



Import/Export

You can use the Import/Export menu in Cisco Unified Communications Manager Bulk Administration Tool (BAT) to export or import parts of the Cisco Unified Communications Manager database to another server, or to the same server with modifications. This reduces the configuration time that is required by importing a preconfigured database to the installed Cisco Unified Communications Manager server.

The following topics provide procedures for carrying out these tasks:

- [Exporting Configuration, page 62-1](#)
- [Editing the .tar File, page 62-7](#)
- [Importing Configuration, page 63-1](#)

Exporting Configuration

To export configuration data from Cisco Unified Communications Manager, use the following procedure.



Note

You cannot export VPN details through Import/Export if you are using the U.S. export unrestricted version of Cisco Unified Communications Manager.

Procedure

Step 1 Choose **Bulk Administration > Import/Export> Export**.

The Export Data window displays.

Step 2 In the Job Information section, enter the .tar file name, without the extension, in the Tar File Name field. BPS uses this filename to export the configuration details.



Note

All files that are exported at the same time get bundled together (.tar) and can be downloaded from the server.

Step 3 In the Select items to Export section, check the appropriate check boxes under System Data from the following options:

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Group

- Date/Time Group
- Device Pool
- Enterprise Parameter
- Location
- Phone NTP Reference
- Region
- Server
- Service Parameter
- SRST
- Security Profile (Phone & SIP Trunk)
- Physical Location
- Device Mobility group
- Presence Group
- LDAP System
- Device Mobility Info
- DHCP Server
- DHCP Subnet
- Application Server
- LDAP Directory
- LDAP Authentication
- MLPP Domain
- Resource Priority Namespace Network Domain
- Resource Priority Namespace List
- CUMA Server Security Profile
- Geo Location
- Geo Location Filter
- Enterprise Phone Configuration
- Certificate
- LDAP Custom Filter

Step 4 Check the appropriate check boxes under Call Routing Data from the following options:

- Application Dial Rules
- CSS (Class of Control)
- Partitions (Class of Control)
- Route Filter
- Time Period (Class of Control)
- Time Schedule (Class of Control)
- Translation Pattern
- AAR Group

- Forced Authorization Codes
- Directory Lookup Dial Rules
- Client Matter Codes
- Call Park
- Call Pickup Group
- Directory Number
- MeetMe Number
- Cisco Attendant Console Pilot Point
- Directed Call Park
- SIP Dial Rules
- Line Group
- Route Group
- Hunt List
- Route List
- Hunt Pilot
- Intercom Route Partition
- Intercom CSS
- Access List
- Route Pattern
- Called Party Transformation Pattern
- SIP Route Pattern
- Intercom Directory Number
- Intercom Translation Pattern
- Calling Party Transformation Pattern
- Time Of Day Access
- Logical Partition Policy
- CCD Requesting Service
- Hosted DN Group
- Block Learned Patterns
- Hosted DN Patterns
- CCD Advertising Service
- External Call Control Profile
- Transformation Profile
- CCD Feature Configuration
- CCD Partition
- Mobility Profile Configuration
- Handoff Configuration
- Enterprise Feature Access Configuration

Step 5 Check the appropriate check boxes under Media Resources from the following options:

- Annunciator
- Conference Bridge
- Media Resource Group
- Media Resource Group List
- Media Termination Point
- Transcoder
- MOH Server
- Mobile Voice Access

Step 6 Check the appropriate check boxes under User Data from the following options:

- SIP Realm
- Application User
- User Group
- Role
- Application User CAPF Profile
- Credential Policy Default
- Credential Policy
- End User
- End User CAPF Profile

Step 7 Check the appropriate check boxes under Device Data from the following options:

- Softkey Template
- Gate Keeper
- Trunk
- SIP Profile
- Phone Services
- Phone Button Template
- Common Phone Profile
- Gateway
- Device Defaults
- Device Profile
- Common Device Configuration
- CTI Route Point
- Phone
- Recording Profile
- Remote Destination
- Remote Destination Profile
- Feature Control Policy
- Default Device Profile

- SIP Normalization Script

Step 8 Check the appropriate check boxes under Advanced Features from the following options:



Note

The check boxes for VPN Profile, VPN Gateway, VPN Group, and VPN Feature Configuration do not appear if you are using the U.S. export unrestricted version of Cisco Unified Communications Manager. You cannot export VPN details through Import/Export if you are using the U.S. export unrestricted version of Cisco Unified Communications Manager.

- Message Waiting Numbers
- Voice Mail Pilot
- Voice Mail Profile
- Voice Mail Port
- SAF Forwarder
- SAF Security Profile
- EMCC Remote Cluster
- EMCC Intercluster Service Profile
- Intercompany Media Engine Server Connections—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Service—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Service—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Services Trust Element—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Services Enrolled Pattern—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Services Enrolled Group—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Services Exclusion Group—Ensure that the Cisco IME server is installed and available before you configure this field.
- Fall Back Profile—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Services Learned Route—Ensure that the Cisco IME server is installed and available before you configure this field.
- VPN Profile
- VPN Gateway
- VPN Group
- EMCC Feature Config
- Intercompany Media Services Firewall—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Services Exclusion Number—Ensure that the Cisco IME server is installed and available before you configure this field.

- Intercompany Media Services E.164 Transformation—Ensure that the Cisco IME server is installed and available before you configure this field.
- Intercompany Media Services Feature Configuration—Ensure that the Cisco IME server is installed and available before you configure this field.
- Fallback Feature Configuration—Ensure that the Cisco IME server is installed and available before you configure this field.
- VPN Feature Configuration

Step 9 You can use the **Select All** button to check all the check boxes at once and the **Clear All** button to clear all the check boxes.

Step 10 In the Job Description field, enter the description that you want to provide for the job. Export Configuration is the default description.

Step 11 You can choose to run the job immediately or later by selecting the corresponding radio button.

Step 12 To check for interdependency of tables to make sure that the related records are also exported, click **Check Dependency**.



Note You can de-select any of the check boxes after checking dependency. You also have the option to skip checking dependency.



Note Check dependency selects dependent items up to one level of dependency. For example, if an item depends on CSS, then only CSS will be selected and the items that CSS depends on will not be selected.

Step 13 To create a job for exporting the selected data, click **Submit**.

A message in the Status section lets you know that the job was submitted successfully.

Step 14 Use the Job Scheduler option in the Bulk Administration main menu to schedule and/or activate this job. For more information on jobs, see the [Chapter 82, “Scheduling Jobs.”](#)

Log Files

Multiple log files are created for a single export transaction. One for the overall transaction, and one each for the items selected for export. These log files display separate results for each item. The log file name is prepended with the item name, to make it easier to identify the logs.

These files can be accessed from the Job Scheduler page.

Additional Topics

See the [“Related Topics”](#) section on page 62-8

Editing the .tar File

The tar file comprises a list of CSV files and a header file. Header file can be used to refer to the details of the server from where the export was carried out and the time when it was carried out. The header file also has details regarding the files in the package.

If you want to make any changes to the configuration after you have exported the required data, you can do so by editing the exported .tar file by using the following procedure.

Procedure

Step 1 Choose **Bulk Administration > Upload/Download Files**.

The Find and List Files page displays.

Step 2 Download the .tar file that you want to update by using the procedure that mentioned in [“Downloading a File” section on page 2-2](#).

Step 3 Un-tar the .tar file to some location on your machine by using the `tar -xvf` command.

The .csv file gets extracted to the location that you specified.



Note The “tar -xvf” command may not work on a Windows server, TAR and UNTAR operations are possible in Windows using 7-Zip, which is a freeware available on the World Wide Web.



Note The name of the .csv file is always the same as the item name.

Step 4 Use MS Excel to edit the .csv file and save your changes.



Note You can edit the .csv file by using Notepad/Wordpad also, but Cisco recommends using MS Excel to edit the .csv file.

Always maintain the same filename and file format for the .csv file. If you add a new file to the tar package, ensure that the file has the same name and file format as it would have if it is exported from Cisco Unified Communications Manager. Also make sure that the new filename is added to the Header file.



Tip If you are expecting to add a new item, always try to export that item from Cisco Unified Communications Manager, even if there are no records for that item. This will create a .csv file with the correct name and file format.

Step 5 Re-tar the files using the `tar -cvf` command while making sure that the new .tar file is saved in the default common location.



Note The “tar -cvf” command may not work on a Windows server, TAR and UNTAR operations are possible in Windows using 7-Zip, which is a freeware available on the World Wide Web.

**Caution**

The .tar files must maintain the original directory structure when you re-tar the files, because BPS looks for .tar files at the default location only.

Step 6 Upload the .tar file for import by using the procedure that is mentioned in “[Uploading a File](#)” section on [page 2-3](#).

**Note**

Make sure that you select the Target as Import/Export and the Transaction Type as Import.

**Note**

If you decide to use notepad or wordpad for the edit, make sure that you add a comma for every new entry in the file format.

**Note**

Import/Export tool does not support updating the password and pin attributes. They are exported in encrypted form in the exported file and hence it cannot be changed to plain text. Entities which have credentials are—Common Phone Profile, SIP Realm, Application User, LDAP Authentication, LDAP Directory, Cisco Attendant Console, and Enduser. Be aware that you must not modify the User ID, User Pkid, Password, and Pin fields in the enduser.csv in the exported file.

Related Topics

- [Exporting Configuration, page 62-1](#)
- [Editing the .tar File, page 62-7](#)
- [Finding a File, page 2-1](#)
- [Downloading a File, page 2-2](#)
- [Uploading a File, page 2-3](#)
- [Deleting a File, page 2-3](#)
- [Importing Configuration, page 63-1](#)