IBM **DataPower Gateway** X3 Model 8496-52X and 8496-53X Migration Using Secure Backup and Restore

R. George Inness, III

IBM **Integration APS Team**

Colt Gustafson

IBM **DataPower L2 Hardware Lead**

Version 1.51

January 2023

Table of Contents

[1 Required Reading and Action(s) Before Starting Migration 3](#_Toc124254027)

[1.1 DataPower Firmware v10.5 3](#_Toc124254028)

[1.1.1 IDG (8436-52X/8436-53X) Restrictions 3](#_Toc124254029)

[1.1.2 Compatibility with API Connect 3](#_Toc124254030)

[1.2 IBM Transformation Extender (ITX) License Update 3](#_Toc124254031)

[2 Introduction 5](#_Toc124254032)

[3. Migration Overview 6](#_Toc124254033)

[4. Inventory 8](#_Toc124254034)

[4.1 WebGUI Method for Inventory 8](#_Toc124254035)

[4.1.1 Firmware Version 9](#_Toc124254036)

[4.1.2 Modules Installed 9](#_Toc124254037)

[4.1.3 System Information 10](#_Toc124254038)

[4.1.4 Network Interfaces 10](#_Toc124254039)

[4.1.5 Inventory the Keys in the HSM if the source appliance is a 53X model 11](#_Toc124254040)

[4.2 CLI Method for Inventory 11](#_Toc124254041)

[4.2.1 Firmware Version 11](#_Toc124254042)

[4.2.2 Modules Installed 12](#_Toc124254043)

[4.2.3 System Information 12](#_Toc124254044)

[4.2.4 Network Interfaces 13](#_Toc124254045)

[4.2.5 Inventory The Keys In the HSM 13](#_Toc124254046)

[5 Planning and Preparation 14](#_Toc124254047)

[5.1 Determine if Actions Required Because of ITX License Changes 14](#_Toc124254048)

[5.2 Review Firmware Changes in Version v10.5 14](#_Toc124254049)

[5.3 High Level Steps in the Execution Phase 15](#_Toc124254050)

[5.3.1 IDG (8436) to IDG X3 (8496) 15](#_Toc124254051)

[5.3.2 IDG X2 (8441) to IDG X3 (8496) 15](#_Toc124254052)

[5.4 Estimated Effort for Tasks in the Execution Phase 16](#_Toc124254053)

[6 Execution 17](#_Toc124254054)

[6.1 Executing Tasks on the WebGUI 17](#_Toc124254055)

[6.1.1 Upgrade Path to firmware v10.5.0 migration tool for the IDG (8436) 17](#_Toc124254056)

[6.1.2 Secure Restore 17](#_Toc124254057)

[6.2 Executing Tasks on the DataPower CLI 18](#_Toc124254058)

[6.2.1 Secure Restore 18](#_Toc124254059)

[6.3 Loading the Private Keys into the HSM using the WebGUI 19](#_Toc124254060)

[Appendices 25](#_Toc124254061)

[APPENDIX A. Possible Gotchas on the Secure Restore 25](#_Toc124254062)

[APPENDIX B. Special Considerations When Only Using The 10 GB Interfaces on the IDG X2 26](#_Toc124254063)

# Required Reading and Action(s) Before Starting Migration

## DataPower Firmware v10.5

The X3 appliances must run the 10.5 or higher firmware and cannot be downgraded to the 10.0.1.x or 2018.4.1.x firmware’s.

### IDG (8436-52X/8436-53X) Restrictions

The 8436 IDG appliances cannot run the 10.5 firmware due to a hardware compatibility issue.

Upon request the support team will provide a special migration firmware tool to allow you to take a secure backup of the IDG appliance.

**Notes:**

* This tool can only be used to create a Secure Backup on the 8436 IDG appliances that can be restored on the IDG X3 (8496-52X and 8496-53X) and perform a “boot switch” to the previous firmware that was installed. **Any other use cases are not supported on the 8436 IDG appliances.**
* You must open a Support Case to obtain the migration tool to be posted in the Support Case. Include the output of the “show license” command on the 8436 IDG so the support team can provide the correct image.
* The migration tool will not be posted on Fix Central or Passport Advantage.
* You must follow the Migrations Steps in this White Paper or your IDGs (8436-52X/8436-53X) could be made unusable.

### Compatibility with API Connect

DataPower firmware v10.5 is compatible with API Connect v10.0.5 with plus or minus one fixpack version. See the table below for examples.

|  |  |  |
| --- | --- | --- |
| **DataPower Version** | **API Connect Version** | **Compatible** |
| v10.5.0.1 | v10.0.5.0 | Yes |
| v10.5.0.3 | v10.0.5.1 | No |

## IBM Transformation Extender (ITX) License Update

Existing DataPower customers using**ITX (formerly WTX)**, with stand-alone entitlement to DataPower Integration module (IM) or DataPower B2B module, can request the ITX activator tool.

You will need to apply the activator **before upgrading** to 10.5 or 10.0.1.9 or higher release as these enforce the new ITX license entitlements. This also includes activation on the IDG X3 (8496-52X or 8496-53X) before doing the Secure Restore.

**How do clients determine if they need the ITX Activator?**

Clients can search their config looking for any reference to tx-map or .dpa files

**What criteria is used to determine if the client is entitled to the ITX Activator?**

* Client must be an existing DataPower client with active entitlement to either the Integration or B2B module and show current ITX usage.
* Clients currently using ITX on physical DataPower appliances or virtual DataPower appliances, can request the ITX Activator at no charge. For new DataPower clients or clients who have just purchased the IM or B2B module, they will need to work the sales teams to determine the steps to purchase the ITX license.
* DataPower entitlements through other programs like API Connect or CP4I are not entitled and there is no way for them to get ITX entitlement

**Existing clients on v10.0.1.8 and lower using ITX must activate the ITX license before upgrading to v10.5 to ensure they do not lose support for the ITX maps and the configuration lost.**

**Note: If you upgrade before activating the ITX license your ITX maps will not work and you will need to:**

* **Roll back the upgrade to the previous version**
* **Activate the ITX license**
* **Upgrade again**

Follow the steps below to get access to the module.

**How do clients get access to ITX Activator?**

The client must open a Support Case against DataPower requesting the ITX Activator. DataPower Support will also verify that the client has active entitlement for either B2B or IM and the usage of ITX-MAP.

**For additional information, see the following DataPower Flash.** <https://www.ibm.com/support/pages/node/6620207>

# Introduction

This White Paper will walk through the migration process of your existing physical DataPowers IBM DataPower Gateways (IDGs) (8436-52X,8436-53X) and IDG X2s (8441-52X,8441-53X) to your IBM IDG X3s (8496-52X,8496-53X) using the Secure Backup and Restore functionality that is built into the appliances.

Another method to migrate to your IDG X3s (8496-52X,8496-53X) is Export/Import functionality. The main difference between the Export/Import functionality and the Secure Backup and Restore functionality is that it does not capture the crypto keys, certificates or users.

The secure backup collateral and the key/cert pair used to create the backup will have to be available off the existing appliance so that it can be used on the new appliance.

**It is critical to follow this process as documented. Review this white paper completely before jumping in and starting any steps.**

Ensurethat you have the latest version of the document that will be available in a pinned post in the IBM DataPower Community. The URL to the community is [IBM DataPower Community](https://community.ibm.com/community/user/integration/communities/community-home?CommunityKey=b13f4693-16ee-422b-9d0b-f5262e25426f)

# Migration Overview

The migration to the IBM DataPower Gateway (IDG) X3 appliance using Secure Backup and Restore is a straightforward process. It is assumed that you have DataPower administration skills, and you and/or the application development team can test the applications/services on the IDG X3 appliance once they have been migrated over.

This white paper will refer to your existing appliance as the “Source” appliance and the new IDG X3 appliance as the “Target” appliance. The “Source” appliance can only be a physical appliance, not a virtual appliance.

Secure Backup must be enabled on the “Source Appliance”. To verify that Secure Backup is enabled, check the backup mode on the “System settings” page on the WebGUI or the “show system” CLI command. If the Backup Mode is normal, not secure, open a Support Case and include the output of the “show system” command to allow L2 generate a scrypt3 file to enable Secure Backup.

The Secure Backup and Restore functionality creates a complete back-up of the “Source” appliance that can be restored on the “Target” appliance with the following exceptions:

* DataPower appliances with the Hardware Security Module (HSM): 8436-52X, 8441-53X and 8496-53X, the private keys stored in the HSM are not captured in the Secure Backup.

Secure Backup and Restore is dependent on the following conditions on both the existing and new appliances:

* Same firmware version. The minimum firmware version on the IDG X3, 8496-52X is v10.5
* Same licenses. If you have enabled all of the modules on the “Target Appliance” and the license/features are different, open a Support Case for further assistance.

The Secure Backup will not capture any of the private keys in the “Source Appliance”’s HSM. For a successful migration, you must have the private keys off of the appliances. Also, no method exists to extract the keys from the “Source Appliance”’s HSM to move to the “Target Appliance”’s HSM.



**The major assumptions in this White Paper are:**

1. You and your team have a detailed understanding on DataPower setup, configuration, and have used the Secure Backup and Restore functionality before. If your team does not have the skills, it is recommend working with your sales team to engage a DataPower Business Partner or IBM Lab Services to put together a proposal for the migration.
2. The migration will be complete configuration of the “Source” appliance to the “Target” appliance.
3. If you are downsizing the number of DataPower appliances, your team has done a performance/capacity study to ensure the number of appliances being migrated perform as needed.
4. The “Target” appliance has been initialized and is available on your company network.

The migration process will be broken down into three phases:

* **Inventory** – Gather the detailed information about the “Source” appliance that is needed for the migration planning
* **Planning and Preparation** – Putting together a migration plan and obtaining the necessary information needed for the migration like the keys and certificates available off of the “Source” appliance
* **Execution** – Executing the migration to the X3 appliance

Before starting the Inventory phase, it is recommended that the “Target” appliance be initialized and on your company network with all the needed licenses enabled.

**Note: If you are using ITX, make sure you have the ITX license enabled on the “Source” and “Target” appliance. Review the Important Information section for further details.**

If you have questions on the migration process and this white paper, please ask in the [IBM DataPower Community](https://community.ibm.com/community/user/integration/communities/community-home?CommunityKey=b13f4693-16ee-422b-9d0b-f5262e25426f) in the upcoming post that will be pinned to the top of the Discussion tab. The post will be monitored by the white paper’s authors and by other community members. This is also where the latest version of the white paper will be posted.

For issues that you have with the DataPower firmware with the “Source” appliance that is an IDG or an IDG X2 that is under support, or with the IDG X3 “Target” appliance, open a Support Case to get the issue resolved following the normal support process.



**The key requirements for a successful migration are:**

1. Replacing the appliances in stages, starting at the lowest level like development and test before migrating production.
2. A plan to test the IDG X3 “Target” appliance.   
   Note: When the IDG X3 reboots after a Secure Restore, the network interfaces will be the same as the “Source” appliance. Ensure the “Source” appliance is powered down to avoid duplicate IP addresses on the network.

# Inventory

In the inventory phase, you will be gathering information on the “Source” appliance and the “Target” appliance. The estimated effort is ten minutes per appliance.

The steps to gather the necessary inventory information are provided for the WebGUI and CLI. Either method will capture the same information so you can choose which method you prefer.



It is recommended that you take screen captures of each WebGUI page and/or the Command Line Interface (CLI) output so you have this information available for when start the planning and execute the plan.

The information captured will be broken down into the following categories:

* Firmware Version – Gather what firmware version you are running
* Modules Installed – Determine what additional add on modules are installed
* Confirmation Secure Backup Is Enabled on “Source” appliance
* If the “Source” appliance is an 8436-53X, Inventory of the Private Keys stored in the HSM
* Network Interfaces – Review what Networking Interfaces are being used the “Source” appliance.

The white paper will provide how to capture this information. For the WebGUI pages, it will provide the text to input in the Search text box so you can load up the page by selecting it.

See the picture below for where the Search text field is located on a WebGUI page.

Graphical user interface, application, Teams

Description automatically generated

## WebGUI Method for Inventory

Diagrama, Forma

Descripción generada automáticamente

### 4.1.1 Firmware Version

Type **Version Information** in the Search text field and select it from the search results to load the Version Information page. You will see a page like this sample:

Table

Description automatically generated

### Modules Installed

Type **Device Features** in the Search text field and select it from the search results to load the Device Features page. You will see a page like this sample:

Table

Description automatically generated

Determine what licenses to install on the new appliances.

* Make sure you are entitled to the correct modules for the new X3 appliance based upon what you have installed on the “Source” appliance.
  + If the Device Features listsTIBCO-EMS, you will need the TIBCO-EMS module.
  + If the Device Features listsAppOpt, you will need the Application Optimization module
  + If the Device Features listsB2B, you will need the B2B module.
  + If the Device Features liststhe following: DataGlue, SQL-ODBC, DCO and IMS, you will need the Integration module.

### System Information

Type **System Settings** in the Search text field and select it from the search results to load the Configure System Settings page. You will see a page like this sample:

Graphical user interface, application

Description automatically generated

If the Backup mode is Normal, open a Support Case requesting a scrypt3 file to enable Secure Backup and include.

### Network Interfaces

Type **Network Interfaces** in the Search text field and select it from the search results to load the Network Interfaces page. You will see a page like this sample:

Table

Description automatically generated

**IMPORTANT notes** If you are migrating an IDG X2

* If you are using either the **eth0** or **eth1** 10GB ports you must remove the configuration before taking the secure backup as the X3 appliance does not have these ports. If the configuration is not removed the network will be in a bad state after the restore on the X3.
* If you are only using the built in 10 GB interfaces next to mgt0 and mgt1, please review appendix A Special Considerations When Only Using The 10 GB Interfaces on the IDG X2.

### Inventory the Keys in the HSM if the source appliance is a 53X model

To check if there are any keys stored on the HSM:

**WebGUI**

Enter “HSM Keys” and navigate to the page:

A picture containing chart

Description automatically generated

Note: it is possible that no keys are stored on the HSM as it is an option to store the keys on the HSM or in the normal crypto storage the same as a non-HSM appliance

## CLI Method for Inventory

Diagrama, Forma

Descripción generada automáticamente

For the CLI, it is recommended that you turn on recording with the program that you are using so you can review the output of the command entered as there is no way to pause the output.

Make sure you are in the default domain.

### Firmware Version

Type **show version** and press enter.

You will see a sample output like this output.

Text

Description automatically generated

### Modules Installed

Type **show features** and press enter.

You will see a sample output like this output.

Table

Description automatically generated

Determine what licenses to install on the new appliances.

* Make sure you are entitled to the correct modules for the new X3 appliance based upon what you have installed on the “Source” appliance.
  + If the “Source” appliance’s **show features** output has TIBCO-EMS, you will need the TIBCO-EMS module.
  + If the “Source” appliance’s **show features** output has AppOpt, you will need the Application Optimization module
  + If the “Source” appliance’s **show features** output has B2B, you need the B2B module.
  + If the “Source” appliance’s **show features** output contains all the following: DataGlue, SQL-ODBC, DCO and IMS, you will need the Integration module.

### System Information

Type **show system** and press enter.

The sample output follows:

Table

Description automatically generated with low confidence

### Network Interfaces

Type **show network** and press enter.

The sample output follows:

Table

Description automatically generated

**IMPORTANT notes if you are migrating an IDG X2**

* If you are using either the **eth0** or **eth1** 10GB ports you must remove the configuration before taking the secure backup as the X3 appliance does not have these ports.   
  If the configuration is not removed the network will be in a bad state after the restore on the X3.
* If you are only using the TBD 10 GB interfaces, please review appendix A Special Considerations When Only Using The 10 GB Interfaces on the IDG X2.

### Inventory The Keys In the HSM

Type show hsm and press enter

The sample output:

Text

Description automatically generated

Note: it is possible that no keys are stored on the HSM as it is an option to store the keys on the HSM or in the normal crypto storage the same as a non-HSM appliance

# Planning and Preparation

Using the details gathered in the Inventory Phase to put together a plan for the migration.

## Determine if Actions Required Because of ITX License Changes

Review Section 1.2 to determine what action items are based upon the ITX License Changes

## Review Firmware Changes in Version v10.5

**Note:** The special v10.5 migration tool for the IDG (8436) can only be used for migration purposes.

It is recommended that you review the DataPower Knowledge Center for each release going to v10.5 to see what features have been deprecated and removed and what features might have behavior changes.

Following is the URL to what is new in v2018. From the URL, you can also view what is new in v10.0.1 and v10.5.

<https://www.ibm.com/docs/en/datapower-gateway/2018.4?topic=gateway-changed-in-201841>

## High Level Steps in the Execution Phase

### IDG (8436) to IDG X3 (8496)

Diagram

Description automatically generated

**Note:** On the IDG, the v10.5 version can only be used for creating a secure backup. It cannot be used for any other purposes.

### IDG X2 (8441) to IDG X3 (8496)

Diagram

Description automatically generated

## Estimated Effort for Tasks in the Execution Phase



**Note:** The estimated effort is per appliance. A Task could take longer depending on the network speeds to upload and download files to and from the appliance.

|  |  |  |
| --- | --- | --- |
| Task | Effort in Hours | Notes |
| If necessary, enable the “Source” and “Target” appliances for ITX. | 1 hour | If an ITX License is being used on the “Source” appliance, open a Support Case to get a SCRYPT3 file to enable ITX. |
| If necessary, enable Secure Backup on the “Source” appliance. | 30 minutes | Open a Support Case to get a SCRYPT3 file to enable Secure Backup. |
| Upgrade the IDG (8436) appliance to the latest v2018.4.1.x fixpack or v10.0.1.x fixpack. | 1 hour | The effort also includes includes the time to upload the SCRYPT3 to the appliance. |
| Secure Backup. | 1 hour | The effort also includes the time to download the Secure Backup files off the appliance. |
| Upgrade to v10.5.0 migration tool on IDG (8436). | 1 hour | The effort also includes the time to upload the SCRYPT3 to the appliance. |
| Upgrade to v10.5.0.2 on the IDG (8496). | 1 hour | The effort also includes the time to upload the SCRYPT3 to the appliance. This upgrade will upgrade low level components in the appliance. |
| Test Restore. | TBD |  |
| Secure Restore. | 1 hour | The effort could be shorter or longer depending on the configuration size. |
| Downgrade the IDG (8436) to the last installed version and restore the configuration. | 1 hour |  |



# Execution

The following Sections describe the special parameters that are unique when executing a task used in the Migration Steps.

## Executing Tasks on the WebGUI

### Upgrade Path to firmware v10.5.0 migration tool for the IDG (8436)

Needed:

Open a support case to request the migration tool.

The IDG must be running a version of the 2018.4.1.x or 10.0.1.x firmware levels.

*Recommend is to be on the latest fix pack level of these firmware releases*.

The next steps are:

Take a secure backup of the IDG to use to restore the current configuration if needed.

Apply the migration tool build to the IDG.

Take a new secure backup to use on the X3.

Perform a roll-back to the previous firmware.

### Secure Restore

Navigate to System Control in the WebGUI and scroll to the Secure Restore section:

Graphical user interface, text, application

Description automatically generated

Enter the machine type and model the Secure Backup was created on.

It is case sensitive so type in exactly as it is below.

A picture containing chart

Description automatically generated

Note: You may also confirm the machine type and model by looking at the manifest file in the secure backup.

## Executing Tasks on the DataPower CLI

### Secure Restore

The cli command to restore on the X3 when in the configuration mode.

Syntax

secure-restore *credentials source* *[validate] [backup-machine-type]*

*credentials*

Specifies the identification credentials to decrypt the secure backup.

*Source*

Specifies the URL of the source directory to restore the backup files from. The supported file system locations are local: and temporary:

The supported remote location is an FTP server.

For the FTP protocol, use the ftp://*user*:*password*@*host*/ format.

*validate*

Indicates whether to validate the backup files or restore from the backup files.

on

Validates the backup files and does not restore from the backup files.

off

Restores from the backup files. This setting is the default value.

backup-machine-type

For the backup-machine-type, enter the machine type the Secure Backup was taken on. It is case sensitive so type in exactly as it is below.

A picture containing chart

Description automatically generated

Note: You may also confirm the machine type and model by looking at the manifest file in the secure backup.

## Loading the Private Keys into the HSM using the WebGUI

**Important note:**

Keys from an HSM in an idg 8436 (HSM2) machine type **are not compatible** the HSM in the 8441 or 8496 (HSM3) appliance types.

The first step is to verify the HSM has been initialized on the 53X appliance.

Once the HSM is initialized then any key that is imported will be loaded on the HSM.

To check the status from the CLI enter: “show crypto-engine”

**Example:**

idg# show crypto-engine

Crypto accelerator type: hsm3

Crypto accelerator status: hsmIsUninitialized

Crypto accelerator FIPS 140-2 level: uninitialized

Crypto accelerator FIPS 140-2 role: notApplicable

Disabled hardware features: none

If this status is: hsmIsUninitialized then you will need to initialize the HSM module with the following commands:

config

crypto

hsm-reinit

y

exit

exit

shutdown reboot

y

Example:

idg(config-crypto)# hsm-reinit

Attention - All private keys in the HSM will be destroyed at next firmware reload.

Do you want to continue? Yes/No [y/n]:y

HSM will be reinitialized at next firmware reload.

idg(config-crypto)# exit

Exiting Crypto mode

idg(config)# exit

idg# shutdown reboot

You have requested a system shutdown :reboot. Do you want to continue? Yes/No [y/n]: y

System about to reboot in 10 seconds

**Note**: See the IBM documentation for the [initialization of the HSM](https://www.ibm.com/docs/en/datapower-gateway/10.5?topic=module-initializing-hsm) and the available options.

**Moving or importing keys**

If you are moving keys from a different HSM equipped appliance you may use the “Clone HSM Key Wrapping Key” process.

Notes:

It is not supported to move keys from the HSM in the 8436 machine type appliances.

If you are just importing keys go to the Importing keys section.

**Moving keys from an HSM appliance** (except for from the 8436 appliance type as this is not supported)

This is a five step process that includes creating the HSM key wrapping domains on each appliance.

Once the key wrapping process is complete then you will be able to export and import the keys between the appliances in the key wrapping domain.

**Step 1**

To allow for the process change the HSM FIPS role to “Officer” on both the source and destination appliances:

Graphical user interface, text, application

Description automatically generated

A reboot is required after setting the role with the “Set HSM IPS Role” button.

Note: it may take 10-15 seconds for the pop up confirmation window to be displayed

Once the reboot is completed you may confirm the Role is set to “Crypto officer” by checking:

CLI command “show crypto-engine”

idg# show crypto-engine

Crypto accelerator type: hsm3

Crypto accelerator status: fullyOperational

Crypto accelerator FIPS 140-2 level: 3

Crypto accelerator FIPS 140-2 role: officer

Disabled hardware features: none

Or the “Crypto Accelerator Status” in the WebGUI:

Text, application

Description automatically generated with medium confidence

**Step 2**

**Note the next steps must be completed in one session as if the WebGUI session times out or the appliance rebooted the process will fail on the last step and you will need to start over with this step.**

On the ***source appliance*** create the first file needed for the key wrapping process.

Enter the name for the first file leave the Input file name as “none” then click the “Clone HSM Key Wrapping Key” and confirm when the confirmation popup window appears.

Note this may take 10-15 seconds

Graphical user interface, application

Description automatically generated

Once this is complete confirm the new file is now listed in the “temporary” directory and save the file to your workstation.

File Management:

Table

Description automatically generated with low confidence

Note: Select

**Step 3**

On the ***destination appliance*** create an output file that uses the file from step 2 as the input file.

In this example it will be the “Testkeyexport1” file.

Upload the file from step 2 to the temporary directory on the ***destination*** appliance.

Note if the file was listed as a text file remove the .txt from the filename on the upload.

Create the “output” file on the ***destination*** appliance:

Graphical user interface, application, Word

Description automatically generated

Download the file from the temporary directory

**Step 4**

On the source appliance create a new output file using the file created in Step 3

Upload the file from step 3 to the temporary directory on the ***source*** appliance.

Note if the file was listed as a text file remove the .txt from the filename on the upload.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

After the steps are complete change the role back to “user” on both appliances.

Once the role is changed back to “user” you may proceed with exporting a crypto object from the ***source*** and import it in the ***destination*** appliance

**To import private keys to the HSM from the WebGUI:**

* Navigate to “Crypto tools” and next open the “Import Crypto Object” tab.
* Select “Private Key” for the Object type.
* Enter the name for the key
* Select the key file to import the key may be manually loaded into the temporary directory or use the “Upload” the key from your workstation.
* Enter the password information if the key object has a password or password alias
* Select “Import Crypto Object” and wait for the popup to confirm the import

Graphical user interface

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Once the import is complete you may confirm the key by issuing the “show hsm” CLI command.

Before the import:

idg# show hsm

Key handle Key type Key URL Bit length Exportable

---------------- -------- ------------------- ---------- ----------

After the import:

idg# show hsm

Key handle Key type Key URL Bit length Exportable

---------------- -------- ------------------- ---------- ----------

000000000000000d private hsm://hsm3/Testkey5 2048 on

000000000000000e public hsm://hsm3/Testkey5 2048 on

Note: The public and private keys are created automatically on the import.

Appendices

## Possible Gotchas on the Secure Restore

**Restore errors:**

**1)** If the validate only option works but the restore fails look in the system logs and if you see errors like:

The cert is not yet valid or object is in the future

This would indicate the time was not set on the replacement

To resolve set the date and time.

Note: In some cases, you may need to perform a reboot for the restore to complete.

**2)** Receive error that file not found in the logs:

Confirm the secure backup file names and location.

Common file name issues noted:

The manifest file is renamed by the browser on download from .xml to .txt

Some file names are changed to all caps

To resolve these issues, rename the files to be correct.

Note: to confirm all the correct files are loaded open the manifest file and it will list:

a) The serial of the appliance the backup came from

b) The firmware version that the restore was created with

c) The files that are required for the restore

Important!! Never edit the contents of the manifest file

**3)** Not all static routes are restored.

If there are missing static routes you will need to add them manually.

Please report this to the support team with examples of what static routes were not included.

**4)** Licenses do not match

If you have enabled all of the modules on the “Target Appliance” and the license/features are different, open a Support Case for further assistance.

Connection issues:

In some cases the network will not immediately recognize the new appliance and in most cases performing a ping of the default gateway (or static route) from the appliance for each configured interface will force the ARP tables to be updated in the switch.

If the ping does not allow you to connect to the appliance over the network engage your network team to assist:

a) Some switches may need the port cleared to establish the connection.

b) In rare cases the switches have the hard coded MAC address listed and will need to be updated to match the new appliance MAC address(es).

c) Firewall rules may need updating

## Special Considerations When Only Using The 10 GB Interfaces on the IDG X2

1. If you are using either the eth0 or eth1 10GB ports, you must remove the configuration from each before taking the backup. This is needed as the X3 appliance does not have these ports and will cause the networking to be in a bad state after the restore.