

IBM Software Group

IBM DataPower Firmware Upgrades and Migration Between Hardware Generations

James Barrett and Pejman Haghighi

jtbarret@us.ibm.com, haghighi@us.ibm.com

Level 2 Software Engineer

July 8th, 2015



WebSphere® Support Technical Exchange

ON DEMAND BUSINESS™

Agenda

- **Firmware Upgrade**
 - ▶ **Upgrade considerations**
 - ▶ Downgrade
 - Roll back
 - Reinit
 - ▶ Virtual Appliances
 - ▶ Troubleshooting Failed upgrade
- Migration
 - ▶ Background
 - ▶ Secure Backup-Restore
 - ▶ Cross Platform Migration
 - ▶ Export/Import

Preliminary Considerations

- Where can I download DataPower Gateway firmware fixpacks?
 - ▶ Fix Central
- How often to upgrade--- twice a year
 - ▶ Apply critical updates
 - ▶ Consider install fixpacks instead of base level
- Upgrade may be performed via WebGUI, Command line (CLI) or XML Management Interface
- Which major releases are supported?
 - ▶ Firmware Lifecycle technote

How Often Should I Upgrade?

- Where can I track information about critical fixes?
 - ▶ [Critical Updates for IBM DataPower Gateways technote](#)
- Due to critical updates, some firmware versions may not be available on Fix Central
 - ▶ The decision to remove some fixpacks is for the protection of the customers, by providing the best code available as we always do

Considerations For Review Before Upgrading

- Deprecated & removed features technote
- Test before upgrading to production
- Plan 6 months in advance of end of support date to allow enough time to test/address potential issues
- Release notes and APAR fixes
 - ▶ Product documentation (Knowledge Center)
 - ▶ Supported firmware versions and recommended upgrade levels

Understanding the Firmware Numbering

- Version.Release.Modification.Fixpack
- Example: 7.1.0.2
- First 3 numbers indicate major release
- Fourth number indicates fixpack
- Upgrading fixpacks: no feature enhancements and implies simplified regression testing
- Upgrading between major releases includes new features and enhancements, implying need for broader regression tests and functional tests



How to Select Firmware Image

- Things to consider:
 - ▶ Include:
 - hardware generation and machine type
 - additional licenses
 - major and minor release
 - ▶ Additional reference: [Knowledge Center upgrade determining firmware images to download](#)

Selecting Image from Fix Central

- Example: XI52 physical appliance; desired firmware level is 7.1.0.4, Tibco license included

← IBM Support Portal

Fix Central

Supported products

Help

Related links

- Go to Fix Central mobile

Download files using HTTPS

WebSphere, IBM DataPower Gateways (7.1.0, All platforms)

→ [Manage your support notifications](#)

Download files using your web browser

Click the download link next to each file to download it.

Order number:	166601089
Total size:	1.88 GB

fix pack: XI52-7199-7.1.0.4-Firmware [Fix list](#)

DataPower-7.1.0.4-XI52-7199

The following files implement this fix.

- [xi7104.scrpt3 \(479.09 MB\)](#)
- [xi7104.tibco.scrpt3 \(479.69 MB\)](#)**
- [xi7104.oradco.scrpt3 \(483.72 MB\)](#)
- [xi7104.tibco.oradco.scrpt3 \(484.33 MB\)](#)
- [aoc-war-7104.tar \(130 KB\)](#)

Steps to Remember During Upgrade

- Make sure someone has physical or remote serial access to login as privileged user
Connecting to the Serial console on DataPower
- Stop traffic (Quiesce and remove from cluster)
- Save any pending changes you want to persist
- Take backup of configuration
- Take an error report to have proactive data in case of issue, so we have historic data to help determine where in upgrade process issue occurred
- Perform shutdown reboot of the appliance

Steps to Remember During Upgrade

- Test to make sure all services are working after the reboot
- Upload the desired firmware image
- Boot image
- Make sure upgrade completes before entering other commands/resuming traffic

Agenda

- **Firmware Upgrade**
 - ▶ Upgrade considerations
 - ▶ **Downgrade**
 - **Roll back**
 - **Reinit**
 - ▶ Virtual Appliances
 - ▶ Troubleshooting Failed upgrade
- **Migration**
 - ▶ Background
 - ▶ Secure Backup-Restore
 - ▶ Cross Platform Migration
 - ▶ Export/Import

Downgrading Firmware- Background

- It is safe to downgrade between 2 fixpacks on the same stream using the upgrade process
- Example : Downgrade from 7.0.0.5 to 7.0.0.2
- Other options:
 - ▶ Rollback to previous image
 - Limited based on previous image
 - ▶ Reinitialization
 - Follow wizard or manually configure



Downgrade: Roll back

- Roll back: This method may be taken if the appliance has been upgraded before
- Useful for backing out a firmware change
- For example: If you upgrade 6.0.0.14 to 6.0.1.10
- This will allow you to roll back to 6.0.0.14
- Doing again would go back to 6.0.1.10
- Rolling back would restore to the configuration to the state prior to upgrading to 6.0.1.10
 - ▶ Example: Changing password of user, if you roll back the new password does not persist

Roll back example

- CLI: Commands **bolded**
xi52# **co**
Global configuration mode
xi52(config)# **flash**
Flash configuration mode
xi52(config-flash)# **boot switch**
- GUI



System Control

Set Time and Date

Date

Time hh:mm:ss

Boot Image

I accept the terms of the license agreements.

Firmware File *

Firmware Roll-Back

Downgrade: Reinitialization

- Technote Using the "reinitialize" CLI command to reconfigure an appliance.
- During reinitialization, all configuration is wiped
 - ▶ Someone should have physical or remote serial access to the appliance for network configuration
- Specify which firmware by using the appropriate image



Downgrade: Reinitialization

- Example of re-init of a xi52 appliance running V7.1.0. CLI Commands **bolded**
- xi52# **co**
- Global configuration mode
- xi52(config)# **flash**
- Flash configuration mode
- xi52(config-flash)# **reinit xi7007.scrypt3**

Downgrade: Reinitialization- Setup

- Press any key means press enter
- Using Wizard
 - Configure required interfaces if not using all don't configure unused interfaces to avoid network configuration issues with strict enforcement feature.
 - Best practice bind to specific IP address and port when setting up management access
 - Initialize RAID if applicable as it's assumed to be initialized in secure restore
- Accept license From WebGUI

Considerations When Reinitializing

- Common criteria mode
 - ▶ Not recommended or necessary for most customers
 - ▶ Only used when appliance needs to be Evaluation Assurance Level 4 (EAL4) certified
 - Knowledgecenter Common Criteria Mode
- Disaster recovery---secure backup
 - ▶ Valuable asset during appliance migration
 - ▶ Cannot be changed after initial setup

Agenda

- **Firmware Upgrade**
 - ▶ Upgrade considerations
 - ▶ Downgrade
 - Roll back
 - Reinit
 - ▶ **Virtual Appliances**
 - ▶ Troubleshooting Failed upgrade
- Migration
 - ▶ Background
 - ▶ Secure Backup-Restore
 - ▶ Cross Platform Migration
 - ▶ Export/Import

Virtual Appliances

- Minimum Requirements
 - ▶ Knowledgecenter v 7.2.0 Virtual Requirements
 - ▶ Absolute minimum of 2 vCPU and 4 GB of RAM are required
 - ▶ Resource requirements depend on the configuration of DataPower services
- IBM suggests carefully considering capacity requirements to allow for sufficient resources to run your services as minimum may not be sufficient
- Recommended default: 8vCPU and 8GB RAM

Virtual Appliances

- All Virtual Appliances must be running 5.0.0.8 or later for upgrading to v 6.0.0 or newer versions
 - ▶ [Supported Upgrade and Downgrade paths for DataPower Virtual Edition](#)
- Contact support if issue with temporary space to upload the v 7.0.0 and later images on a virtual appliances.



Agenda

- **Firmware Upgrade**
 - ▶ Upgrade considerations
 - ▶ Downgrade
 - Roll back
 - Reinit
 - ▶ Virtual Appliances
 - ▶ **Troubleshooting Failed upgrade**
- Migration
 - ▶ Background
 - ▶ Secure Backup-Restore
 - ▶ Cross Platform Migration
 - ▶ Export/Import

What to Do When an Upgrade Fails

- Review error message and “resolution to common problems” in [upgrade technote](#)
- Example: “Error extracting firmware: Firmware parsing error
Upgrade failure in dynamic loader: Firmware parsing error
The dynamic loader failed to upgrade the system (-1).
The resident loader will be used instead.”
- As per technote, download image file again and perform shutdown reboot

What to Do When an Upgrade Fails

- If upgrade fails, best practice is perform shutdown reboot; clearing temp space on appliance
- If you observe an error that does not match any error messages in upgrade technote
 - ▶ Gather a debug log-level error report and screenshot of error
 - ▶ Perform a shutdown reboot of the appliance
 - ▶ Retry upgrade
 - ▶ If the upgrade is unsuccessful after the reboot, open a PMR and attach error report

Post-Upgrade

- Any expired certificates will be deleted after an upgrade or reboot
- Troubleshooting connecting to the WebGUI after upgrade and certificates expired



Known Behaviors

- Many things are cached on a reboot
 - ▶ e.g. keys, certificates, stylesheets, configuration files, etc.
 - ▶ If these are deleted by mistake, that is not noticed until next restart/upgrade
For example: a key is uploaded to the encrypted filesystem
 - ▶ The key object is instantiated
 - ▶ DP reads the file and caches the key data
 - ▶ The file is deleted - Box runs ok; then ...

Known Behaviors(Continued)

- ▶ Box is upgraded, there is no key file so the key object does not come up
- ▶ services fail
- ▶ support gets called that 'upgrade broke the system.'
 - Recommendation: before the upgrade; reboot the box and test to make sure all services are working.
 - Also may be useful to utilize certificate monitor feature to track expired certificates

Known Behaviors Networking

- Behavior changes after upgrading to 7.0.0
 - ▶ Strict enforcement of valid network configuration in version 7.0.0
 - New default setting. Makes sure valid network configuration or blocks non-management traffic
 - When doing initial setup be careful with IPv6 default gateway. Only setup if IPv6 defined

Known Behaviors Networking

- Behavior changes after upgrading to 7.0.0
 - ▶ Change in default metric for default gateways
 - Now default gateways have metric of 200. Affects complex routing configs
 - ▶ 1 Gbit ethernet interfaces fail to link if configured in Full-duplex
 - Use auto-negotiate instead
 - FIN APAR [IT06247](#)

Known Behaviors Security

- Behavior changes after fixpacks
 - ▶ Security fixes were applied to protect users from security vulnerabilities
 - ▶ Verify that configurations work after applying the new firmware or workaround
 - ▶ Example: Disabling SSLv3
 - Make sure SSL proxy profiles still working
 - If you are still using SSLv3 protocol those objects will fail

Agenda

- Firmware Upgrade
 - ▶ Upgrade considerations
 - ▶ Downgrade
 - Roll back
 - Reinit
 - ▶ Virtual Appliances
 - ▶ Troubleshooting Failed upgrade
- **Migration**
 - ▶ **Background**
 - ▶ Secure Backup-Restore
 - ▶ Cross Platform Migration
 - ▶ Export/Import

What is Migration & Why Should I Migrate?

- Migration is the process of transferring a configuration from one appliance to another
- Common reasons for migrating
 - ▶ End of support for a hardware generation
 - ▶ Purchase of a new appliance
 - ▶ Replacement of an appliance
- For example:
 - ▶ Migrating from XI50 to XI52 appliance due to XI50 being out of support

Methods to Migrate

- Secure Backup/Restore
 - ▶ Includes user info and cryptographic data in addition to exported configuration
- Export/Import
 - ▶ Copy of the service configuration
 - ▶ Does not contain private data or user info



Agenda

- Firmware Upgrade
 - ▶ Upgrade considerations
 - ▶ Downgrade
 - Roll back
 - Reinit
 - ▶ Virtual Appliances
 - ▶ Troubleshooting Failed upgrade
- **Migration**
 - ▶ Background
 - ▶ **Secure Backup-Restore**
 - ▶ Cross Platform Migration
 - ▶ Export/Import

Secure Backup

- Way of backing up appliance configuration, including certificates, keys, and user info
- Enabled during initialization and reinitialization
- Performing a secure restore on an appliance also enables secure backup on that appliance
- Example CLI:

```
xg45(config)# secure-backup MyCert ftp://ftpuser:passw0rd@ipaddress:port/BackupDir off off
```

Checking if Secure Backup is Enabled


- To determine whether disaster recovery is available, check value of Backup Mode property
 - ▶ GUI: view the System Settings
 - ▶ CLI: show system
- If the value is Secure, disaster recovery is available

```
xg45# show system

description: DataPower XG45
serial number: 0000000
entitlement id: 0000000
product id: 5725 [Rev None]
  OID: 1.3.6.1.4.1.14685.1.7
uptime: 3 days 08:16:00
contact: (unknown)
  name: (unknown)
location: (unknown)
services: 72
backup mode: secure
product mode: normal
```

Secure Backup Best Practices

- Before secure backup, make sure the appliance is quiesced and taken out of cluster
- RAID and iSCSI
 - ▶ Should be backed via alternate method due to significant resource consumption
 - ▶ Enabled by default, so make sure to take appropriate steps to disable them



The screenshot shows a configuration window titled "Secure Backup". It contains the following fields and controls:

- Crypto certificate:** A dropdown menu with "datapower" selected, followed by "[down]", "+", "...", and "*" buttons.
- Destination:** A text input field containing "local://backup" and an asterisk "*" to its right.
- Include iSCSI:** Radio buttons for "on" and "off", with "off" selected.
- Include RAID:** Radio buttons for "on" and "off", with "off" selected.
- Secure Backup:** A button at the bottom of the form.

Secure Backup Crypto Credential

- Configuration for private keys supported formats:
DER, PEM, PKCS #8, and PKCS #12
- Configuration for certificates supported formats:
DER, PEM, PKCS #7, and PKCS #12
- Can be generated using Crypto Tools on appliance or by other servers/applications
- If generated on appliance make sure to Export Private Key

Secure Backup Best Practices

- Local backups, ensure that enough space is available on the appliance to store backup
- Remote backups, ensure sufficient network bandwidth and space in the target directory
- After backup, protect the backup files as you would any other critical data
- Keep the private key of the public certificate used to create the secure backup; it will be required to restore the secure backup

Secure Backup Best Practices

- You can store the secure backup files locally or remotely. Valid protocols are local, temporary, or File Transfer Protocol (FTP).
- Secure-backup overwrites previous backups when writing to the same destination
- Validate secure backup with secure restore validate to ensure not corrupt
- Keep a copy of installed firmware image as secure restore must be performed on same version



Secure Restore

- What to keep safe for restore
 - ▶ Private Key
 - ▶ Firmware image
 - ▶ Backup file
- Keep in a safe place in case needed
- Make sure someone has physical or remote serial access to login as privileged user
 - ▶ To validate network configuration
- After secure restore is complete, admin password changes back to “admin”

Secure Restore

- Best practice to perform on a clean reinitialized device
 - ▶ Expectation is appliance is initialized meaning startup wizard has been run and RAID configured if applicable
 - ▶ Potential issues if secure restore with RAID when RAID hasn't been initialized
- DWAnswers Best Practices Secure restore with RAID



Agenda

- Firmware Upgrade
 - ▶ Upgrade considerations
 - ▶ Downgrade
 - Roll back
 - Reinit
 - ▶ Virtual Appliances
 - ▶ Troubleshooting Failed upgrade
- **Migration**
 - ▶ Background
 - ▶ Secure Backup-Restore
 - ▶ **Cross Platform Migration**
 - ▶ Export/Import

Cross Platform Migration

- Secure backup-restore from Virtual to Physical and vice versa is not supported
- New IDG (8436) Appliance can be secure restored from appliance models:
 - XG45
 - XI52
 - XB62
 - IDG
- Specify Appliance model during secure restore

Cross Platform Migration Example

- Migrating Virtual XI52 to IDG



The screenshot shows a web-based configuration interface for 'Secure Restore'. The interface includes the following fields and controls:

- Secure Restore** (Section Header)
- Crypto Credential**: A dropdown menu with 'jimidcred' selected, followed by a '+' button, an ellipsis button, and an asterisk.
- Source**: A text input field containing 'local://mydir' and an asterisk.
- Only validate the backup**: Radio buttons for 'on' (selected) and 'off'.
- Appliance model**: A text input field, which is highlighted by a red arrow pointing from the left.
- Secure Restore** (Button)

- Online help → Clicking the hyperlink
 - ▶ Find appropriate Appliance model in table
 - ▶ Can also check using **show version** in CLI

Agenda

- Firmware Upgrade
 - ▶ Upgrade considerations
 - ▶ Downgrade
 - Roll back
 - Reinit
 - ▶ Virtual Appliances
 - ▶ Troubleshooting Failed upgrade
- Migration
 - ▶ Background
 - ▶ Secure backup-restore
 - ▶ Cross platform migration
 - ▶ **Export/Import**



Export/Import

- Export/Import from Virtual to Physical and vice versa is possible/supported
- Creates an export of service configuration
- Need to create new private data or restore from alternate location
- Not supported to migrate config from newer major release to older version eg. 7.0.0.5->6.0.0.0
- Example:



Export

- Copy or move configuration and files between domains
- Create a backup of one or more application domains
- Create a backup of the entire system
- Export configuration and files from the current domain

Next

Cancel

Summary

- Firmware upgrade allows customers to install the latest fixes and new features
- Make sure to install critical updates to avoid exposure to known issues vulnerabilities with high impact
- Follow procedure for upgrade to limit issues and effectively troubleshoot if issue occurs

Summary

- Customers can migrate across platforms and appliances using secure backup and/or export/import
- Make sure to keep Firmware image, Public certificate and Private key safe when using Secure backup-restore
- When using Export/Import for migration be prepared to generate new certificates and keys or to restore from an alternate location as they are not included

Additional Resources - Upgrade

- Knowledge Collection: How to upgrade the firmware on an IBM WebSphere DataPower Gateway Appliance
- How frequently one should apply a fixpack to DataPower Gateway appliance?
- Modified date of local files is changed after a firmware upgrade
- Networking changes in version 7.0.0



Additional Resources - Migration

- Secure backup-Restore for WebSphere DataPower SOA Appliances
- Secure restore for WebSphere DataPower SOA Appliances
- How can I export a private key from DataPower Gateway Appliance?
- Backing up, exporting and importing the configuration of an IBM DataPower Gateway
- Best practices doing secure restore and initializing the RAID
- Migrating old models to IDG with secure restore

Connect with us!

1. Get notified on upcoming webcasts

Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe

2. Tell us what you want to learn

Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com



Questions and Answers

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
<http://www.ibm.com/developerworks/websphere/community/>
- Join the Global WebSphere Community:
<http://www.websphereusergroup.org>
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:
<http://www.ibm.com/software/info/education/assistant>
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
<http://www.ibm.com/software/websphere/support/d2w.html>
- Sign up to receive weekly technical My Notifications emails:
<http://www.ibm.com/software/support/einfo.html>