Troubleshooting Migration Issues

Troubleshooting for the Secure Firewall Migration Tool

A migration typically fails during the Check Point configuration file upload or during the push of the migrated configuration to management center.

Some of the common scenarios where the migration process fails for a Check Point configuration are:

- Files missing from the Check Point Config.zip.
- Invalid files are detected by the Secure Firewall migration tool in the Check Point Cofig.zip
- If the Check Point configuration file is of any compressed file type other than .zip.

Secure Firewall Migration Tool Support Bundle

The Secure Firewall migration tool provides the option to download a support bundle to extract valuable troubleshooting information like log files, DB, and configuration files. Perform the following:

1. On the **Complete Migration** screen, click the **Support** button.

   The Help support page appears.

2. Check the **Support Bundle** check box and then select the configuration files to download.

Note The Log and dB files are selected for download by default.

3. Click **Download**.

   The support bundle file is downloaded as a .zip to your local path. Extract the Zip folder to view the log files, DB, and the Configuration files.

4. Click **Email us** to email the failure details for the technical team.

   You can also attach the downloaded support files to your email.

5. Click **Visit TAC page** to create a TAC case in the Cisco support page.

Note You can open a TAC case at any time during the migration from the support page.

Logs and Other Files Used for Troubleshooting

You can find information that is useful for identifying and troubleshooting issues in the following files.

File	Location
Log file	*<migration_tool_folder>*\logs
Pre-migration report	*<migration_tool_folder>*\resources
Post-migration report	*<migration_tool_folder>*\resources
unparsed file	*<migration_tool_folder>*\resources

Troubleshooting Check Point File Upload Failures

If the Check Point configuration file fails to upload, the reason is typically because the Secure Firewall migration tool could not parse one or more lines in the file.

You can find information about the errors that caused the upload and parsing failure in the following locations:

- Unparsed file—Look at the end of the file to identify the last ignored line of the Check Point configuration file that was successfully parsed.
- Unexpected file—Invalid files detected for Check Point. For example, when zipped using Mac OS, Mac system files are created. Remove the Mac files.
- (For r75–r77.30 only) Incorrectly named files—When Security Policy and NAT Policy files are not named correctly for Check Point. Rename ACL and NAT files correctly.
- Missing files—Some files are missing from the Check Point config.zip file. Add the required files.

Note For r77, manually extract the missing configuration file. For more information, see Export the Check Point Configuration Files for r77.

For r80, use Live Connect to extract the correct configuration file for the secure Firewall migration tool. For more information, see Export the Check Point Configuration Files for r80.

Troubleshooting Example for Check Point: Cannot Find Member of Object Group (For r75–r77.30 Only)

In this example, the Check Point configuration file upload and parsing failed because of error in the configuration of an element.

Step 1 Review the error messages to identify the problem.

This failure generates the following error messages:

Location	Error Message
Secure Firewall migration tool message	Check Point config files parsed with errors. See the Pre-Migration Report error section for parsing errors and Post-Migration Report for push errors that occurs during the push stage.
Log file	[ERROR | objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;" [INFO | objectGroupRules] > "Parsing object-group service:[services_gvxs06]" [INFO | objectGroupRules] > "Parsing object-group service:[services_iphigenia]" [INFO | objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

Step 2 Open the Check Point `services.xml` file.

Step 3 Search the object-group with name as services_gvxs06.

Step 4 Create the missing member for the object-group using the smart dashboard.

Step 5 Export the configuration file again. For more information, see Export the Check Point Configuration Files.

Step 6 If there are no more errors, upload the new Check Point configuration zip file to the Secure Firewall migration tool and continue with the migration.

Troubleshooting Example for Check Point (r80) for Live Connect

Example 1: Request details on Check Point Security Manager.

In this example, the Secure Firewall migration tool requests the details for Check Point Security Manager.

Review the error messages to identify the problem. This failure generates the following error messages:

Location	Error Message
Secure Firewall migration tool message	Screen requests to provide details for Check Point Security Manager.

Location	Error Message
Log file	[ERROR | connect_cp] > "Unable to extract the Extracted-objects.json file due to credentials with insufficient privileges, time-out issues and so on. Refer Secure Firewall migration tool UG for more info." 127.0.0.1 - - [20/Jul/2020 17:20:43] "POST /api/CP/connect HTTP/1.1" 500 -

Incorrect credentials. Follow the steps as mentioned to pre-stage credentials. The credentials used must have a */bin/bash* shell profile on Check Point Gaia for Check Point Security Manager. The same credentials must be staged on Check Point Smart Console Application for Check Point Security Manager with Super User privileges for a normal deployment. The privileges must be Super User if using multi-domain deployment. For more information, see Pre-stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect.

Example 2: Bad File Format

In this example, the Secure Firewall migration tool migration is blocked due to bad file format.

Review the error messages to identify the problem. This failure generates the following error messages:

Location	Error Message
Secure Firewall migration tool message	Blocked
Log file	[ERROR | cp_device_connection] > "Bad file format" 2020-07-20 17:10:57,347 [ERROR | connect_cp] > "Unable to download .tar file." 127.0.0.1 - - [20/Jul/2020 17:10:57] "GET /api/CP/generate_tar_file?package=Standard HTTP/1.1" 500 -

Incorrect credentials. Follow the steps as mentioned to pre-stage credentials. The credentials used must have a */bin/bash* shell profile on Check Point Gaia for Check Point Security Manager. The same credentials must be staged on Check Point Smart Console Application for Check Point Security Manager with Super User privileges. The Super User privileges must be granted if using multi-domain deployment. For more information, see Pre-stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect.

Example 3: Blocked VSX Feature is UNSUPPORTED in Threat Defense

In this example, the Secure Firewall migration tool migration fails due to the blocked VSX feature in the threat defense.

Review the error messages to identify the problem. This failure generates the following error messages:

Location	Error Message
Secure Firewall migration tool message	Blocked VSX Feature is UNSUPPORTED in FTD.
Log file	[ERROR | config_upload] > "VSX Feature is UNSUPPORTED in FTD" Traceback (most recent call last)

Problem Description–This error occurs as the **fw vsx stat** command is deprecated starting with Check Point r80.40.

As a workaround, follow these steps:

1. Unzip the *config.zip* file.
2. Open the *networking.txt* file.

   Here is an example of the sample output:

   ```
   firewall> fw vsx stat
   Deprecated command, Please see sk144112 for alternative
   Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
   ```

   Replace this manually as follows:

   ```
   firewall> fw vsx stat
   VSX is not supported on this platform
   ```

3. Select all the files and compress them to .zip extension.