

I have gathered information regarding the different processes and paths and option available for different types of migration requirement. Based on my information gathering I have summarised those into following sections:

1	The migration process includes the following steps:	<ol style="list-style-type: none"> <li>1. Prepare the source device.</li> <li>2. Archive and download the UCS file.</li> <li>3. Shut down the source device.</li> <li>4. Set up the target device.</li> <li>5. Upload the archived UCS file.</li> <li>6. Load the archived UCS file onto the target device</li> </ol>
2	You can refer the following for detail step by step migration for 3 different scenarios:	<p><a href="https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-migrating-devices-and-configurations-between-different-platforms.html">https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-migrating-devices-and-configurations-between-different-platforms.html</a></p> <p><a href="https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-migrating-devices-and-configurations-between-different-platforms/migration-of-devices-running-different-version-software.html#GUID-7B338A6D-063F-4877-A9C1-CA07DFBADF28">https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-migrating-devices-and-configurations-between-different-platforms/migration-of-devices-running-different-version-software.html#GUID-7B338A6D-063F-4877-A9C1-CA07DFBADF28</a></p> <p><a href="https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-migrating-devices-and-configurations-between-different-platforms/migration-of-devices-running-the-same-software-version.html#GUID-A6D8D704-1C52-485E-916C-3DFF7CDF93F1">https://techdocs.f5.com/en-us/bigip-16-0-0/big-ip-system-migrating-devices-and-configurations-between-different-platforms/migration-of-devices-running-the-same-software-version.html#GUID-A6D8D704-1C52-485E-916C-3DFF7CDF93F1</a></p>
3	For specific to r series migration , we have to go through more or less of these steps:	<p><a href="https://clouddocs.f5.com/training/community/rseries-training/html/migration_to_rseries.html">https://clouddocs.f5.com/training/community/rseries-training/html/migration_to_rseries.html</a></p>
4	<p><b><a href="#">F5 Community Training &amp; LabsSource</a></b>   PDF</p>	<h2>Planning for rSeries Guide¶</h2>

		<ul style="list-style-type: none"> <li>• <a href="#">Introduction</a></li> <li>• <a href="#">Points of Management in rSeries</a></li> <li>• <a href="#">rSeries Appliances</a></li> <li>• <a href="#">rSeries Networking</a></li> <li>• <a href="#">rSeries High Availability</a></li> <li>• <a href="#">rSeries Multitenancy</a></li> <li>• <a href="#">rSeries Performance and Sizing</a></li> <li>• <a href="#">Initial Setup of rSeries F5OS Platform Layer</a></li> <li>• <a href="#">Initial Setup of the rSeries Network Layer</a></li> <li>• <a href="#">Deploying an rSeries Tenant</a></li> <li>• <a href="#">rSeries Inside the Tenant</a></li> <li>• <a href="#">rSeries Software Upgrades</a></li> <li>• <a href="#">rSeries Configuration Backup and Restore</a></li> <li>• <a href="#">rSeries Diagnostics</a></li> <li>• <a href="#">BIG-IQ Support for rSeries</a></li> <li>• <a href="#">Monitoring rSeries Health &amp; Alert Status</a></li> <li>• <a href="#">Monitoring rSeries</a></li> <li>• <a href="#">rSeries F5OS-A SNMP Monitoring and Alerting</a></li> <li>• <a href="#">Migration to rSeries</a></li> </ul>
5	R series training reference	<a href="https://clouddocs.f5.com/training/community/rseries-training/html/">https://clouddocs.f5.com/training/community/rseries-training/html/</a>
6	There is a migration tool by F5 on GITHUB site as follows:	<a href="https://github.com/f5devcentral/f5-journeys">https://github.com/f5devcentral/f5-journeys</a>
7	Here are 3 videos I found and checked on YouTube, in case needed to give details to client we can only take screenshots of these as we don't have the setup to install this tool to	<a href="https://www.youtube.com/watch?v=ILm5OkJRicw">https://www.youtube.com/watch?v=ILm5OkJRicw</a> <a href="https://www.youtube.com/watch?v=sPVZymcciSo">https://www.youtube.com/watch?v=sPVZymcciSo</a>

	run and experiment.	

[Next](#)

## JOURNEYS - BIG-IP upgrade and migration utility

### Contents:

- [Description](#)
- [Journey: Full config migration](#)
- [Journey: Application Service migration](#)
- [Configuration Migration Considerations](#)
- [JOURNEYS Setup Requirements](#)
- [JOURNEYS Installation](#)
- [JOURNEYS Update](#)
- [JOURNEYS API](#)
- [Feature Details](#)
- [Contributing](#)

### Description

JOURNEYS is an application designed to assist F5 Customers with migrating a BIG-IP configuration to a new F5 device and enable new ways of migrating.

#### Supported journeys:

- Full Config migration - migrating a BIG-IP configuration from any version starting at 11.5.0 to a higher one, including VELOS and rSeries systems.
- Application Service migration - migrating mission critical Applications and their dependencies to a new AS3 configuration and deploying it to a BIG-IP instance of choice.

### Journey: Full Config migration

#### Supported features:

- Loading UCS or UCS+AS3 source configurations

- Flagging source configuration feature parity gaps and fixing them with provided built-in solutions
- Load validation
- Deployment of the updated configuration to a destination device, including VELOS and rSeries VM tenants
- Post-migration diagnostics
- Generating detailed PDF reports at every stage of the journey

Full config BIG-IP migrations are supported for software paths according to the following matrix:

				DEST			
	X	11.x	12.x	13.x	14.x	15.x	16.x
	<11.5	X*	X	X	X^	X^	
	12.x		X	X	X	X^	
SRC	13.x			X	X	X	
	14.x				X	X	X
	15.x					X	X
	16.x						X

X^ - an exception compared to the supported upgrade paths listed in the official document [K13845](#) (upgrade allowed only if the source configuration is upgraded to the latest available maintenance release).

X\* - while an upgrade to a 11.x destination system is technically supported on BIG-IP, JOURNEYS does not support deployments to systems running these versions due to a lack of platform-migrate ucs load option (introduced in 12.1.3).

**WARNING:** Migrating Application Services using keys stored in FIPS cards is not supported at the moment, unless the user can restore the FIPS keys with the original (non-fips) ones on the destination platform.

### Known parity gaps

JOURNEYS finds the following configuration elements in the source configuration, which are no longer supported by the BIG-IP running on the destination platform. For every incompatible element found, there will be one or more automatic possible solutions provided.

#### *Common issues*

- **CompatibilityLevel** - BIG-IP devices are divided into three categories/levels based on hardware DoS and sPVA related capabilities. Some devices currently do not have hardware support for features included in levels 1 and 2, so some modifications might be necessary if the source device had one of these categories. For more details about compatibility levels, see [here](#).

Details

- **MGMT-DHCP** - for F5OS tenants (VELOS, rSeries) and vCMP guests, a static IP address is defined when the tenant is deployed, therefore DHCP needs to be disabled.

Details

- **Syslog** - solves [syslog configuration parsing error](#) possible during an upgrade to a destination BIG-IP with version 13.1.0 or higher.

Details

- **TRUNK** - for F5OS tenants (VELOS, rSeries) and vCMP guests, trunks are defined at the F5OS platform layer or vCMP host layer and not within the tenant or guest. Trunks (Link Aggregation Groups in F5OS) are pre-defined in the F5OS platform layer and VLANs are inherited by the tenant. Additionally, on VE BIG-IPs [LACP is not supported](#).

Details

*Velos and rSeries specific issues*

- **AAM** - Application Acceleration Manager is not supported on VELOS and rSeries platforms.

Details

- **CGNAT** - CGNAT ([Carrier Grade NAT](#)) is not supported on this software version.

Details

- **ClassOfService** - CoS or DSCP (Differentiated Services Code Point) is not currently supported on this software version.

Details

- **DoubleTagging** - indicates support for the IEEE 802.1QinQ standard, informally known as Double Tagging or Q-in-Q, is not currently supported on this software version. More info on the feature can be found [here](#).

Details

- **DeviceGroup** - Device Groups are fully supported on VELOS/rSeries tenants. However, when doing a UCS migration using Journeys, the device group needs to

be removed from it to prevent configuration load errors and then re-configured manually once the migrated UCS is loaded on the target platform.

#### Details

- **FixLL** - F5OS tenants currently do not yet support the guaranteed flow acceleration and collision avoidance that FIX Low Latency License provides.

#### Details

- **HTTP3** - Due to a [BIG-IP 15.1.5 bug](#), virtuals containing HTTP3 profiles might fail to load.

#### Details

- **MTU** - since the F5OS tenant currently does not support jumbo frames, we have to limit mtu to 1500.

#### Details

- **PEM** - although keeping the PEM configuration in the configuration files will not cause load errors (it will be discarded when loading the UCS), as for now PEM is not supported in this software version. Journeys removes PEM elements from the configuration to avoid confusion.

#### Details

- **RoundRobin** - Round Robin DAG configuration is not currently supported on this software version.

#### Details

- **SPDAG** - [source/destination DAG \(Service provider DAG\)](#) is not supported in this software version.

#### Details

- **SPVA** - some security Packet Velocity Acceleration (PVA) features do not have hardware support in this software version - these either must be removed or set to use software mode.

#### Details

- **Tunneling** - While they won't cause UCS load errors, tunneling protocols such as VXLAN, IPSEC, GTP-U, GRE, NVGRE are not optimal in this software version due to the lack of hardware support for DAG on tunnel frames using inner header info. Traffic will not be distributed across all the available TMMs due to inefficient disaggregation, affecting performance.

#### Details

- **VirtualWire** - the [virtual-wire feature](#) is not supported in this software version.

## Details

- **VlanGroup** - [vlan-groups](#) aren't supported in this software version and will be defined at the F5OS layer when supported.

## Details

- **VLANMACassignment** - solves an issue with mac assignment set to `vmw-compat` that can happen when migrating from a BIG-IP Virtual Edition.

## Details

- **WildcardWhitelist** - a part of sPVA - extended-entries field in network-whitelist objects is not supported in this software version.

## Details

- **IpPort** - Hardware acceleration of the [Ip Port](#), hash setting is not supported in this software version, enabling it may increase CPU utilization up to 20%.

## Details

**JOURNEYS does not support** feature parity gaps that:

- Reside outside a UCS archive to be migrated, e.g. in a host UCS (not in a guest UCS):
  - Crypto/Compression Guest Isolation - Dedicated/Shared SSL-mode for guests is not supported on VELOS and rSeries. [Feature details.](#)
  - Traffic Rate Limiting (affects vCMP guests only) - assigning a traffic profile for vcmp guests is currently not supported on VELOS and rSeries tenants.
- Do not cause any config load failures on destination devices:
  - [Secure Vault](#) - keys will be instead stored on the tenant file system.
  - Several sPVA features which do not support hardware processing, where software support will occur instead (DDoS HW Vectors (Device and VS), Device/VS Block List, Device Vector Bad Actor (Greylist))
  - Wildcard SYN cookie protection - as above, software processing will replace hardware one.
  - HTTP3 - F5OS tenants currently provide only experimental support for this feature.

## BIG-IP Prerequisites

Mandatory steps before running Full Config migration in JOURNEYS:

1. **Master key transfer** - to allow handling encrypted objects, before running JOURNEYS, you need to set a device master key password on both Source and Destination Systems. There are two ways to do this:
  - i. Copy the Source System master key with `f5mku` and re-key master key on the Destination System:

Important: Whenever possible, use the documented tmsh commands for master and unit key manipulation. Only use the f5mku command with assistance from F5 Support when no tmsh commands exist to perform the task you want.

- Obtain the master key from the Source System by entering the following commands:

- `f5mku -K`

and copy the output. The command output appears similar to the following example:

```
oruIVCHfmVBnwGaSR/+MAA==
```

- Install the master-key that you copied in the previous step to the Destination System using the following syntax:

- `f5mku -r <key_value>`

i. Set master-key password before saving the source UCS file

- Set the device master key password on the Source System by entering the following commands (**remember this password** because you'll need to use the same password on the destination device)

- `tmsh modify sys crypto master-key prompt-for-password`

- `tmsh save sys config`

- Set the master key password on the Destination System by entering the following commands, using the password remembered in the previous step:

- `tmsh modify sys crypto master-key prompt-for-password`

- `tmsh save sys config`

For more details, please refer to:

- [Platform-migrate option overview: K82540512](#)
- [Installing UCS files containing encrypted passwords or passphrases: K9420](#)

## 1. SSH public keys migration

- SSH public keys for passwordless authentication may stop work after UCS migration, since the UCS file may not contain SSH public keys for users.
- If the version is affected by the problem, then:
  - all key files have to be migrated manually from the Source System to the Destination System
  - `/etc/ssh` directory has to be added to the UCS backup configuration of the Source System



- For more details on how to manually migrate SSH keys and verify if your version is affected by the problem, please read:
  - K22327083: UCS backup files do not include the /etc/ssh/ directory <https://support.f5.com/csp/article/K22327083>
  - K17318: Public key SSH authentication may fail after installing a UCS <https://support.f5.com/csp/article/K17318>
  - K13454: Configuring SSH public key authentication on BIG-IP systems (11.x - 15.x) <https://support.f5.com/csp/article/K13454>

## 2. Destination System preparation for JOURNEYS

- Destination BIG-IP should be in Active state.
- If migrating from BIG-IP 14.0.x or lower, ensure that `mgmt-dhcp` value in `sys global-settings` on the Destination System is set to either `disabled` or `enabled`. Any other values - namely `dhcpv4` and `dhcpv6`, available starting at 14.1.0 - will cause an error during configuration loading.
- VLANs, trunks and interfaces should already be configured on vCMP, rSeries and VELOS systems. For more details, please refer to: [Platform-migrate option overview: K82540512](#).  
For VELOS or rSeries tenant configuration, find more information on [F5OS CLI](#).  
VLANs and trunks creation example:

```

4. config
5. vlans vlan 1000 config name Vlan1000 vlan-id 1000
6. vlans vlan 1001 config name Vlan1000 vlan-id 1001
7. vlans vlan 1002 config name Vlan1000 vlan-id 1002
8. top
9. interfaces interface 1.0 ethernet switched-vlan config trunk-vlans 1000
10.     interfaces interface 1.0 ethernet switched-vlan config trunk-vlans
    1001
11.     interfaces interface 1.0 ethernet switched-vlan config trunk-vlans
    1002
12.     commit
13.     end

```

### 1. FIPS/NetHSM keys migration

- Keys stored in FIPS/NetHSM will not be migrated, since the UCS file does not contain keys of these types.
- If FIPS/NetHSM keys are in use by the platform, then:

- all key files have to be migrated manually from the Source System to the Destination System
- For more details on how to manually migrate keys stored in FIPS/NetHSM, please read:
  - [FIPS keys migration](#)
  - [NetHSM keys migration](#)

*BIG-IP account prerequisites*

To ensure all JOURNEYS features work properly, an account with Administrator role and advanced shell (bash) access is required on both source and target hosts. It can be root or any other account. For auditing purposes, a separate account for migration might be desired.

**IMPORTANT:** Due to the above, certain features of JOURNEYS - specifically the ones requiring ssh access to the machine - are not available on BIG-IPs running in the **Appliance mode**. The user will be required to perform manual variants of these steps instead.

## Journey: Application Service Migration

Supported features:

- Loading UCS source configurations.
- Grouping Virtuals into Applications and Tenants, basing on internal dependencies and set preferences.
- Configuration editor for Virtuals with an easy access to updated AS3 conversion previews.
- Converting selected applications into a deployable AS3 declaration using [f5-automation-config-converter](#).
- Deployment of the updated configuration to a specified destination device via AS3.
- Post-migration diagnostics.

### Configuration object grouping

1. **Virtual** - smallest object recognized by JOURNEYS. It includes a single `ltm virtual-server` (represented by a Service in AS3) object and any others referenced by it directly or indirectly - monitors, pools, profiles, etc.
2. **Application** - A group of AS3 objects, including the virtual mentioned above. Logic for initial grouping of virtuals into apps can be manually set via preferences in GUI before loading the ucs. Represented by `folders` on the BIG-IP level.
3. **Tenant** - A group of AS3 applications. By default JOURNEYS creates one tenant per application. `Common` is a special reserved name, representing objects shared between tenants. Represented by `partitions` on the BIG-IP level.

### Application conversion status

Each virtual separately gets assigned a status based on the `f5-automation-config-converter` response. Possible statuses are as follows:

- Green - All virtual objects appear to convert properly.
- Red - Virtual configuration includes some objects that are currently marked as `as3NotConverted` by `f5-automation-config-converter`, and are considered undeployable.
- Black - Error during a virtual config conversion attempt.

Note: If one or more of your apps have a red or black status, you may attempt to use a newer version of `f5-acc-config-converter` by editing the image version inside the `docker-compose.yml` file. Otherwise, please open an issue on [f5devcentral](#) and include configuration contents from the problematic app.

## Additional notes

### *Deployable objects*

Not all required configuration files can be included inside the resulting AS3 json, and need to be installed on the Destination System prior to sending the declaration itself.

If deploying manually, JOURNEYS will prepare a package containing all of the required files alongside with a list of commands to perform on the Destination System.

If deploying via JOURNEYS, the application will install the files automatically.

### *Known issues*

- JOURNEYS does not support keys generated using a physical FIPS card or NetHSM. If there are any applications referring to these keys, deployment of them will fail. For more info about keys migration read: [FIPS/NetHSM keys migration](#)

## Configuration Migration Considerations

### BIG-IP device swap

To minimize downtime, F5 recommends deploying the new hardware alongside existing BIG-IP deployment.

F5 recommends the following procedure for moving production traffic to a new device:

1. Deploy the target device, trying to keep physical connections as close as possible to the old BIG-IP (respective interfaces assigned to the same physical networks)
2. Remove interfaces to existing VLANs on the **new hardware** (this will impact **all** tenants on VELOS/rSeries/vCMP guests).

There are three options to do this:

- i. Disabling interfaces.
- ii. Physically unplugging the network cables.
- iii. Disabling the port on the switch connected to the destination platform.

3. Deploy JOURNEYS-generated config to a new BIG-IP. Note that some validators like LTM module comparison are expected to fail as Virtual Servers will be down.
4. If the configuration was deployed successfully, review the system status. If the status is "REBOOT REQUIRED", perform the reboot before shutting down interfaces on the old BIG-IP system.
5. If you use BIG-IQ, refer to the [article K15938](#) to discover your new BIG-IP device.
6. Shutdown interfaces on the **old BIG-IP system** (this will impact **all** source BIG-IPs).

There are three options to do this:

- i. Disabling interfaces.
  - ii. Physically unplugging the network cables.
  - iii. Disabling the port on the switch connected to the old BIG-IP system.
7. Re-add interfaces to existing VLANs on the **new hardware** (this will impact **all** tenants on VELOS/rSeries/vCMP guests).  
There are three options to do this:
    - i. Re-enable interfaces on the destination platform.
    - ii. Physically unplug the network cables on the source platform, plug the network cables on the destination platform.
    - iii. Enable the port on the switch connected to the destination platform.

## SPDAG/VlanGroup mitigation

If SPDAG or VlanGroup removal mitigation is applied, and a conflicted object is configured on a Virtual Server, JOURNEYS **will remove all VLANs assigned for that particular Virtual Server** - not only the conflicted one. This is done to ensure that JOURNEYS does not produce an invalid configuration (Virtual Servers cannot share identifiers, as they need to be unique).

## Rebuilding device trust:

During migration JOURNEYS will reset the device trust.

F5 recommends one of the following procedures to rebuild the device trust:

- K40832524: Rebuilding device trust using tmsh (11.x - 16.x)  
<https://support.f5.com/csp/article/K40832524>
- K42161405: Rebuilding device trust using the Configuration utility (11.x - 16.x)  
<https://support.f5.com/csp/article/K42161405>

## Restoring backup UCS in case of migration failure

Deployment progress can be tracked on the Summary page. If UCS load fails, it is strongly advised to manually load the backup UCS archive created during the deployment process before any other action is taken on the Destination System.

1. Log to the Destination System:
2. `ssh username@<destination-system-ip>`
  3. Use the command to load the backup UCS:

4. `tmsh load sys ucs <backup_ucs_name*>`

\*The backup UCS archive name is displayed on the Summary page in the Detailed Results in a log entry that should look as follows:

```
Create backup of the Destination System:  
/var/local/ucs/journey_ucs_backup_20211012-103937.ucs
```

## JOURNEYS Setup Requirements

- Install [Docker](#)
- Install [Docker Compose](#)
  - Other alternatives like [Podman](#) combined with [Podman Compose](#) might be viable, but they were not tested

### System requirements

If you are running Journeys App in a VM, F5 recommends using [Ubuntu Desktop](#) with at least 25 GB of free hard drive space. Make sure you do not have an HTTP server installed as it might interfere with Journeys App. Having more resources might be helpful when attempting to parse very complex UCS archives.

## JOURNEYS Installation

### Fetching JOURNEYS

```
git clone https://github.com/f5devcentral/f5-journeys.git  
cd f5-journeys
```

### Preparing the environment

1. Create a directory for all of JOURNEYS operations - modifying configs, logging, etc.

You can use any directory in place of `/tmp/journeys`.

```
mkdir /tmp/journeys
```

Note: keep in mind that the default migration directory is placed in the `/tmp` directory, which is cleaned up upon a system reboot. If longer session persistence is required, please modify this directory path via the `.env` file to a non-temporary one.

2. Prepare an environment file for docker-compose
3. `cp sample.env .env`

If you are using a different working directory than the one shown in the point above, `WORKING_DIRECTORY` variable has to be updated in the `.env` file. Its value should be an absolute path pointing to your custom directory.
4. Fetch services included in the docker-compose configuration file

5. `docker-compose pull`
  6. Print sha digest of downloaded images
7. `docker image ls f5devcentral/f5-bigip-journeys-app --digests`
  8. Examine if image listed in `docker-compose` `journeys/celery-worker` has exactly the same digest that can be found on docker hub repository with the same tag
9. [https://hub.docker.com/r/f5devcentral/f5-bigip-journeys-app/tags?page=1&ordering=last\\_updated](https://hub.docker.com/r/f5devcentral/f5-bigip-journeys-app/tags?page=1&ordering=last_updated)

Note: do not use the application if digests does not match.
10. Start services included in the `docker-compose` configuration file
11. `docker-compose up -d`

Note: services included in the default `docker-compose.yml` file do not allow usage of the `perapp` functionalities. To use them, please refer to [perapp documentation](#).
12. Open your web browser, navigate to:
13. <https://localhost:8443>

and accept self-signed cert to run the application. The certificate itself can be verified by comparing it with the one logged by the main JOURNEYS container.

```
docker logs f5-journeys_journeys_1 2>&1 | grep 'BEGIN CERTIFICATE'
```

## JOURNEYS Update

To update Journeys to the latest version, run the following commands.

1. Clean up the old working directory. Sometimes leftover data might not be compatible with new Journeys version.
2. `rm -rf /tmp/journeys` # or whichever folder you specified in the `.env` file
3. `mkdir /tmp/journeys`
  4. Ensure that your current `.env` file contains all keys present in the `sample.env` file. If not, copy/enter them.
  5. Bring down the old containers, pull the newest changes and start the services again.
6. `docker-compose down`

7. `git pull`

8. `docker-compose up -d`

Older images may then be viewed and removed using the following commands.

```
docker images | grep journeys
docker rmi <image_name>:<version>
```

## JOURNEYS API

An API is exposed by the main `journeys` container (by default on port 8443). Available endpoints are shown in the `openapi-schema.yaml` file, which can also be imported in a tool like [Postman](#) or [Swagger UI](#) for easier exploring and/or usage.

### Known API issues

- Attempting to call an invalid endpoint will return a broken html with a 200 code rather than a 404 error one.

## Feature details

### Diagnostics

Upon deployment of UCS to the Destination System, user will be prompted to select several diagnose methods. These collect information relevant to your system condition and compare its state and configuration with the Source BIG-IP System.

Please keep in mind that only a few of the diagnostics methods can be run without providing a Source System. If the UCS was provided manually and no such system was provided, unavailable options will be locked out.

**IMPORTANT:** User will always be prompted for source and destination credentials right before deployment even if Source System is offline. Destination credentials are valid before loading UCS archive on the target system. Once the UCS is loaded, source credentials (stored at UCS archive provided by a user or downloaded from the Source System) are required to log in.

Details of the diagnostic checks can be evaluated in a resulting pdf report.

Diagnose methods

### Load validation

During the migration process, user will be provided with an option to validate if the configuration being migrated will load on the provided Destination System. This operation utilizes the BIG-IP built in `tmsh sys config verify` functionality to check whether the Destination BIG-IP finds any errors in the provided files. This module temporarily modifies Destination configuration files for testing purposes. After moving on from this step, the Destination System will be reverted back to its original state.

**WARNING:** Due to how `tmsh sys config verify` works, the load validation module has to temporarily heavily modify configuration files on the provided Destination

System. For this reason, to avoid any potential loss of data, it is *not* recommended to use this feature with a device already containing any non-basic configuration.  
WARNING: Please make sure the Destination device is licensed and provisioned with modules corresponding to the UCS configuration being migrated.

WARNING: Load validation can produce false positive output if the configuration contains any parts subject to fix-up scripts built into the BIG-IP ucs load process. These fix-ups cannot be automatically incorporated in the validation module.

WARNING: If the configuration to be validated requires specific values in BigDB.dat file, they must be configured on a destination device before performing the validation, otherwise "load validation" may fail.

Load validation functional details

## Contributing

### Bug reporting

Let us know if something went wrong. By reporting issues, you support development of this project and get a chance of having it fixed soon. Please use bug template available [here](#) and attach the journeys.log file from the working directory (/tmp/journeys by default)