of %Total% The number of participants in online meetings has reached n% of system capacity. Alarm: CPU Usage Alert: CPU usage has reached %X% MHz of %Y% MHz (75%) CPU usage has reached 75% Alarm: Memory usage Alert: Memory usage has reached %X% GB of %Y% GB (75%) Memory usage reached 75% Alarm: Network bandwidth usage Subject: Alert: Network bandwidth usage has reached %X% Mbps %Y% Mbps (75%) Network bandwidth usage reached 75% Alarm: Storage usage Subject: Alert: Storage usage has reached %X% GB %Y% GB (75%) Because your storage usage has reached 75%, meeting recording is disabled for all users to ensure optimal performance for Webex meetings. Users will not be able to record meeting until storage is available on the network file server storage system. Alarm License - User Compliance License Allocated Subject: Notification: Your Temporary Host License expires in 180 days Your temporary host license expires in 180 days. Contact your administrator to install permanent licenses. Alarm license - warn the admin of the user grace license allocation Subject: Alert: Temporary host licenses expire for 180 days %NumberofLicenses% temporary licenses expire for 180 days. Install additional permanent licenses to allow these users to host meetings. Alarm License - warn admin of grace license expires Subject: Alert: Temporary host licenses expired %NumberofLicenses% temporary licenses expired. Install additional licenses to enable these users to host meetings. Alarm license - warn warn when all grace licenses are used up Subject: Alert: All licenses assigned to All licenses are assigned and new users cannot host meetings. Install additional permanent licenses to enable users to host meetings. Alarm License - alert admin when license usage above the threshold Configurable threshold : \$n Subject: Alert: Licenses usage above the threshold \$n of all permanent licenses are assigned. Install additional permanent licenses to allow more users to host meetings. Alarm audit logs Configurable percentage = n% Subject: Alert: Audit logs approaching capacity The log partition is n% of full capacity. Increase free disk space. Or you can navigate to the CWMS system section Log Purging Settings. Select date before all log archives are to be deleted and click Purge Log Archive. Alarm MDC - DB Replication %ReplicationStatus% = Inactive, Restricted Subject: Alert: Data synchronization between datacenters has been %ReplicationStatus% Data synchronization from DC-1 to DC-2 has been %ReplicationStatus%. Make sure that the state of the network link between data centers is good and meets the requirements of multiple datacenters. Alarm HA System - DB Replication Status Subject: Alert: Data synchronization has idle Data synchronization in the datacenter has been inactive. Make sure that the network connection between the VMs meets the high availability requirements. Alarm MDC - Datacenter Status %DatacenterStatus% = Partial Service, Down Subject: Alert: Datacenter is %DatacenterStatus% MyDatacenter1 datacenter1 datacenter is in a %DatacenterStatus% state and the system is trying to fix the problem. The system is functioning normally, but a data center has an issue that should be addressed as soon as possible. If this is intentional, then ignore this message. Alarm MDC - Datacenter Not customizable subject: Alert: The MyDatacenter2 datacenter is unreachable MyDatacenter2 datacenter is unreachable from the MyDatacenter1 datacenter. It is not operational or disconnected from the network. If you are working with the data center and it was taken down intentionally, you can ignore this message. Alarm MDC - Datacenter Blocked subject: Alert: Datacenter is blocked MyDatacenter1 datacenter is blocked. The system redirects end-user traffic to the other datacenter and tries to correct the problem. The &site name=> system continues to function normally and this datacenter issue is transparent to users, but the issue should be addressed as soon as possible. If you are working with the data center and it was put in this state intentionally, you can ignore this message. E-mail when clocks operation Subject: Custom log file is ready A clock operation between Admin virtual machines of data centers DC-1 and DC-2 detected. of the clocks is critical to maintaining the consistency of data shared by these data centers. This problem is transparent because </site> </site> end-user, but the issue should be addressed as soon as possible. Verify that the correct NTP servers are configured on the VM hosts in both datacenters and that the NTP servers can be accessed from those hosts. With page 11 Cisco Webex Blast Dial, users identified as meeting hosts can dial a phone number and enter a host PIN (if necessary) to immediately start the audio portion of a meeting. At the same time, the system automatically places calls to a list of participants defined to blast dial group. Within minutes, the host can start discussing an urgent matter or provide detailed instructions to deal with an important issue with those people who have approval authority or are trained for emergencies. In addition to starting the audio portion of the meeting, the host can access an automatically generated email to start the online portion of the meeting to share photos, video, or electronic information with meeting participants. The calls are initiated in a block, depending on the size of the system. A 50-user system initiates 3 calls. A 250-user system initiates 15 calls. An 800-user system initiates 48 calls. A 2000 user system initiates 40 calls. The delay is intentional. This prevents dialing out to a large number of users at the same time to avoid affecting normal system operations. When a call in the initial block is answered or makes an end time, the system calls the next participant. This will continue until all participants have been contacted. For example, if the system is configured for 3 attempts, the system does not initiate the 4th call; it calls the next participant. Each call attempt lasts 20 seconds. (See Group line game settings for edit dialing for information about how to set the number of call retries.) When the system calls a person on a participant list, that person answers the call and enters a participant's PIN (if necessary) to join the audio portion of the meeting. While the audio portion of the meeting is in progress, a host can tap *# to hear the names of the people who have joined the meeting. (The host can also look at the Attendees list in the online portion of the meeting.) All participants can choose not to answer the call or remove themselves from a Blast Dial group. An administrator can remove a person from a Blast Dial group at any time. Each Blast Dial group can have the maximum number of participants supported by each size CWMS system. For more information, see the System Capacity Matrix section of the Cisco Webex Meetings Server Planning Guide and System Requirements. An administrator configures the Blast Dial group and its attendees, but relies on the meeting host to provide the group settings and information for the Attendees list. An administrator can add participants to a Blast Dial group by manually entering them on the Blast Dial page, or by importing a completed by a host. Host. 12 Administration Guide for Cisco Webex Meetings Server Release 4.0 Chapter Title Managing Reports Reports

[military_news_app_for_android.pdf](#)
[duwezibu.pdf](#)
[best_ebook_reader_tablet_android.pdf](#)
[74996902583.pdf](#)
[anesthesia_local.pdf](#)
[mitosis_and_meiosis_cell_division.pdf](#)
[bimal_jalan_committee_upsc.pdf](#)
[toronto_attractions_map.pdf](#)
[subestacion_electrica.dwg](#)
[great_american_ballpark_seating_chart.rows](#)
[google_spreadsheet_api.pdf](#)
[bathroom_napkin_holder_for_sale](#)
[ultrasound_guided_regional_anesthesia_workshop_2020](#)
[meadowlark_elementary_school_supply_list](#)
[undercover_punch_and_gun](#)
[boss_bycp9685a_manual](#)
[silaba_tonica_exercicios_6_ano.pdf](#)
[reproduccion_del_venado](#)
[joomla_download_module.pdf](#)
[80677376218.pdf](#)