Performing Administrative Operations

This chapter contains the following sections:

About Administrative Operations

You can perform the following administrative operations using Intercloud Fabric:

- Configure system settings.
- Manage Intercloud Fabric licenses.
- Use Intercloud Fabric VM CLI commands.

Configuring System Settings

System settings allow you to perform the following operations:

- View the configuration and reachability status of DNS and NTP servers configured on various ICF components.
- Enable compliance checking on passwords.

Use this procedure to configure system settings.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Administration** > **System Settings**.
See Icons Used in Intercloud Fabric for information regarding the icons used in Intercloud Fabric.

Step 3 Complete the following fields for **NTP Server**.
NTP servers are configured on ICF components to synchronize time. ICF validates the reachability of the NTP servers.

Name	Description
Preferred NTP Server	Enter the IP address of the preferred NTP server.
Status	The status of the preferred server is displayed.
Alternate NTP Server	Enter the IP address of the alternate NTP server.
Status	The status of the alternate server is displayed.

Step 4 Complete the following fields for **DNS Server**.
DNS servers and domain name are configured on ICF components for hostname resolution. ICF validates the reachability of the DNS servers. You must specify at least one DNS server.

Name	Description
Domain Name	Enter the domain name.
Preferred DNS Server	Enter the IP address of the preferred DNS server.
Status	The status of the preferred server is displayed.
Alternate DNS Server	Enter the IP address of the alternate DNS server.
Status	The status of the alternate server is displayed.

Step 5 Click **Enable compliance check on advance password policy** to enable compliance checking on passwords. The Intercloud Fabric default password policy uses a basic compliance check that allows users to create passwords that do not meet security compliance guidelines. If you enable compliance checking, the password policy ensures that any password that a user creates must:

- Contain 8-64 characters
- Contain characters from at least three of the four classes: lower case letters, upper case letters, digits and special characters such as @, #, or $
- Not be based on a dictionary word
- Not contain characters repeated three or more times consecutively

Step 6 Click **Submit**.

Import Providers

The provider list shows which providers Intercloud Fabric for Business supports. You can update the supported providers by importing the latest provider list from Cisco.com.

Before You Begin

- You have downloaded the latest provider list from Cisco.com.
- Ensure that no service requests are running. You must complete all service requests before you import the provider list.
- Perform this operation during the maintenance window. During this operation, all end user sessions will be invalidated.
- If you have already created an ICF link or virtual account for a supported provider, while importing the latest provider list, ensure that the provider is present in the new provider list being imported.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Administration** > **Providers**.
The list of providers is displayed.

Step 3 Click the import icon to import the latest provider list supported by Intercloud Fabric for Business. Before importing the file, you must download the latest provider list from Cisco.com.

Step 4 To download the provider list, do one of the following:

- From Cisco.com, choose **Download Software for this Product** > **Intercloud Fabric** > **Intercloud Fabric for Business**. Select the file and click **Download**.
- Obtain the URL for the latest provider list from your Cisco partner and download the file.
  Note You cannot overwrite the file from a Cisco partner with a file provided by Cisco.

Step 5 Click **Browse** to import the file from your local drive.

Step 6 Click **Import** to import the provider list to Intercloud Fabric.

Step 7 Restart the services using the ICF CLI. See Using Cisco Intercloud Fabric VM CLI Commands, on page 4.

a) Using SSH, connect to the Intercloud Fabric VM CLI as an administrator.
b) Enter the number 6, and press **Enter**.

Step 8 Log in to Intercloud Fabric UI to view the updated provider list.

Using Cisco Intercloud Fabric VM CLI Commands

The Intercloud Fabric VM CLI console enables you to execute common administrative tasks such as showing service status, stopping and starting services, generating logs, and performing other system-related tasks. You can use the options in the following table to execute the Intercloud Fabric VM CLI commands.

Before You Begin

- Ensure that Intercloud Fabric is installed and running.
- Ensure that you use the password configured during the initial setup.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Using SSH, connect to the Intercloud Fabric VM CLI console as an administrator.

Step 3 Enter the number of the option you want, and press **Enter**.

Option	Command	Description
SELECT> *1*	**Ping Hostname/IP Address**	Runs the basic ping command to check if the IP address or hostname is reachable from the Intercloud Fabric host.
SELECT> *2*	**Show Version**	Displays the Intercloud Fabric host version that is running. See the option 2 example below.
SELECT> *3*	**Show Services Status**	Displays if the following processes are running or not: • tomcat • activiti engine • mongoDb • messaging server
SELECT> *4*	**Start Services**	Starts the following processes: • tomcat • activiti engine • mongoDb • messaging server

Option	Command	Description
SELECT> *5*	**Stop Services**	Stops the following processes: • tomcat • activiti engine • mongoDb • messaging server
SELECT> *6*	**Restart Services**	Restarts the following processes: • tomcat • activiti engine • mongoDb • messaging server
SELECT> *7*	**Show tech-support**	Generates all of the Intercloud Fabric logs in .tgz format and saves them to: `/var/logs/icflogs/techlogxxxxx-xx.tgz`
SELECT> *8*	**Show logs**	Displays all of the available logs in Intercloud Fabric.
SELECT> *9*	**Delete logs**	Deletes the specified log files.
SELECT> *10*	**Copy logs**	Copies the tech-support logs to an external SCP/SFTP server. See the option 10 example below.
SELECT> *11*	**Display Container Details**	Displays details of the Intercloud Fabric controller container. See the option 11 example below.
SELECT> *12*	**Display Network Details**	Displays network configurations for Intercloud Fabric. See the option 12 example below.
SELECT> *13*	**Shutdown Appliance**	Shuts down Intercloud Fabric.
SELECT> *14*	**Reboot Appliance**	Reboots the Intercloud Fabric base VM.
SELECT> *15*	**Launch ICFC console**	Displays the Intercloud Fabric controller console. You must log in as root using the same password configured during the initial setup.

Option	Command	Description
SELECT> *16*	**Upgrade**	Uploads the .tar file for upgrade using SCP from an external server.
SELECT> *17*	**Show Device Password**	Displays the device password used to log in to Intercloud Fabric's internal components. See the option 17 example below.
SELECT> *0*	**Quit**	Quits the CLI screen.

Examples of CLI Options

Option 2

```
SELECT> 2

ICF host version: 2.3.1.693
Press return to continue ...
```

Option 10

```
SELECT> 10
       1. SCP logs to external server
       2. SFTP logs to external server
Enter choice [1 or 2]: 1
Specify file name to be copied [filename.tgz] : techlog20160111-213849.tgz
Specify SCP location [it should be in the form: user@ipaddress:/path/.../path/folder] :
host@198.51.100.254:/home/host/username
The authenticity of host '198.51.100.254 (198.51.100.254)' can't be established.
RSA key fingerprint is 5b:da:4a:e9:1e:e5:4b:31:ea:15:d7:63:5c:4f:5c:c4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '198.51.100.254' (RSA) to the list of known hosts.
host@198.51.100.254's password:
techlog20160111-213849.tgz                    100%  35MB  17.3MB/s  00:02
Press return to continue ...
```

Option 11

```
SELECT> 11
-------- ICFC Container Info --------
Name:           icfc
State:          RUNNING
PID:            2662
IP:             10.0.0.1
CPU use:        675.23 seconds
BlkIO use:      15.99 GiB
Memory use:     4.54 GiB
KMem use:       0 bytes
Link:           veth192RG9
 TX bytes:      932.95 KiB
 RX bytes:      27.17 MiB
 Total bytes:   28.08 MiB
Press return to continue ...
```

Option 12

```
SELECT> 12
Network Configuration for cisco-icf
IPv4 Address:    10.255.255.254
Netmask:         255.255.0.0
IPv4 Gateway:    10.0.0.1
DNS IP:          172.31.255.254
Domain name:     cisco.com

Network Configuration for ICFC
IPv4 Address:    10.255.255.255
Netmask:         255.255.0.0
IPv4 Gateway:    10.0.0.1
Press return to continue ...
```

Option 17

```
SELECT> 17

This device password can be used to log in to ICF's internal components:

SamplePassword123
Press return to continue ...
```