

DataPower Integration Appliance XI50  
Version 3.8.1

*Administrators Guide*





DataPower Integration Appliance XI50  
Version 3.8.1

*Administrators Guide*



**Note**

Before using this information and the product it supports, read the information in “Notices and trademarks” on page 235.

**First Edition (June 2010)**

This edition applies to version 3, release 8, modification 1 of IBM WebSphere DataPower Integration Appliance XI50 and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2002, 2010.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

---

## Part 1. Getting Started . . . . . 1

### Chapter 1. Introduction . . . . . 3

Intended audience . . . . .	3
File naming guidelines . . . . .	3
Object naming guidelines . . . . .	4
Typeface conventions . . . . .	4

---

## Part 2. Working with the WebGUI . . . 5

### Chapter 2. WebGUI basics . . . . . 7

Objects on the appliance . . . . .	7
Working with objects . . . . .	7
Accessing the WebGUI . . . . .	7
Welcome screen . . . . .	7
Common WebGUI conventions . . . . .	8
Working with referenced objects . . . . .	8
Working with lists of referenced objects . . . . .	9
Viewing and editing local files during configuration . . . . .	9
Viewing local files . . . . .	10
Editing local files . . . . .	10

### Chapter 3. Common WebGUI tasks. . . 11

Applying and saving changes . . . . .	11
Canceling changes . . . . .	11
Resetting objects . . . . .	11
Deleting objects . . . . .	11
Exporting objects . . . . .	12
Viewing configuration-specific messages. . . . .	12
Viewing messages from the catalog . . . . .	12
Viewing messages from the configuration pane . . . . .	12
Viewing object status . . . . .	12

---

## Part 3. Controlling user access to the appliance . . . . . 15

### Chapter 4. Managing user access . . . 17

Understanding RBM on the DataPower appliance . . . . .	17
Optimizing access on the DataPower appliance . . . . .	18
Capabilities of RBM . . . . .	18
Authenticating users . . . . .	18
Access profile. . . . .	18
User access to resources . . . . .	19
Configuring RBM settings . . . . .	19
RBM using custom authentication . . . . .	21
RBM using LDAP authentication . . . . .	22
RBM using local user authentication . . . . .	24
RBM using RADIUS authentication . . . . .	25
RBM using SAF authentication . . . . .	27
RBM using SPNEGO authentication . . . . .	28
RBM using SSL user certificate . . . . .	30
RBM using XML file authentication . . . . .	31
Defining the password policy . . . . .	33

Defining LDAP Search Parameters objects . . . . .	34
Managing RBM access. . . . .	35
Defining the account policy . . . . .	35
Restoring RBM access from the command line. . . . .	36
Extending RBM access to the WebGUI only. . . . .	36
Enabling the RBM admin-state from the command line . . . . .	37
Publishing an RBM XML file to another appliance . . . . .	37
Flushing the RBM cache . . . . .	37

### Chapter 5. Using the builder to create an RBM policy file . . . . . 39

Using the RBM XML file . . . . .	39
RBM XML file for authentication and authorization . . . . .	39
RBM XML file for authentication . . . . .	41
RBM XML file for authorization . . . . .	42

### Chapter 6. Managing user group accounts . . . . . 45

Creating a group account. . . . .	46
Specifying the access policy . . . . .	46
Example access policies . . . . .	46
Controlling access to the command line . . . . .	47
Adding access to a command group . . . . .	47
Removing access to a command group . . . . .	47

### Chapter 7. Using the Access Policy builder . . . . . 49

Elements of an access policy. . . . .	49
Adding an access policy . . . . .	50
Example access profile that grants full access . . . . .	51
Example access policy that uses wildcards . . . . .	51
Example access policy that grants user management permissions . . . . .	51
Editing an access profile . . . . .	52
Removing an access profile . . . . .	52

### Chapter 8. Managing user accounts . . . 53

Creating user accounts . . . . .	53
Resetting the admin password . . . . .	54
Migrating a user to a new group . . . . .	54
Forcing a password change . . . . .	54
Changing the password for the current user . . . . .	55
SNMP V3 users . . . . .	55
Viewing local SNMP engine ID. . . . .	55
Creating an SNMP V3 account . . . . .	56

---

## Part 4. Managing the appliance . . . 59

### Chapter 9. Securing communication . . 61

Supported cryptographic formats . . . . .	61
Working with keys and certificates . . . . .	61

Creating key-certificate pairs . . . . .	61
Generating keys and certificates . . . . .	62
Exporting keys and certificates . . . . .	63
Importing keys and certificates . . . . .	64
Converting keys to specific formats . . . . .	64
Converting certificates to specific formats . . . . .	65
Working with certificate revocation lists . . . . .	65
Enabling CRL retrieval . . . . .	65
Configuring CRL update policies . . . . .	65
Defining the Certificate Monitor . . . . .	67

## Chapter 10. Managing the appliance

### itself. . . . . 69

Ethernet and VLAN interfaces . . . . .	69
Standby configurations . . . . .	69
Configuring Ethernet interfaces. . . . .	76
Configuring VLAN interfaces . . . . .	77
Defining static routes . . . . .	78
Defining interface failover . . . . .	78
Enabling self-balancing . . . . .	79
Removing an Ethernet interface from the network	80
Initiating a packet-capture session . . . . .	80
Configuring appliance-wide network settings . . . . .	80
DNS Settings . . . . .	82
DNS hosts cache. . . . .	82
Load balancing algorithm . . . . .	82
Configuring the DNS service . . . . .	84
Flushing the DNS hosts cache . . . . .	84
Host Alias . . . . .	84
Working with local host aliases. . . . .	84
Migrating configuration data . . . . .	85
Managing NTP Servers . . . . .	86
Managing the time on the appliance . . . . .	86
Setting the local time and date . . . . .	86
Setting the local time zone . . . . .	87
Creating a custom time zone . . . . .	87
Selecting the reboot configuration . . . . .	88
Configuring throttle settings. . . . .	88
Shutting down the appliance . . . . .	90
Controlling the locate LED (Type 9235) . . . . .	91
Activating the locate LED . . . . .	91
Deactivating the locate LED . . . . .	91
Generating an appliance certificate . . . . .	91
Appliance settings . . . . .	91
Defining appliance-specific information . . . . .	92
Updating the serial number after a replacement	92
Enabling customized interfaces . . . . .	92
Reserving space for the audit log . . . . .	93
Viewing hardware information . . . . .	93
Configuring NFS Settings. . . . .	94
NFS Client Settings. . . . .	94
NFS Dynamic Mounts . . . . .	94
NFS Static Mounts . . . . .	96
Using the iSCSI protocol (Type 9235) . . . . .	98
IQN and EUI formats . . . . .	99
Configuring and initializing an iSCSI volume . . . . .	99
Repairing an iSCSI volume . . . . .	100
Reference objects for iSCSI . . . . .	101
Configuring SNMP Settings . . . . .	102
Configuring global properties . . . . .	102
Configuring subscriptions . . . . .	103

Configuring communities . . . . .	103
Configuring recipients . . . . .	104
Configuring contexts . . . . .	104
Viewing MIBs . . . . .	105
Default event subscriptions. . . . .	105
Sysplex Distributor Target Control Service. . . . .	106
Creating a Sysplex Distributor Target Control	107
Service . . . . .	107
Quiescence . . . . .	107
Quiesce . . . . .	108
Unquiesce . . . . .	108
Checking quiesce and unquiesce status. . . . .	109
Quiescing the appliance . . . . .	109
Unquiescing the appliance . . . . .	109

## Chapter 11. Managing network access to the appliance . . . . . 111

WebGUI access . . . . .	111
Modifying configuration for WebGUI access . . . . .	111
Changing security and connection settings. . . . .	112
Command line access. . . . .	112
Connecting to the serial port . . . . .	112
Connecting using serial over LAN (Type 4195)	113
SSH service . . . . .	114
Enabling Telnet services . . . . .	115
XML Management Interface . . . . .	115
Services overview . . . . .	116
Enabling interface services . . . . .	117
Changing default security and HTTP settings	118
SOAP interface . . . . .	118
General structure of requests . . . . .	119
General structure of responses. . . . .	119
Available operations for requests . . . . .	119
Example request to view status . . . . .	121
Example request to compare configurations . . . . .	122
WSDM interface . . . . .	123
Example request to view the number of client	125
requests . . . . .	125
Example request to view active users . . . . .	126
Example request to view CPU usage . . . . .	126
Example request to view appliance usage . . . . .	127
Example request to view accepted connections	127
Custom SSL proxy profile . . . . .	127
Generating a custom profile . . . . .	127
Removing the profile assignment. . . . .	128
Cryptographic material for the custom profile	128

## Chapter 12. Managing the firmware image. . . . . 129

Applying a firmware image . . . . .	129
Rolling back an upgrade . . . . .	129

## Chapter 13. Managing files . . . . . 131

Directories on the appliance . . . . .	131
Launching the File Management utility. . . . .	133
Displaying directory contents . . . . .	133
Creating a subdirectory . . . . .	133
Deleting a directory . . . . .	134
Refreshing directory contents . . . . .	134
Uploading files from the workstation . . . . .	134

Working with Java Key Stores . . . . .	135	Contents of a secure backup . . . . .	160
Required software . . . . .	135	Conditions . . . . .	160
Granting permissions . . . . .	135	Creating a secure backup of the appliance . . . . .	161
Types of key stores . . . . .	135	Restoring the appliance from a secure backup . . . . .	161
Uploading a file from a Java Key Store . . . . .	135	Validating a secure backup . . . . .	162
Fetching files . . . . .	136		
Copying files . . . . .	136	<b>Chapter 16. Deployment policies . . . . . 163</b>	
Renaming files . . . . .	137	Creating deployment policies . . . . .	163
Moving files . . . . .	137	Using the deployment policy builder . . . . .	164
Viewing files . . . . .	138	Specifying the matching statement . . . . .	165
Editing files . . . . .	138		
Deleting files . . . . .	138	<b>Chapter 17. Managing event logs . . . . . 167</b>	
<b>Chapter 14. Managing auxiliary data storage . . . . . 139</b>		Types of log targets . . . . .	167
Configuring the compact flash . . . . .	139	Configuring log categories . . . . .	168
Managing the file system on the compact flash . . . . .	139	Configuring log targets . . . . .	168
Initializing the file system . . . . .	139	Setting event filters . . . . .	169
Repairing the file system . . . . .	140	Setting object filters . . . . .	169
Configuring the hard disk array . . . . .	140	Setting event triggers . . . . .	170
Managing the file system on the hard disk array . . . . .	140	Setting IP address filters . . . . .	171
Initializing the file system . . . . .	140	Setting event subscriptions . . . . .	171
Repairing the file system . . . . .	140	Viewing logs . . . . .	172
Managing the RAID volume . . . . .	141	Filtering logs . . . . .	172
Activating the volume . . . . .	141	Understanding logs . . . . .	173
Initializing the volume . . . . .	141	Configuring an e-mail pager . . . . .	174
Rebuilding the volume . . . . .	141	Scenario: Defining a load Balancer as a log target . . . . .	174
Deleting the volume . . . . .	141	Scenario: Defining event triggers . . . . .	175
		Starting and stopping a package capture . . . . .	175
		Creating an error report . . . . .	175
		Using a custom message . . . . .	176
<b>Chapter 15. Managing the configuration of the appliance . . . . . 143</b>		<b>Part 5. Referenced objects . . . . . 179</b>	
Managing domains . . . . .	143	<b>Chapter 18. Service objects . . . . . 181</b>	
The default domain . . . . .	143	HTTP Service . . . . .	181
Application domains . . . . .	143	Creating an SSL Proxy service . . . . .	182
Visible domains . . . . .	144	Creating a TCP Proxy service . . . . .	183
Creating application domains . . . . .	144		
Restarting application domains . . . . .	145	<b>Chapter 19. Referenced objects . . . . . 185</b>	
Resetting application domains . . . . .	146	Access Control List . . . . .	185
Quiescing application domains . . . . .	146	Overview . . . . .	185
Unquiescing application domains . . . . .	146	Creating an Access Control List object . . . . .	186
Creating Include Configuration File objects . . . . .	147	Working with Certificate objects . . . . .	186
Creating Import Configuration File objects . . . . .	148	Working with z/OS certificates . . . . .	186
Backing up and exporting configuration data . . . . .	149	Defining Certificate objects . . . . .	187
Backing up the entire appliance . . . . .	149	Defining Identification Credentials objects . . . . .	188
Backing up domains . . . . .	150	Kerberos objects . . . . .	189
Exporting select objects . . . . .	150	Points to remember when using Kerberos . . . . .	190
Copying or moving select objects . . . . .	152	Configuring a Kerberos KDC Server object . . . . .	190
Managing configuration checkpoints . . . . .	154	Configuring a Kerberos Keytab File object . . . . .	191
Defining number configuration checkpoints to allow . . . . .	154	Working with Key objects . . . . .	192
Saving configuration checkpoints . . . . .	154	Working with z/OS keys . . . . .	192
Listing configuration checkpoints . . . . .	155	Defining Key objects . . . . .	192
Rolling back to a configuration checkpoint . . . . .	155	Load balancer groups . . . . .	194
Deleting configuration checkpoints . . . . .	155	Intelligent load distribution . . . . .	194
Importing configuration data . . . . .	156	Algorithms for making load balancing decisions . . . . .	198
Managing changes in configuration data . . . . .	157	Membership . . . . .	199
Comparing configurations . . . . .	158	Health checks . . . . .	200
Reading the change report . . . . .	158	Session affinity . . . . .	200
Reverting changes . . . . .	159	Configuring a load balancer group . . . . .	202
Managing disaster recovery . . . . .	159		

Modifying to use workload management information . . . . .	206
Assigning weight to members . . . . .	207
Disabling members . . . . .	207
Enabling the retrieval of workload management information . . . . .	207
Enabling the retrieval of workload management information for non-WebSphere application servers . . . . .	211
Defining cryptographic profiles . . . . .	216
RADIUS Settings . . . . .	217
NAS-identifier . . . . .	218
Configuring RADIUS Settings . . . . .	218
Adding SSH known hosts . . . . .	219
SSL Proxy Profile objects . . . . .	219
Creating a forward (or client) proxy . . . . .	220
Creating a reverse (or server) proxy . . . . .	220
Creating a two-way proxy . . . . .	221
Validation credentials. . . . .	221
Creating for non-expiring, non-password-protected certificates . . . . .	222
Validation methods . . . . .	222
PKIX validation . . . . .	222
Creating for specific certificates . . . . .	223
WebSphere Cell . . . . .	224
Selecting the update method . . . . .	224

Creating a WebSphere Cell . . . . .	224
NSS Client . . . . .	226
Creating the NSS Client . . . . .	227

## Appendix. User interface customization . . . . . 229

Aspects that can be customized . . . . .	229
Markup supported for the XML file . . . . .	229
Structure of the XML file . . . . .	231
Command line prompt extension definition . . . . .	232
Example messages for WebGUI sessions . . . . .	232
Example pre-login message. . . . .	232
Example post-login message . . . . .	232
Example appliance messages . . . . .	232
Example messages for command line sessions . . . . .	233
Example pre-login message. . . . .	233
Example post-login message . . . . .	233
Example appliance message . . . . .	233
Template of the custom user interface file . . . . .	234

## Notices and trademarks . . . . . 235

Trademarks . . . . .	235
----------------------	-----

## Index . . . . . 237



---

# Part 1. Getting Started

**Chapter 1. Introduction . . . . . 3**  
Intended audience . . . . . 3  
File naming guidelines . . . . . 3  
Object naming guidelines . . . . . 4  
Typeface conventions . . . . . 4



---

## Chapter 1. Introduction

IBM® WebSphere® DataPower® SOA Appliances are purpose-built, easy-to-deploy Network appliances that simplify, help secure, and accelerate your XML and Web Services deployments while extending your SOA infrastructure. These appliances offer an innovative, pragmatic approach to harness the power of SOA while simultaneously enabling you to leverage the value of your existing application, security, and Networking infrastructure investments.

---

### Intended audience

This document is intended for administrators of who are responsible for the configuration and maintenance of the DataPower appliance. Administrators should have the following knowledge:

- Network architecture and concepts
- Internet and transport protocols
- Lightweight Directory Access Protocol (LDAP) and directory services
- Authentication and authorization
- XML and XSLT

Administrators should also be familiar with SSL protocol, key exchange (public and private), digital signatures, cryptographic algorithms, and certificate authorities.

The types of administrators who will work on the appliance include the following broad roles which are found in a typical Enterprise organization:

- A single administrator with the `admin` account who manages day-to-day operations.  
On zBX, this administrator account is renamed: `dp-admin`.
- System administrators who manage access to all objects except Network interfaces.
- Network administrators who manage Network connectivity and real time operational data for the appliance.
- Account administrators who manage users and user groups.
- Access administrators who manage access to all resources, access policies, Role Based Management (RBM), cryptographic keys, authentication, and authorization.
- Lifecycle administrators who manage simple appliance and domain backups, as well as lifecycle migration of primary objects.

---

### File naming guidelines

The maximum length for a file name can be approximately 4128 characters. The name of the base file can be up to 128 characters in length. The base file is the part after the name of the DataPower directory. Examples of directories are `local`, `store`, and `temporary`.

If the directory (or domain) supports subdirectories, the path to the file can have a length of 4000 characters. When you create a domain, its name is the base file name in several DataPower directories when viewed from the default domain.

The following characters are valid in directory and file names:

- a through z
- A through Z
- 0 through 9
- \_ (underscore)
- - (dash)
- . (period)

**Note:** Names cannot contain two consecutive periods (. .).

---

## Object naming guidelines

The object name must be unique in the object namespace. The following characters are valid when specifying the name for an object:

- a through z
- A through Z
- 0 through 9
- \_ (underscore)
- - (dash)
- . (period)

**Note:** Names cannot contain two consecutive periods (. .).

---

## Typeface conventions

The following typeface conventions are used in the documentation:

**bold** Identifies commands, programming keywords, and GUI controls.

*italics* Identifies words and phrases used for emphasis and user-supplied variables.

`monospaced`  
Identifies user-supplied input or computer output.

---

## Part 2. Working with the WebGUI

<b>Chapter 2. WebGUI basics</b>	7
Objects on the appliance	7
Working with objects	7
Accessing the WebGUI	7
Welcome screen	7
Common WebGUI conventions	8
Working with referenced objects	8
Working with lists of referenced objects	9
Viewing and editing local files during configuration	9
Viewing local files	10
Editing local files	10
 <b>Chapter 3. Common WebGUI tasks</b>	 11
Applying and saving changes	11
Canceling changes	11
Resetting objects	11
Deleting objects	11
Exporting objects	12
Viewing configuration-specific messages	12
Viewing messages from the catalog	12
Viewing messages from the configuration pane	12
Viewing object status	12



---

## Chapter 2. WebGUI basics

The WebGUI is the primary interface for managing the appliance itself and for configuring services.

---

### Objects on the appliance

Objects that can be configured on the appliance range from simple to complex. An object is any entity that you configure on the appliance. During configuration, an object can reference another object that can, in turn, reference another object. For example, the configuration of a service references an instance of the XML Manager object that references an instance of the User Agent object. The flexibility in configuration and association of referenced object enables you to meet your business-processing criteria and security requirements.

---

### Working with objects

When configuring services on the appliance, the WebGUI provides an object view and a service view. You can use either view to create or edit the service.

#### Service view

Working in the service view allows less-than-expert level users to build basic, generic objects.

#### Object view

Working in the object view allows expert-level users to build specific, complex, and highly detailed objects.

---

### Accessing the WebGUI

To use the WebGUI, the Web Management Interface must be configured. This interface was defined during the initial firmware setup (during appliance installation) or afterward with the **web-mgmt** command.

To access the WebGUI:

1. Direct your browser to the WebGUI login screen. Use the IP address and port number assigned during the configuration of the Web Management interface. The address uses the HTTPS protocol and has the `https://address:port` format.
2. In the login fields, specify an account name and password.
3. From the **Domain** list, select the domain to which to log in.
4. Click **Login**.

After verifying credentials, the WebGUI displays the Control Panel.

---

### Welcome screen

After successfully logging in, the WebGUI displays its Welcome screen. Visibility of objects in the WebGUI is controlled by a combination of the Role-based management (RBM) object and whether the administrator is in the default domain or an application domain.

This screen is separated into the following areas:

- The banner shows details about the administrator who logged in to the appliance and contains the following controls:
  - The **Domain** list that allows the administrator to switch domains.
  - The **Save Config** button that allows the administrator to persist configuration changes.
  - The **Logout** button that allows the administrator to end the WebGUI session.
- The navigation bar along the left side provides access to related configuration suites and to related management suites. This area contains the following menus:
  - The **Control Panel** returns the administrator to the Welcome screen.
  - The **Status** menu provides access to logs and status providers.
  - The **Services** menu provides access to service configuration objects and objects referenced by service objects. When the administrator selects the item, the WebGUI displays the service view for the object.
  - The **Network** menu provide access to network configuration objects. These objects are to define the network in which the appliance connects. Many of these objects are available in the default domain.
  - The **Administration** menu provides access to managing access to the appliance as well as general appliance settings. Many of these objects are available in the default domain.
  - The **Objects** menu provides access to service configuration objects and objects referenced by service objects. When the administrator selects the item, the WebGUI displays the object view for the object.
- The dashboard that is separated into the following areas:
  - The top area contains icons to access top-level objects for the appliance.
  - The middle area contains icons to access monitoring and troubleshooting utilities.
  - The bottom area contains icons to access file management and administration utilities.

When you click any icon on the dashboard or select any item from the menu, the WebGUI replaces the dashboard with the details for the selected item.

---

## Common WebGUI conventions

In addition to the standard interface controls, the WebGUI uses custom controls to help during the configuration of objects. These controls generally pertain to defining referenced objects.

### Working with referenced objects

When using the WebGUI to create and modify objects, the configuration screen might display an input field to select a referenced object. Figure 1 illustrates this type of input field.

Input  ▼

*Figure 1. Input field for referenced objects*

When the WebGUI displays this type of input field, you can specify the referenced object in the following ways:

- Select the name of an existing referenced object from the list.



- Use the + button to create a new referenced object. When created, the input field contains the name of the newly created referenced object.
- Use the ... button to modify the referenced object whose name is in the input field. When modified, the input field retains the name of the referenced object.

When you click the + button or ... button, the WebGUI launches a new window that displays the configuration screen for that type of object.

## Working with lists of referenced objects

When using the WebGUI to create or modify objects, the configuration screen might display an input list to define a group of referenced objects. The input for this configuration item is the list of referenced objects. Figure 2 illustrates this type of input list.

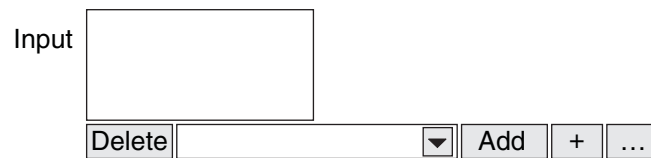


Figure 2. Input list for referenced objects

When the WebGUI displays this type of list, you can manage referenced objects in the following ways:

- Select the name of an existing referenced object from the list. Click **Add** to add it to the list of referenced objects.
- Use the + button to create a new referenced object. When created, the input field contains the name of the new referenced object. Click **Add** to add it to the list of referenced objects.
- Use the ... button to modify the referenced object whose name is in the input field. When modified, the input field retains the name of the referenced object. Click **Add** to add it to the list of referenced objects.
- Select the name of a referenced object from the list (either the input field or the list of referenced objects). Click **Delete** to remove it from the list of referenced objects.

When you click the + button or ... button, the WebGUI launches a new window that displays the configuration screen for that type of object.

---

## Viewing and editing local files during configuration

As you use the WebGUI to select a local file during configuration, the configuration screen might display the **View** and **Edit** buttons beside the selection lists.

Working with files in this way has the following advantages:

- Ensure that the file is the one that you want
- Ability to edit the file to address errors found while defining a configuration
- Use a single session instead of opening another session to manage files through the File Management utility

You cannot view or edit remote files.

## Viewing local files

To view a local file:

1. Select the file from the lists.
2. Click **View** to open the file editor in view mode.
3. Review the file.
4. Click **Cancel**.

## Editing local files

The edited file overwrites the original file.

To edit a local file:

1. Select the file from the lists.
2. Click **Edit** to open the file editor in edit mode.
3. Edit the file as required.
4. Click **Submit** to save changes.
5. Click **Close**.

---

## Chapter 3. Common WebGUI tasks

The majority of objects provide the following common tasks. Not all objects have these tasks available.

- Applying and saving configuration changes
- Canceling changes before saving to the running configuration
- Resetting changes to an object
- Deleting an object
- Exporting the configuration of an object
- Viewing configuration-specific messages of an object
- Viewing status of an object

---

### Applying and saving changes

As you use the WebGUI to manage configurations, click **Apply** to save these changes to the running configuration. Changes that are made to the *running* configuration take effect immediately, but are not persisted to the startup configuration. During an appliance restart these changes are lost.

To retain changes across an appliance restart, click **Save Config**. The changes are saved to the startup configuration. The *startup* or *persistent* configuration is persisted across an appliance restart. By default, the appliance reads the startup configuration from the auto-config.cfg file.

---

### Canceling changes

As you use the WebGUI, click **Cancel** to not save the current changes to the running configuration. If you click **Cancel**, you return to the catalog and lose all changes.

---

### Resetting objects

Independent of whether the settings are saved to the configuration, you can reset an object to its default configuration.

To revert changes to a specific object:

1. Display the catalog for the object.
2. Click the name of the object to reset.
3. Click **Undo**.
4. Follow the prompts.

---

### Deleting objects

You might want to delete objects that are no longer needed. If no object depends on the object to be deleted, you can delete it at any time. Because a DataPower service is a top-level object, you can delete it at any time. Conversely, you cannot delete an object that is active and in use by a higher-level object.

To delete an object:

1. Display the catalog for the object.
2. Click the name of the object to delete.
3. Click **Delete**.
4. Follow the prompts.

Deleting an object deletes that object only. Deleting an object does not delete referenced objects.

---

## Exporting objects

To export an object:

1. Display the catalog for the object.
2. Click the name of the object to export.
3. Click **Export**.
4. Follow the prompts.

---

## Viewing configuration-specific messages

During developing, the configuration might be invalid. To help determine why an object is in the down operational state, you can view configuration messages for a specific object.

This approach is easier than filtering logs.

### Viewing messages from the catalog

To view configuration-specific messages from the catalog:

1. Display the catalog for the object.
2. Click the magnifying glass icon.

### Viewing messages from the configuration pane

To view configuration-specific messages from the configuration pane:

1. Display the catalog for the object.
2. Click the name of the instance.
3. Click **View Logs**.

---

## Viewing object status

You can view the status of an object and all its referenced objects to help determine why a configuration object is in a down operational state. When you view the object status, the WebGUI opens a new window. This window provides the ability to show or hide unused properties.

- To show the unused properties, click **Show**.
- If the display lists unused properties, click **Hide** to hide these properties. Hiding unused properties is the default behavior.

When viewing the object status, the window provides the following information:

- The name of the instance and its type with a control to collapse (hide) or expand (show) referenced objects
- Its configuration state: New, Modified, or Saved
- Its operational state: up or down

- Its administrative state: enabled or disabled
- Details about the detected error, if applicable
- A link (magnifying glass icon) to view the logs for this object

To view the status for an object:

1. Display the catalog for the object.
2. Click the name of the object to view.
3. Click **View Status**.



---

## Part 3. Controlling user access to the appliance

<b>Chapter 4. Managing user access</b> . . . . .	17	Resetting the admin password . . . . .	54
Understanding RBM on the DataPower appliance . . . . .	17	Migrating a user to a new group . . . . .	54
Optimizing access on the DataPower appliance . . . . .	18	Forcing a password change . . . . .	54
Capabilities of RBM . . . . .	18	Changing the password for the current user . . . . .	55
Authenticating users . . . . .	18	SNMP V3 users . . . . .	55
Access profile. . . . .	18	Viewing local SNMP engine ID. . . . .	55
User access to resources . . . . .	19	Creating an SNMP V3 account . . . . .	56
Configuring RBM settings . . . . .	19		
RBM using custom authentication . . . . .	21		
RBM using LDAP authentication . . . . .	22		
RBM using local user authentication . . . . .	24		
RBM using RADIUS authentication . . . . .	25		
RBM using SAF authentication . . . . .	27		
RBM using SPNEGO authentication . . . . .	28		
RBM using SSL user certificate . . . . .	30		
RBM using XML file authentication . . . . .	31		
Defining the password policy . . . . .	33		
Defining LDAP Search Parameters objects . . . . .	34		
Managing RBM access. . . . .	35		
Defining the account policy . . . . .	35		
Restoring RBM access from the command line. . . . .	36		
Extending RBM access to the WebGUI only. . . . .	36		
Enabling the RBM admin-state from the command line . . . . .	37		
Publishing an RBM XML file to another appliance . . . . .	37		
Flushing the RBM cache . . . . .	37		
 <b>Chapter 5. Using the builder to create an RBM policy file.</b> . . . . .	 39		
Using the RBM XML file . . . . .	39		
RBM XML file for authentication and authorization . . . . .	39		
RBM XML file for authentication . . . . .	41		
RBM XML file for authorization . . . . .	42		
 <b>Chapter 6. Managing user group accounts</b> . . . . .	 45		
Creating a group account. . . . .	46		
Specifying the access policy . . . . .	46		
Example access policies . . . . .	46		
Controlling access to the command line . . . . .	47		
Adding access to a command group . . . . .	47		
Removing access to a command group . . . . .	47		
 <b>Chapter 7. Using the Access Policy builder.</b> . . . . .	 49		
Elements of an access policy. . . . .	49		
Adding an access policy . . . . .	50		
Example access profile that grants full access . . . . .	51		
Example access policy that uses wildcards . . . . .	51		
Example access policy that grants user management permissions . . . . .	51		
Editing an access profile . . . . .	52		
Removing an access profile . . . . .	52		
 <b>Chapter 8. Managing user accounts</b> . . . . .	 53		
Creating user accounts . . . . .	53		





---

## Chapter 4. Managing user access

The DataPower appliance manages access through role-based management (RBM). RBM provides a flexible and integrated means to control whether an authenticated user has the necessary privileges to access resources through access policies.

Settings on the RBM policy provide the facility to define a global password policy for locally-defined users.

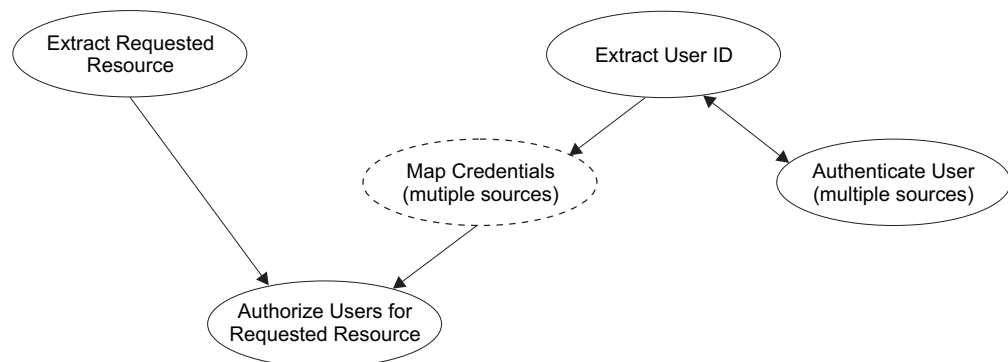
---

### Understanding RBM on the DataPower appliance

RBM controls the relationships between authenticated users and resources. The user logs in to the DataPower appliance. The user is authenticated either by a remote authentication system or by the DataPower appliance. The RBM policy determines whether to allow an authenticated user to access specific resources.

- When authentication uses a remote authentication system, such as an LDAP server, RBM extracts the identity of the authenticated user, maps the identity to a credential, and determines whether to authorize access to the resource based on the credential. If a problem occurs during remote authentication, RBM can use one or more locally-defined fallback users.

Figure 3 illustrates the basic components of RBM and their relationships.



*Figure 3. RBM processing with remote authentication*

- When authentication is local, authentication is by user name and password. The group in which the user is a member determines whether to authorize access to the resource. Users who are not members of a group are not under RBM control.

The RBM policy uses access profiles to determine authorization to resources. An access profile is made up of one or more access policies. Each access policy defines which privileges to provide to a single resource. An access policy can use wildcard characters in regular expressions to define the same set of privileges to multiple resources.

Because RBM distances access policies from individual users, you can modify an access profile that affects a collection of users instead of modifying each user individually. For example, you can modify the access profile in a user group to change resource authorization for all members of that group. Alternatively, you can change the access profile associated with a credential to modify all users who map to that credential.

---

## Optimizing access on the DataPower appliance

To maximize access control and to adhere to best practices, complete the following high-level procedures:

1. Define the global RBM policy. See “Publishing an RBM XML file to another appliance” on page 37.
2. Define the global password policy for locally-defined user accounts. See “Defining the password policy” on page 33.
3. Create groups. See “Creating a group account” on page 46.
4. Create an access profile for each group. See Chapter 7, “Using the Access Policy builder,” on page 49.
5. Create users who are members of groups. See Chapter 8, “Managing user accounts,” on page 53.

---

## Capabilities of RBM

Role-based management consists of the following capabilities:

- Authenticating users
- Evaluating the access profile
- Enforcing access to resources

### Authenticating users

Extract the user identity from the access request and authenticate the user identity that is presented. One of the following methods can be used for user authentication:

**Custom**

An external programmatic method.

**LDAP server**

An external authentication system.

**Local user**

Locally configured user account.

**RADIUS server**

An external authentication system.

**SAF** An external authentication system.

**SPNEGO**

An external Windows Integrated Authentication system.

**SSL user certificate**

An SSL certificate from a connection peer.

**XML file**

A file that contains authentication information.

**Note:** When using an external authentication system, the mapping method to determine the access profile must be a local resource.

### Access profile

The access profile defines the set of privileges for one or more resources on the DataPower appliance. Resources can be as broad as an XML Firewall or as specific as the ability to only configure user profiles that start with the letters foo (as in foo\_one). Privileges for a resource can be one or more of the following:

- Read
- Write
- Add
- Delete
- Execute

A bundle of access rights (also termed access policies) constitutes an access profile. An access profile can originate from any of the following credential mapping sources:

**Custom**

An external programmatic method.

**Local user group**

Locally configured user group.

**XML file**

A file that defines access profiles.

Table 1 lists the supported credential mapping methods for each user authentication method.

*Table 1. Authentication methods and supported credential mapping methods*

Authentication method	Mapping Credentials method		
	Local user group	XML file	Custom
Custom	No	Yes	Yes
LDAP	No	Yes	Yes
Local user	Yes	Yes	Yes
RADIUS	No	Yes	Yes
SAF	No	Yes	Yes
SPNEGO	No	Yes	Yes
SSL user credential	No	Yes	Yes
XML file	Yes	Yes	Yes

## User access to resources

After the user is authenticated and the access profile is evaluated, the DataPower appliance enforces the established access profile. For example, the WebGUI will not display any resource to which the user has no access, and the command line will not recognize commands for any resource to which the user has no access.

If users invoke a command to which they do not have access, the command line displays the following message:

Unknown command or macro (command)

## Configuring RBM settings

The overview of the steps to configure role-based management is as follows:

1. Click **Administration** **Access** **RBM Settings**.
2. Specify whether to enforce the RBM policy for both the WebGUI and the command line or to enforce the RBM policy for the WebGUI only.

On zBX, the RBM policy is enforced for both the WebGUI and the command line. None of the administrative accounts for zBX have the necessary permissions to alter this setting. The options on this page are disabled.

3. Specify whether to allow or restrict access by the `admin` account to serial connections.

On zBX, this option is disabled. None of the administrative accounts for zBX have the necessary permissions to alter this setting.

4. Select the authentication method.

*Table 2. Authentication method and configuration steps*

Authentication method	Configuration steps
Custom	Create a style sheet. Store the file in a local directory, or stage it on an accessible file server.
LDAP	Configure an LDAP server for authentication.
Local user	Use the New User Account wizard to create new users, or use the Manage User Accounts panel to modify an existing user.
RADIUS	Configure a RADIUS server.
SAF	Configure an NSS Client object for authentication with an NSS server.
SPNEGO	Configure a Kerberos keytab to decrypt the client Kerberos ticket.
SSL user certificate	Assign a Validation Credentials for authentication.
XML file	Create XML authentication file with the RBM Policy Editor. Store the file in a local directory, or stage it on an accessible file server.

5. Define a local user account on the appliance, if necessary, as a fallback user when using a remote authentication method.
6. Select the credential mapping method for evaluating access profiles.
7. Save the changes to the running configuration.

**Note:** The change takes affect immediately. At this point, the new settings could disable access to the DataPower appliance for any user who does not have an active session (WebGUI, command line, Telnet, KVM infrastructure of the BladeCenter®, or serial connection). In other words, the changes could disable future access through any of the following methods:

- Any user who attempts to access the appliance through the WebGUI
- Any user who attempts to access the appliance through the command line
- Any user who attempts to access the appliance through a Telnet session
- Any user who attempts to access the appliance using the KVM infrastructure of the BladeCenter
- Any user who attempts to access the appliance using the serial over LAN connection to the Blade
- Any user who attempts to access the appliance through a serial connection (WebGUI or command line).

See “Restoring RBM access from the command line” on page 36 for more information.

8. Optional: Save the changes to the startup configuration.

## RBM using custom authentication

1. Click **Administration** **Access** **RBM Settings**.
2. Retain the default value for **Admin State**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Set **Enforce RBM on CLI** to specify which access approaches the RBM policy enforces. On zBX, this option is on and cannot be configured.
5. Set **Restrict Admin Login** to control access by the `admin` account. On zBX this option is turned off and cannot be configured.
6. Define the user authentication method.
  - a. Click the **Authentication** tab.
  - b. Select **custom** from the **User Authentication Method** list.
  - c. Specify the URL of the custom style sheet for user authentication in the **Custom URL** field.
  - d. From the **Local Login As Fallback** list, select whether to use local user accounts as fallback users. With fallback users, locally-defined users can log in to the appliance if the authentication method fails or in the event of a network outage that affects the primary login authentication (for example, the remote authentication server is down).

**Note:** Local users must be members of local user groups. Each local user must also be defined in the remote authentication server. The password for each local user must match the credentials for a user of the exact same name on the remote server.

- e. When specific users are fallback users, add specific locally-defined, fallback users:
    - 1) From the **Fallback User** list, select a local user.
    - 2) Click **Add**.Repeat the previous step for each locally-defined, fallback user.
  - f. From the **Authentication Cache Mode** list, select the desired caching mode.
  - g. In the **Authentication Cache Lifetime** field, specify an explicit TTL in seconds to retain cached results.
7. Define the mapping credentials method.
    - a. Click the **Credentials** tab.
    - b. From the **Mapping Credentials Method** list, select the method to evaluate access profiles.
      - If custom: In the **Mapping Custom URL** field, specify the URL of the custom style sheet.
      - If an XML file: In the **Mapping RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, "Using the builder to create an RBM policy file," on page 39 for details.

**Note:** Although available, a local user group is not a valid selection.

- c. When the mapping method is a local user group or an XML file: Set **Search LDAP for Group Name** to control whether to perform an LDAP search to retrieve the user's group.
  - If enabled, an LDAP search for the user's group. The authenticated DN of the user along with the LDAP Search Parameters will be used as part of an LDAP search to retrieve the user's group.

- If disabled, the authenticated identity of the user (DN or user group of local user) will be used directly as the input credential.
- d. If enabled, define the LDAP connection.
  - 1) In the **Credentials Server Host** field, specify the IP address or host name of the LDAP server.
  - 2) In the **Credentials Server Port** field, specify the port number of the LDAP server.
  - 3) From the **LDAP SSL Proxy Profile** list, select the profile to establish a secured connection to the LDAP server.
  - 4) Optional: From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings. This setting overrides the settings for the **Credentials Server Host** and **Credentials Server Port** fields.
  - 5) In the **LDAP Bind DN** field, specify the distinguished name (DN) for the LDAP bind operation.
  - 6) In the **LDAP Bind Password** and **LDAP Bind Password** fields, specify the password for the specified DN.
  - 7) From the **LDAP Search Parameters** list, select the LDAP Search Parameters. This parameter set serves as a container for the parameters that an LDAP search operation uses to perform an LDAP search operation to retrieve the group name (DN or attribute value) based on the distinguished name of the authenticated user.
- 8. If you defined local fallback users, optionally define the password policy. See “Defining the password policy” on page 33 for more information.
- 9. Click **Apply** to save the changes to the running configuration.
- 10. Optional: Click **Save Config** to save the changes to the startup configuration.

## RBM using LDAP authentication

LDAP-based implementations require an X.500 DN (for example, `cn=Alice,dc=datapower,dc=com`) and a password. When configuring LDAP for authentication, it is typical to create a base DN (such as `dc=datapower,dc=com`) and then create one entry under this base for each user.

To make LDAP authentication more usable, RBM provides the LDAP suffix. Set the LDAP suffix to the base name under which user entries are found. Unless the LDAP suffix is an empty string, an X.500-compliant DN is built as follows:

- Prepending `cn=` to the user name
- Appending a comma followed by the value of the LDAP suffix

For example, if the LDAP suffix is `dc=datapower,dc=com` and the user name is `Alice`, the DN is mapped as `cn=Alice,dc=datapower,dc=com`

1. Click **Administration** **Access** **RBM Settings**.
2. Retain the default value for **Admin State**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Set **Enforce RBM on CLI** to specify which access approaches the RBM policy enforces. On zBX, this option is on and cannot be configured.
5. Set **Restrict Admin Login** to control access by the `admin` account. On zBX this option is turned off and cannot be configured.
6. Define the user authentication method.
  - a. Click the **Authentication** tab.

- b. From the **User Authentication Method** list, select **LDAP**.
  - 1) In the **Authentication Server Host** field, specify the host name or IP address of the LDAP server.
  - 2) In the **Authentication Server Port** field, specify the port number on the server.
  - 3) From the **LDAP Version** list, select the LDAP version.
  - 4) From the **LDAP SSL Proxy Profile** list, select a profile to establish a secured connection to the LDAP server.
  - 5) From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings.
  - 6) Set **Search LDAP for DN** to control whether to perform an LDAP search to retrieve the user's DN.
    - If enabled, specify the distinguished name (DN) for the LDAP bind operation, the password for the specified DN, and the LDAP Search Parameters set. This parameter set serves as a container for the parameters to perform an LDAP search operation to retrieve the DN.
    - If disabled, specify an LDAP prefix and suffix.
- c. From the **Local Login As Fallback** list, select whether to use local user accounts as fallback users. With fallback users, locally-defined users can log in to the appliance if the authentication method fails or in the event of a network outage that affects the primary login authentication (for example, the remote authentication server is down).

**Note:** Local users must be members of local user groups. Each local user must also be defined in the remote authentication server. The password for each local user must match the credentials for a user of the exact same name on the remote server.

- d. When specific users are fallback users, add specific locally-defined, fallback users:
    - 1) From the **Fallback User** list, select a local user.
    - 2) Click **Add**.

Repeat the previous step for each locally-defined, fallback user.
  - e. From the **Authentication Cache Mode** list, select the desired caching mode.
  - f. In the **Authentication Cache Lifetime** field, specify an explicit TTL in seconds to retain cached results.
7. Define the mapping credentials method.
- a. Click the **Credentials** tab.
  - b. From the **Mapping Credentials Method** list, select the method to evaluate access profiles.
    - If custom: In the **Mapping Custom URL** field, specify the URL of the custom style sheet.
    - If an XML file: In the **Mapping RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, "Using the builder to create an RBM policy file," on page 39 for details.

**Note:** Although available, a local user group is not a valid selection.

- c. When the mapping method is a local user group or an XML file: Set **Search LDAP for Group Name** to control whether to perform an LDAP search to retrieve the user's group.



- If enabled, an LDAP search for the user's group. The authenticated DN of the user along with the LDAP Search Parameters will be used as part of an LDAP search to retrieve the user's group.
  - If disabled, the authenticated identity of the user (DN or user group of local user) will be used directly as the input credential.
- d. If enabled, define the LDAP connection.
    - 1) In the **Credentials Server Host** field, specify the IP address or host name of the LDAP server.
    - 2) In the **Credentials Server Port** field, specify the port number of the LDAP server.
    - 3) From the **LDAP SSL Proxy Profile** list, select the profile to establish a secured connection to the LDAP server.
    - 4) Optional: From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings. This setting overrides the settings for the **Credentials Server Host** and **Credentials Server Port** fields.
    - 5) In the **LDAP Bind DN** field, specify the distinguished name (DN) for the LDAP bind operation.
    - 6) In the **LDAP Bind Password** and **LDAP Bind Password** fields, specify the password for the specified DN.
    - 7) From the **LDAP Search Parameters** list, select the LDAP Search Parameters. This parameter set serves as a container for the parameters that an LDAP search operation uses to perform an LDAP search operation to retrieve the group name (DN or attribute value) based on the distinguished name of the authenticated user.
  8. If you defined local fallback users, optionally define the password policy. See "Defining the password policy" on page 33 for more information.
  9. Click **Apply** to save the changes to the running configuration.
  10. Optional: Click **Save Config** to save the changes to the startup configuration.

## RBM using local user authentication

1. Click **Administration** **Access** **RBM Settings**.
2. Retain the default value for **Admin State**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Set **Enforce RBM on CLI** to specify which access approaches the RBM policy enforces. On zBX, this option is on and cannot be configured.
5. Set **Restrict Admin Login** to control access by the `admin` account. On zBX this option is turned off and cannot be configured.
6. Define the user authentication method.
  - a. Click the **Authentication** tab.
  - b. From the **User Authentication Method** list, select **local user**.
  - c. From the **Authentication Cache Mode** list, select the desired caching mode.
  - d. In the **Authentication Cache Lifetime** field, specify an explicit TTL in seconds to retain cached results.
7. Define the mapping credentials method.
  - a. Click the **Credentials** tab.
  - b. From the **Mapping Credentials Method** list, select the method to evaluate access profiles.



- If custom: In the **Mapping Custom URL** field, specify the URL of the custom style sheet.
  - If a local user group: RBM uses the access profiles for the group. See “Creating a group account” on page 46 for information.
  - If an XML file: In the **Mapping RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, “Using the builder to create an RBM policy file,” on page 39 for details.
- c. When the mapping method is a local user group or an XML file: Set **Search LDAP for Group Name** to control whether to perform an LDAP search to retrieve the user's group.
- If enabled, an LDAP search for the user's group. The authenticated DN of the user along with the LDAP Search Parameters will be used as part of an LDAP search to retrieve the user's group.
  - If disabled, the authenticated identity of the user (DN or user group of local user) will be used directly as the input credential.
- d. If enabled, define the LDAP connection.
- 1) In the **Credentials Server Host** field, specify the IP address or host name of the LDAP server.
  - 2) In the **Credentials Server Port** field, specify the port number of the LDAP server.
  - 3) From the **LDAP SSL Proxy Profile** list, select the profile to establish a secured connection to the LDAP server.
  - 4) Optional: From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings. This setting overrides the settings for the **Credentials Server Host** and **Credentials Server Port** fields.
  - 5) In the **LDAP Bind DN** field, specify the distinguished name (DN) for the LDAP bind operation.
  - 6) In the **LDAP Bind Password** and **LDAP Bind Password** fields, specify the password for the specified DN.
  - 7) From the **LDAP Search Parameters** list, select the LDAP Search Parameters. This parameter set serves as a container for the parameters that an LDAP search operation uses to perform an LDAP search operation to retrieve the group name (DN or attribute value) based on the distinguished name of the authenticated user.
8. Optional: Define the password policy. See “Defining the password policy” on page 33 for more information.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

## RBM using RADIUS authentication

1. Click **Administration** **Access** **RBM Settings**.
2. Retain the default value for **Admin State**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Set **Enforce RBM on CLI** to specify which access approaches the RBM policy enforces. On zBX, this option is on and cannot be configured.
5. Set **Restrict Admin Login** to control access by the `admin` account. On zBX this option is turned off and cannot be configured.
6. Define the user authentication method.
  - a. Click the **Authentication** tab.

- b. From the **User Authentication Method** list, select **radius**.
- c. From the **Local Login As Fallback** list, select whether to use local user accounts as fallback users. With fallback users, locally-defined users can log in to the appliance if the authentication method fails or in the event of a network outage that affects the primary login authentication (for example, the remote authentication server is down).

**Note:** Local users must be members of local user groups. Each local user must also be defined in the remote authentication server. The password for each local user must match the credentials for a user of the exact same name on the remote server.

- d. When specific users are fallback users, add specific locally-defined, fallback users:
    - 1) From the **Fallback User** list, select a local user.
    - 2) Click **Add**.
 Repeat the previous step for each locally-defined, fallback user.
  - e. From the **Authentication Cache Mode** list, select the desired caching mode.
  - f. In the **Authentication Cache Lifetime** field, specify an explicit TTL in seconds to retain cached results.
7. Define the mapping credentials method.
- a. Click the **Credentials** tab.
  - b. From the **Mapping Credentials Method** list, select the method to evaluate access profiles.
    - If custom: In the **Mapping Custom URL** field, specify the URL of the custom style sheet.
    - If an XML file: In the **Mapping RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, “Using the builder to create an RBM policy file,” on page 39 for details.

**Note:** Although available, a local user group is not a valid selection.

- c. When the mapping method is a local user group or an XML file: Set **Search LDAP for Group Name** to control whether to perform an LDAP search to retrieve the user's group.
  - If enabled, an LDAP search for the user's group. The authenticated DN of the user along with the LDAP Search Parameters will be used as part of an LDAP search to retrieve the user's group.
  - If disabled, the authenticated identity of the user (DN or user group of local user) will be used directly as the input credential.
- d. If enabled, define the LDAP connection.
  - 1) In the **Credentials Server Host** field, specify the IP address or host name of the LDAP server.
  - 2) In the **Credentials Server Port** field, specify the port number of the LDAP server.
  - 3) From the **LDAP SSL Proxy Profile** list, select the profile to establish a secured connection to the LDAP server.
  - 4) Optional: From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings. This setting overrides the settings for the **Credentials Server Host** and **Credentials Server Port** fields.

- 5) In the **LDAP Bind DN** field, specify the distinguished name (DN) for the LDAP bind operation.
- 6) In the **LDAP Bind Password** and **LDAP Bind Password** fields, specify the password for the specified DN.
- 7) From the **LDAP Search Parameters** list, select the LDAP Search Parameters. This parameter set serves as a container for the parameters that an LDAP search operation uses to perform an LDAP search operation to retrieve the group name (DN or attribute value) based on the distinguished name of the authenticated user.
8. If you defined local fallback users, optionally define the password policy. See “Defining the password policy” on page 33 for more information.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

## RBM using SAF authentication

1. Click **Administration** **Access** **RBM Settings**.
2. Retain the default value for **Admin State**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Set **Enforce RBM on CLI** to specify which access approaches the RBM policy enforces. On zBX, this option is on and cannot be configured.
5. Set **Restrict Admin Login** to control access by the `admin` account. On zBX this option is turned off and cannot be configured.
6. Define the user authentication method.
  - a. Click the **Authentication** tab.
  - b. From the **User Authentication Method** list, select **saf**.
  - c. From the **NSS Client Configuration** list, select an NSS client. See “NSS Client” on page 226 for more details.
  - d. From the **Local Login As Fallback** list, select whether to use local user accounts as fallback users. With fallback users, locally-defined users can log in to the appliance if the authentication method fails or in the event of a network outage that affects the primary login authentication (for example, the remote authentication server is down).
 

**Note:** Local users must be members of local user groups. Each local user must also be defined in the remote authentication server. The password for each local user must match the credentials for a user of the exact same name on the remote server.
  - e. When specific users are fallback users, add specific locally-defined, fallback users:
    - 1) From the **Fallback User** list, select a local user.
    - 2) Click **Add**.
 Repeat the previous step for each locally-defined, fallback user.
  - f. From the **Authentication Cache Mode** list, select the desired caching mode.
  - g. In the **Authentication Cache Lifetime** field, specify an explicit TTL in seconds to retain cached results.
7. Define the mapping credentials method.
  - a. Click the **Credentials** tab.
  - b. From the **Mapping Credentials Method** list, select the method to evaluate access profiles.

- If custom: In the **Mapping Custom URL** field, specify the URL of the custom style sheet.
- If an XML file: In the **Mapping RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, “Using the builder to create an RBM policy file,” on page 39 for details.

**Note:** Although available, a local user group is not a valid selection.

- c. When the mapping method is a local user group or an XML file: Set **Search LDAP for Group Name** to control whether to perform an LDAP search to retrieve the user's group.
  - If enabled, an LDAP search for the user's group. The authenticated DN of the user along with the LDAP Search Parameters will be used as part of an LDAP search to retrieve the user's group.
  - If disabled, the authenticated identity of the user (DN or user group of local user) will be used directly as the input credential.
- d. If enabled, define the LDAP connection.
  - 1) In the **Credentials Server Host** field, specify the IP address or host name of the LDAP server.
  - 2) In the **Credentials Server Port** field, specify the port number of the LDAP server.
  - 3) From the **LDAP SSL Proxy Profile** list, select the profile to establish a secured connection to the LDAP server.
  - 4) Optional: From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings. This setting overrides the settings for the **Credentials Server Host** and **Credentials Server Port** fields.
  - 5) In the **LDAP Bind DN** field, specify the distinguished name (DN) for the LDAP bind operation.
  - 6) In the **LDAP Bind Password** and **LDAP Bind Password** fields, specify the password for the specified DN.
  - 7) From the **LDAP Search Parameters** list, select the LDAP Search Parameters. This parameter set serves as a container for the parameters that an LDAP search operation uses to perform an LDAP search operation to retrieve the group name (DN or attribute value) based on the distinguished name of the authenticated user.
8. If you defined local fallback users, optionally define the password policy. See “Defining the password policy” on page 33 for more information.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

## RBM using SPNEGO authentication

1. Click **Administration** **Access** **RBM Settings**.
2. Retain the default value for **Admin State**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Set **Enforce RBM on CLI** to specify which access approaches the RBM policy enforces. On zBX, this option is on and cannot be configured.
5. Set **Restrict Admin Login** to control access by the `admin` account. On zBX this option is turned off and cannot be configured.
6. Define the user authentication method.
  - a. Click the **Authentication** tab.

- b. From the **User Authentication Method** list, select **spnego**.
- c. From the **Kerberos Keytab** list, select a keytab file.
- d. From the **Local Login As Fallback** list, select whether to use local user accounts as fallback users. With fallback users, locally-defined users can log in to the appliance if the authentication method fails or in the event of a network outage that affects the primary login authentication (for example, the remote authentication server is down).

**Note:** Local users must be members of local user groups. Each local user must also be defined in the remote authentication server. The password for each local user must match the credentials for a user of the exact same name on the remote server.

- e. When specific users are fallback users, add specific locally-defined, fallback users:
    - 1) From the **Fallback User** list, select a local user.
    - 2) Click **Add**.

Repeat the previous step for each locally-defined, fallback user.
  - f. From the **Authentication Cache Mode** list, select the desired caching mode.
  - g. In the **Authentication Cache Lifetime** field, specify an explicit TTL in seconds to retain cached results.
7. Define the mapping credentials method.
- a. Click the **Credentials** tab.
  - b. From the **Mapping Credentials Method** list, select the method to evaluate access profiles.
    - If custom: In the **Mapping Custom URL** field, specify the URL of the custom style sheet.
    - If an XML file: In the **Mapping RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, “Using the builder to create an RBM policy file,” on page 39 for details.

**Note:** Although available, a local user group is not a valid selection.

- c. When the mapping method is a local user group or an XML file: Set **Search LDAP for Group Name** to control whether to perform an LDAP search to retrieve the user's group.
  - If enabled, an LDAP search for the user's group. The authenticated DN of the user along with the LDAP Search Parameters will be used as part of an LDAP search to retrieve the user's group.
  - If disabled, the authenticated identity of the user (DN or user group of local user) will be used directly as the input credential.
- d. If enabled, define the LDAP connection.
  - 1) In the **Credentials Server Host** field, specify the IP address or host name of the LDAP server.
  - 2) In the **Credentials Server Port** field, specify the port number of the LDAP server.
  - 3) From the **LDAP SSL Proxy Profile** list, select the profile to establish a secured connection to the LDAP server.
  - 4) Optional: From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings. This setting overrides the settings for the **Credentials Server Host** and **Credentials Server Port** fields.

- 5) In the **LDAP Bind DN** field, specify the distinguished name (DN) for the LDAP bind operation.
- 6) In the **LDAP Bind Password** and **LDAP Bind Password** fields, specify the password for the specified DN.
- 7) From the **LDAP Search Parameters** list, select the LDAP Search Parameters. This parameter set serves as a container for the parameters that an LDAP search operation uses to perform an LDAP search operation to retrieve the group name (DN or attribute value) based on the distinguished name of the authenticated user.
8. If you defined local fallback users, optionally define the password policy. See “Defining the password policy” on page 33 for more information.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

## RBM using SSL user certificate

1. Click **Administration** **Access** **RBM Settings**.
2. Retain the default value for **Admin State**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Retain the default value for **Enforce RBM on CLI**. On zBX, this option is on and cannot be configured.

**Note:** If you enable this option, only local fallback users will be able to access the appliance from the command line.

5. Set **Restrict Admin Login** to control access by the **admin** account. On zBX this option is turned off and cannot be configured.
6. Define the user authentication method.
  - a. Click the **Authentication** tab.
  - b. From the **User Authentication Method** list, select **user cert**.
  - c. From the **User Validation Credentials** list, select the credentials set.
  - d. From the **Local Login As Fallback** list, select whether to use local user accounts as fallback users. With fallback users, locally-defined users can log in to the appliance if the authentication method fails or in the event of a network outage that affects the primary login authentication (for example, the remote authentication server is down).

**Note:** Local users must be members of local user groups. Each local user must also be defined in the remote authentication server. The password for each local user must match the credentials for a user of the exact same name on the remote server.

- e. When specific users are fallback users, add specific locally-defined, fallback users:
  - 1) From the **Fallback User** list, select a local user.
  - 2) Click **Add**.

Repeat the previous step for each locally-defined, fallback user.
- f. From the **Authentication Cache Mode** list, select the desired caching mode.
- g. In the **Authentication Cache Lifetime** field, specify an explicit TTL in seconds to retain cached results.
7. Define the mapping credentials method.
  - a. Click the **Credentials** tab.



- b. From the **Mapping Credentials Method** list, select the method to evaluate access profiles.
  - If custom: In the **Mapping Custom URL** field, specify the URL of the custom style sheet.
  - If an XML file: In the **Mapping RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, “Using the builder to create an RBM policy file,” on page 39 for details.

**Note:** Although available, a local user group is not a valid selection.

- c. When the mapping method is a local user group or an XML file: Set **Search LDAP for Group Name** to control whether to perform an LDAP search to retrieve the user's group.
  - If enabled, an LDAP search for the user's group. The authenticated DN of the user along with the LDAP Search Parameters will be used as part of an LDAP search to retrieve the user's group.
  - If disabled, the authenticated identity of the user (DN or user group of local user) will be used directly as the input credential.
- d. If enabled, define the LDAP connection.
  - 1) In the **Credentials Server Host** field, specify the IP address or host name of the LDAP server.
  - 2) In the **Credentials Server Port** field, specify the port number of the LDAP server.
  - 3) From the **LDAP SSL Proxy Profile** list, select the profile to establish a secured connection to the LDAP server.
  - 4) Optional: From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings. This setting overrides the settings for the **Credentials Server Host** and **Credentials Server Port** fields.
  - 5) In the **LDAP Bind DN** field, specify the distinguished name (DN) for the LDAP bind operation.
  - 6) In the **LDAP Bind Password** and **LDAP Bind Password** fields, specify the password for the specified DN.
  - 7) From the **LDAP Search Parameters** list, select the LDAP Search Parameters. This parameter set serves as a container for the parameters that an LDAP search operation uses to perform an LDAP search operation to retrieve the group name (DN or attribute value) based on the distinguished name of the authenticated user.
8. If you defined local fallback users, optionally define the password policy. See “Defining the password policy” on page 33 for more information.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

## RBM using XML file authentication

1. Click **Administration Access RBM Settings**.
2. Retain the default value for **Admin State**. On zBX, this option is enabled and cannot be configured.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Set **Enforce RBM on CLI** to specify which access approaches the RBM policy enforces. On zBX, this option is on and cannot be configured.

5. Set **Restrict Admin Login** to control access by the `admin` account. On zBX this option is turned off and cannot be configured.
6. Define the user authentication method.
  - a. Click the **Authentication** tab.
  - b. From the **User Authentication Method** list, select **xmlfile**.
  - c. In the **Authentication RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, “Using the builder to create an RBM policy file,” on page 39 for more information.
  - d. From the **Local Login As Fallback** list, select whether to use local user accounts as fallback users. With fallback users, locally-defined users can log in to the appliance if the authentication method fails or in the event of a network outage that affects the primary login authentication (for example, the remote authentication server is down).

**Note:** Local users must be members of local user groups. Each local user must also be defined in the remote authentication server. The password for each local user must match the credentials for a user of the exact same name on the remote server.

- e. When specific users are fallback users, add specific locally-defined, fallback users:
    - 1) From the **Fallback User** list, select a local user.
    - 2) Click **Add**.Repeat the previous step for each locally-defined, fallback user.
  - f. From the **Authentication Cache Mode** list, select the desired caching mode.
  - g. In the **Authentication Cache Lifetime** field, specify an explicit TTL in seconds to retain cached results.
7. Define the mapping credentials method.
    - a. Click the **Credentials** tab.
    - b. From the **Mapping Credentials Method** list, select the method to evaluate access profiles.
      - If custom: In the **Mapping Custom URL** field, specify the URL of the custom style sheet.
      - If a local user group: RBM uses the access profiles for the group. See “Creating a group account” on page 46 for information.
      - If an XML file: In the **Mapping RBM Policy URL** field, specify the URL of the RBM file. See Chapter 5, “Using the builder to create an RBM policy file,” on page 39 for details.
    - c. When the mapping method is a local user group or an XML file: Set **Search LDAP for Group Name** to control whether to perform an LDAP search to retrieve the user's group.
      - If enabled, an LDAP search for the user's group. The authenticated DN of the user along with the LDAP Search Parameters will be used as part of an LDAP search to retrieve the user's group.
      - If disabled, the authenticated identity of the user (DN or user group of local user) will be used directly as the input credential.
    - d. If enabled, define the LDAP connection.
      - 1) In the **Credentials Server Host** field, specify the IP address or host name of the LDAP server.
      - 2) In the **Credentials Server Port** field, specify the port number of the LDAP server.



- 3) From the **LDAP SSL Proxy Profile** list, select the profile to establish a secured connection to the LDAP server.
- 4) Optional: From the **LDAP Load Balancer Group** list, select a Load Balancer Group. If selected, LDAP queries will be load-balanced in accordance with the group settings. This setting overrides the settings for the **Credentials Server Host** and **Credentials Server Port** fields.
- 5) In the **LDAP Bind DN** field, specify the distinguished name (DN) for the LDAP bind operation.
- 6) In the **LDAP Bind Password** and **LDAP Bind Password** fields, specify the password for the specified DN.
- 7) From the **LDAP Search Parameters** list, select the LDAP Search Parameters. This parameter set serves as a container for the parameters that an LDAP search operation uses to perform an LDAP search operation to retrieve the group name (DN or attribute value) based on the distinguished name of the authenticated user.
8. If you defined local fallback users, optionally define the password policy. See “Defining the password policy” for more information.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Defining the password policy

The password policy applies to locally-defined user accounts only and is universal to the DataPower appliance. This policy does not apply to any other methods of user authentication.

**Note:** Invoking the **reset** command from the command line while in RBM Settings configuration mode restores not only all RBM default settings but also restores all of the default setting for the password policy.

To define the password policy:

1. Click **Administration** **Access** **RBM Settings**.
2. Click the **Password Policy** tab.
3. In the **Minimum Length** field, specify the minimum number of characters in a password.
4. Define characteristics for passwords.
  - a. Set **Require Mixed Case** to indicate whether to require mixed case passwords.
  - b. Set **Require Non Alphanumeric** to indicate whether to require nonalphanumeric characters in passwords.
  - c. Set **Require Digit** to indicate whether to require numeric characters in passwords.
  - d. Set **Disallow Username as Substring** to indicate whether to allow the inclusion of the user name string in the password. For example, if the user is george, the property controls whether to allow george1! or passgeorgeword as the password.
5. Define password aging.
  - a. Set **Enable Aging** to control password aging. If enabled, define the maximum password age.
  - b. If aging: In the **Maximum Password Age** field, specify the maximum age of the password in days.

6. Define password reuse.
  - a. Set **Disallow Password Reuse** to control the reuse of previous passwords. If enabled, define the reuse history.
  - b. If allowing: In the **Reuse History Size** field, specify the number of past passwords to compare against for reuse.
7. Click **Apply** to save the changes to the running configuration.
8. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Defining LDAP Search Parameters objects

The LDAP Search Parameters object serves as a container for the parameters that are used to perform an LDAP search operation.

### Authentication

The parameters for an LDAP search to retrieve the DN of the user.

### Credentials mapping

The parameters for an LDAP search to retrieve the group name (DN or attribute) based on the DN of the authenticated user.

You need to add a prefix and optionally add a suffix to create the LDAP filter. The prefix and suffix are constructs of the LDAP filter expression, as defined in *LDAP: String Representations of Search Filters*. This filter is used to perform the LDAP search and return matching entries.

To create an LDAP Search Parameters object, use the following procedure:

1. Select **Objects** **Access Settings** **LDAP Search Parameters**.
2. Click **Add** to display the configuration pane.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. Specify the base DN to begin the search in the **LDAP Base DN** field. This value identifies the entry level of the tree used by the **LDAP Scope** property.
7. Specify the name of the attribute to return for each entry that matches the search criteria in the **LDAP Returned Attribute** field. The default is the **dn** attribute.
8. Specify the prefix of the LDAP filter expression in the **LDAP Filter Prefix** field.
 

If the prefix is **mail=** and the user name is **bob@example.com**, the LDAP search filter would be **mail=bob@example.com**
9. Optionally specify the suffix of the LDAP filter expression in the **LDAP Filter Suffix** field.
 

If the prefix is **mail=**, the suffix is **) (c=US))**, and the user name is **bob@example.com**, the LDAP search filter would be **(&(mail=bob@example.com) (c=US))**.
10. Select the depth of the search from the **LDAP Scope** list:
 

**Base** Searches the entry level of the tree only.

### One level

Searches the entry level of the tree and any object that is one-level below the input.

### Subtree

(Default) Search the entry level of the tree and all of its descendents.

11. Click **Apply** to save the changes to the running configuration.
12. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Managing RBM access

### Defining the account policy

The account policy applies to locally-defined user accounts only and is universal to the DataPower appliance. This policy does not apply to any other methods of user authentication.

On zBX, the account policy options cannot be configured.

The account policy tab defines the following limitations:

- The maximum number of consecutive failed login attempts allowed before the account is locked out.
- The duration for which an account is locked out after reaching the maximum number of failed login attempts. The duration applies to all local accounts, including the `admin` account. The only difference is that the `admin` account cannot be locked out until reset. When the duration is 0, the `admin` account is locked out for 120 minutes or until re-enabled by a privileged user.

**Best Practice:** Ensure that there is at least one privileged user who can reset the `admin` account.

- The time after which an idle command line session requires re-authentication.

To define limitations of the account policy, use the following procedure:

1. To display the RBM Settings (Main) screen, select **Administration** **Access RBM Settings**.
2. Click the **Account Policy** tab.
3. In the **Maximum Failed Login** field, enter the maximum number of consecutive failed login attempts allowed before the account is locked out. Use any value of 0 -64. To disable the account lockout altogether, retain the default value of 0. On zBX, this value is set to 0, so the account lockout is disabled.
4. In the **Lockout Duration** field, number of minutes to lock out a local account after exceeding the permitted maximum number of failed login attempts. Instead of locking out accounts for a specific duration, the account can be locked out until re-enabled by a privileged user. Use any value of 0 - 1000. The default is 1. On zBX, this value is set to 1, so local accounts are locked for one minute after exceeding the permitted maximum number of failed login attempts..  
To lock out accounts until reset, set the duration to 0.
5. In the **CLI Timeout** field, enter the number of seconds after which an idle command line session will time out and require re-authentication. Use any value 0 -65535. To disable the idle timer altogether, retain the default value of 0. On zBX, this value is set to 0, so the idle timer is disabled. Do not confuse this value with the **Idle timeout** command that refers to the Web Management Service session timeout.

6. Click **Apply** to save the changes to the running configuration.
7. Optional: Click **Save Config** to save the changes to the startup configuration.

## Restoring RBM access from the command line

In the event that a change to the RBM Settings disables access to the DataPower appliance, restore RBM access.

### Notes:

1. If **Restrict Admin Login** is enabled, a user who is equivalent to the **admin** account must access the appliance using a serial connection or the KVM infrastructure.
2. Do not use the **reset** command while in RBM Settings mode. The **reset** command restores default settings for both the RBM policy and default password policy.

To restore access:

- 1.

## Enabling the RBM admin-state from the command line

To change the RBM administration state with commands:

1. Log in to the DataPower appliance with Telnet, SSH, KVM, or serial access.
2. Log in as the `admin` account (`dp-admin` on zBX) or other account with similar permissions.
3. Enter the `configure terminal` command to enter Global mode.
4. Enter the `rbm` command to enter RBM Settings mode.
5. Enter the `admin-state enabled` command to enable RBM Settings.
6. Enter the `show` command to verify your changes.
7. Enter the `exit` command to return to Global mode.
8. Enter the `clear rbm cache` command to clear the RBM cache.

The RBM Settings are enabled.

## Publishing an RBM XML file to another appliance

After creating or modifying an RBM XML file, you can publish this file to another DataPower appliance. You must have an identical user account with sufficient privileges on the remote appliance.

To publish an RBM XML file:

1. Click **Publish File**.
2. Click **Add**.
3. In the **Remote IP Address** field, specify the IP address of the remote appliance.
4. In the **XML-Mgmt Port** field, specify the port number of the XML Management Interface on the remote appliance.
5. Click **Submit**.
6. Click **Commit**.
7. Click **Done**.

A confirmation window is displayed.

## Flushing the RBM cache

Flushing the RBM cache removes all cached user names and passwords from memory.

To flush the RBM cache:

1. Click **Administration** > **Access** > **RBM Settings**.
2. Click **Flush RBM cache**.



---

## Chapter 5. Using the builder to create an RBM policy file

The RBM Policy file defines credentials that associate authenticated users with Access policies. Access policies establish access permissions for particular resources. For examples of these policies, refer to “Specifying the access policy” on page 46.

Continuing from the RBM using XML file authentication section, when selecting XML as the User Authentication Method of authenticate users, or when selecting XML as the Mapping Credential Method of authorizing resources, the RBM Policy File builder utility guides you while configuring the XML-base RBM file.

The sample `RBMInfo.xml` file is in the store: directory. This RBM policy file must conform to the `AAAInfo.xsd` schema in the store: directory.

---

### Using the RBM XML file

You can use the RBM XML file for the following actions:

#### **Authentication and authorization**

Users are authenticated on the appliance through the global RBM policy by loading an XML file, either the `RBMInfo.xml` file or another XML file, into the Authentication RBM Policy URL field. Users who are authenticated by remote servers are authenticated in the same way.

Users are authorized on the appliance through the global RBM policy by loading an XML file, either the `RBMInfo.xml` file or another XML file, into the Mapping RBM Policy URL field.

Authentication defines access for users. Authorization defines available resources that a user can access. RBM manages the credential mapping between users who have access and resources.

#### **Authentication only**

Users are authenticated on the appliance through the global RBM policy by loading an XML file, either the `RBMInfo.xml` file or another XML file, into the Authentication RBM Policy URL field.

Users who are authenticated by remote servers are authenticated in the same way. Authentication defines access for users.

#### **Authorization only**

Users are authorized on the appliance through the global RBM policy by loading an XML file, either the `RBMInfo.xml` file or another XML file, into the Mapping RBM Policy URL field.

Authorization defines available resources that a user can access.

---

### RBM XML file for authentication and authorization

The `RBMInfo.xml` file includes an `Authenticate` section and a `MapCredentials` section. The `Authenticate` section includes `username`, `password` and `OutputCredential` elements for each user listed in the file. The `MapCredentials` section includes an `InputCredential` element. When the value of the `OutputCredential` from the `Authenticate` section of the file matches the value of the `InputCredential` from the `MapCredential` section of the file, users are both

authenticated and authorized under RBM. Through the name of an existing user group on the appliance, an associated user group defines the access policy used for authenticating users.

On zBX, XML files cannot be used for authentication and authorization.

Follow this procedure to provide credentials and access for authenticated users from the **Administration Access RBM Settings** screen:

1. Accept the (default) **Enabled** Admin State radio button.
2. Optional: In the **Comments** field, enter a descriptive summary.
3. Select **xmlfile** from the User Authentication Method list. The screen refreshes with XML-specific fields.
4. Click the **+** button in the Authentication RBM Policy URL area to launch the RBM Policy File builder.

**Note:** To edit an existing file, select a file from the Authentication RBM Policy URL list, and click the **...** button.

5. From the Name of existing file (optional) lists, select the store: directory, and then select **RBMInfo.xml**.

**Note:** If there is no file displayed in the list:

- Click **Upload** to upload a file on the appliance in the store: directory.
- Click **Fetch** to copy a file on the appliance in the store: directory.

6. Click **Next** to set the Default Credential.

Any user that fails authentication will be granted this credential. Leave this field blank to deny access to all users who fail authentication.

7. Click **Next** to display the User Identities catalog. If this is a new file, no users are listed.

**Note:** If the file exists, click **...** to edit the existing policy.

8. Click **Add** to display the Add a new User Identity Property window.
  - a. Specify a user name in the **Username** field.
  - b. Specify a password in the **Password** field and the next field to confirm the password.
  - c. Specify the name of the credential to assign to this user in the **Credential Name** field. The value in the Credential Name field is stored in the Authenticate section of the RBMInfo.xml file as the value of the **OutputCredential** for this user.
9. Click **Submit** to add the user to the catalog. The initial catalog appears, listing the new user. To add more users, click **Add** and repeat the previous step.
10. Click **Next** to display the Access Profile Mappings catalog. If this is a new file, no access policy maps are listed.
11. Click **Add** to display the Add a New Access Profile Property window.
  - a. Specify the name for the credential in the **Credential Name** field. The name can contain wildcards and regular expressions. It is matched to the credential that is presented by the User Authentication method.
  - b. Create one or more Access Policies for this credential. For details, refer to "Specifying the access policy" on page 46.
  - c. Create the access policy.
  - d. Click **Submit**.



12. The Access Profile Mappings screen refreshes. Click **Next**.
13. The Edit RBM Policy File screen refreshes. This screen allows you to rename the RBM Policy file and add a description.
14. Specify the name of the new file and a brief summary in the fields provided.
15. Click **Next** to display the confirmation window.
16. Click **Commit** to create the file. A confirmation success window appears.
17. Click **Done** to complete the process.

The RBM Settings configuration (Main) screen refreshes with the URL of the new policy file in place.

Continue to configure the RBM policy by:

- Defining a Local Login Fallback user on the appliance.
- Specifying whether to enforce this RBM policy to both the WebGUI and the command line or exclude command line access.
- Specifying whether to allow or restrict access by the admin account.

For information, refer to the “RBM XML file for authentication.”

To publish this file to another DataPower appliance, refer to “Publishing an RBM XML file to another appliance” on page 37 for details.

---

## RBM XML file for authentication

The RBMInfo.xml file includes an Authenticate section that includes username, password and an `OutputCredential` element for each user listed in the file.

On zBX, XML files cannot be used for authentication.

When the `OutputCredential` element matches the name of an existing user group on the appliance, the user group defines the access policy uses for authenticating users.

Follow this procedure to provide credentials and access for authenticated users from the **Administration Access RBM Settings** screen:

1. Accept the (default) **Enabled** Admin State radio button.
2. Optional: In the **Comments** field, enter a descriptive summary.
3. Select **xmlfile** from the User Authentication Method list. The screen refreshes with XML-specific fields.
4. Click the + button in the Authentication RBM Policy URL area to launch the RBM Policy File builder.

**Note:** To edit an existing file, select a file from the Authentication RBM Policy URL list, and click the ... button.

5. From the Name of existing file (optional) lists select the store: directory, and then select **RBMInfo.xml**.

**Note:** If there is no file displayed in the list:

- Click **Upload** to upload a file on the appliance in the store: directory.
  - Click **Fetch** to copy a file on the appliance in the store: directory.
6. Click **Next** to set the Default Credential.

Any user that fails authentication will be granted this credential. Leave this field blank to deny access to all users who fail authentication.

7. Click **Next** to display the User Identities catalog. If this is a new file, no users are listed.

**Note:** If the file exists, click ... to edit the existing policy.

8. Click **Add** to display the Add a new User Identity Property window.
  - a. Specify a user name in the **Username** field.
  - b. Specify a password in the **Password** field and the next field to confirm the password.
  - c. Specify the name of the credential to assign to this user in the **Credential Name** field. The value in the Credential Name field is stored in the Authenticate section of the RBMInfo.xml file as the value of the **OutputCredential** for this user.
9. Click **Submit** to add the user to the catalog. The initial catalog appears, listing the new user. To add more users, click **Add** and repeat the previous step.
10. Click **Next**.
11. Skip the Access Profile Mappings screen. Click **Next**.
12. The Edit RBM Policy File screen refreshes. This screen allows you to rename the RBM Policy file and add a description.
13. Specify the name of the new file and a brief summary in the fields provided.
14. Click **Next** to display the confirmation window.
15. Click **Commit** to create the file. A confirmation success window appears.
16. Click **Done** to complete the process.

The RBM Settings configuration (Main) screen refreshes with the URL of the new policy file in place.

Continue to configure the RBM policy by:

- Defining a Local Login Fallback user on the appliance.
- Specifying whether to enforce this RBM policy to both the WebGUI and the command line or exclude command line access.
- Specifying whether to allow or restrict access by the admin account.

For information, refer to the “RBM XML file for authentication” on page 41.

To publish this file to another DataPower appliance, refer to “Publishing an RBM XML file to another appliance” on page 37 for details.

---

## RBM XML file for authorization

The RBMInfo.xml file includes a MapCredentials section that includes an InputCredential and OutputCredential element.

On zBX, XML files cannot be used for authorization.

When the name of a credential generated by a remote server for an authenticated user (representing the OutputCredential listed in the RBMInfo.xml file) matches the InputCredential listed in the RBMInfo.xml file, access to resources is authorized for this user.

Follow this procedure to provide credentials and access for authenticated users from the **Administration Access RBM Settings** screen:

1. Accept the (Default) **Enabled** Admin State radio button.
2. Optional: In the **Comments** field, enter a descriptive summary.
3. Select **xmlfile** from the Mapping Credentials Method list. The screen refreshes with XML-specific fields.
4. Click the **+** button in the Mapping RBM Policy URL area to launch the RBM Policy File builder.

**Note:** To edit an existing file, select a file from the Mapping RBM Policy URL list, and click the **...** button.

5. Optionally from the Name of existing file lists select the store: directory, and then select **RBMInfo.xml**.

**Note:** If there is no file displayed in the list:

- Click **Upload** to upload a file on the appliance in the store: directory.
- Click **Fetch** to copy a file on the appliance in the store: directory.

6. Click **Next** on the Default Credentials screen.
7. Click **Next** on the User Identities screen.
8. Click **Next** to display the Access Profile Mappings catalog. If this is a new file, no access policy maps are listed.
9. Click **Add** to display the Add a New Access Profile Property window.
  - a. Specify the name for the credential in the **Credential Name** field. The name can contain wildcards and regular expressions. It is matched to the credential that is presented by the User Authentication method.
  - b. Create one or more Access Policies for this credential. For details, refer to “Specifying the access policy” on page 46.
  - c. Click **Add** to display each added access profile to the access policy
  - d. Click **Submit**.
10. The Access Profile Mappings screen refreshes. Click **Next**.
11. The Edit RBM Policy File screen refreshes. This screen allows you to rename the RBM Policy file and add a description.
12. Specify the name of the new file and a brief summary in the fields provided.
13. Click **Next** to display the confirmation window.
14. Click **Commit** to create the file. A confirmation success window appears.
15. Click **Done** to complete the process.

The RBM Settings configuration (Main) screen refreshes with the URL of the new policy file in place.

Continue to configure the RBM policy by:

- Defining a Local Login Fallback user on the appliance
- Specifying whether to enforce this RBM policy to both the WebGUI and the command line or exclude command line access
- Specifying whether to allow or restrict access by the **admin** account

refer to the “RBM XML file for authentication” on page 41.

To publish this file to another DataPower appliance, refer to “Publishing an RBM XML file to another appliance” on page 37 for details.



---

## Chapter 6. Managing user group accounts

**Note:** Previous releases of the DataPower appliance allowed for the creation of user groups. In previous releases, users were assigned the rights to use only command groups. These rights did not extend to DataPower resources. These groups and rights are preserved in this release.

A *user group* represents a collection of users who perform similar duties and require the same level of access to the DataPower appliance. User groups are assigned rights to one or more DataPower resources. When adding these rights to the access profile of the specific user group, each right is known individually as an access policy. A collection of access policies is known as an access profile.

The types of user group accounts on the appliance include:

- User-defined groups. These types of accounts are not resident on a new appliance. You create user-defined groups on the appliance, and define access policies on each group for access to resources from the WebGUI and command line. When created, user-defined groups are controlled by Role-based Management (RBM).
- System-defined group. These types of accounts are resident on a new appliance. Role-based Management (RBM) automatically assigns appropriate rights to each appliance-defined group.

The appliance provides a variety of user group accounts, but these are not visible until you have defined at least one user on the appliance. The following types of user group accounts are available:

- User group accounts that are not domain-limited. These groups always belong to the default domain, and the appliance automatically assigns access rights to each group. These user groups include:
  - A system administrator group that is named `sysadmin`.
  - A network administrator group that is named `netadmin`.
  - An access management group that is named `access`.
  - An account management group that is named `account`.
- User group accounts that are domain-limited. Although these groups are normally limited to an application domain, these groups can be part of the default domain if they are re-configured. The appliance automatically assigns access rights to each group, except the user-defined group. These user groups include:
  - A developer group that is named `developer`.
  - A backup user group that is named `backup`.
  - A guest group that is named `guest` and provided with read-only access.
  - A user-defined group that is named and whose access policy must be defined at the time of creation.

---

## Creating a group account

To create a group:

1. Click **Administration** **Access** **Manager User Groups**.
2. Click **Add**.
3. Specify a name for the user group.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. Click **Build**.
7. Optional: Define command groups for members of this group. Command groups are sets of commands which users, through their associated groups, can access from the command line. Defining command groups is applicable only when **Enforce RBM on CLI** is disabled. See “Controlling access to the command line” on page 47 for details.
8. Click **Apply** to save the changes to the running configuration.
9. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Specifying the access policy

Type the access policy directly into the available horizontal field and click **Add** to add the statement to the configuration. The policy statement takes the following form:

*address/domain/resource?Access=privileges&[field=value]*

- The *address* (appliance address), *domain* (application domain), and *resource* fields must be fully specified or specified with an asterisk (\*). An asterisk matches all values.
- The *privileges* string is comprised of the individual permission symbols that are separated by the plus sign (+) character. For example, the string *a+d+x+r+w* represents add, delete, execute, read, and write permissions.
- The *field* token must be one of the additional fields that can be added to the string. The corresponding *value* can be a PCRE.

---

## Example access policies

The following example access policies include the access profile and a description of assigned rights:

- *\*/\*/?\*Access=r+w+a+d+x*  
All users who are members of this group have read, write, add, delete, and execute rights to every area of the appliance.
- *\*/\*/access/change-password?Access=x*  
All users who are members of this group have execute rights to change passwords on every domain of the appliance.
- *\*/\*/access/radius?Access=r*  
All users who are members of this group have read rights to Radius Settings on every domain of the appliance.

---

## Controlling access to the command line

This section discusses adding and removing access to command groups by user group accounts. Command groups are defined on the **CLI Command Groups** tab of the User Groups configuration screen.

- If **Enforce RBM on CLI** is disabled, the defined access profile applies to WebGUI access only. Command line access is defined by command groups in the User Groups configuration.
- If **Enforce RBM on CLI** is enabled, the defined access profile applies to both WebGUI access and command line access. The runtime ignores any command line access that the User Groups configuration defines.

### Adding access to a command group

Each resource group represents a command suite, not necessarily an individual resource. For information on the members of each resource group, click **Info**. Each command group added represents another resource group to make available to this group from the command line.

To allow access to a command group:

1. Click the **CLI Command Groups** tab.
2. Add a command group.
  - a. From the **Command Group** list, select a resource group.
  - b. Click **Add**.
3. Repeat the previous step for each additional resource group to add.
4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

Members of this group can now access this set of command groups from the command line.

### Removing access to a command group

If members of a group have access to at least one command group, you can remove this access.

To remove access to a command group:

1. Click the **CLI Command Groups** tab.
2. Click the **X** icon that is aligned with the unwanted command group.
3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

Members of this user group can no longer access this set of command groups from the command line.





---

## Chapter 7. Using the Access Policy builder

Each access policy is a statement of access rights for all members of a specified group. RBM enforces these rights on groups throughout the appliance. A collection of individual access policies is known as an access profile. Access profiles are reusable and easier to maintain on groups instead of on individual users.

While configuring a user group account from the **Administration Access Manager User Groups** screen, you can create an access policy by clicking **Build** to display the Access Policy Builder.

---

### Elements of an access policy

When building an access policy statement on the Editing Access Profile Property screen, screen elements appear based on each value selected or added. The full list of elements used for building access policies includes the following terms and definitions:

#### **Device Address**

Identifies the local management IP address of the appliance to which the policy is applied. Leave blank for all.

#### **Application Domain**

Identifies the application domain to which the policy is applied. Select (none) for all or if not applicable to resource type. Accepts regular expressions.

#### **Resource Type**

Identifies the type of the resource to which the policy is applied. Select (any) for all resource types.

#### **Name Match**

Limits the access policy to resources with the specified names. Use a PCRE to select groups of resource instances.

#### **Local Address Match**

Limits the access policy to the specified local addresses. A PCRE expression can be used to select a range of addresses.

#### **Local Port Match**

Limits the access policy to the specified local ports. Use a PCRE expression to select a range of ports.

#### **Directory Match**

Limits the access policy to the specified directories. Applies only to the file resource type and the file management type. Use a PCRE to select sets of directories.

#### **Filename Match**

Limits the access policy to the specified local files. Use a PCRE to select a set of files.

#### **Permissions**

Defines the access rights for the resources that match this policy. Options are Read, Write, Add, Delete, and Execute.

---

## Adding an access policy

Continuing from the “Creating a group account” on page 46, follow these steps to create an access policy:

1. Click **Build** to display the Access Policy builder.
2. Optionally specify an IP address in the **Device Address** field. If left blank, the policy under construction will apply to all local addresses. To use a configured local host alias instead of an IP address, click **Select Alias**, which presents a list of configured local host aliases. For information on Host Aliases, refer to “Working with local host aliases” on page 84.
3. Optionally select a DataPower Application domain from the **Application Domain** list. Using the default value (**none**) causes the policy to apply to all domains.
4. Select one Resource Type from the **Resource Type** list. The Resource Type list includes group headings, which are not selectable. Instead, select an individual resource.

**Note:** Group headings, such as **Login** or **XML Processing**, do not refer to valid, individual resources. These are group headings only.

The screen refreshes after selecting a resource type. Depending on the resource type, additional fields might be displayed.

These additional fields provide a way to restrict, or limit, access permissions. For example, the permissions might apply to only a resource with the specified name in the **Name** field. These fields are optional. When not defined, these permissions extend to all resources of the selected type.

**Note:** These fields are interpreted as PCRE wildcard expressions. A value of **foo** in the **Name** field, for example, matches resources with the names **123foobar**, **afoo**, **foo123** as well as **foo**. To restrict the name to only one match, start the entry with the caret (^) character and end it with the dollar sign (\$) character, as in **^foo\$**. This example matches the name **foo** only.

You can use wildcards in the additional fields. The expression **(. \*)** substitutes for one or more characters. For example, the **Name** field could be expressed as **(. \*)intra(. \*)**, which would match **hr-intranet**, **dev-intranet-releng**, or **ny-intrasystem**. A range can be expressed as **[x-y]**; for example **[0-3]**. You can use any PCRE-compliant expression. Refer to <http://www.pcre.org> for more details.

5. Use the **Permissions** check boxes to establish access permissions.
6. Click **Save**. The window closes. The configuration screen lists the newly built statement in the input field.

**Note:** The appliance had previously added **\*/\*/?\*Access=r** which evaluates to Read access for the appliance, across all domains, on all resources.

7. Click **Add** to add the statement to the access policy under construction.
8. Click **Apply** to save the changes to the running configuration.
9. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Example access profile that grants full access

On the Editing Access Profile Property screen, the following elements define an access policy that grants full access to the appliance:

- Leave the **Device Address** field blank.
- Select none in the **Application Domain** field list.
- Select (any) from the **Resource Type** list.
- Leave the **Local Address Match** field blank.
- Leave the **Local Port Match** field blank.
- Leave the **Directory Match** field blank.
- Leave the **Filename Match** field blank.
- Check all the check boxes listed in the **Permissions** area.

The statement defined, `*/*/?*Access=a+w+r+d+x`, evaluates to Add, Write, Read, Delete and Execute access to the appliance, across all domains, for managing all resources.

**Note:** On the User Group Configuration (Main) screen, remember to promote this statement onto the Access Profile for the user group by clicking **Add**

---

## Example access policy that uses wildcards

On the Editing Access Profile Property screen, the following elements define an access policy that uses wildcards:

- Leave the **Device Address** field blank.
- Select Basics in the **Application Domain** field list.
- Select XML Proxy Service under the Services group heading from the **Resource Type** list.
- Type `^dev(.*)$` as the value in the **Name Match** field.
- Leave the **Local Address Match** field blank.
- Enter 200[04] in the **Local Port Match** field.
- Check the Read and Write check boxes listed in the **Permissions** area.

The statement defined, `*/Basics/Services/xslproxy?Name=^dev(.*)$&LocalPort=200[0-4]&Access=r+w`, evaluates to Read and Write access for the appliance, for the Basics domain, for managing the XSL Proxy resource in the Services category of resources.

**Note:** On the User Group Configuration (Main) screen, remember to promote this statement onto the Access Profile for the user group by clicking **Add**

---

## Example access policy that grants user management permissions

On the Editing Access Profile Property screen, the following elements define an access policy that grants permissions to a specific group for managing user accounts:

- Leave the **Device Address** field blank.
- Select User Account under the Access group heading from the **Resource Type** list.
- Leave the **Name Match** field blank.
- Check all the check boxes listed in the **Permissions** area.

The statement defined, `*/*/access/username?Access=r+w+a+d+x`, evaluates to Read, Write, Add, Delete and Execute access to the appliance, across the default domain, for managing all user names in the Access category of resources.

**Note:** On the User Group Configuration (Main) screen, remember to promote this statement onto the Access Profile for the user group by clicking **Add**.

---

## Editing an access profile

Follow this procedure to edit an access profile statement on an access policy of a user group:

1. Select the **Administration Access Manager User Groups** to display the User Group Configuration (Main) screen.
2. From the **Access Profile** list, select the access policy statement to be edited. The statement is highlighted and appears in the Access Profile field (aligned with the Add and Build buttons).
3. Click **Build**.
4. From the Access Profile Property screen, modify values as necessary.
5. Click **Save**.
6. Click **Add** to add the revised statement to the Access Profile for this user group.
7. Click **Apply** to save the changes to the running configuration.
8. Optional: Click **Save Config** to save the changes to the startup configuration.

**Note:** If there are duplicate access profiles in an access policy, the appliance removes any duplicate access profiles after clicking the **Add** button.

---

## Removing an access profile

Follow this procedure to remove an access profile statement from an access policy of a user group:

1. Select the **Administration Access Manager User Groups** to display the User Group Configuration (Main) screen.
2. From the **Access Profile** list, select the **X** aligned with an unwanted access profile statement.
3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Chapter 8. Managing user accounts

User accounts identify local users. Each local user account is defined by a user name and password. These credentials are used to login to the DataPower appliance and apply the appropriate access profile to the user account. Each user account is defined by an access level property, and can be one of the following types:

### Group-defined

The *group-defined* account type establishes this user as a member of a user group.

On zBX, you can only create *group-defined* user accounts.

### Privileged

The *privileged* account type provides this user with access to the entire resource suite from the WebGUI and CLI on a domain-by-domain basis. Users with privileged access can configure and can monitor all appliance operations until explicitly assigned to an application domain. The privileged user cannot delete the `admin` user or the `dp-admin` user on zBX. Legacy privileged users are part of the default domain until assigned to an Application domain, at which time they are no longer associated with the default domain.

**User** The *user* account type provides this user with access to view configuration details to most, but not all, objects. Customers of previous releases who have users that are not members of a group should migrate those users to a guest group. For information, refer to “Migrating a user to a new group” on page 54.

---

## Creating user accounts

The online help provides details about using this wizard.

Only privileged users, while in the default domain or members of the `sysadmin` group with the correct access policy can manage user accounts.

On zBX, only the `dp-admin` user or users given user account management access rights by `dp-admin`, can manage user accounts. The user must also be in the default domain.

**Note:** Although you can create local users with the **Manage User Accounts** wizard, this method is not the best practice. The best practice is to create new local users with the **New User Account** utility. This utility defines a user who is a member of a group.

To create a user account, select **Administration** **Access** **New User Account**. The wizard prompts for the following information:

1. Restrict this user to a domain (Yes or No).
2. If Yes, select the domain to which to restrict this user.
3. Domain Account Type. If user-defined Group selected in step 2, name of Group or create a new group. For information, refer to “Creating a group account” on page 46.
4. Name of user account.

5. Summary describing the user account (optional).
6. Password and confirmed password for the user account.
7. Click **Commit**.
8. Optional: Click **Save Config** to save the changes to the startup configuration.

To create more user accounts, click **Start** instead of **Done** at the end of the wizard.

---

## Resetting the admin password

To edit a user account always use the **Manage User Accounts** utility. After logging on to the default domain as the administrator, use the following procedure to reset the **admin** password:

1. Select **Administration** **Access** **Manage User Accounts** to display the User Account catalog.
2. Click the target account to display an account-specific User Account Configuration (Main) screen.
3. Change the account password with the **Password** and **Confirm Password** fields.
4. Click **Apply** to save the changes.

**Note:** This procedure cannot be used to modify the administrative passwords for zBX. Instead use the **Reset Password** link on the same page.

---

## Migrating a user to a new group

The **Domain Restriction** controls provide a method of controlling user access to the list of configured domains in the absence of an Access Policy. After domain restrictions are set for a user, that user can login only into the specified domains. If no domain is specified, the user can login into any domain on the device. This setting is superseded by an existing Access Policy for the user.

To edit a user account always use the **Manage User Accounts** utility. Use the following procedure to migrate a user to a new group:

1. Select **Administration** **Access** **Manage User Accounts** to display the User Account catalog.
2. Click the target account to display an account-specific User Account Configuration (Main) screen.
3. Select the access level for this user from the **Access Level** value list.
4. Select the name of an existing group that this user will be associated with from the **User Group** value list.
5. Select the name of an existing domain that this user is restricted to from the **Domain Restriction** value list, or click the + button to create a new domain. Refer to "Creating application domains" on page 144 for more information.
6. Click **Apply** to save the changes.

---

## Forcing a password change

Use the following procedure to make users change their password on their next login:

1. Select **Administration** **Access** **Manage User Accounts** to display the User Account catalog.

2. Click the target account to display an account-specific User Account Configuration (Main) screen.
3. Click **Force Password Change** to mark the password as temporary and to force the user to change the account password on the next login attempt.
4. Respond to prompts.

For information on the Password Policy, refer to “Defining the password policy” on page 33.

---

## Changing the password for the current user

**Note:** If you are currently logged in as `admin`, this procedure changes the `admin` password for both the CLI and WebGUI interfaces.

**Note:** On zBX, if you are currently logged in as `dp-admin`, this procedure changes the `dp-admin` password for both the CLI and WebGUI interfaces.

Use the following procedure when a user wishes to change his or her password:

1. Select **Administration Main System Control** to display the System Control panel.
2. Locate the **Change User Password** section.
  - a. In the **Old Password** field, specify the password for the current user.
  - b. In the **New Password** field, specify the new password.
  - c. In the **Confirm Password** field, specify the new password again.
  - d. Click **Change User Password**.

For information on the Password Policy, refer to “Defining the password policy” on page 33.

---

## SNMP V3 users

This type of user account creates an account and adds SNMP V3 credentials. Each account can have multiple SNMP V3 credentials, one for each SNMP V3 engine that is identified by an engine ID value. The secret for authentication and for privacy can be defined either as a password (passphrase) or localized hexadecimal key. If a password, the value will be hashed and localized with the engine ID.

### Notes:

- Although the User Security Model (USM) supports the direct specification of a key, use a password.
- The current implementation supports an SNMP V3 credential for the local engine ID only. Therefore, there can be only one SNMP V3 credential for each account.

## Viewing local SNMP engine ID

To view the local SNMP engine ID, select **Status Other Network SNMP Status**.

Subject to authentication by the local SNMP engine, this account is granted access to any Management Information Base (MIB) on the local appliance. Generally, MIB access is granted for monitoring or for configuration purposes. Refer to “Configuring SNMP Settings” on page 102 for details.



## Creating an SNMP V3 account

An SNMP V3 account can use authentication and privacy. Authentication provides data integrity and data origin authentication for SNMP exchanges between this user and the local SNMP engine. Privacy provides data encryption and decryption for SNMP exchanges between this user and the local SNMP engine.

**Note:** You cannot define an account without authentication but with privacy.

To create an SNMP V3 account:

1. Click **Administration** **Access** **Manage User Accounts**.
2. Click **Add**.
3. Define the basic account information.
  - a. In the **Name** field, enter the name for the object.
  - b. Set **Administrative State** to identify the administrative state of the configuration.
    - To make inactive, click **disabled**.
    - To make active, click **enabled**.
  - c. Optional: In the **Comments** field, enter a descriptive summary.
  - d. Ignore all other fields.
4. Click the **SNMP V3 User Credentials** tab.
5. Click **Add**.
6. In the **Engine ID** field, specify the engine ID that provides a unique identifier for the SNMP engine to authorize this user. In most cases, retain the default value (0) to specify the local engine ID.
7. Define SNMP authentication.
  - a. From the **Authentication Protocol** list, select the authentication protocol that provides data integrity and data origin authentication for SNMP exchanges between this user and the local SNMP engine.
  - b. From the **Authentication Secret Type** list, select whether the secret is a password or a fully localized key. This property is required when the authentication protocol is MD5 or SHA.
  - c. In the **Authentication Secret** fields, specify and confirm the secret. This property is required when the authentication protocol is MD5 or SHA.
    - If password, specify a plaintext password that is at least eight characters long.
    - If key and MD5 is the authentication protocol, specify the hexadecimal representation of a 16-byte key.
    - If key and SHA is the authentication protocol, specify the hexadecimal representation of a 20-byte key.

You can use colons (:) between each two hexadecimal characters.
8. When the account uses authentication, define SNMP privacy (encryption).
  - a. From the **Privacy Protocol** list, select the symmetric privacy protocol that provides data encryption and decryption for SNMP exchanges between this user and the local SNMP engine.
  - b. From the **Privacy Secret Type** list, select whether the secret is a password or a fully localized key. This property is required when the privacy protocol is AES or DES.
  - c. In the **Privacy Secret** fields, specify and confirm the secret. This property is required when the privacy protocol is AES or DES.



- If password, specify a plaintext password that is at least eight characters long.
- If key and MD5 is the authentication protocol, specify the hexadecimal representation of a 16-byte key.
- If key and SHA is the authentication protocol, specify the hexadecimal representation of a 20-byte key.

You can use colons (:) between each two hexadecimal characters.

9. Click **Save**.
10. Click **Apply** to save the changes to the running configuration.
11. Optional: Click **Save Config** to save the changes to the startup configuration.

Repeat this procedure to create additional SNMP V3 accounts.



---

## Part 4. Managing the appliance

### Chapter 9. Securing communication . . . . . 61

Supported cryptographic formats . . . . .	61
Working with keys and certificates . . . . .	61
Creating key-certificate pairs . . . . .	61
Generating keys and certificates . . . . .	62
Exporting keys and certificates . . . . .	63
Importing keys and certificates . . . . .	64
Converting keys to specific formats . . . . .	64
Converting certificates to specific formats . . . . .	65
Working with certificate revocation lists . . . . .	65
Enabling CRL retrieval . . . . .	65
Configuring CRL update policies . . . . .	65
Defining the Certificate Monitor . . . . .	67

### Chapter 10. Managing the appliance itself . . . . . 69

Ethernet and VLAN interfaces . . . . .	69
Standby configurations . . . . .	69
Standby groups . . . . .	70
Failover support. . . . .	70
Self-balancing support. . . . .	73
Configuring Ethernet interfaces. . . . .	76
Configuring VLAN interfaces . . . . .	77
Defining static routes . . . . .	78
Defining interface failover . . . . .	78
Enabling self-balancing . . . . .	79
Removing an Ethernet interface from the network	80
Initiating a packet-capture session . . . . .	80
Configuring appliance-wide network settings . . . . .	80
DNS Settings . . . . .	82
DNS hosts cache. . . . .	82
Load balancing algorithm . . . . .	82
Scenario: DNS lookup procedure used with	
the first alive load balancing algorithm . . . . .	83
Configuring the DNS service . . . . .	84
Flushing the DNS hosts cache . . . . .	84
Host Alias . . . . .	84
Working with local host aliases. . . . .	84
Migrating configuration data . . . . .	85
Managing NTP Servers . . . . .	86
Managing the time on the appliance . . . . .	86
Setting the local time and date . . . . .	86
Setting the local time zone . . . . .	87
Creating a custom time zone . . . . .	87
Selecting the reboot configuration . . . . .	88
Configuring throttle settings. . . . .	88
Shutting down the appliance . . . . .	90
Controlling the locate LED (Type 9235) . . . . .	91
Activating the locate LED . . . . .	91
Deactivating the locate LED . . . . .	91
Generating an appliance certificate . . . . .	91
Appliance settings . . . . .	91
Defining appliance-specific information . . . . .	92
Updating the serial number after a replacement	92
Enabling customized interfaces . . . . .	92
Reserving space for the audit log . . . . .	93
Viewing hardware information . . . . .	93

Configuring NFS Settings. . . . .	94
NFS Client Settings. . . . .	94
NFS Dynamic Mounts . . . . .	94
Passing parameters to files . . . . .	96
NFS Static Mounts . . . . .	96
Using the iSCSI protocol (Type 9235) . . . . .	98
IQN and EUI formats . . . . .	99
Configuring and initializing an iSCSI volume . . . . .	99
Configuring an iSCSI volume . . . . .	99
Initializing an iSCSI volume . . . . .	100
Repairing an iSCSI volume . . . . .	100
Reference objects for iSCSI . . . . .	101
Configuring an iSCSI Target object . . . . .	101
Configuring an iSCSI Initiator object. . . . .	101
Configuring an iSCSI CHAP object . . . . .	102
Configuring SNMP Settings . . . . .	102
Configuring global properties . . . . .	102
Configuring subscriptions . . . . .	103
Configuring communities . . . . .	103
Configuring recipients . . . . .	104
Configuring contexts . . . . .	104
Viewing MIBs . . . . .	105
Default event subscriptions. . . . .	105
Sysplex Distributor Target Control Service. . . . .	106
Creating a Sysplex Distributor Target Control	
Service . . . . .	107
Quiescence . . . . .	107
Quiesce . . . . .	108
Unquiesce . . . . .	108
Checking quiesce and unquiesce status. . . . .	109
Quiescing the appliance . . . . .	109
Unquiescing the appliance . . . . .	109

### Chapter 11. Managing network access to the appliance . . . . . 111

WebGUI access . . . . .	111
Modifying configuration for WebGUI access . . . . .	111
Changing security and connection settings. . . . .	112
Command line access. . . . .	112
Connecting to the serial port . . . . .	112
Connecting using serial over LAN (Type 4195)	113
SSH service . . . . .	114
Enabling SSH . . . . .	114
SSH login . . . . .	115
Enabling Telnet services . . . . .	115
XML Management Interface . . . . .	115
Services overview . . . . .	116
Enabling interface services . . . . .	117
Changing default security and HTTP settings	118
SOAP interface . . . . .	118
General structure of requests . . . . .	119
General structure of responses. . . . .	119
Available operations for requests . . . . .	119
Example request to view status . . . . .	121
Example request to compare configurations . . . . .	122
WSDM interface . . . . .	123

Example request to view the number of client requests . . . . .	125		Unquiescing application domains. . . . .	146
Example request to view active users . . . . .	126		Creating Include Configuration File objects . . . . .	147
Example request to view CPU usage . . . . .	126		Creating Import Configuration File objects . . . . .	148
Example request to view appliance usage . . . . .	127		Backing up and exporting configuration data. . . . .	149
Example request to view accepted connections . . . . .	127		Backing up the entire appliance . . . . .	149
Custom SSL proxy profile . . . . .	127		Backing up domains . . . . .	150
Generating a custom profile . . . . .	127		Exporting select objects . . . . .	150
Removing the profile assignment. . . . .	128		Copying or moving select objects. . . . .	152
Cryptographic material for the custom profile . . . . .	128		Managing configuration checkpoints . . . . .	154
<b>Chapter 12. Managing the firmware image . . . . .</b>	<b>129</b>		Defining number configuration checkpoints to allow . . . . .	154
Applying a firmware image . . . . .	129		Saving configuration checkpoints. . . . .	154
Rolling back an upgrade . . . . .	129		Listing configuration checkpoints. . . . .	155
<b>Chapter 13. Managing files . . . . .</b>	<b>131</b>		Rolling back to a configuration checkpoint . . . . .	155
Directories on the appliance . . . . .	131		Deleting configuration checkpoints . . . . .	155
Launching the File Management utility. . . . .	133		Importing configuration data . . . . .	156
Displaying directory contents . . . . .	133		Managing changes in configuration data . . . . .	157
Creating a subdirectory . . . . .	133		Comparing configurations . . . . .	158
Deleting a directory . . . . .	134		Reading the change report . . . . .	158
Refreshing directory contents . . . . .	134		Reverting changes. . . . .	159
Uploading files from the workstation . . . . .	134		Managing disaster recovery . . . . .	159
Working with Java Key Stores. . . . .	135		Contents of a secure backup . . . . .	160
Required software. . . . .	135		Conditions . . . . .	160
Granting permissions. . . . .	135		General conditions for a secure backup-restore . . . . .	160
Types of key stores . . . . .	135		Conditions for a secure backup . . . . .	161
Uploading a file from a Java Key Store. . . . .	135		Conditions for a secure restore . . . . .	161
Fetching files . . . . .	136		Creating a secure backup of the appliance. . . . .	161
Copying files . . . . .	136		Restoring the appliance from a secure backup . . . . .	161
Renaming files . . . . .	137		Validating a secure backup . . . . .	162
Moving files. . . . .	137		<b>Chapter 16. Deployment policies . . . . .</b>	<b>163</b>
Viewing files . . . . .	138		Creating deployment policies . . . . .	163
Editing files . . . . .	138		Using the deployment policy builder . . . . .	164
Deleting files . . . . .	138		Specifying the matching statement . . . . .	165
<b>Chapter 14. Managing auxiliary data storage . . . . .</b>	<b>139</b>		<b>Chapter 17. Managing event logs . . . . .</b>	<b>167</b>
Configuring the compact flash. . . . .	139		Types of log targets . . . . .	167
Managing the file system on the compact flash . . . . .	139		Configuring log categories . . . . .	168
Initializing the file system . . . . .	139		Configuring log targets . . . . .	168
Repairing the file system . . . . .	140		Setting event filters . . . . .	169
Configuring the hard disk array . . . . .	140		Setting object filters . . . . .	169
Managing the file system on the hard disk array . . . . .	140		Setting event triggers. . . . .	170
Initializing the file system . . . . .	140		Setting IP address filters. . . . .	171
Repairing the file system . . . . .	140		Setting event subscriptions . . . . .	171
Managing the RAID volume . . . . .	141		Viewing logs . . . . .	172
Activating the volume . . . . .	141		Filtering logs . . . . .	172
Initializing the volume . . . . .	141		Understanding logs . . . . .	173
Rebuilding the volume . . . . .	141		Configuring an e-mail pager . . . . .	174
Deleting the volume . . . . .	141		Scenario: Defining a load Balancer as a log target . . . . .	174
<b>Chapter 15. Managing the configuration of the appliance . . . . .</b>	<b>143</b>		Scenario: Defining event triggers . . . . .	175
Managing domains . . . . .	143		Starting and stopping a package capture . . . . .	175
The default domain . . . . .	143		Creating an error report . . . . .	175
Application domains . . . . .	143		Using a custom message . . . . .	176
Visible domains . . . . .	144			
Creating application domains . . . . .	144			
Restarting application domains . . . . .	145			
Resetting application domains. . . . .	146			
Quiescing application domains . . . . .	146			

---

## Chapter 9. Securing communication

This chapter provide information about securing communication to and from the DataPower appliance. The appliance provide these capabilities with a combination of utilities and objects.

---

### Supported cryptographic formats

Private key objects support the following formats:

- DER
- PEM
- PKCS #8
- PKCS #12

Certificate objects support the following formats:

- DER
- PEM
- PKCS #7
- PKCS #12

Neither key objects nor certificate objects directly support JKS or KDB formats.

---

### Working with keys and certificates

The DataPower appliance provides actions that allow you to work with keys and certificates. With the provided cryptographic tools, you can perform the following actions:

- Create key-certificate pairs
- Generate keys and certificates
- Export keys and certificates
- Import keys and certificates
- Convert keys to specific formats
- Convert certificates to specific formats

Unless you are using an appliance with HSM hardware, you cannot export or import keys. For details about using an HSM-enabled appliance, refer to the *IBM WebSphere DataPower SOA Appliances: Hardware Security Module Guide*.

### Creating key-certificate pairs

When you generate a key, you get a key file and a Certificate Signing Request (CSR) file. The CSR file from the initial key generation is *not* a signed certificate. Send the CSR to a Certificate Authority (CA), such as VeriSign. The CA signs the CSR and returns it to you, which effectively creates the certificate. Load this certificate on the box.

In other words, use the following procedure to create the key-certificate pair:

1. Use the Crypto Tools to create the key and CSR
2. Store the private key on the box and create a Key object that references it.

3. Send the CSR to VeriSign. Do not store it on the box (except in the temporary: directory).
4. VeriSign returns the signed certificate.
5. Store the signed certificate on the box and create a Certificate object that references it.

Optionally, create an Identification Credentials object that references the Key and Certificate objects. When you create the Identification Credentials, the key-certificate pair is validated to ensure that pair is ready for use.

## Generating keys and certificates

You can generate a private cryptographic key and optionally a self-signed certificate from the Crypto Tools page. The Certificate Signing Request (CSR) needed by a certificate authority (CA) is created by default.

If the file is stored in the cert: directory, it cannot be deleted or edited. If a file is stored in the local: directory or in the temporary: directory, it can be deleted and edited.

To generate a key:

1. Click **Administration** **Miscellaneous** **Crypto Tools**.
2. Define the LDAP entry.
  - a. Set **LDAP (reverse) Order of RDNs** to indicate whether to create the LDAP entry in reverse RDN order.
    - on** Creates the entry in reverse RDN order.
    - off** (Default) Creates the entry in forward RDN order.
  - b. Optional: In the **Country Name (C)** field, enter a country name.
  - c. Optional: In the **State or Province (ST)** field, enter a state name or a province name.
  - d. Optional: In the **Locality (L)** field, enter a locality name.
  - e. Optional: In the **Organization (O)** field, enter the name of an organization.
  - f. Optional: In the **Organizational Unit (OU)** field, enter the name of an organizational unit.
  - g. Optional: In the **Organizational Unit 2 (OU)**, **Organizational Unit 3 (OU)**, and **Organizational Unit 4 (OU)** fields, enter the names of additional organizational units.
  - h. In the **Common Name (CN)** field, enter a common name.
3. From the **RSA Key Length** list, select the key length. This defaults to 1024.
4. In the **File Name** field, enter the name of the key file to generate. The value takes the *directory:///name* form. Leave blank to allow the action to create the name.
5. In the **Validity Period** field, enter the number of days that the key is valid.
6. In the **Password** field, enter a password to access the key file. The password must be at least six characters in length.
7. In the **Password Alias** field, enter a password alias to access the key file.
8. Set **Export Private Key** to indicate whether the action writes the key file to the temporary: directory.
  - on** Writes the key file to the temporary: directory.
  - off** (Default) Does not write the key file to the temporary: directory.

9. Set **Generate Self-Signed Certificate** to indicate whether the action creates a self-signed certificate that matches the key.
  - on** (Default) Creates a self-signed certificate.
  - off** Does not create a self-signed certificate.
10. Set **Export Self-Signed Certificate** to indicate whether the action writes the self-signed certificate to the temporary: directory.
  - on** (Default) Writes the self-signed certificate to the temporary: directory.
  - off** Does not write the self-signed certificate to the temporary: directory.
11. Set **Generate Key and Certificate Objects** to indicate whether the action automatically creates the objects from the generated files.
  - on** (Default) Creates the objects from the generated files.
  - off** Does not create the objects from the generated files.
12. In the **Object Name** field, enter the name to use for the Key object and for the Certificate object. Leave blank to allow the action to generate the names from the input information (based on the **Common Name (CN)** or **File Name** property).
13. In the **Using Existing Key Object** field, enter the name of an existing key. If supplied and valid, the action generates a new certificate and a new Certificate Signing Request (CSR) that is based on the key in the identified Key object. In this case, the appliance does not generate a new key.
14. Click **Generate Key** to generate a private key and, if requested, a self-signed certificate. A CSR is created automatically.
15. Follow the prompts.

The CSR can be submitted to a certificate authority (CA) to receive a certificate that is based on this private key. This action creates the following files and objects:

- Creates the private key file in the cert: directory; for example, cert: ///sample-pri vkey. pem
- Creates the CSR in the temporary: directory; for example, temporary: ///sample. csr
- If **Generate Self-Signed Certificate** is enabled, creates a self-signed certificate in the cert: directory; for example, cert: ///sample-sscert. pem
- If **Export Self-Signed Certificate** is enabled, creates a copy of the self-signed certificate in the temporary: directory; for example, temporary: ///sample-sscert. pem
- If **Generate Key and Certificate Objects** is enabled, creates a Key object and a Certificate object

If the action creates a self-signed certificate, you can use this certificate-key pair for the following purposes:

- Establish Identification Credentials
- Encrypt or decrypt XML documents

## Exporting keys and certificates

Use the **Export Crypto Objects** tab of the Crypto Tools screen to export key and certificate objects.

**Note:** If the appliance has HSM hardware, you can export Key objects. For details, refer to *IBM WebSphere DataPower SOA Appliances: Hardware Security Module Guide*.

To export a key or certificate:

1. Click **Administration** **Miscellaneous** **Crypto Tools**.
2. Click the **Export Crypto Object** tab.
3. From the **Object Type** list, select the type of object to export. Any appliance can export certificates. Devices with HSM hardware can export private keys.
4. In the **Object Name** field, enter the exact name of the private key. To view a list of all such objects, select **Objects** **Crypto Objects** **Cryptographic Certificate** (or **Key**).
5. In the **Output File Name** field, enter the name of a file into which to export the key. The name cannot have a file extension. This file is in the temporary: directory of the local file storage area.
6. Click **Export Crypto Object**.

The selected cryptographic object is exported to the identified file. A new file with the name given is created in the temporary: directory. This file can then be copied from the appliance.

Use the File Management utility to access the file.

## Importing keys and certificates

Use the **Import Crypto Objects** tab of the Crypto Tools screen to import key and certificate objects.

Objects that are exported from one DataPower appliance can be imported to another appliance. Importing objects, rather than uploading files, eliminates the need to create objects from files.

**Note:** If the appliance has HSM hardware, you can import Key objects. For details, refer to *IBM WebSphere DataPower SOA Appliances: Hardware Security Module Guide*.

To import a key or certificate:

1. Click **Administration** **Miscellaneous** **Crypto Tools**.
2. Click the **Import Crypto Object** tab.
3. From the **Object Type** list, select the type of object to import. Any appliance can import certificates. Devices with HSM hardware can import private keys.
4. In the **Object Name** field, enter the name of the object to create. This name must be unique in the object namespace.
5. In the **Input File Name** field, select the export package. If the file does not reside on the DataPower appliance, click **Upload** or **Fetch** to transfer the file.
6. Click **Import Crypto Object**.

An object with the specified name is created. Otherwise, an error is returned.

## Converting keys to specific formats

Use the **Convert Crypto Key Object** tab of the Crypto Tools screen to convert a private key object to a specific output format and write it to a file.



If the output format includes private fields of the key, the file must be in the same directory as the configured file of the private key object. The OpenSSH public key format, which is used in `authorized_keys` files, does not contain any private fields. It contains only public fields.

To convert a key object:

1. Click **Administration** **Miscellaneous** **Crypto Tools**.
2. Click the **Convert Crypto Key Object** tab.
3. From the **Key Name** list, select the name of the key object to be converted.
4. In the **Output File Name** field, enter the name of the output file. Use the temporary: `///mykey.pub` format.
5. From the **Output Format** list, select the format of the output file.
6. Click **Convert Crypto Key Object** to convert the specified key object to the specified format.

## Converting certificates to specific formats

Use the **Convert Crypto Certificate Object** tab of the Crypto Tools screen to convert a certificate object to a specific output format and write it to a file.

To convert a certificate object:

1. Click **Administration** **Miscellaneous** **Crypto Tools**.
2. Click the **Convert Crypto Certificate Object** tab.
3. From the **Certificate Name** list, select the name of the certificate object to be converted.
4. In the **Output File Name** field, enter the name of the output file. Use the temporary: `///mycert.pub` format.
5. From the **Output Format** list, select the format of the output file.
6. Click **Convert Crypto Certificate Object** to convert the specified certificate object to the specified format.

---

## Working with certificate revocation lists

A certificate revocation list (CRL) update policy enables the periodic refresh of CRLs. To use CRLs, enable the CRL Retrieval object and configure at least one instance of the CRL Policy object.

**Note:** The appliance supports CRLs that are in the DER format only.

### Enabling CRL retrieval

To enable the CRL update policy:

1. Click **Objects** **Crypto Configuration** **CRL Retrieval**.
2. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.

### Configuring CRL update policies

After enabling the CRL update policy, you need to configure the CRL update policy. To configure the CRL update policy, use the following procedure:

1. Click the **CRL Policy** tab.

2. Click **Add**.
3. Provide the following inputs:

**Policy Name**

Specify the name of the CRL Update Policy.

**Protocol**

Select the protocol that supports access to a CRL server.

**HTTP** (Default) Uses HTTP to enable the CRL update policy.

**LDAP** Uses LDAP to enable the CRL update policy. When selected, this protocol requires additional inputs.

**CRL Issuer Validation Credentials**

Select the validation credentials to apply to the CRL Issuer credentials.

**Refresh Interval**

Specify the refresh interval (the interval, in minutes, between CRL updates).

**Cryptographic Profile**

Optionally specify the name of the Profile object. This profile assigns a *forward* (client) proxy to the CRL Update Policy. The policy uses the client credentials that are referenced by the Profile object when establishing an SSL connection with a CRL server. If not specified, the CRL Update Policy attempts to establish a nonsecure connection with the CRL server.

**Fetch URL**

When enabled through HTTP, specify the location of the target CRL.

**LDAP Server**

When enabled through LDAP, specify the IP address or fully qualified domain name of the CRL server.

**LDAP Port**

When enabled through LDAP, specify the remote LDAP port.

**LDAP Read DN**

When enabled through LDAP, specify the distinguished name of the Certificate Authority (CA) that issued the target CRL.

**LDAP Bind DN**

When enabled through LDAP, specify the account name used to log in to the LDAP server.

**LDAP Bind Password**

When enabled through LDAP, specify the password to use to log in to the LDAP server.

**Confirm LDAP Bind Password**

When enabled through LDAP, again specify the password to use to log in to the LDAP server.

**LDAP Version**

When enabled through LDAP, select the desired LDAP version.

4. Click **Save**.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Defining the Certificate Monitor

The Certificate Monitor is a configurable periodic task that checks the expiration date of all certificates. User-specified values establish both a polling frequency and a notification window during which the monitor generates log messages that record when a specific certificate is nearing its expiration date. The Certificate Monitor scans all certificates when first enabled.

To create a Certificate Monitor:

1. Click **Objects** **Crypto** **Crypto Certificate Monitor**.
2. Provide the following inputs:

### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

### Comments

Optional: Enter a descriptive summary.

### Polling Interval

Specify the frequency in days with which the Certificate Monitor examines expiration dates. For example, the value 3 schedules an expiration scan every 72 hours.

### Reminder Time

Specify the notification window in days before certificate expiration triggers a log event. For example, the value 21 specifies that all scanned certificate objects due to expire in 3 weeks or less generate a log entry.

### Log Level

Select the priority of log messages that are generated in response to an expired certificate or to a certificate that is about to expire (as defined by the **Reminder Time** property).

### Disable Expired Certificates

Specify the response to certificate expiration.

- on** Specifies that on certificate expiration, all objects that use the expired certificate (either directly or through inheritance) are disabled and are no longer in service. For example, certificate expiration triggers the disablement of the associated certificate. Disablement of the certificate triggers the disablement of all firewall credentials, identification credentials, and validation credentials that use the expired certificate. In turn, crypto profiles that use disabled identification credentials and validation credentials are disabled, leading to the disablement of SSL proxy profiles that depend on the now-disabled crypto profiles. Ultimately, the DataPower service can be disabled as the result of certificate expiration.
- off** (Default) Specifies that certificates and credential sets that use the expired certificate are not disabled on certificate expiration.

3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.



---

## Chapter 10. Managing the appliance itself

This chapter contains information about managing the appliance itself and the network in to which it is configured.

---

### Ethernet and VLAN interfaces

The Type 7993 or Type 9235 DataPower appliance provides four Ethernet interfaces. There is one management port, labelled **MGMT**, and three network ports, labelled **ETH0**, **ETH1**, and **ETH2**. You can use all of these ports for network traffic, but best practices suggest restricting the management port to segregate management activities. The labeling of the network ports is different for Blade servers.

The Type 4195 Blade appliance also provides four Ethernet interfaces by default. The two 1 Gbps Ethernet interfaces are numbered **eth1** and **eth2**. The 10 Gbps Ethernet interfaces are numbered **eth7** and **eth9**. You can use all of these ports for network traffic. The ports connect to switch bays in the BladeCenter chassis. The numbering of the ports matches that of the switch bay, for example, Ethernet interface **eth7** connects to switch bay 7 in the chassis.

**Note:** On the expansion card on the front of the blade appliance, there are plastic covers over the Ethernet interfaces. These interfaces are inoperable. Do not remove these covers, and do not attempt to use these ports.

A virtual LAN (VLAN) allows multiple logical LANs to coexist on the same Ethernet segment. VLAN packets are identified by the IEEE 802.1Q tagging protocol. This protocol allows for DataPower appliances on different VLANs to use a switch or router with layer-3 capabilities to communicate as if they were on different physical LANs. You can create multiple VLANs on a single Ethernet interface.

**Note:** All models of DataPower appliances except for B2B Appliance XB60 appliances support IPv6 addresses.

### Standby configurations

The standby configuration for an interface (Ethernet or VLAN) defines the standby policies for the group to which this interface belongs. A *standby group* is the collection of interfaces on different appliances in the multicast domain that share the responsibility for one virtual IP address. If at least one member of a standby group can reach the multicast domain, the virtual IP group will receive the traffic.

#### Restrictions:

- Only one interface, either Ethernet or VLAN, on a given physical Ethernet interface can have a standby configuration. Therefore, only one physical interface on an appliance can have a standby configuration with a particular standby group.
- The virtual IP address of the standby group must be on the same IP subnet as the primary address of the interface.

The multicast domain is defined by the group of interfaces that can receive traffic on the IP address 224.0.0.2 (the all-routers IP multicast group) from each other. If

the multicast domain becomes partitioned, which is an unusual situation, a member in each partition becomes the active member to handle connections in its partition.

## Standby groups

A standby group is the group of interfaces on the same network segment that share the responsibility for one virtual IP address. Each member in a standby group must have the following configuration:

- Be assigned to the same group.
- Use the same virtual IP address.
- Use the same security token (first four and last four authentication bytes).

For each standby group there is one active member and one or more passive members. The interface with the highest priority seeks to be the active member. Do not assign the same priority to multiple interfaces. If multiple interfaces have the same priority, all seek to be the active member. Depending on priority and preemption, the following behavior occurs when an active member becomes unavailable and later becomes available:

- If the active member in the standby group becomes unavailable, failover occurs. A *failover* is when the passive member with the next highest priority seeks to be the active member.
- If the previously active member in the standby group becomes available and is set for preemption, takeover occurs. A *takeover* is when a previous active member becomes available and seeks to be the active member.

When configured, the interfaces in the standby group operate in either failover mode or in self-balancing mode with failover support.

### Failover mode

In failover mode, the active member receives all TCP connections and processes all requests. All requests and responses go through the active member. If the active member becomes unavailable, the passive member with the next highest priority becomes the active member.

### Self-balancing mode

Self-balancing is an extension of failover. In self-balancing mode, the active member manages all TCP connections to the virtual IP address. When a client requests of a new TCP connection, the active member selects a member of the standby group to act as the endpoint for the connection. The active member tracks the capacities of the members to select the member with the most available capacity to act as the endpoint. The selected member completes the establishment of the connection. The active member forwards all segments of the TCP connection to the member that is acting as the endpoint for this connection.

If the active member becomes unavailable, the passive member with the next highest priority becomes the active member. When failover occurs, the connection assignments to all members are lost and all existing TCP connections to all members are broken.

## Failover support

In failover mode, the active member receives all TCP connections and processes all requests. All requests and responses go through the active member. If the active member becomes unavailable, the passive member with the next highest priority becomes the active member.

A failover configuration ensures that an interface on one appliance is available if the active member on another appliance becomes unavailable. An interface might become unavailable as a result of an internal hardware failure, an intermittent network failure, or another failure.

The interface that is the active member changes only under the following conditions:

- The interface goes down or is disconnected.
- Another interface in the group is assigned a higher priority and preemption is enabled.

| Table 3 defines a sample standby group configuration in failover mode. The sample shows appliances using the eth0 interface. The scenario would also be valid if some or all of these appliances are Blade appliances using, for example, the eth1 interface.

Table 3. Sample standby group configuration in failover mode

	Appliance 1	Appliance 2	Appliance 3
Interface	ETH0	ETH0	ETH0
Group	50		
Virtual IP address	192.168.1.100		
Physical IP address	192.168.1.10/23	192.168.1.11/23	192.168.1.12/23
Priority	100	90	80

Figure 4 illustrates the configuration in Table 3 and the resulting connection processing.

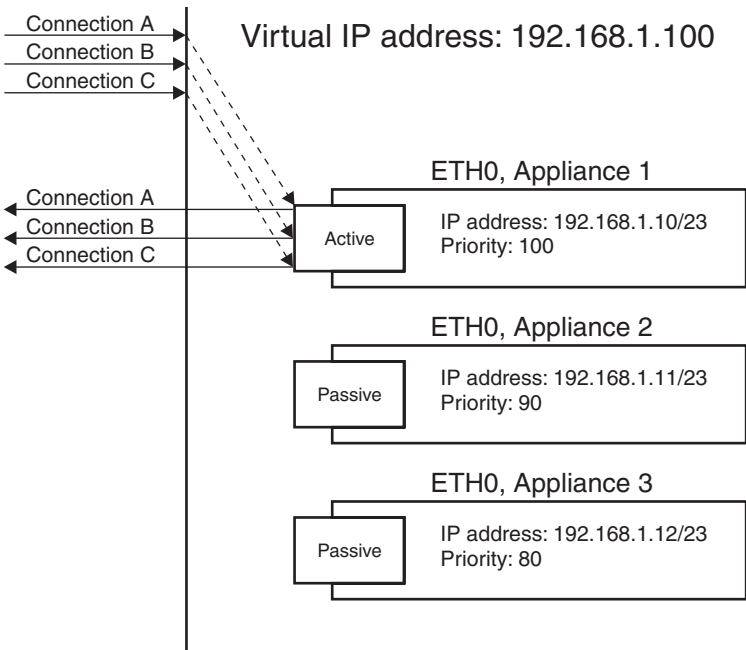


Figure 4. Standby group in failover mode

The processing for connections A, B, and C is as follows:

- Connection A:

1. A client sends Connection A to 192.168.1.100.
  2. The active member, ETH0 on Appliance 1, receives and establishes a TCP connection.
  3. The service on the allocated listening port on ETH0 processes the request.
  4. The service uses Connection A to return the response to the client.
- Connection B:
    1. A client sends Connection B to 192.168.1.100.
    2. The active member, ETH0 on Appliance 1, receives and establishes a TCP connection.
    3. The service on the allocated listening port on ETH0 processes the request.
    4. The service uses Connection B to return the response to the client.
  - Connection C:
    1. A client sends Connection C to 192.168.1.100.
    2. The active member, ETH0 on Appliance 1, receives and establishes a TCP connection.
    3. The service on the allocated listening port on ETH0 processes the request.
    4. The service uses Connection C to return the response to the client.

Now assume that ETH0 on Appliance 1 in standby group 50 becomes unavailable. Because ETH0 on Appliance 2 has the next highest priority (90), it becomes the active member. Figure 5 illustrates connection processing after failover.

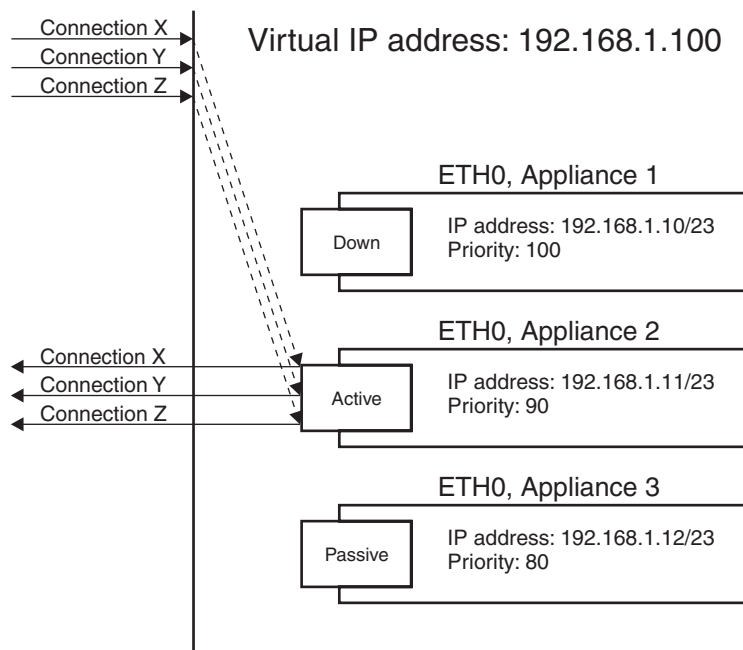


Figure 5. Standby group in failover mode after failover

Because of failover, the processing for connections X, Y, and Z is as follows:

- Connection X:
  1. A client sends Connection X to 192.168.1.100.
  2. The active member, ETH0 on Appliance 2, receives and establishes a TCP connection.
  3. The service on the allocated listening port on ETH0 processes the request.



4. The service uses **Connection X** to return the response to the client.
- **Connection Y:**
    1. A client sends **Connection Y** to 192.168.1.100.
    2. The active member, **ETH0** on **Appliance 2**, receives and establishes a TCP connection.
    3. The service on the allocated listening port on **ETH0** processes the request.
    4. The service uses **Connection Y** to return the response to the client.
  - **Connection Z:**
    1. A client sends **Connection Z** to 192.168.1.100.
    2. The active member, **ETH0** on **Appliance 2**, receives and establishes a TCP connection.
    3. The service on the allocated listening port on **ETH0** processes the request.
    4. The service uses **Connection Z** to return the response to the client.

Now assume that **ETH0** on **Appliance 1** in standby group 50 becomes available and preemption was enabled. **ETH0** on **Appliance 1** becomes the active member again. Request processing as illustrated in Figure 4 on page 71 resumes.

**Note:** When takeover occurs, connection assignments are lost and TCP connections are broken.

## Self-balancing support

Self-balancing extends failover to allow appliances to which the interfaces are members to share client workload.

Self-balancing is an option that allows an interface in a standby group to participate in connection distribution for load-balancing. After an administrator enables self-balancing on two or more interfaces in a standby group, the active member begins to distribute incoming connections among all self-balancing members. All incoming packets for connections that are addressed to a virtual IP address are delivered to the active member. The active member decides which member should process each connection and forwards all packets for this connection to this member for processing. The member that processes the connection responds directly to the client.

In self-balancing mode, the priority setting still controls the failover policy. If the active member becomes unavailable, the member with the next highest priority becomes the active member and take ownership of the virtual IP address. The newly active member assumes the responsibility of distributing incoming connections.

The advantages of self-balancing are as follows:

- Increased performance
- Better utilization of DataPower appliance resources
- Increased availability

**Note:** The following services are not self balanced:

- Administrative services, which include the Web management service, the XML management interface, Telnet, and SSH.
- FTP server front side handlers

Self-balancing works with non-polling, NAT clean connections. Members of the standby group do not need to be the same model. However, all appliances in the standby group must have the Option for Application Optimization feature.

Table 4 defines a sample standby group in self-balancing mode.

Table 4. Sample standby group configuration in self-balancing mode

	Appliance 1	Appliance 2	Appliance 3
Interface	ETH0	ETH0	ETH0
Group	50		
Virtual IP address	192.168.1.100		
Physical IP address	192.168.1.10/23	192.168.1.11/23	192.168.1.12/23
Priority	100	90	80
Enable/Disable Self-balancing	On	On	On

Figure 6 illustrates the configuration in Table 4 and the resulting connection processing.

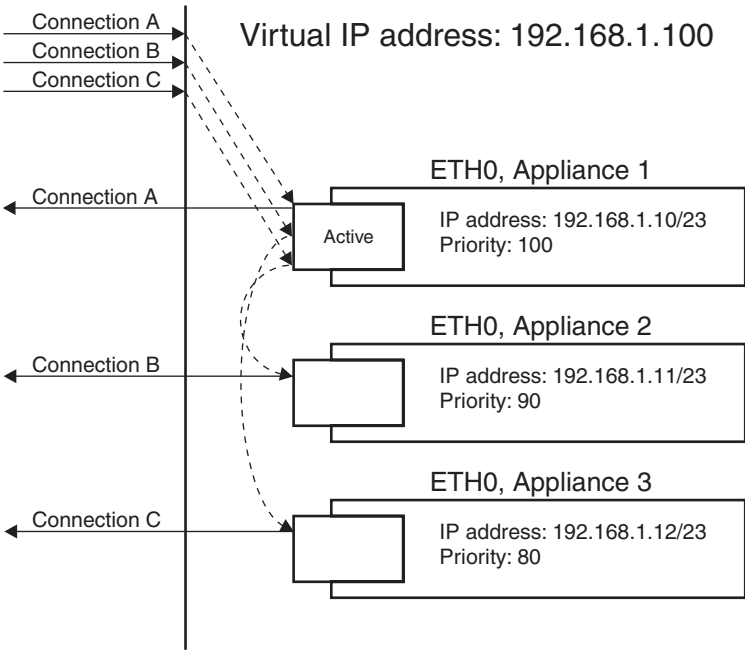


Figure 6. Standby group in self-balancing mode

The processing for connections A, B, and C is as follows:

- Connection A:
  1. A client sends Connection A to 192.168.1.100.
  2. The active member, ETH0 on Appliance 1, receives the TCP connection, reviews the capabilities of all members in the standby group, and forwards the TCP connection to itself.
  3. The service on the allocated listening port on ETH0 establishes a TCP connection and processes the request.
  4. The service on Appliance 1 returns the response to the client.

- Connection B:
  1. A client sends Connection B to 192.168.1.100.
  2. The active member, ETH0 on Appliance 1, receives the TCP connection, reviews the capabilities of all members in the standby group, and forward the TCP connection to ETH0 on Appliance 2.
  3. The service on the allocated listening port on ETH0 on Appliance 2 establishes a TCP connection and processes the request.
  4. The service on Appliance 2 returns the response to the client.
- Connection C:
  1. A client sends Connection C to 192.168.1.100.
  2. The active member, ETH0 on Appliance 1, receives the TCP connection, reviews the capabilities of all members in the standby group, and forward the TCP connection to ETH0 on Appliance 3.
  3. The service on the allocated listening port on ETH0 on Appliance 3 establishes a TCP connection and processes the request.
  4. The service on Appliance 3 returns the response to the client.

Now assume that ETH0 on Appliance 1 in standby group 50 becomes unavailable. Because ETH0 on Appliance 2 has the next highest priority (90), it becomes the active member. Figure 7 illustrates connection processing after failover.

**Note:** When failover occurs, the self-balancing connections assignments are lost and TCP connections are broken.

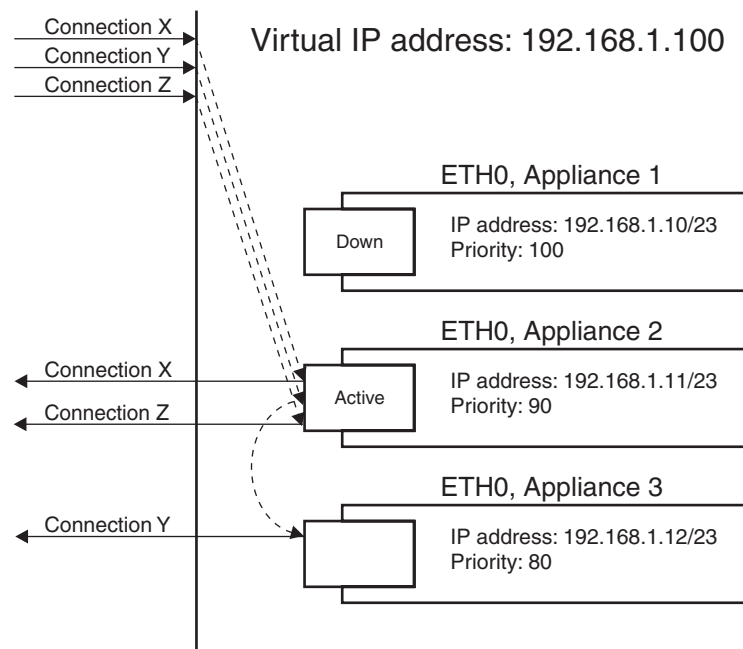


Figure 7. Standby group in self-balancing mode after failover

Because of failover, the processing for connections X, Y, and Z is as follows:

- Connection X:
  1. A client sends Connection X to 192.168.1.100.
  2. The active member, ETH0 on Appliance 2, receives the TCP connection, reviews the capabilities of all members in the standby group, and forwards the TCP connection to itself.

3. The service on the allocated listening port on **ETH0** establishes a TCP connection and processes the request.
4. The service on **Appliance 2** returns the response to the client.
- **Connection Y:**
  1. A client sends **Connection Y** to 192.168.1.100.
  2. The active member, **ETH0** on **Appliance 2**, receives the TCP connection, reviews the capabilities of all members in the standby group, and forward the TCP connection to **ETH0** on **Appliance 3**.
  3. The service on the allocated listening port on **ETH0** on **Appliance 3** establishes a TCP connection and processes the request.
  4. The service on **Appliance 3** returns the response to the client.
- **Connection Z:**
  1. A client sends **Connection Z** to 192.168.1.100.
  2. The active member, **ETH0** on **Appliance 2**, receives the TCP connection, reviews the capabilities of all members in the standby group, and forwards the TCP connection to itself.
  3. The service on the allocated listening port on **ETH0** establishes a TCP connection and processes the request.
  4. The service on **Appliance 2** returns the response to the client.

Now assume that **ETH0** on **Appliance 1** in standby group 50 becomes available and preemption was enabled. **ETH0** on **Appliance 1** becomes the active member again. Connection processing as illustrated in Figure 6 on page 74 resumes.

## Configuring Ethernet interfaces

On older Type 9235 appliances, you cannot modify the **Physical Mode** property for the **ETH1** and **ETH2** Ethernet interfaces. The Blade appliance does not allow setting **Physical Mode** on any Ethernet interface.

To provision local Ethernet interfaces:

1. Click **Network Interface Ethernet Interface**.
2. Click the name of the interface.
3. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
4. Define the network configuration of the interface. Normally IP addresses of infrastructure devices are fixed configuration. Use the Dynamic Host Configuration Protocol (DHCP) only if you have a reason to obtain addresses dynamically.

Set the primary IP address.

- For an IPv4 address, set **Use DHCP** to control whether to obtain the address using Dynamic Host Configuration Protocol (DHCP).
  - For an IPv6 address, in the **IP Address** field, specify the IP address and subnet mask in CIDR format.
5. Optional: Modify the way the Ethernet interface works within the network.
    - Set the default gateway.
    - Define secondary IP addresses.
    - Ensure that Address Resolution Protocol (ARP) is enabled.

- For an IPv6 address, determine whether to use address autoconfiguration. If manual, define Stateless Address Autoconfiguration (SLAAC) and Duplicate Address Detection (DAD) behavior.
  - Change the maximum transmission unit (MTU) for its default value of 1500.
  - Change the MAC (physical) address from the “burned-in” value on the network interface card (NIC). The NIC provides the physical interface. The address must be in hexadecimal format, for example 00: 11: 22: 33: 44: 55: EE.
  - Change the physical setting for operational mode interface speed and duplex.
6. Optional: Add static routes to the routing table. For details, refer to “Defining static routes” on page 78.
  7. Optional: Define standby controls for interface failover. For details, refer to “Defining interface failover” on page 78.
  8. Click **Apply** to save the changes to the running configuration.
  9. Optional: Click **Save Config** to save the changes to the startup configuration.

For information about these properties, refer to the online help.

## Configuring VLAN interfaces

To configure VLAN interfaces:

1. Click **Network** **Interface** **VLAN Sub-Interface**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. Define the network configuration of the interface.
  - a. Set the primary IP address.
    - For an IPv4 address, set **Use DHCP** to control whether to obtain the address using Dynamic Host Configuration Protocol (DHCP).
    - For an IPv6 address, in the **IP Address** field, specify the IP address and subnet mask in CIDR format.
  - b. Set the default gateway.
  - c. Define secondary IP addresses.
  - d. For an IPv4 address, determine whether to enable Address Resolution Protocol (ARP).
  - e. For an IPv6 address, determine how whether to use address autoconfiguration. If manual, define Stateless Address Autoconfiguration (SLAAC) and Duplicate Address Detection (DAD) behavior.
7. Associate the VLAN interface to an Ethernet interface.
  - a. Select the Ethernet interface to provide connectivity.
  - b. Specify the identifier.
  - c. Specify the outbound priority.
8. Optional: Add static routes to the routing table. For details, refer to “Defining static routes” on page 78.
9. Optional: Define standby controls for interface failover. For details, refer to “Defining interface failover” on page 78.

10. Click **Apply** to save the changes to the running configuration.
11. Optional: Click **Save Config** to save the changes to the startup configuration.

For information about these properties, refer to the online help.

## Defining static routes

To add static routes to an interface during configuration:

1. Click the **Static Routes** tab.
2. Add a static route to the routing table.
  - a. Click **Add** to display the property window.
  - b. Define the properties for the static route. For information about these properties, refer to the online help.
    - Its destination network address
    - The network address of its next-hop router (gateway)
    - Its routing preference (metric)
  - c. Click **Save** to commit the static route and return to the configuration screen.
3. Repeat the previous step to add another static route to the routing table.

For information about these properties, refer to the online help.

## Defining interface failover

To define standby controls for failover, define the properties on the **Standby Control** tab. For information about these properties, refer to the online help.

**Note:** Only one interface on a given physical interface (either base Ethernet or VLAN) can use standby.

The failover configuration requires the configuration of all participating interfaces with the following requirements:

- All interfaces must be on the same subnet, on the same broadcast domain.
- The switches must use the fast spanning tree protocol.
- Only one interface on a device can be in a particular standby group.
- All interfaces must be assigned to the group number.

The group number must be distinct from all other group numbers that are being used by IP routers or switches in the same multicast domain. The active interface in the group will change its Ethernet MAC address to 00:00:0C:07:AC:XX, where XX is the group number. This number must be unique among all standby groups on a given appliance.

- All interfaces must use the same virtual IP address. This address serves as the destination address.
- All interfaces must use the same security token (first four and last four authentication bytes).

If the interface is to be the active member, define preemption to indicate whether this interface returns to the active role when it becomes available. When preemption happens, all TCP connections to the virtual IP address are lost. Control of the standby group (the virtual IP address) moves to the interface that is preempting (becoming the active member). However, TCP connections cannot move.

If the interface is to be a passive member, assign a priority that is less than that of the active member.

One issue to consider when defining failover is that a device will try to be the active member of the standby group even if all its other interfaces are down.

## Enabling self-balancing

Self-balancing extends failover to allow interfaces in a standby group to share client workload.

### Before you begin

Define a failover configuration for the interfaces in the standby group.

### About this task

Enable each interface in the standby group to share the processing of incoming connections.

#### Notes:

- All services that listen on the associated interface become self-balanced services.
- On each appliance, equivalent services must be bound to identical ports.

### Procedure

1. Access the interface configuration.
  - For an Ethernet interface, Click **Network** **Interface** **Ethernet Interface**.
  - For a VLAN interface, Click **Network** **Interface** **VLAN Sub-Interface**.
2. Click the name of the interface.
3. Click the **Standby Control** tab.
4. Set **Enable/Disable self-balancing** to **on**.
5. Click **Apply**.
6. Optional: Click **Save Config**.

### Results

The interface is enabled for self-balancing. Use the following status providers to validate or to troubleshoot standby configurations:

- To verify standby control status, click **Status** **IP Network** **Standby**
- To verify that the local services are configured correctly for self-balancing, click **Status** **IP Networks** **Local Self-Balanced Services**
- To review the services for all self-balanced members, click **Status** **Other Networks** **Self-Balanced Service Status**

### What to do next

Repeat for all members (interfaces) of the standby group. All standby settings, except priority, must be the same.

## Removing an Ethernet interface from the network

The administrative state of an Ethernet interface can be changed from **enabled** to **disabled** while Ethernet cables are still physically connected to the appliance. Use this method to remove the appliance from the network without physically removing network cables.

## Initiating a packet-capture session

You can initiate a packet-capture session on an Ethernet or VLAN interface. The data in a packet capture is saved in the pcap format. Use a utility, such as **tcpdump** or **ethereal**, to interpret the file.

**Note:** You can only initiate a packet capture in the default domain.



## Comments

Optional: Enter a descriptive summary.

## ICMP Disable

Populate the list with one or more control message types. The appliance will not generate messages that are not in the list.

## ECN Disable

Disable the generation of explicit congestion notification (ECN) TCP sessions. For details see RFC 3183. By default, this TCP option is enabled.

## Destination Based Routing

Set to control the way that the DataPower appliance determines the route to return responses (the outbound packet) to the originating client (destination of the outbound packet).

- If enabled, interface selection is based on the best path to the client, regardless of the receiving interface or the service. Best path is determined by static routes that are bound to the available interfaces. Destination-based routing is for backward compatibility only. Enable destination-based routing only if an upgrade disables existing connectivity.
- If disabled, interface selection is based on the interface that is bound to the address of the service that generated the response. If the service is bound to a single address, responses are routed using the interface that is assigned to that address. If the service is bound to more than one address (a configuration of 0.0.0.0), responses are routed using the interface that received the original client request (not the interface that is bound to the service that generated the response).

## Relaxed Interface Isolation

Set to relax isolation of network interfaces. As a security policy, the interface that receives the network packet must also be configured with the IP address that is the destination address of the packet. Enabling this option relaxes that restriction so that the packet is allowed if the interface it arrives on contains an IP address in the same subnet as the destination address of the packet. Whether the interface that receives a packet is used for the response depends on the behavior that is established with **Destination Based Routing**. By default, if the request is addressed to 10.10.1.2 but received on 10.10.1.3 (which relaxed interface isolation allows), the reply uses interface 10.10.1.2. The requesting client, therefore, receives an answer with a source IP address that matches the address of the destination of the request.

## Never Enforce Interface Isolation

Set to turn on or turn off enforced interface isolation. If enabled, any interface that is bound to the destination service can receive the packet.

## TCP Retries

Specify the maximum number of times to retry a TCP SYN, in the case when no TCP acknowledgement is received in response.

## ARP Retries

Specify the maximum number of times to retry a failed ARP.

## ARP Retry Interval

Specify the time to wait before retrying failed ARP.

### **TCP Segmentation Offload on Ethernet**

Determines whether the Ethernet device drivers and chips are allowed to perform TCP Segmentation Offload. Disable this option only if customer support diagnosed that you are encountering this problem. After re-enabling TCP Segmentation Offload, restart the appliance for the change to take effect.

- If enabled, enables the TCP Segmentation Offload feature of all Ethernet device drivers and chips.
- If disabled, disables the TCP Segmentation Offload feature of all Ethernet device drivers and chips that have this feature and support disabling it.

### **Ignore packets with a source address that the interface cannot route**

Determines whether incoming packets with a source address that cannot be routed by that interface are accepted and processed. Enabling this option ignores such packets, which effectively disables source routing.

- If enabled, ignores incoming packets with a source address that cannot be routed by that interface.
- If disabled, accepts and processes incoming packets with a source address that cannot be routed by that interface.

### **Enable TCP Window Scaling**

Determines whether to enable TCP window scaling which allows negotiation of window sizes greater than 64 KB. Disabling this option might help workaround TCP systems that do not understand or that misinterpret window scaling.

- If enabled, enables TCP window scaling.
- If disabled, disables TCP window scaling.

3. Click **Apply** to save the changes to the running configuration.

4. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## **DNS Settings**

The appliance maintains a domain name table that enables the use of non-fully qualified domain names (host names) in lieu of IP addresses. The appliance attempts to resolve a host name with any domain in the domain name table. The host name is resolved by the initial match.

### **DNS hosts cache**

The results obtained in the response to DNS resolution requests are cached by the appliance to improve performance. In the case where a name server responds with an IP address for a particular host name, the time to live (TTL) value used to maintain this entry in the DNS cache is the TTL value specified by the name server in the DNS response, or 10 seconds, whichever is greater.

In the case where a DNS response indicates that the host name provided in the request did not have an associated IP address, the appliance caches the negative result for 30 seconds.

### **Load balancing algorithm**

The load balancing algorithm for DNS servers specifies the order that the appliance queries the DNS servers when resolving host names. There are two available algorithms:

- Round Robin
- First Alive

The round robin algorithm maintains a list of servers and forwards a new connection to the next server on the list.

The first alive algorithm uses the concept of a primary server and one or more backup servers. When the primary server is healthy, all connections are forwarded to this server. When the primary server is quarantined or unhealthy, connections are forwarded to backup servers. The primary server is the first server in the members list.

### **Scenario: DNS lookup procedure used with the first alive load balancing algorithm**

When you use first alive for the load balancing algorithm, adjust the behavior of the DNS lookup by specifying the following properties in the DNS settings:

- The name servers, up to a maximum of three
- The global retries property to specify the maximum number of times that the appliance will retry sending a query to the list of name servers before returning an error.
- The global timeout property to specify the number of seconds the resolver waits for a response from a remote DNS server before retrying the query via a different DNS server

The following scenario explains how these properties are used when the appliance resolves a given address, for example `www.example.com`. Initially, the timeout value used is the global timeout property.

1. The appliance sends a UDP datagram to the primary name server and waits up to the timeout value in order to receive a response.
2. If a response is received, it is processed, and the result is returned to the caller.
3. If the primary server fails to respond within the timeout, the appliance sends a UDP datagram to the secondary name server (if specified), and waits up to the timeout value to receive a response.
4. If a response is received, it is processed, and the result is returned to the caller.
5. If the secondary name server does not respond within the timeout, the appliance sends a UDP datagram to the tertiary name server (if specified), and waits up to the timeout value to receive a response.
6. If a response is received, it is processed, and the result is returned to the caller.
7. If no response is received from the tertiary server within the timeout value, the number of times that the list of DNS servers has been traversed is compared to the global retries.
  - a. If the specified number of retries has been reached, an error is returned to the caller and the attempt to resolve the address ends.
  - b. If the number of global retries has not been reached, the timeout value is incrementally adjusted depending on the number of name servers, the global timeout, and the number of times that the list of name servers has been tried.
  - c. The appliance continues the attempts to resolve the address starting with step 1 but using newly calculated timeout value.

UDP will be used as the transport protocol unless the appliance detects that the size of the datagram to send to a name server exceeds the maximum size of a UDP packet (64 KB), in which case TCP will be used instead. In the case where the

response from a name server is truncated, the request is retried using TCP. This retry is not counted against the specified number of retries.

## Configuring the DNS service

To configure the DNS service:

1. Click **Network Interface DNS Settings**.
2. On the **Main** tab, enable the DNS service and provide the basic settings.
3. On the **Search Domains** tab, define the domains to search for a match when a partial host name is submitted to the DNS service. Use the directional arrows to define the desired order of the search domains.
4. On the **DNS Servers** tab, define the list of DNS servers to contact to locate the DNS server to use for DNS name resolution. Use the directional arrows to define the desired order of DNS servers.
5. On the **Static Hosts** tab, define the list of host-address maps for static hosts.
6. Click **Apply** to save the changes to the running configuration.
7. Optional: Click **Save Config** to save the changes to the startup configuration.

For information about properties, see the online help.

## Flushing the DNS hosts cache

The appliances maintains a cache of DNS hosts. To flush the cache, click **Flush DNS Cache**.

This action is available on the following WebGUI screens:

- On the object page for DNS Settings (**Network Interface DNS Settings**)
- On the status page for DNS Cached Hosts (**Status IP-Network DNS Cached Hosts**)

---

## Host Alias

This feature allows any service that binds to a particular IP address to bind to a local host alias, rather than a specific address. For example, an XSL Proxy could be configured (bound) to the local IP address 10.10.1.1 (which in turn was assigned to one of the Ethernet interfaces that is configured on the DataPower appliance). Using the local host alias feature, you could bind the XSL Proxy to an alias name, such as proxy1. The host alias, in turn, is bound to a valid local IP address, such as 10.10.1.1.

Local host aliases can be useful when exporting configurations to other machines; for example, a staging appliance on subnet 10 to a production appliance on subnet 135. The exported configuration uses a local host alias that can be defined on the appliance where the configuration is being imported. However, the local host alias on the appliance where the configuration is being imported can bind to a different local IP address. No IP address change is required during migration.

## Working with local host aliases

**Note:** Changing the IP address that is assigned to an alias will cause all services that use the alias to rebind to the new address.

Deleting an alias brings down the operational state of all services that use the alias.

When created, local host aliases can be used in place of IP addresses for many services. The following services can use host aliases:

- XML Firewall service
- XSL Proxy service
- HTTP service
- TCP Proxy service
- SSL Proxy service
- XSL Coprocessor service

**Note:** Although the **Select Alias** button is on the Log Targets page, any host alias resolves to local IP address 0. Specify IP addresses instead.

For example, to use an alias perform the following steps:

1. Select **Objects Services New XSL Proxy**.
2. Click **Select Alias** to assign a host alias for the local IP address instead of the actual IP address of an Ethernet interface.
3. Click **Apply** to set the appliance address to the selected alias.

After a service is set to use an alias, the exported configuration identifies the alias in the exported configuration file. You can change the real IP address of the service by editing the alias to use a different IP address.

## Migrating configuration data

Implementing the local host alias feature for migration of configuration data requires the following steps:

1. Use the Host Alias screen to establish aliases
2. Set the configuration of each service (such as an XML Firewall or XSL Proxy) to use the host aliases.

Select **Network Interface Host Alias** to display the Host Alias catalog.

Click **Add** to display the Host Alias Configuration screen that you use to create a new host alias.

**Name** Specify the alias name. This name cannot begin with the reserved letters “eth” or “mgt”.

**Administrative State**

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

**Comments** Optional: Enter a descriptive summary.

**IP Address** Specify a local IP address.

**Note:** Select **Status Ethernet Interfaces** to view a list of all configured interfaces and IP addresses.

Click **Apply** to save the changes to the running configuration.

Optional: Click **Save Config** to save the changes to the startup configuration.

You can verify that new aliases were applied by selecting **Status** **DNS Static Hosts**.

---

## Managing NTP Servers

You can use the WebGUI to identify NTP (Network Time Protocol) servers. After at least one NTP server is identified, the appliance acts as a Simple Network Time Protocol (SNTP) client as described in RFC 2030. The time that is retrieved from this server can be different from the time that is displayed on the WebGUI due to the Time Settings on the local appliance. Refer to “Managing the time on the appliance.”

By default, the appliance issues requests to the first NTP server in the list. If this server is not available, the appliance attempts to contact the next server in the list.

To manage NTP servers, use the following procedure:

1. Select **Network** **Interface** **NTP Service** to display the NTP Service Configuration screen.
2. Provide the following inputs:

### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

### Comments

Optional: Enter a descriptive summary.

### NTP Server

Specify the host name or IP address of an NTP server.

Click **Add** to add this server to the list of available servers. Servers are contacted in the listed order.

### Refresh Interval

Specify the interval (in seconds) between the time-of-day requests that are generated by the appliance when acting as an SNTP client. The default is 900.

3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Managing the time on the appliance

The time on the appliance consists of the following specifications:

- Setting the local time and date
- Setting the time zone

The date and time settings with the setting for the time zone determine the displayed time. The time zone setting allows the administrator to set a time zone and any daylight savings time adjustments.

## Setting the local time and date

To set the local time and date, use the following procedure:

1. Select **Administration** **Main** **System Control** to display the System Control panel.

2. Locate Set Time and Date section.
  - a. In the **Date** field, specify the date in *yyyy-mm-dd* format.
  - b. In the **Time** field, specify the time in *hh:mm:ss* format.
  - c. Click **Set Time and Date** to display a confirmation window.
3. Click **Confirm**.
4. Click **Close**.

## Setting the local time zone

The time zone for the local time affects the time displayed by the local appliance. The appliance clock runs on Zulu time. If daylight savings time applies to the selected time zone, the appliance adjusts the displayed time when a daylight savings time boundary is crossed.

To set the local time, use the following procedure:

1. Select **Administration** **Device** **Time Settings** to display the Time Settings Configuration screen.
2. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
3. From the **Local Time Zone** list, select the time zone.
4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

## Creating a custom time zone

To create a custom time zone, use the following procedure:

1. Select **Administration** **Device** **Time Settings** to display the Time Settings Configuration screen.
2. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
3. From the **Local Time Zone** list, select **Custom (user defined)**.
4. Provide the following information:

**Name** A name for this custom time zone, which is appended to the time. Specify up to 6 characters. For example, if Name is set to **PKD**, the time appears as **Fri Jan 14 04:32:10 2005 PKD**

### Direction from UTC

Select East (Asia is East of UTC) or West (North America is West of UTC).

### Hours from UTC

Specify an integer indicating the hour offset from UTC.

### Minutes from UTC

Specify an integer indicating the minute offset from UTC.

### Daylight Savings Time (DST) Offset

Specify an integer that indicates the offset to be implemented when Daylight Savings Time is in effect. This value is 0 by default.



**DST Name**

A symbolic name for daylight savings time. Specify up to 6 characters. This name will be appended to the time display when daylight savings time applies.

**DST Start Month**

Select a month to indicate when DST starts.

**DST Start Week**

Specify an integer (such as 1 to indicate the first week of the month) to indicate when DST starts.

**DST Start Day**

Select a day to indicate when DST starts.

**DST Start Hours**

Specify an integer between 0 and 23 to indicate when DST starts.

**DST Start Minutes**

Specify an integer between 0 and 59 to indicate when DST starts.

**DST Stop Month**

Select a month to indicate when DST stops.

**DST Stop Week**

Specify an integer (such as 1 to indicate the first week of the month) to indicate when DST stops.

**DST Stop Day**

Select a day to indicate when DST stops.

**DST Stop Hours**

Specify an integer between 0 and 23 to indicate when DST stops.

**DST Stop Minutes**

Specify an integer between 0 and 59 to indicate when DST stops.

---

## Selecting the reboot configuration

To select a firmware image to load the next time the appliance reboots, use the following procedure:

1. Select **Administration** **Main** **System Control** to display the System Control panel.
2. Locate the **Select Configuration** section.
3. Select a configuration file. If the file is not in the list, click **Upload** to upload the file to the appliance.
4. Click **Select Configuration**.

The selected configuration file will be used the next time the appliance is rebooted.

---

## Configuring throttle settings

The appliance monitors its memory usage, temporary file space usage, and XML Names usage. The appliance reacts to low conditions by refusing to accept new connections. If the refusal to accept new connections does not free sufficient resources after a certain duration, the appliance responds by restarting itself.

This process, referred to as throttling, works as follows:

- When the number of available XML Names falls below the *XML Names threshold* (a measure of free XML Names expressed as a percentage of the total XML



Names), the appliance writes an alert to the log. This message indicates that the appliance detected a shortage of free XML Names. When you receive this alert, the percentage of available XML Names is below the defined threshold. After you receive this alert, schedule a reload as soon as possible to prevent an unscheduled reboot. If the available XML Names is less than 5% available, the appliance reloads. For xg3 and xg4ng hardware acceleration an attempt to free XML Names is attempted prior to reaching the warn level.

- When free memory or file space falls below the *throttle-threshold* (a measure of free memory or file space expressed as a percentage of total memory), the appliance refuses to accept new connections. By default, the throttle-threshold is set to 20 (20% of total memory or file space).
- If the amount of free memory or file space does not rise above the throttle-threshold in the specified timeout (expressed in seconds), the appliance restarts. By default, the timeout is set to 30 (seconds).
- If free memory or file space falls below the *kill-threshold* (also a measure of free memory or file space expressed as a percentage of total memory or file space), the appliance restarts immediately. By default, the kill-threshold is set to 5 (5% of total memory or file space).
- If free memory falls below the throttle-threshold and the backlog is configured, the appliance routes a configurable number of connection requests to the backlog queue. When a request is routed to the backlog queue, the configurable backlog-time begins for that request. The appliance delays processing requests in the backlog queue until sufficient memory is free or until the configured backlog-time for a request elapses. When sufficient memory is free, the appliance processes all requests in the backlog queue. If the backlog-time for a request elapses, the appliance rejects that request. If the backlog queue reaches the configured backlog-size, new requests replace previously received requests. If backlog-size is set to 0, no requests are routed to the backlog queue.  
A request is immediately rejected if the appliance does not allocate sufficient resources to route the request to the backlog queue. If such an event occurs, and the request arrives over a new connection, an `ifrejectconn` error is logged. If the request arrives over an existing TCP connection, an `fsphreject` error is logged.

To enable or disable throttling and to customize configuration properties, use the following procedure:

1. Select **Administration** **Device** **Throttle Settings** to display the Throttle Settings Configuration screen.
2. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. Specify the throttle-threshold for available memory in the **Memory Throttle At** field. This threshold is the point at which the appliance stops accepting new connections. Use an integer in the range 0 through 100. A value of 0 disables throttling. The default is 20.
5. Specify the kill-threshold of minimal available memory in the **Memory Terminate At** field. This threshold is the point at which the appliance restarts. Use an integer in the range 0 through 100. This integer must be less than the throttle-threshold. The default is 5.
6. Specify the throttle-threshold for available temporary space in the **Temp File Space Throttle At** field. This threshold is the point at which the appliance

stops accepting new connections. Use an integer in the range 0 through 100. A value of 0 disables throttling. The default is 0.

7. Specify the kill-threshold of minimal available temporary space in the **Temp File Space Terminate At** field. This threshold is the point at which the appliance restarts. Use an integer in the range 0 through 100. This integer must be less than the throttle-threshold. The default is 5.
8. Specify the threshold for available XML Names in the **XML Names Warn At** field. This threshold is the point at which the appliance writes an alert to the log about a shortage of XML Names. Use an integer in the range 5 through 65. The default is 10.
9. Specify the amount of time that the appliance waits to restart after reaching a defined threshold in the **Timeout** field. The default is 30 seconds.
10. Set **Status Log** to control the collection of throttle log messages. The default is **off**.
11. If **on**, select the priority of the message from the **Log Level** list. The priority is the criticality of the periodic status log. The default is **debug**.
12. Set **Environmental Monitor** to control the collection of environment log messages about fan speed and about power supply status. The default is **on**.
13. In the **Backlog Size** field, specify the number of connection requests that the appliance routes to the backlog queue. Use a value of 0 - 500. The default is 0.
14. In the **Backlog Timeout** field, specify the time (in seconds) that requests remain in the backlog queue. Use a value that is less than the timeout value of your browser. The default is 30.
15. Click **Apply** to save the changes to the running configuration.
16. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Shutting down the appliance

To shut down the DataPower appliance, use the following procedure:

1. Select **Administration Main System Control** to display the System Control panel.
2. Locate the **Shutdown** section.
3. Use the **Mode** list to select the shut down type.

### Reboot System

Shuts down the appliance and restarts the appliance. Temporary files are lost.

### Reload Firmware

Restarts the appliance without a reboot. Temporary files are not lost.

### Halt System

Shuts down the appliance.

4. In the **Delay** field, specify the amount of time (in seconds) to wait before starting the shut down procedure. Valid value is an integer in the range of 0 through 65535. The default is 1 second. A value of 0 denotes immediate shut down.
5. Click **Shutdown** to initiate the shut down procedure.

---

## Controlling the locate LED (Type 9235)

Type 9235 appliances have a locate LED light that the DataPower firmware can activate and deactivate. The locate LED is on the front of the appliance.

- When activated, the locate LED light is illuminated in blue.
- When deactivated, the locate LED light is not illuminated.

Only administrators in the default domain with the appropriate permissions can control the locate LED.

### Activating the locate LED

To activate the locate LED, use the following procedure:

1. Select **Administration Main System Control** to display the System Control panel.
2. Locate the **Control Locate LED** section.
3. Click **on**.
4. Click **Control Locate LED**.
5. Follow the prompts.

### Deactivating the locate LED

To deactivate the locate LED, use the following procedure:

1. Select **Administration Main System Control** to display the System Control panel.
2. Locate the **Control Locate LED** section.
3. Click **off**.
4. Click **Control Locate LED**.
5. Follow the prompts.

---

## Generating an appliance certificate

To generate a certificate for the appliance, which can be a self-signed certificate, use the following procedure:

1. Select **Administration Main System Control** to display the System Control panel.
2. Locate the **Generate Device Certificate** section.
  - a. In the **Common Name (CN)** field, specify the common name for the appliance.
  - b. For **Generate Self-Signed Certificate**, select **on** (default) to generate a self-signed certificate; otherwise, select **off**.
  - c. Click **Generate Device Certificate**.

---

## Appliance settings

The DataPower appliance uses system settings for the following purposes:

- Define appliance-specific information, such as contact information, location, and name
- Update serial number after a replacement
- Enable interface for custom messages display and custom command line prompts

- Reserve disk space for the audit log
- Define information about the hardware for use by the SNMP system table, such as serial number, and model type

## Defining appliance-specific information

You might want to define the information about the appliance to distinguish one from another when problems occurs. Although this information is optional. This appliance-specific information will be beneficial or necessary in the following situations:

- A problem occurs and you need to contact a person or group to resolve. You can identify contact information in any manner. For example, you can specify names, phone numbers, e-mail address or group aliases, or any combination of these details.
- A problem occurs and you need to locate the appliance. You can identify the location in the any manner. For example, you can specify the position in the rack.
- The appliance needs to identify itself to a remote server to establish a connection or your business want to enable a custom command line prompt. If undefined, the system identifies itself as (unknown). Some servers accept this identifier and other do not. For example, some mail servers, need an identifier for the HELO exchange.

To define appliance-specific information:

1. Select **Administration** **Device** **System Settings**.
2. In the **Contact** field, enter the person responsible for managing this appliance by name, telephone number, e-mail address, or a combination of these details.
3. In the **System Identifier** field, enter the name of the appliance. Define an identifier that consists of only ASCII letters and number.
4. In the **Location** field, enter the location of the appliance.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

## Updating the serial number after a replacement

The original serial number of an appliance identifies the level of support defined with the appliance purchase. Without the original serial number, IBM cannot entitle the replacement for maintenance or warranty service. The serial number for the replacement appliance is the read-only **Serial Number** property.

To update the serial number after receiving a replacement:

1. Select **Administration** **Device** **System Settings**.
2. In the **Entitlement Number** field, enter the original serial number of the appliance.
3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

## Enabling customized interfaces

You can create an XML file that customizes the user interfaces. This XML file can define the following behaviors:

- Custom messages to display in the WebGUI and from the command line
- The custom prompt for the command line

The file must reside in the local: or store: directory on the appliance. The file cannot reside on a mounted file system, such as iSCSI. After creating this file, validate that the file is conformant with the `dp-user-interface.xsd` schema.

For information about creating this file, refer to “User interface customization,” on page 229.

To enable customized interfaces:

1. Select **Administration** **Device** **System Settings**.
2. In the **Custom User Interface File** fields, specify the location of the file.
3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

## Reserving space for the audit log

The reserve space is the amount of disk space to reserve to prevent the loss of audit events in case of a full disk. The value must be at least four kilobytes less than the total amount of free space that is currently available on the file system. The value of 0 disables the reserve function.

If the appliance is forced to release the audit reserve:

- All data services will be forced into an operational down state and cease to process traffic.
- All administrative services, such as the WebGUI, Telnet, and so forth, will continue to work.

When the appliance forces the release, the log will contain a message that states that the disk space for audit events is low.

Before restoring the appliance to service, a privileged administrator needs to free up disk space. When there is enough available disk space for normal operations, the administration can restart the appliance, which will resume the processing of traffic.

To reserve disk space to record events in the audit log:

1. Select **Administration** **Device** **System Settings**.
2. In the **Audit Reserve Space** field, enter the amount of disk space in kilobytes to reserve.
3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

## Viewing hardware information

Information about the hardware is part of the SNMP system table. The settings that define this information is read-only and cannot be modified. The following properties are read-only:

- **Administrative State**
- **Product OID**
- **Description**
- **Serial Number**
- **Product ID**
- **Services**
- **Product Mode**

To view this information, select **Administration** **Device** **System Settings**.

---

## Configuring NFS Settings

### NFS Client Settings

Specify global NFS client properties for either dynamic mounts or static mounts.

### NFS Dynamic Mounts

Enable and disable dynamic NFS mounted directories. Dynamic mounts are used for unscheduled retrieval of URLs.

### NFS Static Mounts

Enable and disable static NFS mounted directories. Static mounts are used for logging to NFS servers and for responses from an FTP Server Front Side Handler.

## NFS Client Settings

Before establishing NFS static or dynamic mount points, you must set global NFS client properties as follows.

Select **Objects** **Network** **NFS Client Settings** to display the NFS Client Settings screen.

1. Provide the following inputs:

#### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

#### Comments

Optional: Enter a descriptive summary.

#### Mount Refresh Time

Specify the frequency of mount re-validation; the property defaults to a value of 10 seconds.

#### Kerberos Keytab

Specify the keytab to use for Kerberos 5 authentication or create a new Kerberos Keytab. For information, refer to *Understanding SPNEGO*.

2. Click **Apply** to save the changes to the running configuration.
3. Optional: Click **Save Config** to save the changes to the startup configuration.

## NFS Dynamic Mounts

To create or edit an **NFS Dynamic Mount** object, which supports unscheduled URL retrieval and remains active only until the expiration of an inactivity timer, follow this procedure:

1. Select **Objects** **Network** **NFS Dynamic Mounts** to display the NFS Dynamic Mounts Configuration screen.
2. Provide the following values:

#### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

### Comments

Optional: Enter a descriptive summary.

### NFS Version

Specify the preferred NFS protocol version for mount. If the Version is 3, but the server only implements Version 2, the client will fall back to Version 2. If the Version is 4, there is no fallback, since the remote export paths are not the same. The default is 3.

After specifying this value, the screen refreshes.

### Transport Protocol

For NFS version 2 or version 3, select the transport protocol to use when initiating the mount. If TCP is selected and it is not available on the NFS server, UDP will be used instead.

For NFS version 4, this property is ignored. NFS version 4 only supports TCP.

### Authentication Protocol

When NFS Version is 4, select the authentication protocol.

#### AUTH\_SYS

(Default) Indicate the original NFS scheme.

**krb5** Indicate the authentication version to use based on the Kerberos Credentials stored on the appliance.

**krb5i** Indicate the authentication version to use based on the Kerberos Credentials stored on the appliance, and includes a secure hash to protect the NFS data from being changed by the network.

**krb5p** Indicate the authentication version to use based on the Kerberos Credentials stored on the appliance, includes a secure hash to protect the NFS data from being changed by the network, and also includes data encryption so that the data cannot be read or changed by the network.

### Local IP Address

When NFS Version is 4, identify the local appliance addresses monitored by this NFS server for incoming requests. Retain the default value (0.0.0.0) if you want this server to monitor all active (provisioned) interfaces.

You can use a host alias instead of a local IP address. Click **Select Alias** to choose a local host alias. Refer to "Host Alias" on page 84 for more information.

### Read-Only

Specify the mount-specific file access privileges.

**on** Specify read-only file access.

**off** (Default) Specify read/write file access.

### Read Size

Specify an integer determining the size, in bytes, of file reads. The default is 4096. Use a smaller value if this size proves difficult for the server to maintain.



**Write Size**

Specify an integer determining the size, in bytes, of file writes. The default is 4096. Use a smaller value if this size proves difficult for the server to maintain.

**Retransmission Timeout**

Specify an integer to determine the retransmission timeout, in tenths of seconds. Use a value in the range of 1 through 600. The default is 7. If the appliance cannot successfully complete an operation after 0.7 seconds (assuming default value), the retransmission fails.

**Maximum Retransmissions**

Specify an integer to determine the number of times a retransmission will be attempted before the operation fails completely. Use an integer in the range of 1 through 60. The default is 3. After three retransmissions (assuming default value), the operation is deemed unsuccessful.

**Inactivity Timeout**

Specify the idle time, in seconds, that triggers tear down of the dynamic mount. The default is 900.

**Mount Timeout**

Specify the maximum time, in seconds, that the appliance attempts to establish a dynamic mount. The default is 30.

3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

**Passing parameters to files**

It is possible to employ parameters in the `dpnfs:` syntax. The following example includes parameters:

```
dpnfs: //fred/test.xml?a=b&c=d
```

**Note:** When parameters are used in the URL syntax, the appliance will first attempt to open a file with a name that includes the parameter specifications. If that fails, the appliance will then attempt to open the file using the name specified prior to the `?` in the URL.

These parameters are passed to the file that is being opened. Style sheets, for example, can then use these parameters.

## NFS Static Mounts

To create or edit an **NFS Static Mount** object, which is mounted and maintained as long as its resident domain is up, follow this procedure:

1. Select **Objects** **Network** **NFS Static Mounts** to display the NFS Static Mounts catalog.
2. To edit an existing NFS Static Mount object, click the name of the object. To create a new NFS Static Mount object, click **Add** to display the NFS Static Mounts configuration (Main) screen.

**Name** Specify a unique name for this NFS Static Mount object. This name is used in the `dpnfs:` syntax to designate the mounted directory. For example, if this name is `server1dir`, then files contained in this mount point can be accessed using a syntax such as `dpnfs: //server1dir/subdirectory/filename.ext`.



### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

### Comments

Optional: Enter a descriptive summary.

### Remote NFS Export

Specify the URL of the remote exported mount point in the form *host:/path*, where *host* is the DNS name of the host, and *path* is the path exported by the host to mount. This path must be exported on the host given or the static mount will fail.

### Local Filesystem Access

Enable or disable command line access to the mount point that is identified by the **Remote NFS Export** property.

- on** Indicates that the mount point is accessible from the command line. The NFS mount will be available through the command line under the *nfs-mount* folder, where *mount* is the name of the mount point.
- off** (Default) Indicates that the mount point is not accessible from the command line.

### NFS Version

Specify the preferred NFS protocol version for this mount. If the Version is 3, but the server only implements Version 2, the client will fall back to Version 2. If the Version is 4, there is no fallback, since the remote export paths are not the same. The default is 3.

After specifying this value, the screen refreshes.

### Transport Protocol

For NFS version 2 or version 3, select the transport protocol to use when initiating the mount. If TCP is selected and it is not available on the NFS server, UDP will be used instead.

For NFS version 4, this property is ignored. NFS version 4 only supports TCP.

### Authentication Protocol

When NFS Version is 4, select the authentication protocol.

#### AUTH\_SYS

(Default) Indicate the original NFS scheme.

**krb5** Indicate the authentication version to use is based on the Kerberos Credentials that are stored on the appliance.

**krb5i** Indicate the authentication version to use is based on the Kerberos Credentials that are stored on the appliance and includes a secure hash to protect the NFS data from being changed by the network.

**krb5p** Indicate the authentication version to use is based on the Kerberos Credentials that are stored on the appliance, includes a secure hash to protect the NFS data from being changed by the network, and includes data encryption so that the data cannot be read or changed by the network.

### Local IP Address

When NFS version 4, identify the local appliance addresses monitored by this NFS server for incoming requests. Retain the default value (0.0.0.0) if you want this server to monitor all active (provisioned) interfaces.

You can use a host alias instead of a local IP address. Click **Select Alias** to choose a local host alias. Refer to “Host Alias” on page 84 for more information.

### Read-Only

Specify the mount-specific file access privileges.

**on** Indicates read-only file access.

**off** (Default) Indicates read-write file access.

When mounting the same NFS version 4 mount point in different domains, the first mount sets file access privileges. For example, if `domain-A` mounts `host: /foo` as read-only access and then `domain-B` mounts `host: /foo` as read-write access, both mounts are read-only.

### Read Size

Specify the size of a read operation in bytes. The default is 4096. Specify a smaller number if this size proves difficult for the server to maintain.

### Write Size

Specify the size of a write operation in bytes. The default is 4096. Specify a smaller number if this size proves difficult for the server to maintain.

### Retransmission Timeout

Specify an integer to determine the retransmission timeout, in tenths of seconds. Use a value in the range of 1 through 600. The default is 7. If the appliance cannot successfully complete an operation after 0.7 seconds (assuming default value), the retransmission fails.

### Maximum Retransmissions

Specify an integer to determine the number of times a retransmission will be attempted before the operation fails completely. Use an integer in the range of 1 through 60. The default is 3. After three retransmissions (assuming default value), the operation is deemed unsuccessful.

3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Using the iSCSI protocol (Type 9235)

Type 9235 appliances support any of the available Ethernet interfaces for iSCSI network connections. To use iSCSI, configure an iSCSI Volume object. This object access a volume (LUN) on the remote iSCSI server.

For information about Ethernet interfaces, refer to “Configuring Ethernet interfaces” on page 76.

The configuration of the iSCSI Volume object, involves the configuration of the following objects:

### iSCSI Initiator

The Initiator establishes communications between the appliance and the remote iSCSI server. The Initiator is enabled by default with a default iSCSI name.

### iSCSI Challenge Handshake Authentication Protocol (CHAP)

Optional: The CHAP is the handshake that authenticates the credentials on the appliance with the remote iSCSI server.

### iSCSI Target

The target defines the connection information to the remote iSCSI server.

The appliance, through the iSCSI Initiator, can use the iSCSI protocol to communicate with the remote iSCSI server. The iSCSI Initiator negotiates through the iSCSI CHAP to establish connectivity. When connected, an iSCSI session is started.

After configuring and initializing an iSCSI volume, you can manage files on the iSCSI volume as if they were local. During startup, the volume is mounted under the local: and logstore: directories in each application domain.

## IQN and EUI formats

The iSCSI Initiator is defined on the DataPower appliance by an iSCSI qualified name (IQN).

Each iSCSI target is defined on the DataPower appliance by an IQN or by an IEEE Extended Unique Identifier (EUI).

**IQN** Specifies a worldwide unique and valid name for the iSCSI Initiator or iSCSI target instances. The name, based on IETF RFC 3270, can be between 1 and 244 characters in length. Sample formats are `iqn.2001-04.com.example` or `iqn.2001-04.com.example:storage.disk2.sys1.xyz`.

**EUI** Specifies a worldwide unique and valid name for iSCSI target instances. The name, based on IETF RFC 3270, is a hexadecimal value that can be between 1 and 244 characters in length. A sample format is `eui.02004567A425678D`.

## Configuring and initializing an iSCSI volume

The LUN setting and its read-only or read-write setting on an iSCSI volume are disclosed to the iSCSI Initiator by the iSCSI target.

After configuring and initializing an iSCSI volume, you can access the remote iSCSI file system from the local: and logstore: directories in each application domain.

To access an iSCSI volume on a remote iSCSI server, use the following high-level procedure:

1. Configure the volume
2. Initialize the volume.

### Configuring an iSCSI volume

To configure the iSCSI volume:

1. Click **Administration** **Storage Devices** **iSCSI Volume**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.

4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. Set **Read-Only** to indicate whether the files on the volume have read-only access.
  - on** Sets the file system to read-only access.
  - off** (Default) Sets the file system to read-write access.
7. Specify the directory under which to make the files on the volume available in the **Directory** field.
8. Specify the logical unit number (LUN) in the **LUN** field. Use an integer in the range of 0 through 255.
9. Select the instance of the iSCSI Target object to which to bind the iSCSI volume from the **iSCSI Target** list. Refer to “Configuring an iSCSI Target object” on page 101 for more information.
10. Click **Apply** to save the changes to the running configuration.
11. Optional: Click **Save Config** to save the changes to the startup configuration.

### Initializing an iSCSI volume

Initializing the iSCSI volume allows it to be made active. The iSCSI volume must be disabled before it can be initialized.

To initialize the iSCSI volume:

1. Click **Objects** **Network Settings** **iSCSI Volume**.
2. Click the instance name.
3. Set **Administrative State** to **disabled**.
4. Click **Apply** to save the changes to the running configuration.
5. Click **Initialize File System**.
6. Follow the prompts to complete the initialization.
7. Set **Administrative State** to **enabled**.
8. Click **Apply** to save the changes to the running configuration.
9. Optional: Click **Save Config** to save the changes to the startup configuration.

### Repairing an iSCSI volume

You might need to repair the iSCSI volume if its contents were corrupted by an abnormal shutdown or other error. Before you can repair a volume, you must disable it. After repairing the volume, you must enable it.

To repair the iSCSI volume on the appliance:

1. Click **Objects** **Network Settings** **iSCSI Volume**.
2. Click the instance name to display the configuration pane.
3. Set **Administrative State** to **disabled**.
4. Click **Apply** to save the changes to the running configuration.
5. Click **Repair File System**.
6. Follow the prompts.
7. Set **Administrative State** to **enabled**.
8. Click **Apply** to save the changes to the running configuration.

- Optional: Click **Save Config** to save the changes to the startup configuration.

## Reference objects for iSCSI

The following reference objects are defined to use the iSCSI protocol:

- iSCSI Target
- iSCSI Initiator
- Optional: iSCSI CHAP

### Configuring an iSCSI Target object

The iSCSI target waits for SCSI commands. An iSCSI target cannot initiate an iSCSI session. The iSCSI target is a connection instance of a remote iSCSI target.

To configure an iSCSI target:

- Click **Objects** **Network Settings** **iSCSI Target**.
- Click **Add**.
- In the **Name** field, enter the name for the object.
- Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
- Optional: In the **Comments** field, enter a descriptive summary.
- Specify the IQN or EUI of the iSCSI Target on the remote iSCSI server in the **Target Name** field. Refer to “IQN and EUI formats” on page 99 for details.
- Specify the host name or IP address of the remote iSCSI server in the **Host** field.
- Specify the listening port on the remote iSCSI server in the **Port** field. The default is 3260.
- Optional: Select the CHAP instance to use for authentication from the **CHAP** list. Refer to “Configuring an iSCSI CHAP object” on page 102 for more information.
- Click **Apply** to save the changes to the running configuration.
- Optional: Click **Save Config** to save the changes to the startup configuration.

### Configuring an iSCSI Initiator object

The iSCSI Initiator is responsible for the management of iSCSI communications. The iSCSI Initiator initiates the iSCSI session between the DataPower appliance and the iSCSI target.

To configure the iSCSI Initiator:

- Click **Objects** **Network Settings** **iSCSI Initiator**.
- Optional: In the **Comments** field, enter a descriptive summary.
- Optional: Change the IQN in the **iSCSI Name** field. The IQN is already defined but not visible. To view this value, click **Status** **Other Network** **iSCSI Initiator Status**.
- Click **Apply** to save the changes to the running configuration.
- Optional: Click **Save Config** to save the changes to the startup configuration.

## Configuring an iSCSI CHAP object

The iSCSI Challenge Handshake Authentication Protocol (CHAP) optionally defines the credentials to use to authenticate the DataPower appliance with the remote iSCSI server. The CHAP presents credentials to the iSCSI target instances during startup.

To configure the iSCSI CHAP:

1. Click **Objects** **Network Settings** **iSCSI CHAP**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. Specify the user name for the CHAP in the **User Name** field.
7. Specify the password for this user in the **Password** field.
8. Specify the password again in the **Confirm Password** field.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Configuring SNMP Settings

The appliance supports SNMP versions 1, 2c, and 3. You can do anything with version 3 that you can do with version 1 or version 2c. With version 3, you can securely perform these operations in terms of encryption and authentication, but not in terms of inform requests.

The configuration of SNMP consists of the following procedures:

- Configuring global properties
- Configuring event subscriptions
- Configuring communities
- Configuring recipients
- Configuring contexts

As part of the configuration process, you can view enterprise MIBs.

### Configuring global properties

The global (or basic) SNMP properties define the generic properties for the local SNMP entity. The local SNMP entity monitors the defined address-port for incoming SNMP requests. Without a defined local address or the default value of 0.0.0.0, the local SNMP entity monitors all local IP addresses for incoming SNMP requests.

Additionally, you can configure an SNMP log that issues logging events in the form of SNMP traps or notifications. See “Configuring log categories” on page 168 for information about SNMP logs.

To configure global properties:

1. Click **Administration** **Access** **SNMP Settings**.

2. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. In the **Local IP Address** field, specify the IP address of the Ethernet interface. To use a host alias, click **Select Alias** to select an alias. See “Host Alias” on page 84 for more information.
5. In the **Local Port** field, specify the port of the Ethernet interface.
6. To implement version 3 user-based security or to implement version 3 notifications, use the **SNMPv3 Users** controls to compile a list of SNMP users. See “SNMP V3 users” on page 55 for more information.
  - a. From the **SNMPv3 Security Level** list, select the settings for authentication and privacy.
  - b. From the **SNMPv3 Access Level** list, select the access privilege for SNMP V3 users.
7. Click **Apply** to save the changes to the running configuration.
8. Optional: Click **Save Config** to save the changes to the startup configuration.

## Configuring subscriptions

To configure SNMP subscriptions that generate traps:

1. Click **Administration Access SNMP Settings**.
2. Click the **Trap Event Subscriptions** tab.
3. Define whether to use the set of DataPower-provided event subscriptions.
  - a. Use **Enable Default Event Subscriptions** to indicate whether to enable or disable the use of default event subscriptions. See “Default event subscriptions” on page 105 for information about these subscriptions.
  - b. When enabled, define events and the overall priority of the set.
    - 1) From the **Minimum Priority** list, select the minimum event priority.
    - 2) Use the **Event Subscriptions** controls to compile a list of events that generate traps.
4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

## Configuring communities

Many operational environments support only two SNMP communities:

- A public (read-only) community is restricted to SNMP **get** operations, which means that these communities can read but cannot change system values.
- A private (read-write) community has access to both SNMP **get** and **set** operations. These communities can read and change system values.

However, there is no limit to the number of communities that can be supported, nor is there any limit to the number of SNMP managers that can be contained in a specific community.

To identify remote SNMP managers or engines that are granted access to the appliance:

1. Click **Administration Access SNMP Settings**.
2. Click the **SNMP V1/V2c Communities** tab.



3. Click **Add**.
  - a. In the **Community** field, specify the SNMP community name. An SNMP community name (essentially a password) is included in the incoming SNMP message header.
  - b. From the **Associated Domain** list, select the application domain to which this community is granted access.
  - c. From the **Mode** list, select the domain-specific access privileges accorded to this community.
  - d. In the **Remote Host Address** field, specify the IP address of an SNMP manager that belongs to this community.
  - e. Click **Save**.
4. Repeat the previous step to add additional communities.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

## Configuring recipients

The SNMP agent or engine issues the following generic events that are referred to as notifications in SNMP version 3 and traps in earlier versions:

- authenticationFailure
- linkDown
- coldStart
- linkUp

To designate notification recipients:

1. Click **Administration Access SNMP Settings**.
2. Click the **Trap and Notification Targets** tab.
3. Click **Add**.
  - a. In the **Remote Host Address** field, specify the IP address of a recipient. The IP address must be unique for each recipient and is the notification target.
  - b. In the **Remote Port** field, specify the port that the remote SNMP manager (or engine) monitors for incoming traps.
  - c. In the **Community** field, specify the community name to access the remote SNMP manager. If issuing version 3 notifications, leave blank.
  - d. From the **Version** list, select the protocol version.
  - e. When the protocol version is 3: In the **Security Name** field, specify an SNMP version 3 user who is associated with the recipient.
  - f. From the **Security Level** list, select the authentication and privacy. Authentication and privacy are used to authenticate and encrypt notifications.
  - g. Click **Save**.
4. Repeat the previous step to designate additional recipients.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

## Configuring contexts

An SNMP version 3 context is defined in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, as a physical



or logical collection of management information accessible by an SNMP entity. In terms of the DataPower appliance, an SNMP context equates to an application domain.

To map application domains to SNMP contexts:

1. Click **Administration** **Access** **SNMP Settings**.
2. Click the **SNMPv3 Contexts** tab.
3. Click **Add**.
  - a. In the **Context Name** field, specify the context name. You can use the name of the mapped application domain as the context name.
  - b. From the **Application Domain** list, select the application domain to map to the context name.
  - c. Click **Save**.
4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

## Viewing MIBs

To view enterprise MIBs:

1. Click **Administration** **Access** **SNMP Settings**.
2. Click the **Enterprise MIBs** tab.
3. Click any listed MIB to view its details.

## Default event subscriptions

Some SNMP subscriptions are system defaults, and if you remove or alter these subscriptions they will, by default, reactivate after the next system restart. You can configure the subscription settings so that default event subscriptions are not used and thus not reactivated after restarting the system. Use the **Enable Default Event Subscriptions** option on the **Trap Event Subscriptions** tab of the **SNMP Settings** page to configure this behavior.

You can define an SNMP log target to define event subscriptions. If you define a log target then disable the **Enable Default Event Subscriptions** option. See “Configuring log categories” on page 168 for information about SNMP logs.

The following is a list of the default event subscriptions:

- 0x00030002 (Out of memory)
- 0x00230003 (Unable to allocate execution resources)
- 0x00330002 (Memory full)
- 0x00b30014 (Duplicate IP address)
- 0x00e30001 (NTP - Cannot Resolve Server Name)
- 0x00e40008 (NTP Timeout Error)
- 0x00f30008 (File is expired)
- 0x01530001 (Time zone config mismatch.)
- 0x01a2000e (Installed battery is nearing end of life.)
- 0x01a40001 (Throttling connections due to low memory)
- 0x01a40005 (Throttling connections due to low temporary file space)
- 0x01a40008 (Throttling connections due to low number of free ports)
- 0x01b10006 (Microcode load failed)
- 0x01b10009 (uncertified HSM firmware detected)

- 0x01b20002 (HSM is uninitialized)
- 0x01b20004 (HSM PED login failed)
- 0x01b20008 (HSM password login failed)
- 0x02220001 (Power supply failure.)
- 0x02220003 (Internal cooling fan has stopped.)
- 0x02240002 (Internal cooling fan has slowed)

**Notes:**

1. "Microcode load fail" is specific to HSM devices.
2. "File is expired" refers to the Crypto Certificate file.

---

## Sysplex Distributor Target Control Service

The Sysplex Distributor Target Control Service on the DataPower appliance establishes control connections with the z/OS® Sysplex Distributor that allow the z/OS Sysplex Distributor to intelligently distribute traffic across multiple DataPower appliances.

**Note:** The ability to use the Sysplex Distributor Target Control Service requires the Option for Application Optimization feature.

The Target Control Service performs the following actions:

- Listens to the z/OS Sysplex Distributor for details on the virtual IP address in which the z/OS Sysplex Distributor is interested.
- Reports the health of the DataPower appliance to the z/OS Sysplex Distributor.
- Sends the TCP state conditions of various TCP connections to the z/OS Sysplex Distributor so that the z/OS Sysplex Distributor has current TCP state information, for instance, whether connections are open or closed.

Multiple z/OS Sysplex Distributors can establish control connections to the single Sysplex Distributor Target Control Service on the DataPower appliance. When the Sysplex Distributor Target Control Service is disabled, existing z/OS Sysplex Distributor control connections are closed.

The Sysplex Distributor Target Control Service is not in the path of data requests. For example, when the z/OS Sysplex Distributor receives an HTTP request from a client, the data request is processed as follows:

1. The z/OS Sysplex Distributor sets up a TCP connection to the DataPower appliance and processes the request.
2. The DataPower appliance processes the request.
3. The response from the DataPower appliance goes directly back to client.

The response from the DataPower appliance does not go through the z/OS Sysplex Distributor.

### z/OS Sysplex Distributor takeover

With a backup z/OS Sysplex Distributor for redundancy, if the primary z/OS Sysplex Distributor is unavailable, planned or unplanned takeover occurs. The Sysplex Distributor Target Control Service handles both cases.

The takeover by the backup z/OS Sysplex Distributor from the primary one should result in connections successfully migrating to the backup. Established connections continue to flow in case of a planned takeover. When the queries

complete, the backup should detect that the TCP connections close and perform the clean up. There should be no failed connections.

## Creating a Sysplex Distributor Target Control Service

Create a Sysplex Distributor Target Control Service on the DataPower appliance to establish a control connection with the z/OS Sysplex Distributor. The z/OS Sysplex Distributor communicates with the Target Control Service on the DataPower appliance to set up a listener for the specified virtual IP address.

### About this task

The Sysplex Distributor Target Control Service is the only configuration object necessary for z/OS Sysplex Distributor support. The Sysplex Distributor Target Control Service is defined in the default domain and applies to both IPv4 and IPv6 control connections.

To create a Sysplex Distributor Target Control Service, use the following procedure:

### Procedure

1. Click **Objects** **ZOS Configurations** **Sysplex Distributor Target Control Service**.
2. Retain the default setting for **Admin State**. To place in an inactive administrative state, click **disabled**.
3. Optional: In the **Comments** field, enter a descriptive summary.
4. In the **Local IP Address** field, enter the address on which the Target Control Service listens. The default of 0.0.0.0 indicates that the service is active on all addresses. Click **Select Alias** to use an alias for this value.
5. Optional: In the **Port Number** field, change the port number on which the Target Control Service monitors.
6. Optional: From the **SSL Proxy** list, select the SSL proxy profile for a secured connection.
7. Click **Apply** to save the changes to the running configuration information.
8. Optional: Click **Save Config** to save the changes to the startup configuration.

### What to do next

The Sysplex Distributor administrator must configure the z/OS Sysplex Distributor with a set of DataPower appliances as endpoints. The following configuration parameters are required:

- DataPower appliances that are available to accept requests.
- Interested pairs (virtual IP address, listener).

At the end of the handshake on the control connection, the DataPower appliances should be fully configured to accept queries on the virtual IP addresses.

---

## Quiescence

You can quiesce a DataPower appliance to transition the operational state of the domains, services, and handlers to down in a controlled manner.

You can have finer grained control by applying quiescence at the following levels:

- Domains

- Services
- Protocol handlers

## Quiesce

The appliance quiesce operation performs the following actions:

- Waits for at most the specified time for transactions to complete
- Transitions protocol handlers to the **down** operational state
- Transitions services to the **down** operational state
- Transitions domains to the **down** operational state

When the default domain is quiesced, it does not change to the **down** operational state.

When the appliance is quiesced, the operational state of all application domains and all services, including those services in the default domain, is **down**. New services that are created in application domains remain **down** until the appliance is unquiesced. However, unlike in application domains, new services that are created in the default domain might take requests immediately.

The quiesce operation is hierarchical and uses parent-child relationships to determine all domains, services, and handlers to quiesce. First, the children are quiesced. The parent is quiesced last. For example, if you quiesce a service, all handlers associated with that service are quiesced. (This might include handlers that are used in other services.)

When you use the quiesce action, the quiesce operation completes, the state changes to “quiesced”, and a log notification is sent. The operational state changes to **down** for the children but this state does not indicate that the quiesce is complete. The **down** operational state prevents new requests from being processed. In most cases, the quiesced object becomes quiesced at the timeout period.

## Unquiesce

You can unquiesce a quiesced appliance, domain, service, or handler without restarting the appliance. When you request an unquiesce operation, the quiesced domains, services, and handlers are unquiesced as follows:

- Handlers transition to the **up** operational state
- Services transition to the **up** operational state
- Domains transition to the **up** operational state

The running configuration reflects any changes that were applied while the appliance was in the quiesced state.

Unquiescing a protocol handler does not bring the operational state of the handler to **up** if the enclosing service is quiesced. Likewise, unquiescing a service does not bring the operational state of the service to **up** if the domain is quiesced. Instead, use the unquiesce action at the same level that you used the quiesce action. For example, if you quiesce a service and consequently quiesce all of the protocol handlers used by that service, unquiesce the service to unquiesce the protocol handlers rather than unquiescing the handlers themselves.

When a domain is quiesced, if you add a new service or handler to that domain, the service or handler will not transition to the **up** operational state until the domain is unquiesced.

## Checking quiesce and unquiesce status

A quiesce might be done to perform configuration activities on the appliance with all traffic stopped. As opposed to setting the administration state of all domains to disabled, which can drop connections, quiescing an appliance causes domains, services, and handlers to wait for at most the specified time for transactions to complete. The following list provides the possible quiesce states:

- Quiescing
- Quiesced
- Unquiescing
- Error

When you quiesce the appliance or a domain, service, or handler, you can asynchronously view the progress of the quiesce using the following methods:

- View the domain quiesce state in the domain status in the default domain.
- Verify that the appliance quiesce is complete by checking that all domains are quiesced in the domain status.
- When the log level is set to notice, check for the log message that indicates the quiesce is complete.
- Add a log target to trap the quiesce complete message.
- Retrieve the status provider to get the quiesce state with `dp: get-status`.

## Quiescing the appliance

To quiesce the appliance:

1. Click **Administration** **Main** **System Control**.
2. Locate the **Quiesce** section.
3. Specify the **Timeout** in seconds.
4. Click **Quiesce**.
5. Click **Confirm**.
6. Click **Close**.

## Unquiescing the appliance

To unquiesce the appliance:

1. Click **Administration** **Main** **System Control**.
2. Locate the **Unquiesce** section.
3. Click **Unquiesce**.
4. Click **Confirm**.
5. Click **Close**.

Alternatively, restart the appliance. A restart will unquiesce domains, services, and handlers that are quiesced. The quiesce state does not persist across an appliance reboot.



---

## Chapter 11. Managing network access to the appliance

The DataPower appliance has the following administrative interfaces:

- The Web-based graphical user interface (WebGUI)
- The command line through a Telnet connection, an SSH connection, or the serial port or on a Blade server through the serial over LAN infrastructure or the KVM switch infrastructure of the BladeCenter; see the BladeCenter documentation for details on configuring the serial over LAN and the KVM.
- The SOAP-based XML management interface

Regardless of the administrative interface, properly authenticated and authorized users can access the entire range of configuration and status data.

By default, all remote interfaces are shut down (disabled). In this situation, the only way to enable them is through a serial connection or on a Blade server the KVM switch infrastructure of the BladeCenter.

---

### WebGUI access

The WebGUI must be enabled and available before you can perform any activity through the Web management interface. Access to the WebGUI should be enabled by the person who performed the initial installation and firmware setup of the DataPower appliance. Instructions for performing these tasks are in the model-specific *Installation Guide*.

### Modifying configuration for WebGUI access

Access to the appliance via the WebGUI is supported by a dedicated HTTP server that you configured during the initial firmware setup.

To modify access to the WebGUI:

1. Click **Network Management Web Management Service**.
2. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
3. In the **Local IP Address** field, enter the local IP address the appliance monitors for incoming WebGUI requests. To use a host alias instead of a local IP address, click **Select Alias** and choose the local host alias. See “Host Alias” on page 84 for more information.
4. Optional: In the **Local Port** field, change the port on which the appliance monitors for incoming WebGUI requests.
5. Optional: Click the ... button beside the **Access Control List** field to modify the configuration of the **web-mgmt** Access Control List. See “Access Control List” on page 185 for more information.
6. Optional: In the **Comments** field, enter a descriptive summary.
7. Optional: Set **Save Config Overwrite** to **off** to require a manual step to prevent overwriting a hand-edit startup configuration. The default is that

saving a configuration (**Save Config** button or **write memory** command) overwrites the startup configuration (config:///autoconfig.cfg) with a copy of the running configuration.

8. Optional: In the **Idle Timeout**, enter the period of inactivity after which the WebGUI closes the connection. To disable the timer, enter 0.
9. Optional: Change the default SSL and HTTP connections settings. For details, see “Changing security and connection settings.”
10. Click **Apply** to save the changes to the running configuration.
11. Optional: Click **Save Config** to save the changes to the startup configuration.

## Changing security and connection settings

By default, connections to the WebGUI use internal cryptographic material and the HTTP settings in the default user agent.

To change the default security and HTTP settings for accessing the WebGUI:

1. Click **Network Management Web Management Service**.
2. Click the **Advanced** tab.
3. Optional: From the **Custom SSL Proxy Profile** list, select the profile to secure the connection to the WebGUI.
  - To generate and assign a device-specific SSL proxy profile, see “Custom SSL proxy profile” on page 127.
  - To create and assign another SSL proxy profile, see “SSL Proxy Profile objects” on page 219.
4. Optional: From the **Custom User Agent** list, select the agent that defines the HTTP connection settings.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Command line access

You can access the command line in one the following ways:

- Direct connection through the serial port
- For Type 4195 models: Direct connection through the serial over LAN infrastructure
- For Type 4195 models: Direct connection through the KVM switch infrastructure of the BladeCenter
- Remote connection through the SSH service
- Remote connection through the Telnet service

In the most secure environments, all remote administrative interfaces are disabled. In these environments, all administration must be done by only those who have physical access to the appliance in the datacenter.

## Connecting to the serial port

The serial port is hard-wired to a command line administration shell. For a Blade, the connection uses the serial over LAN infrastructure.

To make the serial connection:

1. Use the null-modem cable or a USB-to-serial converter cable to connect the terminal or PC to the **SERIAL** connector on the appliance.



2. Ensure that the terminal or PC is configured for standard 9600 8N1 and no flow control operation. 8N1 is a notation for a serial configuration in asynchronous mode, where there are eight (8) data bits, no (N) parity bit, and one (1) stop bit.

When properly connected, the terminal or PC should prompt for credentials.

For more information about defining the initial setup through the serial port, see the model-specific *Installation Guide*.

## Connecting using serial over LAN (Type 4195)

On an Integration Blade XI50B the command line interface is available using serial over LAN.

Serial over LAN requires a subnet and underlying virtual local area network (VLAN) that is implemented by a LAN Switch I/O Module installed in I/O module Bay 1 of the BladeCenter chassis. The subnet and VLAN are entirely internal to each BladeCenter chassis and are not externally accessible.

To enable serial over LAN:

1. Restart the blade server and immediately give the blade server control of the BladeCenter unit shared keyboard, video, and mouse ports.
  - a. If you are managing the blade server by using the BladeCenter system console, press the KVM select button on the blade server.
  - b. If you are managing the blade server from a remote location, see the *IBM BladeCenter Management Module User's Guide* or *IBM BladeCenter Management Module Command-Line Interface Reference Guide* for information and instructions.
2. When the prompt Press <F1> Setup is displayed, press F1. If you have set an administrator password, you must type the administrator password to access the full Setup-utility menu. If you do not type the administrator password, a limited Setup-utility menu is available.
3. Select System Settings and then press Enter.
4. Select Devices and I/O Ports and then press Enter.
5. Select Console Redirection Settings and then press Enter.
6. From the Console Redirection Settings menu:
  - a. If you are using a serial breakout cable, set COM Port 1 to Enable; otherwise, set it to Disable.
  - b. Set COM Port 2 to Enable.
  - c. Set Remote Console to Enable.
  - d. Set Legacy Option ROM Display to COM Port 2.
  - e. Set the following COM2 Settings:
    - 1) Make sure that the Baud Rate is set to 115200.

**Note:** The settings for Data Bits, Parity, and Stop Bits are static and cannot be changed.

- 2) Set Terminal Emulation to ANSI (default) or VT100, depending on your system configuration.
- 3) Set Active After Boot to Enable.
- 4) Set Flow Control to Hardware.

7. Press **Esc** four times; then, press **Y**, when prompted, to save settings and restart the Blade server.

After the blade server has restarted, you can establish an SOL session to it using the advanced management module CLI.

More detailed information about configuring the serial over LAN connection can be found in the *IBM BladeCenter Serial Over LAN Setup Guide*. Prerequisite information can be found in the *IBM BladeCenter HS22 Type 7870 Installation and User's Guide*.

## SSH service

By default, the SSH service is disabled. When enabled, the SSH service binds to the defined local IP-address-port combination. Without an explicit local address, the SSH service attempts to bind to the management Ethernet interface (**mgmt**). If the management Ethernet interface is not defined, the SSH service binds to all configured interfaces.

Be sure to define an explicit IP address to isolate management traffic from application data traffic.

### Enabling SSH

To enable the SSH service:

1. Click **Network Management SSH Service**.
2. Set **Administrative State** to **enabled**.
3. In the **Local IP Address** field, enter the local IP address the appliance monitors for incoming SSH requests. To use a host alias instead of a local IP address, click **Select Alias** and choose the local host alias. See "Host Alias" on page 84 for more information.
4. Optional: In the **Local Port** field, change the port on which the appliance monitors for incoming SSH requests.
5. Optional: Click the ... button beside the **Access Control List** field to modify the configuration of the **ssh** Access Control List. See "Access Control List" on page 185 for more information.

Provide the following inputs:

#### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

#### Local IP Address

Optionally bind SSH to a specific active (provisioned) appliance interface.

Without an explicit address assignment, SSH, once enabled, first attempts to bind to the appliance management port. If the management port has not been previously configured, SSH binds to all configured appliance interfaces.

Click **Apply** to save the changes to the running configuration.

Optional: Click **Save Config** to save the changes to the startup configuration.

## SSH login

Although many servers use password authentication for SSH login, the DataPower appliance requires an interactive process to protect credentials during the SSL handshake. The DataPower appliance initiates a secure channel and provides for an encrypted login process.

As a side-effect of the initial connection (and depending on your SSH client), you might see the following extraneous prompt that you can bypass by pressing Enter:  
login as:

At this point, the screen shows a warning about unauthorized access and the prompt for the login credentials.

The follow screen shows this process.

```
login as:  
Unauthorized access prohibited.  
login:
```

## Enabling Telnet services

Telnet services is available for backward compatibility and are not recommended due to their unencrypted nature. To ensure an encrypted connection and verify the cryptographic authenticity of the server, SSH is a more secure choice.

To create and enable a Telnet service:

1. Click **Network Management Telnet Service**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. In the **Local IP Address** field, enter the local IP address the appliance monitors for incoming Telnet requests. To use a host alias instead of a local IP address, click **Select Alias** and choose the local host alias. See “Host Alias” on page 84 for more information.
6. In the **Local Port** field, enter the port the appliance monitors for incoming Telnet requests.
7. Optional: From the **Access Control List** list, select ACL that allows and denies access to the Telnet service. See “Access Control List” on page 185 for more information.
8. Click **Apply** to save the changes to the running configuration.
9. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## XML Management Interface

The DataPower appliance can be configured and managed completely through the XML Management Interface. When enabled, this interface allows administrators to send status and configuration requests to the DataPower appliance through a standard SOAP interface. The URL for this interface takes the following form:

`https://appliance_ip:port/service_uri`

For example:

`https://192.168.1.25:5550/service/mgmt/current`

This interface requires the HTTPS protocol for communication. By default, the interface acts as an SSL server, using the default keys that are installed in the appliance. These keys are the same keys that are used for the WebGUI and SSH interfaces.

## Services overview

The appliance supports a range of administrative services through the XML Management Interface. An overview of these services are as follows:

- Device Configuration and Management using SOAP XML requests and responses. The appliance offers an older version of this interface (v2004) and the current version.

### SOAP Management URI

Enables processing of messages that are received on any (\*) URI for older applications. One example would be an application that posts SOAP management requests to `"/`. By default, this service is enabled.

### SOAP Configuration Management

Enables support for SOAP Configuration Management. The URI for the SOAP Configuration Management is `/service/mgmt/current`. By default, this service is enabled.

### SOAP Configuration Management (v2004)

Enables support for legacy SOAP Management format. The URI for the SOAP Configuration Management is `/service/mgmt/2004`. By default, this service is enabled.

Refer to “SOAP interface” on page 118 for more information.

- WS-Management Endpoint implementing portions of the WS-Management specification.

### WS-Management Endpoint

Enables a management endpoint that supports the WS-Management family of protocols. The URI for the WS-Management endpoint is `/service/ws-management`.

- WSDM Endpoint, implementing portions of the WSDM specification.

### WSDM Endpoint

Enables a management endpoint that supports the WSDM 1.0 family of protocols. The URI for the WSDM 1.0 endpoint is `/service/wsdm-10`.

Service can be obtained at the following URI:

`/service/wsdm-10`

Refer to “WSDM interface” on page 123 for more details.

The following interfaces are implemented but not used for configuring the appliance:

### AMP Endpoint

Enables the appliance to expose a proprietary management interface protocol that is used for multi-box management. Multi-box management uses an external tool. By default, this service is enabled.

### SLM Endpoint

Enables a management endpoint that supports the SLM protocol. The URI

for the SLM protocol is /service/slm/datashare/1.0. The SLM protocol is used to exchange real time transaction monitoring and statistics used by the Service Level Monitoring peer. This service is not a public Web service. By default, this service is enabled.

#### **UDDI Subscription**

Enables the appliance to listen for UDDI subscription notifications that are sent by remote UDDI registries.

## **Enabling interface services**

You can enable a single XML Management Interface (that is accessible by an authorized user) to provide external access to configuration and status data. By default, the XML Management Interface runs SSL and uses HTTP Basic Authentication (user name and password).

On zBX, the XML Management Interface settings are read-only. None of the administrative accounts for zBX have the necessary permissions to alter these settings. The options on this page are disabled.

To enable the desired interface services:

1. Select **(Network Management XML Management Interface)** to display the XML Management Configuration (Main) screen.
2. Provide the following inputs:

#### **Administrative State**

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

#### **Local IP Address**

The IP interface address monitored for incoming management requests.

If you want the XML Management Interface to monitor all active interfaces, retain the default value (0.0.0.0).

You can use a host alias instead of a local IP address. Click **Select Alias** to choose a local host alias. Refer to “Host Alias” on page 84 for more information.

#### **Port Number**

The specific UDP port (in the range 1 through 65535) monitored by the XML Management Interface.

#### **Access Control List**

To employ an ACL other than the default for connection to the XML Management Interface, click the + button to create a new one. Refer to “Access Control List” on page 185 for more information.

#### **Comments**

Optional: Enter a descriptive summary.

#### **Enabled Services**

Use the check boxes to enable (selected) or disable (not selected) support for various management protocols. For details about these services, refer to “Services overview” on page 116.

When the SLM endpoint is enabled.

- a. Click the **SLM** tab.

- b. Use the **SLM Update Interval** field to specify the interval, in seconds, between data updates that are issued by the appliance.
3. Click **Apply** to save the changes to the running configuration.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

The XML Management Interface requires basic HTTP authentication of the administrative user who is configured on the appliance. Typically, HTTP authentication requires the default **admin** account and corresponding password.

## Changing default security and HTTP settings

To change default security settings and HTTP connections settings, use the following procedure:

1. Select (**Network Management XML Management Interface** to display the XML Management Configuration (Main) screen.
2. Click the **Advanced** tab to display the XML Management Interface configuration (Advanced) screen.
3. Provide the following inputs:

### Custom SSL Proxy Profile

Select an SSL Proxy Profile from the list. The SSL Proxy Profile references the certificates and keys for the SSL connection to the XML Management Interface.

By default, the DataPower appliance uses a self-signed certificate, not an SSL Proxy Profile. This field offers an opportunity to select a different SSL Proxy Profile.

Refer to “SSL Proxy Profile objects” on page 219 for more information.

### Custom User Agent

Select an instance of the User Agent object from the list. The User Agent object defines how to retrieve resources from remote servers.

4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## SOAP interface

The SOAP Interface provides many of the same capabilities that the WebGUI and commands provide. However, the SOAP Interface is a programmatic interface, while the WebGUI or the command line are non-programmatic.

To use the SOAP Interface, you must be able to read XML schemas to create a valid XML request. This document provides basic details only.

The SOAP Interface is described by the following set of files that are in the store: directory.

### xml-mgmt.xsd

The schema file that defines the non-primitive management types in SOAP messages.

### xml-mgmt-base.xsd

The schema file that defines the primitive management types in SOAP messages.

**xml-mgmt-ops.xsd**

The schema file that defines the operations that can be sent in SOAP requests.

**xml-mgmt.wsdl**

The WSDL file that defines the services that are available through the SOAP Interface.

**Note:** If you submit a request without credentials, the appliance returns a fault instead of a response.

## General structure of requests

The general structure of request documents is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://www.w3.org/2001/12/soap-envelope">
  <env:Body>
    <dp:request xmlns:dp="http://www.datapower.com/schemas/management">
      :
    </dp:request>
  </env:Body>
</env:Envelope>
```

The request can contain the `domain` attribute to specify in which application domain to perform the operation.

## General structure of responses

The general structure of response documents is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope">
  <env:Body>
    <dp:response xmlns:dp="http://www.datapower.com/schemas/management">
      <dp:timestamp>timestamp</dp:timestamp>
      :
    </dp:response>
  </env:Body>
</env:Envelope>
```

## Available operations for requests

The `<request>` element can contain any combination of the operations that are defined in the store: `///xml-mgmt-ops.xsd` schema file. The SOAP Interface supports the following operations:

**Retrieve a login token**

Define the `<dp:get-samlart>` element. To retrieve, as a binary token, the SAML artifact that is in use for the current session:

```
<dp:get-samlart user="bmclarke" password="n0w0y@g3r" />
```

**Retrieve a status object (also known as a status provider)**

Define the `<dp:get-status>` element. To retrieve all status objects:

```
<dp:get-status />
```

To retrieve a specific status object:

```
<dp:get-status class="StatusEnum" />
```

Refer to the `StatusEnum` type in the store: `///xml-mgmt.xsd` schema file for the list of the supported status objects.



### Compare configurations

Define the <dp: get-diff> element. Refer to the store:///xml-mgmt-ops.xsd schema file for details about the structure for this request.

### Generate a conformance report

Define the <dp: get-conformance-report> element. Refer to the store:///xml-mgmt-ops.xsd schema file for details about the structure for this request.

### List files and directories

Define the <dp: get-filesystem> element. To list the root contents of the file system:

```
<dp: get-filesystem />
```

To list the contents of a directory:

```
<dp: get-filesystem location="directory" />
```

### Retrieve log data

Define the <dp: get-log> element. To retrieve all log data:

```
<dp: get-log />
```

To retrieve log data for a specific log target:

```
<dp: get-log name="logTarget" />
```

### Download a file.

Define the <dp: get-file> element. To download a file:

```
<dp: get-file name="directory:///file" />
```

### Upload a file

Define the <dp: set-file> element. To upload a file to a specific location:

```
<dp: set-file name="directory:///file">  
    *** base64 encoded file ***  
</dp: set-file>
```

The request must contain the name and location of the file to upload to the appliance. The name attribute on the element defines the destination.

### Export configuration data

Define the <dp: do-export> element. Refer to the store:///xml-mgmt-ops.xsd schema file for details about the structure for this request.

To export a domain configuration, define the <dp: do-backup> element.

### Import configuration data

Define the <dp: do-import> element. Refer to the store:///xml-mgmt-ops.xsd schema file for details about the structure for this request.

To import a domain configuration, define the <dp: do-restore> element.

### Create a backup of a domain

Define the <dp: do-backup> element. Refer to the store:///xml-mgmt-ops.xsd schema file for details about the structure for this request.

### Restore a domain from a backup

Define the <dp: do-restore> element. Refer to the store:///xml-mgmt-ops.xsd schema file for details about the structure for this request.

### Perform a specific action

Define the <dp: do-action> element. The node for each action in a request requires a different definition. For example to shutdown the appliance after 30 seconds and restart:



```

<dp:do-action>
  <ActionShutdown>
    <Mode>reboot</Mode>
    <Delay>30</Delay>
  </ActionShutdown>
</dp:do-action>

```

Refer to the `AnyActionElement` type in the store:///xml-mgmt.xsd schema file for the list of the supported actions.

### Create an object

Define the `<dp:set-config>` element. To create an object:

```

<dp:set-config>
:
</dp:set-config>

```

Refer to the `AnyConfigElement` type in the store:///xml-mgmt.xsd schema file for the list of the supported objects.

### Retrieve object configuration

Define the `<dp:get-config>` element. To retrieve the configuration of all objects:

```

<dp:get-config />

```

To retrieve the configuration of all objects of a specific class:

```

<dp:get-config class="ConfigEnum" />

```

To retrieve the configuration of a specific objects:

```

<dp:get-config class="ConfigEnum" name="name" />

```

Refer to the `ConfigEnum` type in the store:///xml-mgmt.xsd schema file for the list of the supported objects.

### Modify the configuration of an object

Define the `<dp:modify-config>` element. To modify an object:

```

<dp:modify-config>
:
</dp:modify-config>

```

Refer to the `AnyModifyElement` type in the store:///xml-mgmt.xsd schema file for the list of the supported objects.

### Delete an object

Define the `<dp:del-config>` element. To delete an object:

```

<dp:delete-config>
:
</dp:delete-config>

```

Refer to the `AnyDeleteElement` type in the store:///xml-mgmt.xsd schema file for the list of the supported objects.

## Example request to view status

The following example uses the `curl` program to post a request to the XML Management Interface (10.10.13.7:1080) to view object status. The request is contained in the `get-status.xml` file.

```

$ curl -k -u user:password -d @get-status.xml https://10.10.13.7:1080

```

- k** Enables the performance of a nonsecure SSL connection and transfer. (no certificate checking)
- u user:password**  
Specifies the user name and password for server authentication.
- d** Sends the data in an HTTP POST request.

### Sample request

The get-status.xml request could contain the following message.

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://www.w3.org/2001/12/soap-envelope">
  <env:Body>
    <dp:request xmlns:dp="http://www.datapower.com/schemas/management">
      <dp:get-status class="ActiveUsers"/>
    </dp:request>
  </env:Body>
</env:Envelope>
```

### Sample response

The get-status.xml request could generate the following response on success.

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Body>
    <dp:response xmlns:dp="http://www.datapower.com/schemas/management">
      <dp:timestamp>2007-07-30T13:58:28-04:00</dp:timestamp>
      <dp:status>
        <ActiveUsers>
          <session>1</session>
          <name>wlynych</name>
          <connection>serial-port</connection>
          <address/>
          <login>Fri May 23 12:31:02 2003</login>
        </ActiveUsers>
      </dp:status>
    </dp:response>
  </env:Body>
</env:Envelope>
```

The get-status.xml request could generate the following response on authentication failure.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright (c) 1999-2003 DataPower Technology, Inc. All Rights Reserved. -->
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Body>
    <dp:response>
      <dp:result>Authentication failure</dp:result>
    </dp:response>
  </env:Body>
</env:Envelope>
```

## Example request to compare configurations

The following example uses the **curl** program to post a request to the XML Management Interface (10.10.13.7:1080) to compare configurations. The request is contained in the get-diff.xml file.

```
$ curl -k -u user:password -d @get-diff.xml https://10.10.13.7:1080
```

- k** Enables the performance of a nonsecure SSL connection and transfer. (no certificate checking)
- u user:password**  
Specifies the user name and password for server authentication.

**-d** Sends the data in an HTTP POST request.

### Sample request

The `get-diff.xml` request could contain the following message. This message compares an exported configuration (after converting the export file to its base-64 encoded equivalent) to the running configuration.

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://www.w3.org/2001/12/soap-envelope">
  <env:Body>
    <dp:request xmlns:dp="http://www.datapower.com/schemas/management">
      <dp:get-diff>
        <dp:from>
          <dp:export>base-64 encoded data</dp:export>
        </dp:from>
        <dp:to>
          <dp:object class="all-classes" name="all-objects"/>
        </dp:to>
      </dp:get-diff>
    </dp:request>
  </env:Body>
</env:Envelope>
```

### Sample response

The `get-diff.xml` request could generate a response that contains multiple object elements. Each element object shows its current configuration. Each affected object in the configuration has one of the following attributes at the object node:

`new="true"`

Indicates an object that was added to the configuration.

`modified="true"`

Indicates an object that was modified in the configuration.

`removed="true"`

Indicates an object that was deleted from the configuration.

Review the response for these attributes to determine which objects were added to, deleted from, or modified in the configuration. For example, the following item in the response shows that the `GetDiff2XMLFirewall` matching rule was added.

```
<Matching new="true" name="GetDiff2XMLFirewall"
  xmlns:env="http://www.w3.org/2003/05/soap-envelope"
  xmlns:dp="http://www.datapower.com/schemas/management">
  <mAdminState>enabled</mAdminState>
  <MatchRules>
    <Type>url</Type>
    <HttpTag />
    <HttpValue />
    <Url>*</Url>
    <ErrorCode />
    <XPATHEXpression />
  </MatchRules>
  <MatchWithPCRE>off</MatchWithPCRE>
  <CombineWithOr>off</CombineWithOr>
</Matching>
```

---

## WSDM interface

The DataPower appliance includes an implementation of the Web Services Distributed Management (WSDM) protocol specification (Version 1.0 OASIS, February 2006). When enabled, this implementation provides a protocol-specific interface for managing Web Service endpoints that were instantiated on the appliance through Web Service Proxy objects.

You can use the sample `wsdm.xml` and `wsdmfirm.xml` files in the store: directory to request information from the WSDM interface.

You can use the sample `wsrp-status.xsd` schema in the store: directory to request information from the WSDM interface.

`http://IP-address:WSDM-port/service/wsdm10/wsrp-status.xsd`

You can use the sample `xml-mgmt-wsdm.wsdl` file, which is generated dynamically on the appliance, to extract supported status properties. Retrieve this WSDL file from the router by sending a request to the following URL:

`/service/wsdm10?wsdl`

You can discover the capabilities of the WSDM endpoint by issuing a request to return a management capability list.

```
<?xml version="1.0" encoding="UTF-8"?>
<s12:Envelope
  xmlns:s12="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2003/03/addressing"
  xmlns:wsrp="http://docs.oasis-open.org/wsrp/2004/06/
    wsrf-WS-ResourceProperties-1.2-draft-01.xsd"
  xmlns:muws-p1="http://docs.oasis-open.org/wsdm/2004/12/muws/wsdm-muws-part1.xsd"
  xmlns:muws-p2="http://docs.oasis-open.org/wsdm/2004/12/muws/wsdm-muws-part2.xsd"
  xmlns:mows="http://docs.oasis-open.org/wsdm/2004/12/mows/wsdm-mows.xsd"
  xmlns:mows-1-1="http://docs.oasis-open.org/wsdm/mows-2.xsd"
  xmlns:dpt="http://www.datapower.com/schemas/transactions">

  <s12:Header>
    <wsa:Action>
      http://docs.oasis-open.org/wsrp/2004/06/WS-ResourceProperties/
        GetResourceProperty
    </wsa:Action>
    <wsa:To s12:mustUnderstand="1">
      https://127.0.0.1:5550/service/wsdm10>
    </wsa:To>
    <dpt:DomainDisambiguator>wsdm</dpt:DomainDisambiguator>
    <dpt:ResourceTypeDisambiguator>wsm/endpoint</dpt:ResourceTypeDisambiguator>
    <dpt:InstanceDisambiguator>
      http://0.0.0.0:14000/wsdm/service-a
    </dpt:InstanceDisambiguator>
  </s12:Header>
  <s12:Body>
    <wsrp:GetResourceProperty>
      muws-p1:ManageabilityCapability
    </wsrp:GetResourceProperty>
  </s12:Body>
</s12:Envelope>
```

Note that the `<dpt:DomainDisambiguator>` node must be set to an existing application domain on the appliance or set to default. If the domain does not exist, an error will result.

The request returns a list of capabilities, such as the following list:

```
<s12:Envelope xmlns:dpt="http://www.datapower.com/schemas/transactions"
  xmlns:mows="http://docs.oasis-open.org/wsdm/2004/12/mows/wsdm-mows.xsd"
  xmlns:mows-1-1="http://docs.oasis-open.org/wsdm/mows-2.xsd"
  xmlns:muws-p1="http://docs.oasis-open.org/wsdm/2004/12/muws/wsdm-muws-part1.xsd"
  xmlns:muws-p2="http://docs.oasis-open.org/wsdm/2004/12/muws/wsdm-muws-part2.xsd"
  xmlns:s12="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2003/03/addressing"
  xmlns:wsrp="http://docs.oasis-open.org/wsrp/2004/06/
```

```

wsrf-WS-ResourceProperties-1.2-draft-01.xsd">

<s12: Header>
  <wsa0: Action xmlns:wsa0="http://schemas.xmlsoap.org/ws/2003/03/addressing">
    http://docs.oasis-open.org/wsrf/2004/06/WS-ResourceProperties/
    GetResourcePropertyResponse
  </wsa0: Action>
</s12: Header>
<s12: Body>
  <wsrp: GetResourcePropertyResponse>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/wsdm/2004/12/muws/capabilities/Identity
    </muws-p1: ManageabilityCapability>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/wsdm/2004/12/muws/capabilities/
      ManageabilityCharacteristics
    </muws-p1: ManageabilityCapability>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/wsdm/2004/12/muws/capabilities/OperationalStatus
    </muws-p1: ManageabilityCapability>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/wsdm/2004/12/mows/capabilities/OperationalStatus
    </muws-p1: ManageabilityCapability>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/wsdm/2004/12/muws/capabilities/Metrics
    </muws-p1: ManageabilityCapability>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/wsdm/2004/12/mows/capabilities/Identification
    </muws-p1: ManageabilityCapability>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/wsdm/2004/12/mows/capabilities/Metrics
    </muws-p1: ManageabilityCapability>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/mows-2/capabilities/Metrics
    </muws-p1: ManageabilityCapability>
    <muws-p1: ManageabilityCapability>
      http://docs.oasis-open.org/mows-2/capabilities/OperationMetrics
    </muws-p1: ManageabilityCapability>
  </wsrp: GetResourcePropertyResponse>
</s12: Body>
</s12: Envelope>

```

This list contains the supported capabilities. Use the standards-specified request formats to use these capabilities.

## Example request to view the number of client requests

The following example shows a request to view the number of client requests to the particular service.

```

<?xml version="1.0" encoding="UTF-8"?>
<s12: Envelope
  xmlns:s12="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2003/03/addressing"
  xmlns:wsrp="http://docs.oasis-open.org/wsrf/2004/06/
    wsrf-WS-ResourceProperties-1.2-draft-01.xsd"
  xmlns:muws-p1="http://docs.oasis-open.org/wsdm/2004/12/muws/wsdm-muws-part1.xsd"
  xmlns:muws-p2="http://docs.oasis-open.org/wsdm/2004/12/muws/wsdm-muws-part2.xsd"
  xmlns:mows="http://docs.oasis-open.org/wsdm/2004/12/mows/wsdm-mows.xsd"
  xmlns:mows-1-1="http://docs.oasis-open.org/wsdm/mows-2.xsd"
  xmlns:dpt="http://www.datapower.com/schemas/transactions">

  <s12: Header>
    <wsa: Action>
      http://docs.oasis-open.org/wsrf/2004/06/WS-ResourceProperties/
      GetResourceProperty
    </wsa: Action>

```

```

<wsa:To s12:mustUnderstand="1">
  https://127.0.0.1:5550/service/wsdml0
</wsa:To>
<dpt:DomainDisambiguator>wsdm</dpt:DomainDisambiguator>
<dpt:ResourceTypeDisambiguator>wsm/endpoint</dpt:ResourceTypeDisambiguator>
<dpt:InstanceDisambiguator>
  http://0.0.0.0:14000/wsdm/service-a
</dpt:InstanceDisambiguator>
</s12:Header>
<s12:Body>
  <wsrp:GetResourceProperty>
    mows:NumberOfRequests
  </wsrp:GetResourceProperty>
</s12:Body>
</s12:Envelope>

```

## Example request to view active users

The following example shows a request to view active users on the appliance:

```

<s12:Body>
  <wsrp:GetResourcePropertyResponse
    xmlns:mows-1-1="http://docs.oasis-open.org/wsdm/mows-2.xsd">
    <status.active-users xmlns="http://www.datapower.com/schemas/management">
      <ActiveUsers>
        <session>48</session>
        <name>admin</name>
        <connection>web-gui</connection>
        <address>10.10.13.35</address>
        <login>Tues Oct 16 08:53:33 2007</login>
        <domain>default</domain>
        <session>49</session>
        <name>CLIAdmin</name>
        <connection>cli</connection>
        <address>10.10.13.35</address>
        <login>Tues Oct 16 08:54:12 2007</login>
        <domain>default</domain>
        <session>50</session>
        <name>JulieSmith</name>
        <connection>web-gui</connection>
        <address>10.10.13.35</address>
        <login>Tues Oct 16 08:54:48 2007</login>
        <domain>default</domain>
      </ActiveUsers>
    </status.active-users>
  </wsrp:GetResourcePropertyResponse>
</s12:Body>

```

## Example request to view CPU usage

The following example shows a request to view CPU usage on the appliance:

```

<s12:Body>
  <wsrp:GetResourcePropertyResponse
    xmlns:mows-1-1="http://docs.oasis-open.org/wsdm/mows-2.xsd">
    <status.cpu xmlns="http://www.datapower.com/schemas/management">
      <CPUUsage>
        <tenSeconds>23</tenSeconds>
        <oneMinute>24</oneMinute>
        <tenMinutes>22</tenMinutes>
        <oneHour>23</oneHour>
        <oneDay>23</oneDay>
      </CPUUsage>
    </status.cpu>
  </wsrp:GetResourcePropertyResponse>
</s12:Body>

```

## Example request to view appliance usage

The following example shows a request to view appliance usage on the appliance:

```
<s12: Body>
  <wsrp: GetResourcePropertyResponse
    xmlns:mows-1-1="http://docs.oasis-open.org/wsdm/mows-2.xsd">
    <status.system xmlns="http://www.datapower.com/schemas/management">
      <SystemUsage>
        <Interval>1000</Interval>
        <Load>30</Load>
        <WorkList>0</WorkList>
      </SystemUsage>
    </status.system>
  </wsrp: GetResourcePropertyResponse>
</s12: Body>
```

## Example request to view accepted connections

The following example shows a request to view accepted connections on the appliance:

```
<s12: Body>
  <wsrp: GetResourcePropertyResponse
    xmlns:mows-1-1="http://docs.oasis-open.org/wsdm/mows-2.xsd">
    <status.accepted-connections
      xmlns="http://www.datapower.com/schemas/management">
      <ConnectionsAccepted>
        <tenSeconds>0</tenSeconds>
        <oneMinute>0</oneMinute>
        <tenMinutes>5</tenMinutes>
        <oneHour>613</oneHour>
        <oneDay>8979</oneDay>
      </ConnectionsAccepted>
    </status.accepted-connections>
  </wsrp: GetResourcePropertyResponse>
</s12: Body>
```

---

## Custom SSL proxy profile

The configuration of the Web management interface (WebGUI) and XML management interface uses an SSL proxy profile to secure connections from clients. By default, the DataPower appliance uses a self-signed certificate during the SSL handshake. Instead of using this SSL proxy profile, you can create a custom SSL proxy profile that uses different keys and certificates.

## Generating a custom profile

Generating a certificate from the Web Management Service pane creates and assigns an SSL proxy profile that is based on the generated self-signed certificate and private key.

To generate a custom SSL proxy profile for WebGUI sessions:

1. Click **Network Management Web Management Service**.
2. Click **Generate Certificate** beside the **Local IP Address** field.
3. Click **Confirm** to create the device-id SSL proxy profile and its required cryptographic material.
4. Verify the assignment of the SSL proxy profile.
  - a. Click the **Advanced** tab.
  - b. Verify that the selection for the **Custom SSL Proxy Profile** list is device-id.
5. Click **Apply** to save the changes to the running configuration.

6. Optional: Click **Save Config** to save the changes to the startup configuration.

## Removing the profile assignment

If you inadvertently saved the configuration and the assigned SSL profile is incorrectly configured, no one will be able to access the WebGUI. Because you cannot access the WebGUI, you must use the command line (serial connection or SSH).

To remove the custom SSL proxy profile from the command line:

1. Access the command line from an SSH client or serial connection.
2. From the command line, enter the follow sequence of commands:

```
configure terminal
web-mgmt
no ssl
exit
write memory
```
3. Enter `y` to save the configuration.
4. Although the configuration for WebGUI access is set to use the internal cryptographic material, enter `exit` to close the command line session.

If you defined the same SSL proxy profile for the XML management interface, you can access WebGUI and assign a different SSL proxy profile to secure both WebGUI and XML management interface sessions.

## Cryptographic material for the custom profile

If desired, you can review the configuration changes before saving the configuration. To view the changes, click the **Review changes** link.

If you saved the configuration, you can still verify that the appropriate cryptographic materials (files and objects) were created.

To verify whether the files exist, use the **File Management** utility. The file system should contain the following files:

- The `cert:///device-id-privkey.pem` file that contains the generated private key
- The `cert:///device-id-sscert.pem` file that contains the generated self-signed certificate

To verify whether the objects exist, access the following configurations:

- The `device-id` key that references the `device-id-privkey.pem` file
- The `device-id` certificate that references the `device-id-sscert.pem` file
- The `device-id` identification credentials set that references the `device-id` key and the `device-id` certificate
- The `device-id` reverse (server) profile set that references the `device-id` identification credentials set
- The `device-id` SSL proxy profile that references the `device-id` reverse (server) profile



---

## Chapter 12. Managing the firmware image

Before performing a firmware upgrade, contact IBM Customer Support and refer to the *IBM WebSphere DataPower SOA Appliances: Upgrade and Rollback Guide*. This document is available on the DataPower Support Web site.

---

### Applying a firmware image

Use the following procedure to apply a firmware image, which might be an upgrade:

1. Select **Administration Main System Control** to display the System Control panel.
2. Locate the **Boot Image** section of the System Control panel.
3. If the desired firmware file is not on the appliance, click **Upload** or **Fetch**. Refer to Chapter 13, “Managing files,” on page 131 for details.
4. From the **Firmware File** list, select the firmware file.
5. Click **Boot Image** to boot the appliance with the selected file.
6. Click **Confirm** to apply the upgrade and reboot the appliance.

An additional confirmation screen is display that confirms that the firmware file was installed.

The appliance can take up to 3 minutes to reboot.

---

### Rolling back an upgrade

Use the following procedure to roll back to the previous firmware image:

1. Select **Administration Main System Control** to display the System Control panel.
2. Locate the Firmware Roll-Back section of the System Control panel.
3. Click **Firmware Roll-Back**.
4. Click **Confirm**.

The appliance is rolled back to the last-installed release.



---

## Chapter 13. Managing files

The appliance provides a File Management utility to administer files stored in the predefined directories and in any user defined subdirectories.

---

### Directories on the appliance

The file system contains many examples and critical configuration files. These directories and their contents are as follows:

**audit:** This directory contains the audit logs. Each appliance contains only one audit: directory. This directory cannot be the destination of a copy. This directory is available from the command line in the default domain only.

To view from the WebGUI, click **Status View Logs Audit Log**.

**cert:** This encrypted directory contains private key and certificate files that services use in the domain. You can add, delete, and view files, but you cannot modify these files while in the domain. Each application domain contains one cert: directory. This directory is not shared across domains.

**chkpoints:**

This directory contains the configuration checkpoint files for the appliance. Each application domain contains one chkpoints: directory. This directory is not shared across domains. During an upgrade, the operation deletes the contents of this directory.

**config:**

This directory contains the configuration files for the appliance. Each application domain contains one config: directory. This directory is not shared across domains.

**dpcert:**

This encrypted directory contains files that the appliance itself uses. This directory is available from the command line in the default domain only.

**export:**

This directory contains the exported configurations that are created with the Export Configuration utility. Each application domain contains one export: directory. This directory is not shared across domains.

**image:** This directory contains the firmware images (primary and secondary) for the appliance. This directory is where firmware images are stored typically during an upload or fetch operation. Each appliance contains only one image: directory. This directory is available in the default domain only. During an upgrade, the operation deletes the contents of this directory.

**local:** This directory contains miscellaneous files that are used by the services within the domain, such as XSL, XSD, and WSDL files. Each application domain contains one local: directory. This directory can be made visible to other domains. When viewed from other domains, the directory name changes from local: to the name of the application domain.

**logstore:**

This directory contains log files that are stored for future reference. Typically, the logging targets use the logtemp: directory for active logs. You

can move log files to the logstore: directory. Each application domain contains one logstore: directory. This directory is not shared across domains.

**logtemp:**

This directory is the default location of log files, such as the appliance-wide default log. This directory can hold only 13 MB. This directory cannot be the destination of a copy. Each application domain contains one logtemp: directory. This directory is not shared across domains.

**pubcert:**

This encrypted directory contains the security certificates that are used commonly by Web browsers. These certificates are used to establish security credentials. Each appliance contains only one pubcert: directory. This directory is shared across domains.

**sharedcert:**

This encrypted directory contains security certificates that are shared with partners. Each appliance contains only one sharedcert: directory. This directory is shared across domains. However, you must be in default domain to create or upload keys and certificates.

**store:** This directory contains example style sheets, default style sheets, and schemas that are used by the local appliance. Do not modify the files in this directory.

Each appliance contains only one store: directory. By default, this directory is visible to all domains. You can make changes to the contents of this directory from the default domain only.

The store: directory has the following subdirectories:

**meta** This encrypted subdirectory contains files that are used by the appliance itself.

**msgcat**

This subdirectory contains the message catalogs.

**policies**

This subdirectory contains the following subdirectories. The contents of these subdirectories affect Web services policy.

**custom**

This subdirectory contains custom style sheets.

**mappings**

This subdirectory contains mapping style sheets.

**templates**

This subdirectory contains XML files.

**profiles**

This subdirectory contains style sheets that are used by DataPower services.

**schemas**

This subdirectory contains schemas that are used by DataPower services.

**dp**

This encrypted subdirectory contains files that are used by the appliance itself. This subdirectory is available from the command line only.

### **pubcerts**

This encrypted subdirectory contains files that are used by the appliance itself. This subdirectory is available from the command line only.

### **tasktemplates:**

This directory contains the XSL files that define the display of specialized WebGUI screens. Each appliance contains only one tasktemplates: directory. This directory is visible to the default domain only.

### **temporary:**

This directory is used as temporary disk space by processing rules. Each application domain contains one temporary: directory. This directory is not shared across domains. During an upgrade, the operation deletes the contents of this directory.

---

## **Launching the File Management utility**

To manage files, launch the File Management utility with one of the following methods:

- Select the File Management icon from the **Files and Administration** section of the Control Panel.
- Select **Administration Main File Management**.

Either method displays the File Management screen. The initial screen shows the top level directories.

---

## **Displaying directory contents**

To display (expand) the contents of a directory, perform the following procedure:

1. Launch the File Management utility. Refer to “Launching the File Management utility” for details.
2. Select the directory to display its contents.

To hide (collapse) the content-view of a directory, select that directory again.

---

## **Creating a subdirectory**

Subdirectories can only be created under the **local:** directory or one of its subdirectories.

Follow these steps to create a subdirectory under the **local:** directory or one of its subdirectories:

1. Launch the File Management utility. Refer to “Launching the File Management utility” for details.
2. From the Action column, click **Actions** aligned with the directory for the subdirectory to be created.
3. Click **Create Subdirectory**. The File Management screen displays.
4. Enter the name of the new subdirectory in the directory Name field.
5. Click **Confirm Create**. The File Management screen refreshes.
6. Click **Continue**. The File Management screen displays the top-level directories only.

---

## Deleting a directory

Directories can only be deleted in the **local:** directory or one of its subdirectories.

Follow these steps to delete a directory under the **local:** directory or one of its subdirectories:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. From the Action column, click **Actions** aligned with the directory to be deleted.
3. Click **Delete Directory**. The File Management screen displays.
4. Click **Confirm Delete**. The File Management screen refreshes.
5. Click **Continue**. The File Management screen displays the top-level directories only.

---

## Refreshing directory contents

To refresh contents, click the **Refresh Page** icon. The WebGUI redraws the File Management screen. The screen displays the top-level directories only.

---

## Uploading files from the workstation

Use the following procedure to upload a file from your workstation to the appliance:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory into which you want to upload the file.
3. Click **Actions** in that row to open the Directory Actions menu.
4. Click **Upload Files** to display the File Upload screen.
5. Specify the path-qualified name of the workstation file in the **File to upload** field, or click **Browse** to locate the file on the workstation.
6. Specify the file name in the **Save as** field.  
  
**Note:** If you used browsing to select the file or if you navigated to this field using the tab key, the field contains the file name.
7. To add another file to be uploaded:
  - a. Click **Add**.
  - b. Repeat steps 5 and 6.
8. If one of the files already exists in the selected directory and you want to overwrite this file, check the **Overwrite Existing Files** check box. If you do not select this check box and the file already exists, the file is not uploaded.
9. Click **Upload**.
10. When the appliance reports success (or an error is the file already existed), click **Continue** to return to the File Management screen.

The target directory now contains the uploaded files. To verify, use the procedure described in “Displaying directory contents” on page 133.

---

## Working with Java Key Stores

A Java Key Store (JKS) is a Sun-proprietary format file that contains private keys and certificates. The `java.security` package and sub-packages access the data in the JKS to carry out their cryptographic operations.

### Required software

JKS support requires the following software on the WebGUI workstation:

- Version 1.4.2 of the Java runtime environment (j2re1.4.2)
- SDK (j2sdk1.4.2)
- Internet Explorer

**Note:** You must have the JRE or Java SDK `/bin` path name in the Windows PATH environment variable on the WebGUI workstation. The Java Key Store file cannot reside on any of the local directories. It must be uploaded from a workstation.

### Granting permissions

In addition, the user must have the grant permission for the upload in the `.java.policy` file on the workstation that contains the Java Key Store files. The following example `.java.policy` file should be defined on the workstation computer before starting the upload:

```
grant {  
    permission java.io.FilePermission "<<ALL FILES>>", "read";  
    permission java.util.PropertyPermission "*", "read";  
    permission java.lang.RuntimePermission "accessClassInPackage.sun.*";  
};
```

You can grant read-only permission to the JKS file.

### Types of key stores

Sun offers two common methods to support key store creation:

- Sun Java 2.1.4.2 runtime environment or SDK use a program called **keytool** to create and manage a JKS-type file store with no provider name.
- SunJCE (Java Crypto Extension) generates a JCEKS-type (Java Crypto Extension Key Store) file store with the provider name SunJCE.

You must know the key store type to successfully upload files from a JKS.

### Uploading a file from a Java Key Store

Use the following procedure to upload a file from a Java Key Store (JKS) to the appliance:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory into which you want to upload the file.
3. Click **Actions** in that row to open the Directory Actions menu.
4. Click **Upload Files** to display the File Upload screen.
5. Click the **Java Key Store** radio button to display the JKS Upload screen.

**Note:** When you click the **Java Key Store** radio button, the Java Console of the browser opens and shows whether the Java Key Store Access

Applet is running. If the applet cannot be accessed, you cannot upload JKS files. Ensure that your browser is enabled to use the Java 1.4.2 applet.

6. Specify the full path to the target JKS in the **Java key store** field or click **Browse**.
7. Specify JKS or JCEKS (the JKS type) in the **Key store type** field.
8. If the type is JCEKS, specify SunJCE (the provider name) in the **Key store provider** field. Otherwise, leave blank.
9. Specify the JKS password in the **Key store password** field.
10. Identify the files to upload with the **Key to upload** list. Use the **Refresh** button, if necessary.
11. Specify the key-specific password in the **Key password** field.
12. Specify the file name in the **Save as** field.
13. If the file already exists in the selected directory and you want to overwrite this file, check the **Overwrite Existing Files** check box. If you do not select this check box and the file already exists, the file is not uploaded.
14. Click **Upload**.
15. When the appliance reports success, click **Continue** to return to the File Management screen.

The target directory now contains the uploaded key or certificate. To verify that the file exists, use the procedure described in “Displaying directory contents” on page 133.

If the upload fails, look at the Java Console of the browser to determine whether an exception was thrown.

---

## Fetching files

Use the following procedure to retrieve a file from a remote URL (fetch) and store that file in a specified directory on the appliance:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory into which you want to upload the file.
3. Click **Actions** in that row to open the Directory Actions menu.
4. Click **Fetch Files** to display the Fetch File screen.
5. Specify the location of the file in the **Source URL** field.
6. Specify the file name in the **Save as** field.
7. If the file already exists in the selected directory and you want to overwrite this file, check the **Overwrite Existing Files** check box. If you do not select this check box and the file already exists, the file is not uploaded.
8. Click **Fetch**.
9. When the appliance reports success, click **Continue** to return to the File Management screen.

The target directory now contains the retrieved file. To verify, use the procedure described in “Displaying directory contents” on page 133.

---

## Copying files

Use the following procedure to copy a file from one directory to another:



1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory that contains the files to be copied.
3. Select files by clicking the box adjacent to the file name.
4. Scroll to the top or bottom of the screen and click **Copy** to display the File Copy screen.
5. From the **New Directory Name** list, select the target directory.
6. Specify the name for the file, if different, in the **New File Name** field.
7. If one of the selected files already exists in its associated target directory and you want to overwrite this file, check the **Overwrite Existing Files** check box. If you do not select this check box and the file already exists, the file is not copied.
8. Click **Confirm Copy** to copy the files to the target directories.
9. When the appliance reports success, click **Continue** to return to the File Management screen.

The target directories now contain the copied files. To verify that the files exist, use the procedure described in “Displaying directory contents” on page 133.

---

## Renaming files

Use the following procedure to rename a file:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory that contains the files to be copied.
3. Select files by clicking the box adjacent to the file name.
4. Click **Rename** to display the File Rename screen.
5. Specify the name of the file in the **New File Name** field.
6. If one of the selected files already exists in the target directory and you want to overwrite this file, check the **Overwrite Existing Files** check box. If you do not select this check box and the file already exists, the file is not copied.
7. Click **Confirm Rename**.
8. When the appliance reports success, click **Continue** to return to the File Management screen.

The target directories now contain the renamed files. To verify that the files exist, use the procedure described in “Displaying directory contents” on page 133.

---

## Moving files

Use the following procedure to move a file from one directory to another:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory that contains the files to be moved.
3. Select files by clicking the box adjacent to the file name.
4. Click **Move** to display the Move File screen.
5. From the **New Directory** list, select the target directory.
6. If one of the selected files already exists in its directory and you want to overwrite this file, select the **Overwrite Existing Files** check box. If you do not select this check box and the file already exists, the file is not moved.

7. Click **Confirm Move**.
8. When the appliance reports success, click **Continue** to return to the File Management screen.

The target directories now contain the moved files. To verify that the files exist, use the procedure described in “Displaying directory contents” on page 133.

---

## Viewing files

Use the following procedure to view a text file:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory that contains the file.
3. Click the file to open a browser that contains the file.

When finished viewing the file, close the browser.

---

## Editing files

Use the following procedure to edit a text file:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory that contains the files to be edited.
3. Select the file to be edited by clicking **Edit** in the row that is associated with that file. The WebGUI displays a file preview.
4. Click **Edit** to change to Edit Mode.
5. Edit the file as required.
6. Click **Submit** to complete the edit process.
7. When the appliance reports success, click **Close** to return to the File Management screen.

---

## Deleting files

Use the following procedure to delete a file:

1. Launch the File Management utility. Refer to “Launching the File Management utility” on page 133 for details.
2. Navigate to the directory that contains the files to be deleted.
3. Select files by clicking the box adjacent to the file name.
4. Scroll to the top or bottom of the screen and click **Delete** to display the Delete File screen.
5. Click **Confirm Delete** to delete the files.
6. When the appliance reports success, click **Continue** to return to the File Management screen.

The selected files were deleted. To verify that the files no longer exist, use the procedure described in “Displaying directory contents” on page 133.

---

## Chapter 14. Managing auxiliary data storage

Depending on the model, each Type 9235 appliance has one of the following types of auxiliary data storage:

- Compact flash storage card
- Hard disk array

After you configure and enable auxiliary data storage, you can access the available files in defined subdirectory. This subdirectory is in the local: and logstore: directories in each application domain.

**Note:** Other model types for DataPower appliances do not provide hardware to support auxiliary data storage.

---

### Configuring the compact flash

To configure the compact flash as auxiliary data storage

1. Click **Administration** **Storage Devices** **Compact Flash**.
2. Click the name of the compact flash.
3. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
4. Set **Read-Only** to indicate whether the files on the compact flash have read-only access.
5. In the **Directory** field, specify the directory under which to make the files on the compact flash available in the local: and logstore: directories in each application domain.
6. Click **Apply** to save the changes to the running configuration.
7. Optional: Click **Save Config** to save the changes to the startup configuration.

---

### Managing the file system on the compact flash

To manage the file system on the compact flash, you might need to perform one of the following actions:

- Initialize the file system
- Repair the file system

#### Initializing the file system

Initializing the file system on the compact flash allows it to be made active. When invoked against auxiliary data storage that contains content, this action destroys the existing content.

To initialize the file system on the compact flash:

1. Click **Administration** **Storage Devices** **Compact Flash**.
2. Click the name of the compact flash.
3. Click **Initialize File System**.
4. Follow the prompts.

## Repairing the file system

You might need to repair the file system on the compact flash if its contents were corrupted by an abnormal shutdown of the appliance or other error.

To repair the file system on the compact flash:

1. Click **Administration** **Storage Devices** **Compact Flash**.
2. Click the name of the compact flash.
3. Click **Repair File System**.
4. Follow the prompts.

---

## Configuring the hard disk array

To configure the hard disk array as auxiliary data storage:

1. Click **Administration** **Storage Devices** **Hard Disk Array**.
2. Click the name of the hard disk array.
3. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
4. In the **Directory** field, specify the directory under which to make the files on the hard disk array available in the local: and logstore: directories in each application domain.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Managing the file system on the hard disk array

To manage the file system on the hard disk array, you might need to perform one of the following actions:

- Initialize the file system
- Repair the file system

### Initializing the file system

Initializing the file system on the hard disk array allows it to be made active. When invoked against auxiliary data storage that contains content, this action destroys the existing content.

To initialize the file system on the hard disk array:

1. Click **Administration** **Storage Devices** **Hard Disk Array**.
2. Click the name of the hard disk array.
3. Click **Initialize File System**.
4. Follow the prompts.

### Repairing the file system

You might need to repair the file system on the hard disk array if its contents were corrupted by an abnormal shutdown of the appliance or other error.

To repair the file system on the hard disk array:

1. Click **Administration** **Storage Devices** **Hard Disk Array**.

2. Click the name of the hard disk array.
3. Click **Repair File System**.
4. Follow the prompts.

---

## Managing the RAID volume

To manage the RAID volume of the hard disk array, you might need to perform one of the following actions:

- Activate the volume
- Initialize the volume
- Rebuild the volume
- Delete the volume

### Activating the volume

You might need to activate the RAID volume to change the state of the hard disk array to active. Generally, you need to perform this action when the hard disk array volume is in the inactive state, typically with the foreign volume inactive state. After activating the RAID volume, it will be accepted as a local volume.

To activate the RAID volume of the hard disk array:

1. Click **Administration** **Storage Devices** **Hard Disk Array**.
2. Click the name of the hard disk array.
3. Click **Activate RAID-1 Array**.
4. Follow the prompts.

### Initializing the volume

You might need to initialize the RAID volume. This action makes the disks into a RAID volume. This action destroys all content.

To initialize the RAID volume of the hard disk array:

1. Click **Administration** **Storage Devices** **Hard Disk Array**.
2. Click the name of the hard disk array.
3. Click **Initialize RAID-1 Array**.
4. Follow the prompts.

### Rebuilding the volume

You might need to rebuild the RAID volume. This action copies the contents from the primary disk in the array to the secondary disk.

To rebuild the RAID volume of the hard disk array:

1. Click **Administration** **Storage Devices** **Hard Disk Array**.
2. Click the name of the hard disk array.
3. Click **Rebuild RAID-1 Array**.
4. Follow the prompts.

### Deleting the volume

You might need to delete the RAID volume. This action makes the disks that are presently a RAID volume no longer a RAID volume. This action destroys all content, including all metadata.

To delete the RAID volume of the hard disk array:

1. Click **Administration** **Storage Devices** **Hard Disk Array**.
2. Click the name of the hard disk array.
3. Click **Delete RAID-1 Array**.
4. Follow the prompts.

---

## Chapter 15. Managing the configuration of the appliance

This chapter provides information about managing the configuration of the appliance, managing application domains, and importing and exporting configurations.

---

### Managing domains

When initialized, a DataPower appliance has a default domain. The appliance supports the addition of application domains. An *application domain* consists of those resources that are configured to provide and support one or more services.

After an administrator logs in to an application domain, all configuration activities apply to only this application domain. This control provides a level of administrative partitioning and safety. For example, administrators in `domainA` cannot alter services in `domainB`.

If you create or delete an application domain from the command line, existing WebGUI sessions cannot detect this change. Therefore, if you create a new application domain, a WebGUI administrator cannot switch to this application domain. Conversely if you delete an application domain, a WebGUI administrator can switch to this now nonexistent domain.

### The default domain

A number of appliance-wide resources and settings can be defined only in the default domain. The following list contains a subset of the appliance-wide resources that can be set in default domain only:

- Network interfaces
- Users and access controls
- Application domains

After any user enters an application domain, either through logging in or switching domains, that user can no longer access appliance-wide resources. When viewed from the main navigation area, these resources are disabled.

The default domain cannot be deleted.

### Application domains

Application domains can be created in only the default domain.

When configuring an application domain, specific directories in other domains can be made visible.

Administrators can be assigned to specific application domains to allow for greater administrative control. Administrators that are restricted to specific application domains, can perform activities in only those application domains (provided that the administrator has the appropriate access controls). Services defined in one application domain cannot be shared with another application domain.

Application domains can be restarted independently without affecting any other domain and without requiring a restart of the entire appliance. When a domain is

restarted, the persisted configuration file for that domain is used, which might change the running configuration of the domain.

A domain can read its configuration from a locally stored file or from a file that is stored on a remote, central configuration server. The use of a remote configuration file enables centralized management of multiple domains across multiple appliances.

When creating a new application domain from an imported package, refer to “Importing configuration data” on page 156.

## Visible domains

When the default domain or an application domain is made visible during configuration, the domain being configured can see specific directories from the specified visible domains. Being able to see the files in a directory allows resource configurations to be common across application domains.

- When the default domain is made visible, the application domain being configured has read access to the store: directory of the default domain. When viewed through the File Management utility, the directory shows up in the listing as store. By default, the default domain is visible to all application domains. The store: directory contains DataPower-supplied processing resources, such as style sheets, schemas, and files for authentication and authorization.
- When an application domain is made visible, the application domain being configured has read access to the local: directory of the specified application domain. When viewed through the File Management utility, the directory shows up in the listing as the domain name. For example, if domainB is made visible to domainA, the local: directory of domainB would show up as domainB when viewed from domainA.

**Note:** References to visible domains are explicit, not bidirectional. If domainA is made visible to domainB, domainB cannot see domainA. In this case, you cannot make domainA visible to domainB. References to visible domains cannot be circular.

## Creating application domains

To create an application:

1. Click **Administration** **Configuration** **Application Domain**.
2. Click **Add**.
  - a. In the **Name** field, enter the name for the object.
  - b. Set **Administrative State** to identify the administrative state of the configuration.
    - To make inactive, click **disabled**.
    - To make active, click **enabled**.
  - c. Optional: In the **Comments** field, enter a descriptive summary.
  - d. Use the **Visible Domains** controls to select the application domains that this application domain can see.
  - e. Use the **local: File Permissions** check boxes to select the desired file access permissions. These permissions apply to the local: directory of the new application domain.



- f. Use the '**local:**' **File Monitoring** check boxes to select the desired monitoring and logging states for files in the local: directory. Logging and auditing each creates a record of file accesses and activities that can be useful at a later date to determine changes to files.
3. Define the type of domain configuration mode to use.
  - a. Click the **Configuration** tab.
  - b. In the **Configuration Checkpoint Limit** field, specify the maximum number of configuration checkpoints to allow.
  - c. From the **Configuration Mode** list, select the desired configuration mode.
 

**Local** (Default) Reads the domain configuration from a local configuration file.

#### **Import**

Imports the domain configuration from a remote configuration file.

- 1) In the **Import URL** field, specify a URL for the file.
- 2) From the **Import Format** list, select the file format.
- 3) Optional: From the **Deployment Policy** list, select a deployment policy. The package to import is preprocessed before being applied to the configuration file. For more information, refer to Chapter 16, "Deployment policies," on page 163.
- 4) Set **Local IP Rewrite** to indicate whether to allow local IP addresses to be rewritten to match equivalent interfaces on the appliance.
- 5) Click **Apply** to save the changes to the running configuration.
- 6) Optional: Click **Save Config** to save the changes to the startup configuration.

## **Restarting application domains**

You can restart an application domain, including the default domain, without restarting the entire appliance. The application domain is reloaded using the currently saved configuration for the domain. The saved configuration could be different than the running configuration of the domain. If the running configuration of the domain is different than the saved configuration, a notice appears at the top of the screen.

You can restart application domains in one of the following ways:

- From the System Control panel
- From the Application Domain catalog

### **Restarting from the System Control panel**

To restart the current application domain from the System Control panel:

1. Click **Administration** **Main** **System Control**.
2. Locate the **Restart Domain** section.
3. Click **Restart Domain**.
4. Follow the prompts.

### **Restarting from the catalog**

To restart an application domain from the catalog:

1. Click **Administration** **Configuration** **Application Domain**.
2. Click on the name of the domain.
3. Click **Restart Domain**.

4. Follow the prompts.

## Resetting application domains

You can reset an application domain, including the default domain, to delete the configuration of the domain. Resetting a domain is different from deleting and recreating a domain.

- Resetting a domain deletes all configured objects in the domain but retains the configuration of the domain and retains all files in the local directory.
- Deleting a domain deletes all configured objects in the domain, deletes all files in the domain, and deletes the configuration of the domain itself.

You can reset domains in one of the following ways:

- From the System Control pane
- From the Application Domain catalog

### Resetting from the System Control pane

To reset the current application domain from the System Control panel:

1. Click **Administration Main System Control**.
2. Locate the **Reset Domain** section.
3. Click **Reset Domain**.
4. Follow the prompts.

### Resetting from the catalog

To reset an application domain from the catalog:

1. Click **Administration Configuration Application Domain**.
2. Click on the name of the domain.
3. Click **Reset Domain**.
4. Follow the prompts.

## Quiescing application domains

To quiesce an application domain:

1. Click **Administration Configuration Application Domain**.
2. Click on the name of the domain.
3. Click **Quiesce**.
4. Specify the **Timeout** in seconds. The minimum timeout is 60 seconds.
5. Click **Quiesce**.
6. Click **Confirm**.
7. Click **Close**.

## Unquiescing application domains

To unquiesce an application domain and all the associated services and handlers:

1. Click **Administration Configuration Application Domain**.
2. Click on the name of the domain.
3. Click **Unquiesce**.
4. Click **Confirm**.
5. Click **Close**.

---

## Creating Include Configuration File objects

Include Configuration File objects allow you to include configuration information from an external configuration file in the local configuration information. This external file can be stored on a centralized configuration server or another DataPower appliance. The information in the Include Configuration File object is appended to the local configuration information when the configuration of the DataPower appliance is reloaded (such as during appliance reboot, firmware reload, or domain restart).

An Include Configuration File object can include configuration information only. On the other hand, an Import Configuration File object is a configuration package that can include both configuration information and supporting files.

To append configuration information from an external file to the local configuration information:

1. Click **Objects Configuration Management Include Configuration File**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. Specify the URL of the configuration file in the **URL of Configuration File** field. For example, specify `https://config.server.com/datapower/firewalls.cfg`.
7. Set **Execute on Startup** to indicate whether to import the configuration package at startup.

<b>on</b>	(Default) Imports the configuration package at startup. The configuration is marked external and cannot be saved to the startup configuration. This behavior is equivalent to always importing the configuration.
<b>off</b>	Imports the configuration package when manually triggered. The configuration is not marked external and can be saved to the startup configuration. This behavior is equivalent to importing the configuration one time.
8. When retrieving the configuration file, select when to retrieve the configuration file with **Interface Detection**.

<b>on</b>	Retrieves the configuration file after the local interface is up.
<b>off</b>	(Default) Retrieves the configuration file at appliance reload without waiting for the local interface to be up.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

**Note:** Unless you click **Save Config**, the included configuration file will not take affect when the appliance is started.

---

## Creating Import Configuration File objects

Import Configuration File objects allow you to import a configuration package from an external configuration file into the local configuration information. The external file can be stored on a centralized configuration server or another DataPower appliance. The configuration data and files in the configuration file is added to the local configuration information when the configuration of the DataPower appliance is reloaded (such as during appliance reboot, firmware reload, or domain restart). The default configuration of an Import Configuration File object does not provide warnings about conflicts with existing files and objects.

An Import Configuration File object is a configuration package that can include both configuration information and supporting files. On the other hand, an Include Configuration File object can include configuration information only.

To import a configuration package from an external file to the local configuration information, perform the following procedure:

1. Select **Objects** **Configuration Management** **Import Configuration File** to display the catalog.
2. Click the name of an existing configuration package to edit it, or click **Add** to create a new one. The Import Configuration File configuration screen is displayed.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. Specify the URL of the configuration package in the **URL of Configuration Package** field. For example, specify `https://config.server.com/datapower/firewalls.zip`.

**Note:** You cannot use the SCP or SFTP protocol to retrieve a configuration package. All other URL protocols are available; for example, HTTP, HTTPS, or FTP.

7. Select the package format from the **Format of Configuration Package** list.
8. Set **Overwrite Files** to control the overwrite behavior.
9. Set **Overwrite Objects** to control the overwrite behavior.
10. Optional: Select a deployment policy that preprocesses the configuration package from the **Deployment Policy** list. For more information, refer to Chapter 16, “Deployment policies,” on page 163.
11. Set **Local IP Rewrite** to indicate whether to rewrite local IP addresses on import. When rewriting, for example, a service in the configuration package that binds to `eth1` is rewritten to bind to `eth1` when imported.
12. Set **Import on Startup** to indicate whether to import the configuration package at startup.
  - If enabled, the configuration is marked **external** and cannot be saved to the startup configuration. This behavior is equivalent to always importing the configuration.

- If disabled, the configuration is not marked external and can be saved to the startup configuration. This behavior is equivalent to importing the configuration one time.
13. Click **Apply** to save the changes to the running configuration.
  14. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Backing up and exporting configuration data

The backup and export utility copies specified configuration data from the appliance to a file in the export: directory. You can download the file to your workstation.

**Note:** Exported configuration data should not be imported to an appliance with an earlier release level. Between releases, configuration data for properties can change. If you attempt to import configuration data from an appliance of a later release level into an appliance of an earlier release level, the operation might report success, but the configuration data might not be the same. Therefore, use this utility to exchange configuration data among appliances of the same release level.

You can use this utility to perform the following operations:

- Create a backup of the entire appliance
- Create a backup of one or more application domains
- Export select objects from the current domain
- Copy or move select objects between domains

**Note:** The following objects are *never* exported:

- User account objects
- Certificate objects
- Key objects (HSM appliances only)

The following files are *never* exported:

- Log files
- Firmware files

To ensure that all other objects and files are exported, use the `admin` account. On zBX use the `dp-admin` account. For any other user, only objects and files that are accessible to that user are included in the export package.

To start a back up or export operation, select **Administration** **Configuration** **Export Configuration** to display the initial Export Configuration screen. This screen provides the following export options:

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

## Backing up the entire appliance

Use the following procedure to back up (export) all configuration data for the appliance.

1. Select **Administration Configuration Export Configuration** to display the Initial Export Configuration screen.
2. Select **Create a backup of the entire system** and click **Next** to display the File Name screen.
  - a. Optional: In the **Comments** field, enter a descriptive summary.
  - b. Optional: Create or select the name of a Deployment Policy to accept, filter, or modify a configuration during import.
  - c. The **Export File Name** defaults to export (.zip). If a file of this name exists in the export: directory, it is overwritten.
  - d. Click **Next**. The configuration of the entire appliance is backed up. When the backup completes, the file is in the export: directory. You can download this file to your workstation. The Import Configuration utility requires that the export file resides on your workstation.
3. Optional: Click **Download** to download the file to your workstation.
4. Click **Done** to close this window and return to the Control Panel.

The export file can be accessed from the export: directory. If downloaded, the export file is on your workstation.

## Backing up domains

Best practice is to periodically back up all domains individually.

To back up configuration information for one or more application domains, follow this procedure:

1. Select **Administration Configuration Export Configuration** to display the Initial Export Configuration screen.
2. Select **Create a backup of one or more application domains** and click **Next** to display the selection screen.
3. Provide the following inputs:
  - a. Optional: In the **Comments** field, enter a descriptive summary.
  - b. Optional: Create or select the name of a Deployment Policy to accept, filter, or modify a configuration during import.
  - c. The **Export File Name** defaults to export (.zip). If a file of this name exists in the export: directory, it is overwritten.
  - d. Select the check boxes adjacent to each domain to export.
  - e. Click **Next**

When the backup completes, the file is in the export: directory. You can download the export file to your workstation. The Import Configuration utility requires that the export file resides on your workstation.

4. Optional: Click **Download** to download the file to your workstation.
5. Click **Done** to close this window and return to the Control Panel.

The export file can be accessed from the export: directory. If downloaded, the export file is on your workstation.

## Exporting select objects

The Export Configuration utility remains available from the initial Export Configuration screen. To export select objects and files, use the following procedure:

1. Select **Administration** **Configuration** **Export Configuration** to display the Initial Export Configuration screen.
2. Select **Export configuration and files from the current domain** and click **Next** to display the Export Configuration screen.
3. Provide the following inputs:
  - a. Optional: In the **Comments** field, enter a descriptive summary.
  - b. Optional: Create or select the name of a Deployment Policy to accept, filter, or modify a configuration during import.
  - c. The **Export File Name** defaults to export (.xml or .zip depending on the selected export format). If a file of this name exists in the export: directory, it is overwritten.
  - d. Use the **To** radio buttons to specify the export format.

#### **XML Config**

Exports configuration data as XML files. Include Configuration files are referenced in the XML document only, they are not included.

#### **ZIP Bundle**

Exports configuration data in compressed ZIP format. Include Configuration files are in the bundle.

- e. Use the **Configuration** radio button to specify the data to export.

#### **Currently running configuration**

Exports the configuration data from the running configuration, not the startup configuration.

#### **Last persisted configuration**

Exports the configuration data from the startup configuration, not the current running configuration.

- f. Use the **Referenced Objects** radio buttons to specify the scope of the data to export.

#### **Include only the selected base objects**

Exports only the configuration data for the selected objects.

#### **Include all objects required by selected base objects**

Exports configuration data for the selected objects and all objects that are required by the selected objects. For example, if exporting an XSL Proxy, the export includes configuration data for the XSL Proxy, the assigned XML manager, and all associated matching rules, processing policies, processing rules, cryptographic certificates, credentials, and keys.

- g. Use the **Export Files** radio buttons to specify the scope of the data to export.

#### **Export no files**

No files are included in the export. If, for example, the selected objects use files, such as a style sheet, those files are not included. This option is useful when the configuration data itself is all that is needed.

#### **Export files referenced by exported objects**

In addition to the selected objects (and possibly referenced objects), exports *public* files that are associated with the selected objects.

**Note:** The export does not include *private* files. These files are in the cert: and sharedcert: directories.



### Export all local files

Exports *public* files that are associated with the selected objects and all files that are in the following directories:

- config:
- local:
- pubcert:
- store:
- tasktemplates:

- h. From the **Objects** list, select the type or class of configuration data to export.

After selecting an entry, all instances of that type or class are listed in the left-hand box.

- 1) Select the objects from the left-hand list. To select multiple objects, select objects in combination with the Shift and Control keys.
- 2) Click > to move the selected object to the **Selected Base Objects** list.

- i. Adjust the **Selected Base Objects** list, if necessary.

- 1) Select objects in the right-hand list. To select multiple objects, select objects in combination with the Shift and Control keys.
- 2) Click < to remove the selected objects or click << to remove all objects from the **Selected Base Objects** list.

- j. Click **Show Contents** at any time to display all contents marked for inclusion in the export.

- k. Click **Next**.

When the backup completes, the file is in the export: directory. You can download the export file to your workstation. The Import Configuration utility requires that the export file resides on your workstation.

4. Optional: Click **Download** to download the file to your workstation.
5. Click **Done** to close this window and return to the Control Panel.

The export file can be accessed from the export: directory. If downloaded, the export file is on your workstation.

## Copying or moving select objects

The copy or move utility is available from the initial Export Configuration screen. To copy or move selected objects and files, use the following procedure:

1. Select **Administration Configuration Export Configuration** to display the Initial Export Configuration screen.
2. Select **Copy or move configuration and files between domains** and click **Next** to display the Export Configuration screen.
  - a. Optional: Create or select the name of a Deployment Policy to accept, filter, or modify a configuration during import.
  - b. Use **Delete After Export** to indicate whether the operation is a copy or move operation.
    - on** Indicates a move operation.
    - off** Indicates a copy operation.
  - c. Use the **Configuration** radio button to specify the data to export.



**Currently running configuration**

Exports the configuration data from the running configuration, not the startup configuration.

**Last persisted configuration**

Exports the configuration data from the startup configuration, not the current running configuration.

- d. Use the **Referenced Objects** radio buttons to specify the scope of the data to export.

**Include only the selected base objects**

Exports only the configuration data for the selected objects.

**Include all objects required by selected base objects**

Exports configuration data for the selected objects and all objects that are required by the selected objects. For example, if exporting an XSL Proxy, the export includes configuration data for the XSL Proxy, the assigned XML manager, and all associated matching rules, processing policies, processing rules, cryptographic certificates, credentials, and keys.

- e. Use the **Export Files** radio buttons to specify the scope of the data to export.

**Export no files**

No files are included in the export. If, for example, the selected objects use files, such as a style sheet, those files are not included. This option is useful when the configuration data itself is all that is needed.

**Export files referenced by exported objects**

In addition to the selected objects (and possibly referenced objects), exports *public* files that are associated with the selected objects.

**Note:** The export does not include *private* files. These files are in the *cert:* and *sharedcert:* directories.

**Export all local files**

Exports *public* files associated with the selected objects and all files contained in the following directories:

- config:
- image:
- pubcert:
- store:
- tasktemplates:

- f. From the **Objects** list, select the type or class of configuration data to export. After selecting an entry, all instances of that type or class are listed in the left-hand box.
- 1) Select the objects from the left-hand list. To select multiple objects, select objects in combination with the Shift and Control keys.
  - 2) Click the > button to move the selected objects to the **Selected Base Objects** list.
- g. Adjust the **Selected Base Objects** list, if necessary.
- 1) Select objects in the right-hand list. To select multiple objects, select objects in combination with the Shift and Control keys.

- 2) Click **<** to remove the selected objects or click **<<** to remove all objects from the **Selected Base Objects** list.
3. Click **Show Contents** at any time to display all contents marked for inclusion in the export.
4. Click **Next** to display the Import File window.
  - a. From the **Domain** list, select the domain where the configuration data is to be imported.
  - b. Click **Import** to initiate file transfer.
5. Respond to WebGUI prompts.
6. Click **Done** to close the Import File screen.

---

## Managing configuration checkpoints

A configuration checkpoint contains configuration data from a specific point in time. The configuration checkpoint might be equivalent to the persistent configuration, might be equivalent to the running configuration, or might be different from the persisted configuration or running configuration.

Within each application domain, the administrator who is associated with the **admin** account defines the number of configuration checkpoints to allow. You can save up to the allowed number of configuration checkpoints.

On zBX, the configuration checkpoint data is not configurable. None of the administrative accounts for zBX have the necessary permissions to alter these settings.

When saved, a ZIP formatted file for the configuration checkpoint is written to the `chkpoints:` directory for that application domain. During an upgrade, the operation deletes the contents of this directory.

## Defining number configuration checkpoints to allow

The administrator who is associated with the **admin** account can define the number of checkpoint configurations to allow for each application domain.

On zBX, the configuration checkpoint data is read-only. None of the administrative accounts for zBX have the necessary permissions to alter these settings. The options on this page are disabled.

To define the number of checkpoint to allow for an application domain:

1. Click **Administration Configuration Application Domain**.
2. Click the specific application domain.
3. Click the **Configuration** tab.
4. In the **Configuration Checkpoint Limit** field, specify the number of checkpoint configuration to allow.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

## Saving configuration checkpoints

Do not click **Save Config** to save a configuration checkpoint. This button does not allow you the option of saving a configuration checkpoint.

To save a configuration checkpoint:

1. Click **Administration Configuration Configuration Checkpoints**.
2. In the **Checkpoint Name** field, specify the name of the configuration checkpoint.
3. Click **Save Checkpoint**.
4. Respond to prompts.

A ZIP-formatted configuration file of the specified name is written to the `chkpoints:` directory. During an upgrade, the operation deletes the contents of this directory.

You cannot overwrite a configuration checkpoint. You must first delete the original configuration checkpoint before saving a new configuration checkpoint of the same name. For details, see “Deleting configuration checkpoints.”

## Listing configuration checkpoints

You can view the list of saved configuration checkpoint in one of the following ways:

- From the Configuration Checkpoints screen
- From the File Management screen

### Listing from the Configuration Checkpoints screen

To view from the Configuration Checkpoints screen, click **Administration Configuration Configuration Checkpoints**. This screen displays the list of saved configuration checkpoints at the time by name and timestamp.

This section of the screen provides the following actions:

#### Rollback

Loads the configuration that is defined in the configuration checkpoint.

#### Remove

Deletes the checkpoint configuration from the `chkpoints:` directory.

#### Compare

Launches the Compare Configuration utility. For details, see “Comparing configurations” on page 158.

### Listing from the File Management utility

To view from the File Management utility:

1. Select the **File Management** icon from the Control Panel.
2. Expand the `chkpoints:` directory.

## Rolling back to a configuration checkpoint

To load the configuration that is defined in the configuration checkpoint:

1. Click **Administration Configuration Configuration Checkpoints**.
2. Click the checkpoint to which to roll back.
3. Click **Rollback**.
4. Respond to prompts.

## Deleting configuration checkpoints

You can delete configuration checkpoints in one of the following ways:

- From the Configuration Checkpoints screen
- From the File Management screen

## Deleting from the Configuration Checkpoints screen

To delete from the Configuration Checkpoints screen:

1. Click **Administration** **Configuration** **Configuration Checkpoints**.
2. Click the checkpoint to delete.
3. Click **Remove**.
4. Respond to prompts.

## Deleting from the File Management screen

To delete from the File Management screen:

1. Click the **File Management** icon from the Control Panel.
2. Expand the checkpoints: directory.
3. Select the check box beside the checkpoint file.
4. Click **Delete**.
5. Respond to prompts.

---

## Importing configuration data

The import utility copies specified configuration data from your workstation to the DataPower appliance.

**Note:** Exported configuration data should not be imported to an appliance with an earlier release level. Between releases, configuration data for properties can change. If you attempt to import configuration data from an appliance of a later release level into an appliance of an earlier release level, the operation might report success, but the configuration data might not be the same. Therefore, use this utility to exchange configuration data among appliances of the same release level.

While importing a configuration, you can:

- Set the local address bindings of services contained in the export package to match the equivalent interfaces of the local device with **Rewrite Local Service Addresses** (optional).
- Add, modify or delete values in the configuration package being imported whose values match the defined matching statement in a deployment policy with the **Use Deployment Policy** list (optional).

Best practice when the goal is to add, modify or delete values in a configuration package is to use a deployment policy while importing the configuration package.

To import configuration data:

1. Click **Administration** **Configuration** **Import Configuration**.
  - a. Use the **From** radio buttons to specify the import format.

### XML Config

Imports configuration data as XML files.

### ZIP Bundle

Imports configuration data in compressed ZIP format.

- b. Retain the selection of the **File** radio button.
- c. Click **Browse** to select the file to import.
- d. Retain the selection of (none) for the **Use Deployment Policy** list. For more information, refer to the Chapter 16, "Deployment policies," on page 163.

- e. Set **Rewrite Local Service Addresses** to control whether to substitute IP addresses:
2. Click **Next** to display the Select Application Domains for Import window. If there are no objects in the configuration you are importing, skip to step 6c. When importing from any domain other than default, the imported configuration applies only to the current domain. The WebGUI might display an error message when importing data that was exported from the default domain.
3. Select the desired domains. To select all domains, click **All**. To deselect selected domains, click **None**. If a selected domain does not exist on the appliance, as indicated, it will be created.
4. Click **Next** to display the Import Object Selection List window.
5. Select the objects to import.

**Note:** Click **Save Config** to save the configuration for each domain that contains imported objects or files.

To effectively complete an appliance import (restore), use the `admin` account or `dp-admin` account on zBX. The appliance to be restored must also first be re-initialized through the command line.

6. Click **Next** to display the Import Summary window, which details the contents of the target file. In some cases, the summary might indicate differences in file versions.

**Note:** Warnings can appear on this screen that alert you to a range of possible conflicts that the imported configuration might cause. Depending on the warning, you might want to create a new application domain, or you might want to choose not to overwrite objects or files.

- a. Select each item to overwrite. To select all item, click **All**. To deselect selected items, click **None**. Only selected items are imported.
- b. Click **Import** to initiate file transfer.

At the completion of the import process, the WebGUI displays the Object Import Results window, which details the results.

- c. Click **Done** to close this window.

If more than one domain is being imported, the Import Summary window is displayed for the next domain to import.

---

## Managing changes in configuration data

You can create a report that lists the differences between two configurations. Generally, the two configurations that are being compared are the persisted configuration and the running configuration. However, you can compare either configuration to a saved version of the configuration. These saved versions of the configuration can be an exported configuration (XML format or ZIP format), a backup configuration (ZIP format only), or a configuration checkpoint.

When you compare configurations, the report provides a list of objects that changed between the two configurations and the changes that were made to these objects. The report lists how the configuration changed:

- An object was added
- An object was deleted
- An object was modified

## Comparing configurations

To compare configurations, use the following procedure:

1. Select **Administration Configuration Compare Configuration** to display the Configuration Comparison screen.
2. From the **From** list, select which configuration to be the first configuration source; and from the **To** list, select which configuration to be the second configuration source. The source for each of the configurations can be one of the following:

### **Persisted Configuration**

The last saved configuration on the appliance. This is the default in the **From** list.

### **Running Configuration**

The configuration that is currently running on the appliance. This is the default in the **To** list.

### **Domain Configuration**

The last saved or currently running domain configuration on the appliance.

### **XML Configuration**

The XML file that was created during an export operation. This file has an .xcfg extension.

### **Export ZIP Bundle**

A ZIP file that was created during an export operation. This file has a .zip extension.

### **Backup ZIP Bundle**

A ZIP file that was created during backup operation. This file has a .zip extension.

### **Checkpoint**

A ZIP file that was created through a save checkpoint operation. This file has a .zip extension and is in the chkpoint: directory.

3. When the source (**From** or **To**) is **XML Configuration**, **Export ZIP Bundle**, or **Backup ZIP Bundle**, specify or browse for and select the configuration file. Also, create or select a deployment **Policy** that can be used to accept, filter, or modify a configuration.
4. When the source (**From** or **To**) is **Checkpoint**, select the checkpoint from the **Checkpoint** list.
5. From the **View** list, select whether the report lists only changed objects between the configurations or all objects in the configurations. The default is changed objects only.
6. Click **Run Comparison** to generate the report.

The results are displayed below the horizontal rule.

## Reading the change report

After running a comparison, the results are displayed below the horizontal rule. Review the report to determine whether these changes should be saved to the startup configuration, reverted to their original settings, saved to a configuration checkpoint, or a combination of these operations.

Each item in the report contains the following data:

<b>Type</b>	The object type
<b>Name</b>	The name of the object
<b>Property</b>	The name of the property
<b>From</b>	The value of the property as defined in the <b>From</b> source
<b>To</b>	The value of the property as defined in the <b>To</b> source
<b>Change</b>	The type of change between the <b>From</b> source and the <b>To</b> source. The change is one of the following values: <ul style="list-style-type: none"> <li>• <b>modified</b></li> <li>• <b>added</b></li> <li>• <b>deleted</b></li> </ul>

Beside each item is a check box.

## Reverting changes

After running a comparison and reviewing the results, you can revert select changes or all changes between the two configurations. You can revert changes at the property level only. To revert changes to select properties for an object, use the object-specific configuration screens.

To revert changes, use the following procedures:

1. Determine which objects to revert:
  - To revert select objects, select the check box beside those objects.
  - To revert all objects, click **Select All**.
2. Click **Undo Selected**.

The results are displayed on a new screen.

If a selected object is a referenced object, it cannot be deleted until after the deletion of its parent object. You might need to run the comparison multiple times to delete referenced objects. For example, you cannot delete certificates that are referenced by a validation credentials list until after the deletion of the validation credentials list itself.

---

## Managing disaster recovery

On a DataPower appliance, disaster recovery is the ability to create a secure backup that you can use to recover the complete configuration of a lost appliance. Disaster recovery uses a backup-restore process.

**Note:** Disaster recovery is available only if you enabled disaster recovery mode during the initial firmware setup of the appliance. If not enabled, you must reinitialize the appliance with the **reinitialize** command and enable disaster recovery. To determine if disaster recovery is available, click **Administration Device System Settings**. If the Backup Mode property is set to Secure, disaster recovery is available.

The backup-restore process must be used among appliances that are at the same firmware level and have the same compatible configuration (auxiliary storage, iSCSI, and so forth).

Unlike a standard backup, a secure backup contains private data from the appliance (certificates, keys, and user data), which the appliance encrypts with a customer-provided certificate and a DataPower certificate. The backup also contains an unencrypted XML manifest file, which includes information such as the date of the backup and the firmware level, model, and serial number of the backed-up appliance. You cannot view the encrypted private data, but you can view the unencrypted manifest file.

You can refer to the manifest files of multiple backups to determine which backup you want to restore. For example, you can identify which backup has an applicable firmware level. You can also use this information during the restore process to validate that a specific backup can be restored on an appliance.

A secure backup does not back up data that is on the HSM.

You can use the backup-restore process during the end-of-life migration to move configuration details from one appliance to another.

## Contents of a secure backup

A secure backup creates the `backupmanifest.xml` manifest file and some or all of the following files:

- `root.tgz`
- `store.tgz`
- `config.tgz`
- `local.tgz`
- `cert.tgz`
- `dpcert.tgz`
- `sharedcert.tgz`
- `chkpoints.tgz`
- `raid-volume.tgz`
- `compact-flash.tgz`
- `iscsi-value.tgz`

## Conditions

Several general conditions apply to the secure backup-restore process. Some additional conditions apply specifically to a secure backup, and some additional conditions apply specifically to a secure restore.

### General conditions for a secure backup-restore

The following general conditions apply to a secure backup-restore:

- You must use the backup-restore process among appliances that are at the same firmware level and have the same configuration (auxiliary storage, iSCSI, and so forth).
- You can use a single backup to restore all appliances for an environment that has multiple appliances. When the restore is complete, you must resolve any differences, such as IP addresses, among the appliances.
- Protect the backup files in the same way that you protect all other critical data. Although encrypted, these files contain certificates, keys, and user data that might be of interest to an attacker.



- If possible, use methods other than the backup-restore process to back up iSCSI and RAID data because backing up this data can require a significant amount of time.
- Each backup applies only to a specific firmware release. Therefore, perform a secure backup after each firmware upgrade.

### Conditions for a secure backup

The following conditions apply to a secure backup:

- You must not make local configuration changes while you are performing a secure backup.
- You can back up only locally persisted startup configurations.
- You can specify a remote or local destination for the backup. If local, use a protocol such as Secure Copy (SCP) to copy the backup to a remote directory.

### Conditions for a secure restore

The following conditions apply to a secure restore:

- The restore process reboots the appliance. Therefore, stop any work that is currently running on the appliance before you begin a restore.
- After you begin a secure restore, you cannot recover any existing data on the appliance.

## Creating a secure backup of the appliance

To create a secure back up the appliance configuration:

1. Click **Administration** **Main** **System Control**.
2. Locate the **Secure Backup** section.
3. From the **Crypto certificate** list, select the certificate to encrypt the secure backup.
4. In the **Destination** field, enter the URL of the target directory for the backup files.
5. Optional: For **Include iSCSI**, specify whether to back up iSCSI data.
6. Optional: For **Include RAID**, specify whether to back up RAID data.
7. Click **Secure Backup**.
8. When prompted, click **Confirm**.

## Restoring the appliance from a secure backup

### CAUTION:

**A secure restore does not merge data. The restore deletes all private data (certificates, keys, and user data) that is currently on the target appliance.**

To restore the appliance configuration from a secure backup:

1. Click **Administration** **Main** **System Control**.
2. Locate the **Secure Restore** section.
3. From the **Crypto credentials** list, select the identification credentials to decrypt the backup.
4. In the **Source** field, enter the URL of the source directory that contains the backup files.
5. Click **Secure Restore**.
6. When prompted, click **Confirm**.

To ensure appliance security, use the **admin** account (dp-admin on zBX) account to log in to the appliance, and change the password when prompted.

## Validating a secure backup

To validate a secure backup:

1. Click **Administration** **Main** **System Control**.
2. Locate the **Secure Restore** section.
3. From the **Crypto credentials** list, select the credentials to decrypt the backup.
4. In the **Source** field, enter the URL of the source directory that contains the backup files.
5. Set **Only validate the backup** to indicate that you want to only validate the backup files, not perform a restore.
6. Click **Secure Restore**.
7. When prompted, click **Confirm**.

---

## Chapter 16. Deployment policies

Deployment policies use fine-grained matching statements and clause types to control the inclusion of configuration data from imported configuration packages.

Depending on the clause type, the deployment policy can perform the follow types configuration management against the imported configuration package:

- Use an *accepted configuration* to include resources in the package that match specified criteria.
- Use a *filtered configuration* to delete resources in the package that match specified criteria.
- Use a *modified configuration* to modify resources in the package that match the specified criteria. Modified configurations support the following actions:

**Add** Adds the property with the identified value during the import.

**Changed**

Substitutes the value for the identified property during the import.

**Deleted**

Deletes the property during the import.

The processing sequence is as follows:

1. Process the accepted configuration, the *whitelist*, to always include resources that match.
2. Process the filtered configuration, the *blacklist*, to always delete resources that match.
3. Process the modified configuration to change the resources based on the defined action type.

---

### Creating deployment policies

A deployment policy is a sequence of accepted, filtered, and modified configurations that respectively include, delete, or change configuration data in the configuration package during the import. When specifying the matching statement, you can use the builder or manually specify the statement.

- For details about using the builder to define the statement, refer to “Using the deployment policy builder” on page 164.
- For details about manually specifying the statement, refer to “Specifying the matching statement” on page 165.

**Note:** You cannot modify the administrative state of a deployment policy.

To create a deployment policy:

1. Click **Objects Configuration Management Deployment Policy**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. Optional: In the **Comments** field, enter a descriptive summary.
5. Define accept clauses.
  - a. Specify the matching statement in the **Accepted Configuration** field, or click **Build**.

- b. Click **Add**.  
Repeat this step to define another accept clause.
6. Define filter clauses.
  - a. Specify the matching statement in the **Filtered Configuration** field, or click **Build**.
  - b. Click **Add**.  
Repeat this step to define another filter clause.
7. Define modify clauses on the **Modified Configuration** tab.
  - a. Click **Add** to display the Modified Configuration property window.
  - b. Specify the matching statement for the modify clause in the **Configuration Match** field, or click **Build**.
  - c. Select the type of configuration modification from the **Modification Type** list.
 

**Add Configuration**  
Adds a configuration setting.

**Delete Configuration**  
Deletes a configuration setting.

**Change Configuration**  
Changes a configuration setting.
  - d. If adding a configuration, specify the name of the property to add in the **Configuration Property** field.
  - e. If adding or changing a configuration, specify the value of the property to add or modify in the **Configuration Value** field.
  - f. Click **Save** to return to the configuration screen.  
Repeat this step to define another modify clause.
8. Click **Apply** to save the changes to the running configuration.
9. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Using the deployment policy builder

Deployment policies include a builder to help create matching statements in the following format:

```
address/domain/resource[?Name=resource-name
&Property=property-name&Value=property-value]
```

To access the builder, click **Build**. This button is associated with the following properties:

- **Accepted Configuration** on the **Main** tab
- **Filtered Configuration** on the **Main** tab
- **Configuration Match** in the properties Window that the WebGUI displays after clicking **Add** on the **Modified Configuration** tab

To create a matching statement with the builder, use the following procedure:

1. Click **Build** to open the builder.
2. Specify the IP address or host alias in the **Device Address** field. The value \* matches all IP addresses.
3. Select the name of the application domain from the **Application Domain** list. The selection **(none)** matches all domains.

4. Select the resource type from the **Resource Type** list. The select (**all resources**) matches all resource types.
5. Optional: In the **Name Match (PCRE)** field, specify a name match for a resource. This property limits the matching statement to resources of the specified name. Use a PCRE to select groups of resource instances. For example, `foo*` would match all resources with names that start with `foo`.
6. Optional: From the **Configuration Property** list, select the name of the configuration property. This property limits the matching statement to resources of the specified property.
7. Optional: In the **Configuration Value Match (PCRE)** field, specify the value for the configuration property. This property limits the matching statement to resources of the specified value. Use a PCRE Match Expression to select groups of configuration property values.
8. Click **Save**.

The statement is added to the list of matching statements.

---

## Specifying the matching statement

Instead of using the builder, you can manually specify the matching statement. Matching statements have the following format:

```
address/domain/resource[?Name=resource-name  
&Property=property-name&Value=property-value]
```

*address*

Specifies the IP address or host alias. The value `*` matches all IP addresses.

*domain* Specifies the name of the application domain. The value `*` matches all domains.

*resource*

Specifies the resource type. The value `*` matches all resource types.

*Name=resource-name*

Optionally specifies a name match for a resource. This property limits the matching statement to resources of the specified name. Use a PCRE to select groups of resource instances. For example, `foo*` would match all resources with names that start with `foo`.

*Property=property-name*

Optionally specifies the name of the configuration property. This property limits the matching statement to resources of the specified property.

*Value=property-value*

Optionally specifies the value for the configuration property. This property limits the matching statement to resources of the specified property.

PCRE documentation is available at the following Web site:

<http://www.pcre.org>



---

## Chapter 17. Managing event logs

Log targets are for event logging, not transaction logging. Log targets capture events in the following situations:

- During the processing of messages through a processing policy.
- Because of some internal process or hardware status change.

**Note:** To implement transaction logging, use a log action in a processing policy.

Different types of log targets might include one or more of the following capabilities:

- Archive files through rotation or upload
- Encrypt and sign files or messages
- Forward messages to remote servers

---

### Types of log targets

The following types of log targets are available:

**Cache** Writes log entries to memory.

#### Console

Writes log entries to the screen when using Telnet, SSH, the KVM switch infrastructure of the BladeCenter, or command line access through a serial connection.

**File** Writes log entries to a file on the appliance. This file can be archived using the rotate or upload method. The file can be sent as e-mail. The entire file can be encrypted and signed.

Depending on the machine type, the supported location can differ.

#### Type 7993 (9003)

Supports the local file system.

#### Type 9235

Supports the local file system and the model-specific, auxiliary data storage (compact flash or hard disk array).

#### Type 4195

Supports the local file system and auxiliary data storage (hard disk array).

**NFS** Writes log entries to a file on a remote NFS server. The file can be archived using the rotate or upload method. The file can be sent as e-mail. The entire file can be encrypted and signed. The processing rate can be limited.

**SMTP** Forwards log entries as e-mail to configured addresses. Log content can be encrypted or signed before sending. The processing rate can be limited.

#### SNMP

Forwards log entries as SNMP traps issued to all configured recipients. The processing rate can be limited.

**SOAP** Forwards log entries as SOAP messages. The URL can be set. The processing rate can be limited.

Ti-1.2TDs33bpoib The is mo009.9 lay



3. Define the properties of the log target. Each type of log target provides different configuration properties. For information about the properties, see the online help.
4. Optional: Define event filters. See “Setting event filters” for details.
5. Optional: Define object filters. See “Setting object filters” for details.
6. Optional: Define event triggers. See “Setting event triggers” on page 170 for details.
7. Optional: Define IP address filters. See “Setting IP address filters” on page 171 for details.
8. Define event subscriptions. See “Setting event subscriptions” on page 171 for details.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Setting event filters

You can create filters for the log target based on event codes.

- An *event subscription filter* allows only those messages that contain the configured event codes to be written to this log target. With this filter, you can create a log target that collects only log messages for a specific set of event codes.
- An *event suppression filter* suppresses those messages that contain the configured event codes to be written to this log target. With this filter, you can create a log target that collects a wide range of log messages except for a specific set of event codes.

To set an event filter:

1. Click **Administration** **Miscellaneous** **Manage Log Targets**.
2. Click the name of the log target to modify.
3. Click the **Event Filters** tab.
4. Set event codes with one of the following methods:
  - Enter specific event codes:
    - a. In the **Event Code** field beside the **Add** button, enter a valid event code.
    - b. Click **Add**.
  - Select specific event codes for the available list:
    - a. Click **Select Code**.
    - b. Click **Select** that corresponds with the desired event code.
    - c. Click **Add**.

Click **Help** for information about the event code.

The log target still requires at least one event subscription. The subscription can be set to all. See “Setting event subscriptions” on page 171 for details.

---

## Setting object filters

You can use the Object Filters pane to create object filters for log targets. Object filters allow only those log messages for specific objects to be written to this log target. Object filters are based on object classes. With this filter, you can create a log target that collects only log messages for specific object classes. You can further restrict the filter to particular instances of these classes.

To define an object filter:

1. Click **Administration** **Miscellaneous** **Manage Log Targets**.
2. Click the name of the log target to modify.
3. Click the **Object Filters** tab.
4. Click the name of an existing object filter to edit it, or click **Add** to create a new object filter.
5. Define the object filter:
  - a. From the **Object Type** list, select an object type. This filter restricts messages to only those messages that are generated by the selected object type.
  - b. In the **Object Name** field, enter the name of an existing instance of the selected object type.
  - c. Set **Add Referenced Objects** to indicate whether to log messages for objects that the selected instance references.

**on**      Logs messages for all objects that the selected instance references.

**off**      (Default) Logs messages for only the selected instance.
  - d. Click **Save**.

---

## Setting event triggers

You can use the event triggers to automatically run commands when specific messages are logged. Typical usage would be to generate an error report when a rarely observed but recurring message is logged.

To define an event trigger:

1. Click **Administration** **Miscellaneous** **Manage Log Targets**.
2. Click the name of the log target to modify.
3. Click the **Event triggers** tab.
4. Click the name of an existing event trigger to edit it, or click **Add** to create a new event trigger.
5. Define the event trigger:
  - a. In the **Message ID** field, enter the ID of the message that will trigger the command. You can obtain the ID for specific messages from the WebGUI control panel. Click **View Logs**, messages are described in the **message** column and the associated ID is found in the **msgid** column.
  - b. In the **Regular Expression** field, optionally enter a regular expression that, when specified, must match the log message in order to trigger the CLI command.
  - c. In the **Only Once** field, indicate whether the command should be triggered each time the trigger conditions are met, or only the first time.
    - On - the command is triggered only the first time the conditions are met.
    - Off (Default) - the command is triggered each time the conditions are met.
  - d. In the **Only this Trigger** field, indicate whether other commands that would be triggered by the same condition should be processed or not.
    - on (Default) - other commands that would be triggered by the same conditions will not be processed.
    - off - other commands that would be triggered by the same conditions will process as normal.

- e. In the **CLI command** field enter a command to run when the trigger conditions are met.
- f. Click **Save**.

When an event is triggered the triggering message is logged as usual and the next entry in the log will be the triggered command. This second log entry will be prefaced with the words "Event Trigger command".

To keep track of which event triggers have run you can configure a custom log target that subscribes only to the message ID of the triggered commands. The triggered commands are logged at the "notice" level, ensure that you set the log level to "notice". See "Configuring log targets" on page 168 for details.

See "Scenario: Defining event triggers" on page 175 for examples of how to define event triggers.

---

## Setting IP address filters

You can use the IP Address Filters page to create IP address filters for log targets. IP address filters allow only those log messages from specific IP addresses to be written to this log target.

To define an IP address filter:

1. Click **Administration** **Miscellaneous** **Manage Log Targets**.
2. Click the name of the log target to modify.
3. Click the **IP Address Filters** tab.
4. Click **Add**.
5. Add an IP address:
  - a. In the **IP Address** field, enter an IP address. This filter restricts messages to those that the selected IP address generates.
  - b. Click **Apply**.
6. Repeat the previous step to add another IP address.

---

## Setting event subscriptions

You can subscribe the current log target to particular event categories. Some example categories include:

**auth**    Authorization events  
**mgmt**    Configuration management events  
**xslt**    XSLT processing events

For each event category chosen (including the **all** category), you can establish a priority level which must be met before the log message will be captured by the current log target.

**Note:** To allow the target to capture messages, at least one event subscription must be configured, which can be for "all" events. If no event subscriptions are set, no events are included by default.

1. Click the **Event Subscriptions** tab.
2. Click the name of a pre-configured subscription, or click **Add**.
3. Provide the following information.

### Event Category

Select one event category. Refer to “Configuring log categories” on page 168 for more information.

### Minimum Event Priority

Select a minimum event priority. The priorities are hierarchical; the lowest is listed last.

It is possible to generate custom events by creating a style sheet that uses the DataPower-specific version of the `<xsl:message>` extension element. For example:

```
<xsl:message dp:type="custom"></xsl:message>
<xsl:message dp:type="custom" dp:priority="error"></xsl:message>
```

The first entry is treated as an information-level message. The second entry is treated as an error-level message. For additional information on this extension element, refer to the *IBM WebSphere DataPower SOA Appliances: Extension Elements and Functions Catalog*.

4. Click **Submit**.
5. Create as many event subscriptions as desired by clicking **Add**.
6. Click **Apply** to save the changes to the running configuration.
7. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Viewing logs

You can view the default log and any log target on the appliance if it has the following configuration:

- Type of file or cache; not console, NFS, SMTP, SNMP, SOAP, syslog, or syslog-ng
- Format of XML; not CBE, CSV, raw, or text.

**Note:** To view plain text files, display the file with the file management utility.

To view XML log files:

1. From the control panel, click the **View Logs** icon.
2. Optional: Filter messages based on log target, domain, log category, and severity.

Alternatively, click **Status** **View Logs** **System Logs**.

## Filtering logs

While viewing the default log, you can control which messages to view.

To filter messages:

1. From the **Target** list, select which XML based, file or cache log target to view.
2. From the **Filter** lists, select how to filter the messages. You can filter based on the following criteria:
  - From the first list, select the domain (available in only the default domain)
  - From the second list, select the log category
  - From the third list, select the message level

## Understanding logs

The log file is displayed as a table. Each row of the table represents an event. The columns of the table provide detailed information about that event. The columns are described below:

**time** The time at which this event occurred. By default the logged events are sorted by time, most recent first.

**category**

Events are categorized so that you can easily find events that you are interested in. There are predefined categories but you can also add custom log categories. For a complete list of predefined categories, click **Objects**, **Logging Configuration**, and then click **Log Category**.

**level** The message level provides an indication of the importance of the event. You can configure the logging so that only events with a certain message level are recorded.

**domain** (available in only the default domain)

Reports the domain with which the event is associated. Messages associated with the default domain do not contain this value.

**transaction ID**

The transaction ID of the event if applicable. Multiple events can be associated with a single transaction ID.

**direction**

Direction of the message in a request-response message sequence. The table cannot be sorted by direction. Possible values for this column are:

**request**

A request transaction.

**response**

A response transaction.

**error** An error occurred during transaction processing.

**health** A status check within load-balancing groups.

**scheduled**

A scheduled processing rule for an XML manager.

**call** A scheduled processing rule for an XML manager that uses the *call* action.

**no value**

A message that is not part of a request-response message sequence.

**client** The client IP address that submitted the request.

**message ID**

A message ID that identifies the event. Multiple events can share the same message ID.

**message**

A short description of the event. This entry is a link which can be followed to obtain more information about the event, including suggestions for dealing with any problems. The table cannot be sorted by the message.

When viewing the log file you can sort the messages by clicking on the relevant column header.

Messages from the same transaction or service will have the same tid value. Thus to search for errors associated with a certain service:

1. Examine the log to identify the tid value for the service.
2. Filter the log by this tid value. The resulting subset of the log messages contains only those messages relevant to the service in question.
3. Sort the messages by level. The more important messages are listed at the top.
4. When you have identified the relevant log message, click on the message for more information.

---

## Configuring an e-mail pager

The DataPower appliance provides a wizard to help you create an SMTP log target (pager) that sends e-mail to a configured address. The e-mail contains all critical log events.

To use the wizard to create this type of log target:

1. Click **Administration** **Miscellaneous** **New E-mail Pager**.
2. Optional: Adjust the log target name.
3. Optional: Adjust the summary comment.
4. Click **Next** to continue.
5. Enter the e-mail address to send the log messages.
6. Enter the IP address or domain name of the e-mail relay server in your network.
7. Click **Next** to continue.
8. Click **Commit** to create the log target.
9. Click **Done** to exit.
10. Optional: Click **Again** to create another e-mail pager.

Results: Click **Administration** **Miscellaneous** **Manage Log Targets**. The catalog lists the SMTP log target.

To test the log target:

1. From the Control Panel, click the **Troubleshooting** icon.
2. On the Troubleshooting page, generate a critical log event.
3. Log in to the e-mail account and verify receipt of the message.

---

## Scenario: Defining a load Balancer as a log target

The following scenario explains how to use a load balancer as the static target for a TCP-based, network log target. This scenario creates new objects and provides information about only the configuration that is required for load balancing. However, you can modify existing objects.

1. Create the syslog-group Load Balancer Group and define syslog-1 and syslog-2 as members that reference the actual servers.

The configuration of a DataPower service defines the default port on the backend servers. You can override the default server port for one or more members with the **Mapped Server Port** property.

2. Modify the default XML Manager by adding the syslog-group group to the **Load Balancer Groups** list.

3. Create a Log Target, for example the allSyslogMessages Log Target, and specify syslog-group (the Load Balancer Group object) as the host in the **Remote Host** field. Refer to “Configuring log targets” on page 168 for more information.

## Scenario: Defining event triggers

The following scenarios explain how to define event triggers for a variety of situations.

- Starting and stopping a packet capture.
- Creating an error report when a discrete service encounters a problem.
- Using a custom message

### Starting and stopping a package capture

This scenario uses an event triggers to control a packet capture. Set **Only Once** to **on**, so that multiple packet captures are not launched. A second event trigger, using the same message identifier, stops the packet capture. In this case, set **Only this Trigger** to **on** for the first event trigger, otherwise the command to stop the packet capture is immediately triggered by the same message that started the packet capture. Table 5 lists the configuration for the first event trigger, and Table 6 lists the configuration for the second trigger.

Table 5. Settings to start the packet capture

Property	Value
Message ID	0x999999
Only Once	on
Only this Trigger	on
CLI command	interface eth0; packet-capture temporary:///capture -1 250

Table 6. Settings to stop the packet capture

Property	Value
Message ID	0x999999
Only Once	on
Only this Trigger	on
CLI command	interface eth0; stop-processing "no packet-capture temporary:///capture

### Creating an error report

This scenario creates an error report when a discrete service encounters a problem. The service is identified by its class or name in the regular expression field. Table 7 lists the configuration for this event trigger.

Table 7. Settings to create an error report

Property	Value
Message ID	0x80400036
Regular Expression	throttle
Only Once	off
Only this Trigger	on

Table 7. Settings to create an error report (continued)

Property	Value
CLI command	save error-report

## Using a custom message

This scenario uses a custom message to trigger an event. When you manually create a log entry, it does not have an assigned message identifier. Therefore, you cannot use these log entries cannot to trigger events. However, you can create a custom message with a message identifier with the `xsl:message` extension element. To define this element, define the following attributes for the custom message:

- `dp:type` — The user-defined attribute that indicates the custom log category
- `dp:priority` — The priority level of the message
- `dp:id` — The identifier of the resultant message.

A message identifier is provided for your use. This identifier is referenced by the `$DPLOG_XSLT_USER_CUSTOM` constant. Assign only this value to the `dp:id` attribute. The following fragment defines a custom message:

```
<xsl:message dp:type="my_concern" dp:priority="debug"
  dp:id="$DPLOG_XSLT_USER_CUSTOM" >
  I need to trigger an event.
</xsl:message>
```

When you have created a custom message in this way, you can then set an event trigger on this message identifier. Table 8 lists the configuration for this event trigger.

Table 8. Settings to use a custom message

Property	Value
Message ID	value_of_\$DPLOG_XSLT_USER_CUSTOM
Only Once	off
Only this Trigger	on
CLI command	save error-report

The value of `value_of_$DPLOG_XSLT_USER_CUSTOM` for the **Message ID** field is the value of the provided constant.

You are constrained to this message identifier for all custom messages. However you can use the content of the custom message in the **Regular Expression** field of the event filter to set different triggers for different custom messages. For example you can define the following different custom messages:

```
<xsl:message dp:type="my_concern" dp:priority="debug"
  dp:id="$DPLOG_XSLT_USER_CUSTOM" >
  I need to trigger event1.
</xsl:message>
<xsl:message dp:type="my_concern" dp:priority="debug"
  dp:id="$DPLOG_XSLT_USER_CUSTOM" >
  I need to trigger event2.
</xsl:message>
```

These messages will have the same message identifier, but can be distinguished by the value of the **Regular Expression** field. Table 9 on page 177 lists the



configuration for the first custom message, and Table 10 lists the configuration for the second custom message.

*Table 9. Settings for the first custom message*

Property	Value
Message ID	value_of_\$DPL0G_XSLT_USER_CUSTOM
Regular Expression	event1
Only Once	off
Only this Trigger	on
CLI command	save error-report

*Table 10. Settings for the second custom message*

Property	Value
Message ID	value_of_\$DPL0G_XSLT_USER_CUSTOM
Regular Expression	event2
Only Once	off
Only this Trigger	on
CLI command	interface eth0; packet-capture temporary:///capture -1 250



---

## Part 5. Referenced objects

<b>Chapter 18. Service objects</b> . . . . .	181		Modifying a load balancing group to use workload management information for non-WebSphere application servers . . . . .	215
HTTP Service . . . . .	181		Defining cryptographic profiles . . . . .	216
Creating an SSL Proxy service . . . . .	182		RADIUS Settings . . . . .	217
Creating a TCP Proxy service . . . . .	183		NAS-identifier . . . . .	218
<b>Chapter 19. Referenced objects</b> . . . . .	185		Configuring RADIUS Settings . . . . .	218
Access Control List . . . . .	185		Adding SSH known hosts . . . . .	219
Overview . . . . .	185		SSL Proxy Profile objects . . . . .	219
Creating an Access Control List object . . . . .	186		Creating a forward (or client) proxy . . . . .	220
Working with Certificate objects . . . . .	186		Creating a reverse (or server) proxy . . . . .	220
Working with z/OS certificates . . . . .	186		Creating a two-way proxy . . . . .	221
Defining Certificate objects . . . . .	187		Validation credentials . . . . .	221
Defining Identification Credentials objects . . . . .	188		Creating for non-expiring, non-password-protected certificates . . . . .	222
Kerberos objects . . . . .	189		Validation methods . . . . .	222
Points to remember when using Kerberos . . . . .	190		PKIX validation . . . . .	222
Configuring a Kerberos KDC Server object . . . . .	190		Creating for specific certificates . . . . .	223
Configuring a Kerberos Keytab File object . . . . .	191		WebSphere Cell . . . . .	224
Working with Key objects . . . . .	192		Selecting the update method . . . . .	224
Working with z/OS keys . . . . .	192		Creating a WebSphere Cell . . . . .	224
Defining Key objects . . . . .	192		NSS Client . . . . .	226
Load balancer groups . . . . .	194		Creating the NSS Client . . . . .	227
Intelligent load distribution . . . . .	194			
Algorithms for making load balancing decisions . . . . .	198			
Membership . . . . .	199			
Health checks . . . . .	200			
Health states of members . . . . .	200			
Session affinity . . . . .	200			
Types of session affinity . . . . .	201			
Session affinity modes and where to configure . . . . .	202			
Configuring a load balancer group . . . . .	202			
Defining the base configuration . . . . .	203			
Adding static members . . . . .	204			
Overriding session affinity in a WebSphere cell . . . . .	204			
Defining health checks . . . . .	205			
Modifying to use workload management information . . . . .	206			
Assigning weight to members . . . . .	207			
Disabling members . . . . .	207			
Enabling the retrieval of workload management information . . . . .	207			
Installing the OSGi bundle . . . . .	208			
Installing the ODCInfo application . . . . .	208			
Starting the ODCInfo application . . . . .	209			
Uninstalling the OSGi bundle . . . . .	210			
Uninstalling the ODCInfo application . . . . .	211			
Enabling the retrieval of workload management information for non-WebSphere application servers . . . . .	211			
Defining the XML Document for non-WebSphere servers . . . . .	212			
Creating an XML Firewall to validate the XML document . . . . .	214			
Creating a WebSphere Cell for non-WebSphere application servers . . . . .	214			



---

## Chapter 18. Service objects

This chapter describes how to create and manage service objects from the object view.

You can access the following service objects from the **Objects Services** menu:

### **HTTP Service**

Creates an HTTP server

### **SSL Proxy Service**

Creates a secure SSL-based relay or forwarding service

### **TCP Proxy Service**

Creates a nonsecure TCP-based relay or forwarding service

---

## HTTP Service

You can create an HTTP service that serves documents from a specified directory on the appliance.

To create an HTTP service, use the following procedure:

1. Select **Objects Services HTTP Service** to display the catalog.
2. Click **Add** to display the HTTP Service configuration screen.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.

5. Specify the local IP address to monitor in the **Local IP Address** field. Retain the default value (0. 0. 0. 0) to bind to all local interfaces.

To use a local Host Alias instead of a static IP address, click **Host Alias**. A Host Alias allows you to specify a locally configured alias that resolves to a static IP address. Aliasing can help when moving configurations across systems.

6. Optional: In the **Comments** field, enter a descriptive summary.
7. Select a priority for scheduling or for resource allocation from the **Service Priority** list.

**High** Receives above normal priority.

**Low** Receives below normal priority.

**Normal**

(Default) Receives normal priority.

8. Specify the port to monitor in the **Port Number** field. The default is 80.
9. Select the operational mode from the **Mode** list.

**Echo** Input is looped back to the sender. This mode is intended for test and debug environments.

**Normal**

(Default) Enables standard HTTP server operation

10. Optionally specify the value for the Server response header in the **Identifier** field. The Server response header generally contains information (name and version) that describes the application software. By default, the inclusion of the Server response header is suppressed.

**Note:** Consider the security implications before revealing version information.

11. Specify the local directory from which to serve documents in the **Base Directory** field.

config: ///

Identifies the config directory.

local: ///

Identifies the local directory.

store: ///

(Default) Identifies the store directory.

temporary: ///

Identifies the temporary directory.

12. Optionally use the **Start Page** controls to identify the page to load when an client accesses this service. Without a start page, this service displays a directory listing for the defined base directory.
13. Optionally select an Access Control List from the **Access Control List** list. Refer to “Access Control List” on page 185 for more information.
14. Click **Apply** to save the changes to the running configuration.
15. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Creating an SSL Proxy service

You can create an SSL Proxy service that uses a secure connection to relay all traffic received on a specified local address to a specified remote peer. If the local address is 0.0.0.0, binds to all local interfaces. You can use an SSL Proxy service to enable the transmission of syslog-ng from an SSL application (for example, Stunnel).

In this configuration, the **Administrative State** property is read-only.

To create an SSL Proxy:

1. Click **Objects Services SSL Proxy Service**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. In the **Local IP Address**, specify the local IP address to monitor.
5. From the **Service Priority** list, select a priority for scheduling or resource allocation.
6. In the **Port Number** field, specify the port to monitor.
7. In the **Remote Host** field, specify the host name or IP address of the remote host to send SSL traffic.
8. In the **Remote Port** field, specify the port on the remote host.
9. From the **SSL Proxy Profile** list, select a client SSL Proxy Profile that identifies the keys and certificates to use in the handshake.
10. Click **Apply** to save the changes to the running configuration.
11. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Creating a TCP Proxy service

You can create a TCP Proxy service that uses a TCP connection to relay or forward all traffic that is received on a specified local address (or host alias) to a specified remote peer. If the local address is 0.0.0.0, binds to all local interfaces.

In this configuration, the **Administrative State** property is read-only.

To create a TCP Proxy:

1. Click **Objects Services TCP Proxy Service**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. In the **Local IP Address**, specify the local IP address to monitor.
5. From the **Service Priority** list, select a priority for scheduling or resource allocation.
6. In the **Port Number** field, specify the port to monitor.
7. In the **Remote Host** field, specify the host name or IP address of the remote host to send TCP traffic.
8. In the **Remote Port** field, specify the port on the remote host.
9. Click **Apply** to save the changes to the running configuration.
10. Optional: Click **Save Config** to save the changes to the startup configuration.





---

## Chapter 19. Referenced objects

---

### Access Control List

An Access Control List (ACL) object consists of a sequence of `allow` and `deny` clauses. Each clause identifies an IP address or range of addresses that allow or that deny access to a service.

The DataPower appliance provides the following Access Control List object:

- `ssh` for use by the SSH service
- `web-mgmt` for use by the Web Management Service
- `xml-mgmt` for use by the XML Management Interface

Each of these objects, when enabled, provides full access from all IPv4 addresses. If the Ethernet for the local address for these services supports IPv6 addresses, modify its Access Control List object to include an `allow` clauses for specific or all IPv6 addresses.

### Overview

An ACL is associated with a specific DataPower service. An ACL grants access to the service to only addresses that are defined by the `allow` clause. All other addresses are denied access.

Candidate addresses are evaluated sequentially against each clause in the ACL. A candidate address is denied or granted access in accordance with the first clause that matches. Consequently, the order of clauses in the ACL is vital.

For example, the following ACL fails its intended purpose. The address range that is specified by the `deny` clause (192.168.14.224 through 192.168.14.255) is granted access before the `allow` clause.

```
allow 192.168.14.0/24
deny 192.168.14.0/27
```

However, as shown in the following example, reversing the order of the clauses achieves the desired effect.

```
deny 192.168.14.0/27
allow 192.168.14.0/24
```

An ACL that contains only `deny` clauses effectively disables a service by denying access to all addresses. To complete an ACL, include an IP family-specific `allow` clause to ensure that addresses that are not explicitly denied access are granted access:

- `allow 0.0.0.0` if only IPv4
- `allow ::/0` if a combination of IPv4 and IPv6

The following example denies access to two ranges of addresses and allows access to all other IPv4 addresses.

```
deny 10.10.10.0/24
deny 172.16.0.0/16
allow 0.0.0.0
```

## Creating an Access Control List object

To create an ACL, use the following procedure:

1. Select **Objects** **Access Settings** **Access Control List** to display the catalog.
2. Click **Add** to display the configuration screen.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Define the allow and deny clauses on the **Entry** tab.
  - a. Click **Add** to display the Property window.
  - b. From the **Access** list, select the type of clause to create.

**Allow** Indicates an allow clause.

**Deny** Indicates an deny clause.
  - c. In the **Address Range** field, specify an IP address with its prefix length (net mask). Use a forward slash (/) between the address and the prefix length. Examples of address ranges are as follows:
    - 10. 10. 100. 0/28 specifies the IPv4 address range from 10. 10. 100. 0 through 10. 10. 100. 15
    - 10. 10. 100. 9/32 specifies the single IPv4 address
    - 0. 0. 0. 0 (without a prefix length) specifies all IPv4 addresses
    - :: /0 specifies all IPv4 and IPv6 addresses
  - d. Click **Save**.Repeat this step for each additional clause.
6. Click **Apply** to save the changes to the running configuration.
7. Optional: Click **Save Config** to save the changes to the startup configuration.

If you delete a clause, the WebGUI does not prompt for confirmation. If you inadvertently delete a clause, click **Cancel** and **OK** to restore the ACL to its prior configuration.

---

## Working with Certificate objects

A Certificate object that provides an added layer of security by supplying a indirect reference (or *alias*) to a certificate file. The alias provided by the Certificate object is later used in the creation of a Firewall Credentials, an Identification Credentials, or a Validation Credentials.

## Working with z/OS certificates

DataPower appliances can use the secure certificate storage and services that z/OS NSS provides. This capability allows you to create certificate objects using certificates retrieved from z/OS. A certificate retrieved from z/OS is used the same way a local certificate is used to perform encryption and signature verification.

To create certificate objects, the DataPower appliance communicates with z/OS using an NSS client object. The NSS client object must be defined and in the up operational state when you create certificate objects that use z/OS certificates. The retrieved z/OS certificate remains local on the appliance until the associated

application domain or the appliance is restarted. For more information about the NSS client object, see “NSS Client” on page 226.

To access and use z/OS certificates, the NSS client object on DataPower must have permission to access the z/OS certificate. See your z/OS documentation for more information on these settings.

## Defining Certificate objects

To create and configure a Certificate, use the following procedure:

1. Select **Objects** **Crypto Configuration** **Crypto Certificate**.
2. Click **Add** to display the configuration pane.
3. Provide the following inputs:

**Name** Specify the name of the object.

### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

### File Name

Specify the local certificate file or the remote z/OS certificate file.

For a local certificate file, access a list of files, contained in the cert: or pubcert: file repository, and select the file that contains the certificate referenced by this Certificate object.

- Click **Upload** or **Fetch** to transfer the file.
- Click **Details** to display information about the selected certificate file.

For a remote z/OS certificate file, specify the location and the file name.

- Select **saf-cert://** from the **File Name** list.
- Specify the file name using the following format:

*nssclient/ZOSCERTLABEL*

*nssclient*

Specifies an existing NSS client object.

*ZOSCERTLABEL*

Specifies the label name of an existing SAF certificate residing on the z/OS system.

### Password

Depending of business security policies, provide one of the following:

- If local security policies provide for password-protected keys, specify the password (or a password alias).
- If local policies do not support password protection, leave blank.
- If key files are protected by a plaintext password, specify the password.

**Note:** Plaintext passwords appear as such in the configuration script.

- If key files are protected by an aliased password, specify the alias.

The CLI provides a **password-map** command that uses a locally-generated key to 3DES encrypt a password used to access a private key file. The command maps the encrypted password to a

password alias in a password map file. The password map and the locally-generated key are saved to separate files on the appliance. Plaintext passwords are *not* stored in memory or saved on the appliance.

#### Password Alias

Specify if the text entered in the **Password** field is a plaintext password or a password alias.

- on** Identifies the text as a password alias for an encrypted password
- off** (Default) Identifies the text as a plaintext password

#### Ignore Expiration Dates

Allow the creation of a certificate prior to its activation date (the NotBefore value in the certificate) or after its expiration date (the NotAfter value in the certificate).

- off** (Default) Prevents the creation of certificates outside of their internal expiration values.
- on** Creates the certificate and places it in the up state. Although the certificate is in the up state, objects that reference the certificate use the internal expiration values. In other words, the certificate itself is in the up state, but Validation Credentials, Firewall Credentials, or Identification Credentials that references the certificate adhere to the internal expiration values.

In other words, the certificate itself is in the up state, but Validation Credentials, Firewall Credentials, or Identification Credentials that references the certificate adhere to the internal expiration values. If the certificate is used for a certificate chain validation from a Validation Credentials and the certificate is not valid, validation fails. Similarly, if the certificate is used from an Identification Credentials, the DataPower appliance sends the certificate to the SSL peer for an SSL connection, but the peer can reject the certificate as not valid.

4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Defining Identification Credentials objects

An Identification Credentials objects consists of a Key object and a Certificate object. An Identification Credentials object identifies the matched public key cryptography public and private keys that an object uses for SSL authentication. An Identification Credentials object can be used in document encryption, document decryption, and digital signature operations.

To create an Identification Credentials object, use the following procedure:

1. Select **Objects** **Crypto Configuration** **Crypto Identification Credentials**.
2. Click **Add** to display the configuration pane.
3. Provide the following inputs:

**Name** Specify the name of the object.

#### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.

- To make active, click **enabled**.

#### **Crypto Key**

Access a list of all Key objects, and select the Key object for this Identification Credentials. Refer to “Defining Key objects” on page 192 for more information.

#### **Certificate**

Access a list of all Certificate objects, and select the Certificate object for this Identification Credentials. Refer to “Defining Certificate objects” on page 187 for more information.

#### **Intermediate CA Certificate**

Intermediate CA certificates might be required when the CA that is signing this certificate is not widely-recognized. If the intermediate CA certificate is also signed by a less recognized CA, an additional intermediate CA certificate might be required for that CA. You can specify as many intermediate certificates as are required.

If necessary, use the list of available Certificate objects to establish a verifiable trust-chain. A *trust-chain* consists of one or more Certification Authority (CA) certificates and provides a linked path from the certificate that is in the Identification Credentials to a CA that is trusted by a remote appliance. The trust chain enables the appliance to authenticate the certificate.

4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## **Kerberos objects**

A basic description of the Kerberos authentication protocol is helpful for understanding the support provided by the DataPower appliance.

The Kerberos authentication protocol uses a star topology. The *Key Distribution Center* (KDC) is at the center of the star. Each Kerberos *principal* (a human, a computer client, or an instance of a service running a specific computer) is registered with the KDC and has a shared secret known only to the principal and to the KDC. This shared secret takes the form of a password for human principals and a randomly generated *keytab* file for nonhuman principals.

When a Kerberos client (for example, Alice) wants to communicate securely with a Kerberos server (for example, the FTP service), Alice must access KDC of her Kerberos realm and request a ticket for the FTP service. At this point, the KDC has the option of requiring pre-authentication before responding, or the KDC can immediately issue the ticket to Alice.

The KDC response contains two items:

- A randomly generated session key encrypted with Alice's shared secret
- A ticket for the FTP service

The ticket contains:

- The idobj for Alice
- The idobj for the FTP service
- A ticket lifetime
- Another copy of the session key

The ticket is encrypted with the shared secret of the FTP service principal. Consequently, there are two encrypted copies of the session key (one for Alice, and one for the FTP service).

At this point, Alice uses her shared secret to decrypt her copy of the session key and generates an *authenticator* (which proves that the person talking to the FTP service is the client for which this ticket was issued, and not a malicious user replaying a previously issued ticket) that she sends along with her ticket to the FTP service. The ticket plus authenticator is called an *AP-REQ message*.

When the FTP service receives the AP-REQ from Alice, it decrypts the ticket and verifies the authenticator. At this point the FTP server has authenticated Alice, and they share a session key which can be used to secure the rest of their communications.

## Points to remember when using Kerberos

When using Kerberos, keep the following points in mind:

- Both clients and servers are principals in the KDC database. More accurately, services running on server computers are principals in the KDC database.
- A client principal must request a separate ticket for each server with which it communicates.
- Services must have a name and shared secret registered with the KDC.
- A service must have access to its shared secret to decrypt Kerberos tickets.
- A Kerberos ticket that is issued by a KDC contains the cryptographic material that allows both the client and the server to generate the same session key.
- All Kerberos cryptographic operations are symmetric in nature.
- In an AAA Policy, Kerberos is an idobj extraction, authentication protocol, or both.
- Kerberos is not an authorization protocol.

There is no restriction in Kerberos that specifies which clients can request tickets for a particular service.

**Note:** Microsoft Windows, when configured to use an Active Directory domain, is based on a security infrastructure that is, at its core, Kerberos. As of Windows 2000, authentication in a Windows domain is handled by Kerberos. Such authentication is entirely transparent to the user. Refer to *Understanding SPNEGO* for implementation details.

## Configuring a Kerberos KDC Server object

Use the following procedure to configure a Kerberos KDC Server:

1. Select **Objects** **Crypto** **Kerberos KDC server** to display the Kerberos KDC Server catalog.
2. Click **Add** to display the Kerberos KDC Server configuration screen.
3. Provide the following inputs:

### Name

Specify the name of the object.

### Administrative State

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

**Comments**

Optional: Enter a descriptive summary.

**Kerberos realm name**

Specify the name of the Kerberos realm that is serviced by this KDC. There is exactly one KDC per Kerberos realm.

**Kerberos KDC Server**

Specify the host name or IP address of the KDC server. Click **Ping** to verify connectivity.

**Use TCP**

Select whether to use UDP or TCP as the Transport Layer protocol to access the KDC server.

**on** Use Transmission Control Protocol (TCP)

**off** (Default) Use User Datagram Protocol (UDP)

**Server Port Number**

Specify the UDP or TCP port that is monitored by the KDC for incoming Kerberos requests. The default is 88.

**UDP Timeout**

When the Transport Layer protocol is UDP, specify the UDP timeout.

4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

## Configuring a Kerberos Keytab File object

A Kerberos Keytab file contains the keys needed to decrypt the ticket presented by a client attempting to obtain services. Previously, only a password was required. This has been changed to an encrypted key for added security. The Kerberos Keytab File object identifies the file that contains the keys needed to decrypt the ticket.

Use the following procedure to configure a Kerberos Keytab File:

1. Select **Objects** **Crypto** **Kerberos Keytab**.
2. Click **Add** to display the configuration pane.
3. Provide the following inputs:

**Name**

Specify the name of the object.

**Administrative State**

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

**Comments**

Optional: Enter a descriptive summary.

**File Name**

Select the keytab file. This list includes files that are stored in the encrypted and protected cert: directory of the appliance. If the file does not reside on the appliance, click **Upload** or **Fetch** to transfer the file.

**Note:** This file is not generated on the DataPower appliance. It is generated through the Kerberos system itself.

4. Click **Apply** to save the changes to the running configuration.



5. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Working with Key objects

A key is an object that provides an added layer of security by supplying a indirect reference (or *alias*) to a file that contains a private key. The alias provided by the Key object is later used in the creation of a Firewall Credentials or Identification Credentials object.

### Working with z/OS keys

DataPower appliances can use the secure private key storage and services that z/OS NSS provides. This capability allows you to access private keys on z/OS and to perform the following operations:

- Retrieve private keys from z/OS
- Create key objects using retrieved keys
- Create key objects using remote keys that are stored on z/OS
- Submit requests to z/OS to decrypt data using a certificate's private key
- Submit requests to z/OS to generate a digital signature using a certificate's private key

Use a key object created with a private key that is retrieved from z/OS the same way you use a key object created with a local private key. Use a key object created with a private key that is stored on z/OS to make requests for decryption or signature generation on the z/OS system.

To create key objects, the DataPower appliance communicates with z/OS using an NSS client object. The NSS client object must be defined and in the up operational state when you create key objects.

To use a retrieved z/OS key, the key must be a SAF key that is not stored in ICSF. The SAF key is cached locally on the appliance until the associated application domain or the appliance is restarted.

To use a remote z/OS key, the key must be a SAF key that is stored in ICSF. The SAF key is never taken off of your z/OS system. Therefore, the NSS client object must be in the up operational state when using remote key objects. For more information about the NSS client object, see “NSS Client” on page 226.

To access and use z/OS keys, the NSS client object on DataPower must have permission to access the z/OS keys. See your z/OS documentation for more information on these settings.

### Defining Key objects

To create and configure a Key object, use the following procedure:

1. Select **Objects** **Crypto Configuration** **Crypto Key**.
2. Click **Add** to display the configuration pane.
3. Provide the following inputs:

**Name**

Specify the name of the object.

**Administrative State**

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.



- To make active, click **enabled**.

### File Name

Specify the local private key file or the remote z/OS private key file.

For a local key file, access a list of files, contained in the cert: file repository, and select the file that contains the private key aliased by this Key object. Click **Upload** or **Fetch** to transfer the file.

**Note:** Keys can be retrieved from a Java Key Store residing on the local workstation. Click **Java Key Store** on the **Upload** field. Refer to “Uploading files from the workstation” on page 134 for more information.

For a remote z/OS key file, specify the location and the file name.

- Select **saf-key://** or **saf-remote-key://** from the **File Name** list.
- Specify the file name using the following format:

*nssclient/ZOSKEYLABEL*

*nssclient*

Specifies an existing NSS client object.

*ZOSKEYLABEL*

Specifies the label name of an existing SAF key residing on the z/OS system. A **saf-key://** must be a SAF key that is not stored in ICSF. A **saf-remote-key://** must be a SAF key that is stored in ICSF.

### Password

Depending on business security policies, provide one of the following:

- If local security policies provide for password-protected keys, specify the password (or a password alias).
- If local policies do not support password protection, leave blank.
- If key files are protected by a plaintext password, specify the password.

**Note:** Plaintext passwords appear as such in the configuration script.

- If key files are protected by an aliased password, specify the alias.

The CLI provides a **password-map** command that uses a locally-generated key to 3DES encrypt a password used to access a private key file. The command maps the encrypted password to a password alias in a password map file. The password map and the locally-generated key are saved to separate files on the appliance. Plaintext passwords are *not* stored in memory or saved on the appliance.

### Password Alias

Specify if the text entered in the **Password** field is a plaintext password or a password alias.

**on** Identifies the text as a password alias for an encrypted password.

**off** (Default) Identifies the text as a plaintext password.

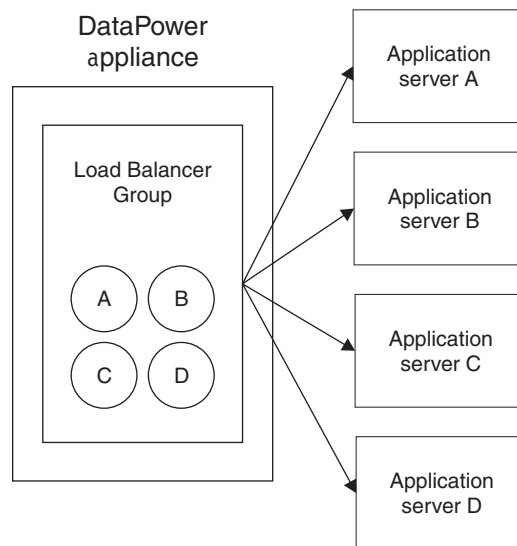
4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Load balancer groups

A load balancer group is a server pool that can provide redundancy among a collection of servers. A load balancer group can be used as the remote server for a DataPower service or can be used to provide failover support for LDAP or IMS<sup>™</sup> Connect servers. A request to connect to a load balancer group results in the selection of a healthy server to receive an incoming client request.

Figure 8 shows the load balancer group with four members



*Figure 8. Load balancer group with static members to support load balancing*

Depending on the algorithm that makes load-balancing decisions, each load balancer group can support 64 or 512 members. The following algorithms support 64 members:

- Least connections
- Weighted least connections
- Weighted round robin

## Intelligent load distribution

Intelligent load distribution uses a load balancer group to distribute workload more efficiently across application servers by providing the ability to dynamically change configuration data about membership, weight of members, and session affinity.

**Note:** The ability to use intelligent load distribution requires the Option for Application Optimization feature.

To get the full benefit of intelligent load distribution, you need to define a configuration on the DataPower appliance and install an application on the deployment manager of a WebSphere Application Server cell.

- On the DataPower appliance, you need to define a load balancer group that references a WebSphere cell configuration.
- On the deployment manager of a WebSphere Application Server cell, you need to install the WebSphere On Demand Configuration (ODCInfo) application.

Figure 9 shows the required configuration.

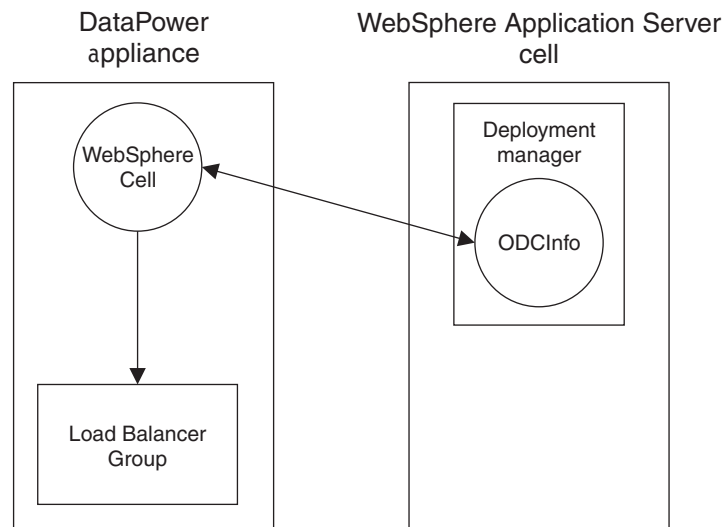


Figure 9. Configuration to support intelligent load distribution

The communication between the DataPower appliance and the cell in the WebSphere environment is as follows:

1. The ODCInfo application retrieves data about the application servers in the cell.
2. The WebSphere cell configuration retrieves the information from the ODCInfo application and updates the data in the load balancer group.
3. The load balancer group uses this data to adapt to changing traffic conditions and application server capabilities to optimally distribute traffic among the application servers in the cell.

If your application server must maintain session affinity, you can configure session affinity to override load balancing decisions.

## Application intelligence

Application intelligence is an extension of intelligent load distribution. With application intelligence, the load balancer group is designed to use application specific information from the application servers to optimize routing decisions. Specifically, the following application information is used to make routing decisions:

- Virtual host group information
- Web module information
- Application and application edition information
- Routing rules

Using this information, the load balancer group can ensure that a request is targeted to a specific application and the application is running. If application edition rollout is used, the request is routed to the new edition when it comes online. If a request is for an application that is not available on any of the application servers, the appliance rejects the request and returns a 404 or Not Found error response to indicate that there is no matching application. This saves processing on the application server. If the application is found, but is not active on a server, a 500 or Internal Server error response is returned.

Application intelligence supports the following two main aspects:

- Application routing  
Provides load balancing based on application knowledge on the back end.
- Application rollout  
Provides the ability to replace a running application edition with a new edition with little or no traffic loss. Supports atomic and group rollout in a WebSphere Virtual Enterprise cluster with full quiescent capabilities.

Application routing uses application knowledge about the back-end servers to make routing decisions. For example, assume an application is running on a subset of a cluster. Without application routing, requests would be distributed to all servers including the ones not running that application. This would put additional pressure on the back-end servers to redirect traffic. This scenario is one that occurs during the rollout of an application. There are periods of time where an application is running on some subset of the servers in a cluster.

The application routing decision is made based on the `Host:` header and the URI of the incoming HTTP request to route the request to the appropriate application server. For a request to be properly routed, the `Host:` header must contain a value that matches the `vHostGroup` host and port information defined in the WebSphere Cell. And, the URI must match the URI information defined in the WebSphere Cell WebModules and WebRouteWorkClasses. If the matching is unsuccessful, a 404 response code is returned. With application routing disabled, the appliance cannot respond with a 404 response. Instead, it forwards the request to one of the servers in the Cell regardless of the active applications on that server. HTTP/1.0 requests that typically do not contain `Host:` headers will be answered with 404 responses.

Application rollout, a feature available on WebSphere Virtual Enterprise, replaces an active edition of an application with a new edition. For additional information on application editions, see the WebSphere Virtual Enterprise documentation on application edition management.

The DataPower appliance supports the following types of application rollout:

- Group rollout  
Performs a rollout of a new edition using a defined group size that specifies the number of nodes to process at a time.
- Atomic rollout  
Performs a rollout of a new edition replacing the edition on half of the cluster members at a time. Serves all user requests with a consistent edition of the application.

Two settings are used to enable application intelligence in the load balancer group:

- In the load balancer group, enable application routing
- In the WebSphere Cell object, set the update method to subscribe so that the appliance receives faster notification of state changes

See the tasks for configuring these objects for additional information.

## Required software

For full support of dynamic membership and weights, you must install WebSphere Application Server Network Deployment or WebSphere Virtual Enterprise.

- For WebSphere Application Server Network Deployment, an administrator uses the WebSphere Administrative Console to manually update the membership and weight information of application servers.
- For WebSphere Virtual Enterprise, membership and weight information is updated dynamically based on runtime conditions. To enable dynamic updates, an administrator uses the WebSphere Administrative Console to enable dynamic workload management.

Backend servers other than WebSphere Application Server Network Deployment or WebSphere Virtual Enterprise support a smaller feature set. Non-WebSphere application servers can be used in the following configurations:

- As members of a WebSphere Virtual Enterprise cluster
- As members of an application server cluster whose membership, weights, and session affinity are controlled with a custom application

## Advantages with WebSphere servers

After enabling intelligent load distribution for a load balancer group of WebSphere servers, the load balancer group can take advantage of the following features:

- Application routing that provides the ability to route based on URI or host values
- Edition rollout that provides rollout of a new edition of an application in a seamless fashion
- The ability to dynamically update membership. This feature addresses the addition or removal of WebSphere servers in the WebSphere cell.
- The ability to dynamically update the weight of members to adapt to changes in traffic conditions. This feature addresses the following conditions:
  - When an application server is overloaded, its weight is reduced to receive less traffic
  - When an application server is under utilized, its weight is increased to receive more traffic
- The ability to use the weighted least connection algorithm to optimally distribute traffic to application servers.
- Automatic session affinity configuration based on the WAS DM configuration as well as the ability to override this configuration

## Advantages with non-WebSphere servers

After enabling intelligent load distribution for a load balancer group of non-WebSphere servers, the load balancer group can take advantage of the following features:

- The ability to dynamically update membership when using a custom application that provides the workload management information. This feature addresses the addition or removal of WebSphere servers in the WebSphere cell.
- The ability to dynamically update the weight of members to adapt to changes in traffic conditions when using a custom application that provides the workload management information.
- The ability to use the weighted least connection algorithm to optimally distribute traffic to application servers.
- The ability to use session affinity through explicit configuration on the DataPower appliance.

## Algorithms for making load balancing decisions

Load balancer groups use algorithms to make load balancing decisions. The decision determines to which remote server to forward a new connection.

Load balancer groups support weighted and non-weighted algorithms:

- First alive
- Hash
- Least connections
- Round robin
- Weighted least connections
- Weighted round robin

A weighted algorithm uses weight (or preference) to help determine which server receives the next request. A server with a higher weight receives more traffic than one with a lower weight. The percentage of traffic that is sent to each server is approximately equal to its weight divided by the cumulative weight of all servers in the group.

A non-weighted algorithm assumes that the capacity of all servers in the group to be equivalent. Although non-weighted algorithms are typically faster than weighted algorithms, some non-weighted algorithms, such as the hash algorithm, could send more traffic to some servers. If there are servers with different capacities in the group, processing cannot optimize the capacities of all the servers.

### First alive

The *first alive* algorithm uses the concept of a primary server and backup servers.

- The *primary* server is the first server in the members list.
- A *backup* server is any subsequent server in the members list.

When the primary server is healthy, the DataPower service forwards all connections to this server. When the primary server is quarantined or convalescent, the DataPower service forwards connections to the next server in the list.

### Hash

The *hash* algorithm uses the IP address of the client or the value of an HTTP header as the basis for server selection.

When using an HTTP header, use the **Load Balancer Hash Header** property to identify the header to read. This property is available for only Multi-Protocol Gateway and Web Service Proxy services. Additionally, this property is available on only the **Main** tab in the object view.

With the hash algorithm, the same client is served by the same server. Use this algorithm for applications that require the storage of server-side state information, such as cookies.

### Least connections

The *least connections* algorithm maintains a record of active server connections and forward a new connection to the server with the least number of active connections.

## Round robin

The *round robin* algorithm maintains a list of servers and forwards a new connection to the next server in the members list.

## Weighted least connections

The *weighted least connections* algorithm maintains a weighted list of application servers with their number of active connections and forwards a new connection to an application server based on a combination of its proportion to the weight (or preference) and number of active connections.

This algorithm uses more computation times than the least connection algorithm. However, the additional computation results in distributing the traffic more efficiently to the server that is most capable of handling the request.

This algorithm applies to application servers, not authentication or authorization servers, and requires the Option for Application Optimization feature.

## Weighted round robin

The *weighted round robin* algorithm maintains a weighted list of servers and forwards new connections in proportion to the weight (or preference) of each server.

This algorithm uses more computation times than the round robin algorithm. However, the additional computation results in distributing the traffic more efficiently to the server that is most capable of handling the request.

## Membership

A load balancer group generally contains two or more members. Members can be defined through static or dynamic membership.

### Static membership

A load balancer group that uses a static membership configuration contains the configuration settings that an administrator on the DataPower appliance explicitly defined and persisted. These configuration settings do not change except under the following conditions:

- The processing of a style sheet changes configuration settings for group members
- An administrator enables and configures the workload management feature

### Dynamic configuration

A load balancer group that uses a dynamic membership configuration retrieves membership data through the workload management feature. To create a dynamic membership configuration, you need to enable and configure the workload management feature.

Even after enabling and configuring the workload management feature, a firmware load uses the persisted configuration. Only after retrieving the workload management information and updating the membership of the load balancer group can the load balancer group use dynamic weight and membership information in any load balancing decision.

When enabled, the load balancer group retrieves runtime information from the WebSphere On Demand Configuration (ODCInfo) application. This information overrides the membership information in the running configuration of the load balancer group. The retrieved workload management information alters the membership and weight of application server members in the load balancer group so that the load balancer group can route traffic to the application server that can best handle the load.

As new servers are brought online or as existing servers are taken offline, the membership information in the load balancer group adapts to these changes.

## Health checks

A health check is essentially a scheduled rule that sends the same request to each member. The successful completion of the health check requires that the server passes normal TCP and HTTP connection criteria. Optionally, the health check contains a filter to test the response from the server. If the filter accepts the response, the server is considered to be healthy; otherwise, it is considered to be convalescent.

### Health states of members

The health of each member of a load balancer group is one of the following states:

- Healthy or up
- Quarantined or softdown
- Convalescent or down

**Healthy:** By default, all servers are considered *healthy* and are eligible to receive forwarded client requests. When healthy, its health state is *up*.

**Quarantined:** During a normal HTTP transaction or the TCP ping, a failure to connect to a server causes the server to be *quarantined* until a dampening period elapses. When the dampening period elapses, the server returns to the healthy state and becomes eligible to receive forwarded client requests. When quarantined, its health state is *softdown*.

While quarantined, the server is:

- Removed from the server pool
- Ineligible to receive forwarded client requests
- Excluded from the optional health check

**Convalescent:** Optionally, you can associate a periodic health check with a load balancer group. If the health check fails, the server is *convalescent*. The server is not considered to be healthy until it passes a health check. When convalescent, its health state is *down*.

While convalescent, the server is:

- Removed from the server pool
- Ineligible to receive forwarded client requests

## Session affinity

Session affinity overrides the load-balancing algorithm by directing all requests in a session to a specific application server. For some applications to work correctly, the application requires session affinity between the client and the application server.



Session affinity enhances application performance by using in-memory caching, not a database. Session affinity uses cookies to track session information and, potentially, to maintain login credentials.

With session affinity, the application server that handles the first client request generates session information and places it in a `Set-Cookie` header in the response. The client inserts this information in a `Cookie` header in all future requests in this session with this application server.

Session affinity populates these cookies with a session ID that contains the following information:

- An identifier for the recovery of session data
- Routing information to ensure that all requests in this session are always routed to the same application server

By default, session affinity is enabled for load balancer groups.

- For WebSphere servers, the load balancer group uses the session affinity information provided by the application server.
- For non-WebSphere servers, you must configure session affinity.

## Types of session affinity

A load balancer group supports the following types (or modes) of session affinity:

- Passive
- Active
- Active-conditional

Although session affinity applies to both static and dynamic configurations, you must use a static configuration for active or active-conditional session affinity for non-WebSphere servers.

## Passive session affinity

Passive session affinity can be used with only WebSphere servers.

You cannot define passive session affinity in the load balancer group configuration on the DataPower appliance. To configure passive session affinity, an administrator must use the WebSphere Administrative Console to define passive session affinity at the WebSphere cluster level.

In passive mode, the application server inserts the `Set-Cookie` header in the HTTP response. The DataPower appliance reads and acts on this cookie for all subsequent requests in this session from this client. The appliance does not add or update this cookie.

## Active session affinity

Active session affinity is for non-WebSphere servers that do not use cookies.

In active mode, the DataPower appliance always creates session affinity to the first request and continues to route subsequent requests to the same application server.

## Active-conditional session affinity

Active-conditional session affinity is for non-WebSphere servers that use cookies.

In active-conditional mode, the DataPower appliance recognizes when an application server establishes session affinity by comparing the Set-Cookie header in the response to a list of cluster-specific cookie names.

- If the response header contains a Set-Cookie header from the list, the appliance inserts in the response an additional Set-Cookie header with routing information.
- If the response header does not contain a Set-Cookie header from the list, the appliance does not insert a Set-Cookie header.

## Session affinity modes and where to configure

Depending on the session affinity mode to enforce and the type of application server, you need to define the configuration differently.

### Passive session affinity

Passive session affinity cannot be configured from the DataPower appliance. Use the WebSphere Administrative Console to configure passive session affinity at the WebSphere cluster level.

### Active session affinity

Active session affinity can be configured from the DataPower appliance or from the WebSphere Administrative Console. For active session affinity the application servers can be WebSphere or non-WebSphere servers

To configure active session affinity from the DataPower appliance, override WebSphere cell session affinity and define the insertion cookie information (such as name, path, and domain).

### Active-conditional session affinity

Active-conditional session affinity can be configured from the DataPower appliance or from the WebSphere Administrative Console. For active-conditional session affinity the application servers can be WebSphere or non-WebSphere servers

Depending on the type of application server, you must define the list of cluster-specific cookies differently.

- For WebSphere servers, define the list at the cluster level from WebSphere Administrative Console.
- For non-WebSphere servers, define the list as part of the load balancer group configuration from the DataPower appliance.

To configure active-conditional session affinity from the DataPower appliance, override WebSphere cell session affinity, define the list of cookies to monitor, and define the insertion cookie information (such as name, path, and domain).

## Configuring a load balancer group

The configuration of a load balancer group consists of the following activities:

1. Click **Objects** **Network** **Load Balancer Group**.
2. Click **Add**.
3. On the **Main** tab, define the base configuration.
4. On the **Members** tab, define server members.
  - Required for groups of LDAP or IMS Connect servers.

- Required for groups of non-WebSphere servers.
  - Optional for groups of WebSphere servers that will use intelligent load distribution. Requires the Option for Application Optimization feature.
5. Optional: On the **Session Affinity** tab, override the session affinity from a WebSphere cell. Requires the Option for Application Optimization feature.
  6. Optional: On the **Health** tab, define health check criteria.
  7. Click **Apply** to save the changes to the running configuration.
  8. Optional: Click **Save Config** to save the changes to the startup configuration.

## Defining the base configuration

A base configuration create a load balancer group without members.

To define the base configuration:

1. Click **Objects Network Load Balancer Group**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. From the **Algorithm** list, select the algorithm to select the actual server.
7. Optional: In the **Damp Time** field, enter the number of seconds that a server remains in an softdown state. This setting does not impact servers that are in the down state.
8. Optional: Set **Do not Bypass Down State** to **on** to disable connection forwarding to any member. This setting makes the next connection attempt when at least one member is in the up state.
9. Optional: Set **Try Every Server Before Failing** to **on** to send the request to each server until one responds or all fail. Each server that fails is set to the softdown state.
10. Optional: Set **Masquerade as Group Name** to **on** to use the name of the load balancer group, not the host name of the member, in the message header.
11. Click **Apply** to save the changes to the running configuration.
12. Optional: Click **Save Config** to save the changes to the startup configuration.

With the base configuration, you might need to define static members. You must define static members for the following groups of servers:

- Groups of LDAP servers
- Groups of IMS Connect servers
- Groups of application servers that do not retrieve workload management information through the ODCInfo application

For configuration details, refer to “Adding static members” on page 204.

For groups of WebSphere servers that retrieve workload management information through the ODCInfo application, you can optionally define static members. However, after retrieving the workload management information from the WebSphere cell, static members are disabled.

## Adding static members

To add static members to an existing load balancer group:

1. Click **Objects** **Network** **Load Balancer Group**.
2. Click the name of the load balancer group to modify.
3. Click the **Members** tab.
4. Add static members.
  - a. Click **Add**.
  - b. In the **Actual Host** field, enter the IP address or the domain-qualified host name of the member.
  - c. For weighted algorithms: In the **Weight** field, enter the relative weight (preference). The greater the value, the more likely this server is to receive a connection request.
  - d. In the **Mapped Server Port** field, enter the member-specific target port or retain the default value to use the DataPower service-defined port.

By default, member servers are contacted on the DataPower service-defined port. However, if you have services running on different ports for different member servers, explicitly identify the member-specific target port. If you specify a nonzero value, that member server will always be contacted on this port.
  - e. In the **Health Port** field, enter the member-specific health port or retain the default value to use the load balancer group-defined port.

A nonzero value overrides the value for the **Remote Port** property of the health check. This property is available during the configuration of the health check on the **Health** tab.
  - f. Retain the default setting for **Admin State**. To place in an inactive administrative state, click **disabled**.
  - g. Click **Save**.
5. Repeat the previous step to add another server as a static member.
6. Click **Apply** to save the changes to the running configuration.
7. Optional: Click **Save Config** to save the changes to the startup configuration.

## Overriding session affinity in a WebSphere cell

If you use non-WebSphere application servers and you need session affinity, you can override session affinity from the WebSphere cell. When overriding session affinity, you can use either active or active-conditional session affinity.

### Before you begin

Determine the type of session affinity that your non-WebSphere application server needs (active or active-conditional). Configure a load balancer group with members that are non-WebSphere application servers.

### About this task

Modify a load balancer group to support session affinity for non-WebSphere application servers.

This functionality requires the Option for Application Optimization feature.

## Procedure

1. Click **Network Other Load Balancer Group**
2. Click the name of load balancer group.
3. Click the **Session Affinity** tab.
4. Set the **Override WebSphere Cell Configuration** check box. The pane refreshes to display additional parameters.
5. From the **Mode** list, select the type of session affinity.
6. For active-conditional: Define the cookies to monitor.
  - a. In the **Monitored Cookies** field, enter the name of the cookie to monitor.
  - b. Click **Add**
7. Optional: Repeat the previous step to add another cookie. The configuration requires at least one cookie.
8. Click **Apply** to save the changes to the running configuration information.
9. Click **Save Config** to save the changes to the startup configuration.

## Results

Session affinity is enabled for non-WebSphere application servers.

## Defining health checks

To define the health check:

1. Click **Objects Network Load Balancer Group**.
2. Click the name of a load balancer group to modify.
3. Click the **Health** tab.
4. Set **Enabled** to **on**.
5. For standard health checks: In the **URI** field, enter the non-server (file path) portion of the target URI. That is, specify the URI to receive the client request that is generated by the rule.
6. In the **Remote Port** field, enter the port on the target server to receive the query.

You can override this value for one or more members of the load balancer group with the **Health Port** property. This property is available during the configuration of member servers in the group.

The response from the server is evaluated to determine the health status of each member server in the group. The request is sent to the target URI and remote port.
7. From the **Health Check Type** list, select the type of health check to perform.
8. Optional for standard health checks: Set **Send SOAP Request?** to **off** to access the target URI with an HTTP **GET** operation instead of the default HTTP **POST** operation.
9. For SOAP requests with an HTTP **POST** operation: In the **SOAP Request Document** field, enter the location (URL) of the SOAP message to send as the request.
10. In the **Timeout** field, enter the number of seconds to wait for the completion of the health check.
11. In the **Frequency** field, enter the number of seconds between health checks.
12. For standard health checks: Define the filter for a valid server response.
  - a. In the **XPath Expression**, enter the XPath expression that must be found in a valid server response. Use the XPath tool to help define the expression.

- b. In the **XSL Health Check Filter** field, enter the location (URL) of the style sheet to filter the server response.
13. Optional for standard health checks: From the **SSL proxy profile** list, select the SSL proxy profile to provide for a secured connection.
14. Click **Apply** to save the changes to the running configuration.
15. Optional: Click **Save Config** to save the changes to the startup configuration.

## Modifying to use workload management information

Modify the configuration of a load balancer group to request workload management information from the ODCInfo application on the WebSphere deployment manager.

### Before you begin

Configure a load balancer group.

### About this task

Configure the load balancer group to request workload management information from the ODCInfo application. The load balancer groups uses the WebSphere Cell configuration to gather information about the application servers in the WebSphere cell. The WebSphere Cell configuration that is referenced by the load balancer group forwards this information to the load balancer group.

**Note:** Until the load balancer group successfully receives the workload management information from the ODCInfo application, it uses the members defined as part of its running configuration.

### Procedure

1. Click **Objects** **Network Settings** **Load Balancer Group**.
2. Click the name of the load balancer group to modify.
3. Modify a load balancer group to use the workload management information from the WebSphere cell (WebSphere deployment manager).
  - a. Set **Retrieve Workload Management Information** to **on**. The WebGUI refreshes to display additional properties.
  - b. From **Workload Management Retrieval** list, select **WebSphere Cell**.
  - c. From **WebSphere Cell Subscription** list, select a WebSphere Cell configuration.
  - d. In **Workload Management Group Name** field, enter the name of the WebSphere cluster.
4. Set **Enable Application Routing** to **on** to use application intelligence. When using application edition, either atomic or group rollout, set the **Update Method** of the WebSphere Cell object to subscribe.
5. Review the session affinity information on the **Session Affinity** tab to ensure that session affinity is correctly configured.
6. Click **Apply** to save the changes to the running configuration information.
7. Click **Save Config** to save the changes to the startup configuration.

### Results

The load balancer group begins to request information from the ODCInfo application.

## Assigning weight to members

A load balancer group uses the weight of its members when making load balancing decisions based on a weighted algorithm. Weight is not relevant for a load balancer group that uses a non-weighted algorithm.

To assign weight to members.

1. Click **Objects** **Network** **Load Balancer Group**.
2. Click the name of the load balancer group to modify.
3. Click the **Members** tab.
4. Change the weight for a specific member.
  - a. Click the pencil icon to edit the member.
  - b. In the **Weight** field, change the value.
  - c. Click **Save**.
5. Repeat the previous step to modify another member.
6. Click **Apply** to save the changes to the running configuration.
7. Optional: Click **Save Config** to save the changes to the startup configuration.

## Disabling members

If you need to disable a member, you can disable the member from the load balancer group without deleting the member from the group.

To disable specific members to not participate in load balancing decisions:

1. Click **Objects** **Network** **Load Balancer Group**.
2. Click the name of the load balancer group to modify.
3. Click the **Members** tab.
4. Disable members.
  - a. Click the pencil icon to edit the member.
  - b. Set **Administrative State** to **disabled** to place the member in an inactive administrative state.
  - c. Click **Save**.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

## Enabling the retrieval of workload management information

For WebSphere application servers, complete the following procedure to install and configure the WebSphere On Demand Configuration (ODCInfo) application. When installed, the ODCInfo application helps provide intelligent load distribution through the retrieval of workload management information.

### Before you begin

Identify the types of application servers in your WebSphere cell (WebSphere Application Server) environment. Download the following ODCInfo files:

- `com.ibm.datapower.odc.osgi.jar`
- `ODCInfo_ND61.war`
- `ODCInfoCheckInstall.jacl`
- `ODCInfoDeploy.jacl`
- `ODCInfoStart.jacl`



- `ODCInfoUninstall.jacl`

from the directory `/A0` on your CD-ROM or Fix Central.

## About this task

Install and configure the ODCInfo application on the deployment manager of the WebSphere cell.

### Procedure

1. Install the Open Services Gateway initiative (OSGi) bundle.
2. Install the ODCInfo application on the deployment manager.
3. Start the ODCInfo application.
4. Create or modify a load balancer group to use the ODCInfo application to retrieve workload management information from the WebSphere cell.

### Installing the OSGi bundle

Install the Open Services Gateway initiative (OSGi) bundle on the WebSphere Application Server deployment manager.

### Before you begin

Download the `com.ibm.datapower.odc.osgi.jar` file.

**Note:** Uninstall any previous version of the OSGi bundle before installing another version.

## About this task

The OSGi bundle is used to enable the ODCInfo application to interface with the WebSphere Application server.

### Procedure

1. Copy `com.ibm.datapower.odc.osgi.jar` to the `<WAS_HOME>/plugins` directory of the WebSphere Application Server deployment manager.
2. Navigate to the `/bin` directory under `<WAS_HOME>`. For example:

```
cd /opt/IBM/WebSphere/AppServer/bin
```

3. Run the following command: `./osgiCfgInit.sh`
4. Start the OSGi console: `./osgiConsole.sh`.
5. From the console, run the following command:

```
diag com.ibm.datapower.odc.osgi
```

6. Verify that a message states: No unresolved constraints.

## What to do next

Install the ODCInfo application.

### Installing the ODCInfo application

Use a script to install the ODCInfo application on the WebSphere deployment manager. The ODCInfo application provides runtime information to the load balancer group on the DataPower appliance to optimize dynamic load distribution.



## Before you begin

Ensure the WebSphere Application Server product is installed and is running before installing the ODCInfo application. Verify that the OSGi bundle installation is complete.

**Note:** Uninstall any previous version of the ODCInfo application before installing another version.

## About this task

Install the ODCInfo application on the application server that contains the deployment manager for a cell. The ODCInfo application collects information about application servers in the cluster, such as changes in weights or if an application server was added or removed from the cluster.

## Procedure

1. Copy the ODCInfo\_ND61.war file, ODCInfoCheckInstall.jacl, ODCInfoStart.jacl, and ODCInfoDeploy.jacl to a local directory on the deployment manager. The ODCInfo\_ND61.war file applies to both WebSphere ND 6.1 and 7.0 releases.
2. Log in from the command line to the deployment manager.
3. Navigate to the /bin directory under the deployment manager profile. For example:

```
cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin
```

4. Install the ODCInfo application by entering:

```
./wsadmin.sh -f script_path/ODCInfoDeploy.jacl dmgr_server_name  
dmgr_node_name path_to_war_file ODCInfo
```

For example:

```
./wsadmin.sh -f /tmp/ODCInfoDeploy.jacl dmgr wasnode2CellManager01  
/tmp/ODCInfo_ND61.war ODCInfo
```

5. Verify the installation by entering:

```
./wsadmin.sh -f script_path/ODCInfoCheckInstall.jacl cellName  
dmgr_server_name ODCInfo
```

A message is displayed indicating whether the application is installed.

6. Ensure that you define the host name and port for the ODCInfo application as a **host\_alias** for the **default\_host** under WebSphere Application Server **virtual hosts**. For additional information, see the topic on configuring virtual hosts in the WebSphere Application Server documentation.

## What to do next

Start the ODCInfo application.

## Starting the ODCInfo application

Start the ODCInfo application to begin collecting the remote topology and application information.

## Before you begin

The ODCInfo application must be installed and running on the deployment manager of the WebSphere cell (WebSphere environment).

## About this task

Start the ODCInfo application to begin collecting information about the application servers in the WebSphere cell (WebSphere environment).

## Procedure

1. Copy `ODCInfoStart.jacl` to a local directory on the deployment manager.
2. Log in from the command line to the deployment manager.
3. Navigate to the `/bin` directory under the deployment manager profile.

```
cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin
```

4. Start the application by entering:

```
./wsadmin.sh -f script_path/ODCInfoStart.jacl cellName  
dmgr_node_name ODCInfo
```

For example:

```
./wsadmin.sh -f /tmp/ODCInfoStart.jacl dpblade34Cell101  
dpblade34CellManager01 ODCInfo
```

5. Verify that the ODCInfo application started.
  - a. Log in to the WebSphere Administrative Console.
  - b. Click **Applications** **Enterprise Applications**.

## What to do next

Create or modify a DataPower load balancer group.

## Uninstalling the OSGi bundle

To remove the OSGi bundle from the WebSphere Application Server deployment manager, run the uninstall command.

## About this task

Before installing a new version of the OSGi bundle, uninstall any previous version.

## Procedure

1. Navigate to the `/bin` directory under `<WAS_HOME>`. For example:

```
cd /opt/IBM/WebSphere/AppServer/bin
```

2. Start the OSGi console: `./osgiConsole.sh`.
3. From the console, run the following command:

```
uninstall com.ibm.datapower.odc.osgi
```

4. From the `<WAS_HOME>/plugins` directory, delete the `com.ibm.datapower.odc.osgi.jar` file.

## Uninstalling the ODCInfo application

To remove the ODCInfo application from the deployment manager, run the `ODCInfoUninstall` script.

### About this task

Before installing a new version of the ODCInfo application, you must uninstall the old version.

### Procedure

1. Copy the `ODCInfoUninstall.jacl` file to a local directory on the WebSphere deployment manager.
2. Log in from the command line to the deployment manager.
3. Navigate to the **bin** directory of the deployment manager profile. For example:

```
cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin
```

4. Uninstall the application by entering:

```
./wsadmin.sh -f script_path/ODCInfoUninstall.jacl cellName  
dmgr_server_name ODCInfo
```

For example:

```
./wsadmin.sh -f /tmp/ODCInfoUninstall.jacl wasnode2Cell01 dmgr  
ODCInfo
```

5. Verify by entering:

```
./wsadmin.sh -f script_path/ODCInfoCheckInstall.jacl cellName  
dmgr_server_name ODCInfo
```

The response indicates success or failure.

### What to do next

Install the ODCInfo application.

## Enabling the retrieval of workload management information for non-WebSphere application servers

Non-WebSphere application server clusters can use a subset of the features of workload management when a custom software application provides the load balancing configuration data. This section describes the necessary configuration on the DataPower appliance and explains the required format of the configuration data in order for an application other than the ODCInfo application to dynamically modify the load balancer group members.

### Before you begin

The custom software application must be able to provide a properly formatted response to a GET request. The response contains the configuration data for current information about the host weights or if a new host has been added or removed from the cluster.

## About this task

On the DataPower appliance, define the required and optional configurations. Correctly format the XML document and include it in a GET response from your software application.

## Procedure

1. Create or modify a custom software application to provide a properly formatted XML document in the GET response
2. Optional: Define an XML Firewall on the DataPower appliance if you want the appliance to perform schema validation on the XML document
3. Create a WebSphere Cell for non-WebSphere application servers
4. Modify a load balancer group to use workload management information for non-WebSphere application servers

## Results

The following steps describe the message flow and processing actions that are enabled with this configuration:

1. The WebSphere Cell sends an HTTP, or an HTTPS, GET request to the custom software application periodically.
2. The custom software application returns an HTTP, or an HTTPS, response containing load balancer group member configuration information to the WebSphere Cell or optionally to the XML Firewall.
3. Optional: The XML Firewall performs schema validation, as defined in the ODCInfo.xsd schema, on the XML document in the response.
4. The load balancer group uses the configuration data in the response to determine traffic routing when the appliance receives requests directed to the load balancer group.

## Defining the XML Document for non-WebSphere servers

Define the XML document that the custom software application provides in response to the GET request.

When not using the ODCInfo application, a custom software application must be able to respond to a GET request with a properly formatted XML document. The response contains the configuration data for new and current cluster members. This section describes how to properly format the response XML document.

## Before you begin

When not using the ODCInfo application, you must create a custom software application that responds to an HTTP, or an HTTPS, GET request with an XML document that defines the cluster configuration information.

## Define the XML elements

The following XML elements must be specified in the response document:

### **clusterData**

Contains all of the clusters that were requested. The version attribute is associated with the version of the custom software application and is optional.

## cluster

Contains all information associated with a single cluster or workload management group.

- The cluster structure name attribute specifies the name given to the cluster and corresponds with the workload management group name in the DataPower load balancer group
- The version attribute specifies what revision of the data is sent to the DataPower appliance. The version is used to determine if there are any updates to the information since the previous poll. If the version attribute is not present, a manual algorithm is used to determine if the structure has changed.

## affinityMode

The value attribute contains what type of session affinity to use for this cluster. Valid values are active, active-conditional, passive, or null. The affinityMode must be the same for all applications within the load balancer group.

## cookieNames

The value attribute contains a comma (,) separated list of session cookie names used by any of the applications installed to this load balancer group. This list is used for active-conditional or passive session affinity.

**Note:** If you are unfamiliar with WebSphere Application Server passive session affinity, you should use active-conditional session affinity.

## protocol

The type attribute specifies the protocol. Valid values are http or https. No other transport protocols are supported for this function.

## member

The member contains the host (hostname), port number, id (unique identifier for this application server), and weight associated with this application server instance over this transport protocol.

## Example

A properly formatted GET response for a single cluster, that is single workload group name:

```
<?xml version="1.0"?>
  <clusterData version="3.8.1.0">
    <cluster name="myCluster">
      <affinityMode value="active-conditional"/>
      <cookieNames value="WSJSESSIONID, JSESSIONID, SSLJSESSIONID"/>
      <protocol type="http">
        <member host="myhost34.example.com" port="9081" id="13jbh6o3q" weight="20"/>
        <member host="myhost33.example.com" port="9081" id="13jbh6qko" weight="20"/>
        <member host="myhost32.example.com" port="9081" id="140pntcf3" weight="20"/>
      </protocol>
      <protocol type="https">
        <member host="myhost34.example.com" port="9444" id="13jbh6o3q" weight="20"/>
        <member host="myhost33.example.com" port="9444" id="13jbh6qko" weight="20"/>
        <member host="myhost32.example.com" port="9444" id="140pntcf3" weight="20"/>
      </protocol>
    </cluster>
  </clusterData>
```

## What to do next

Optionally, define an XML Firewall on the DataPower appliance if you want the appliance to perform schema validation on the XML document.

## Creating an XML Firewall to validate the XML document

Optionally, create an XML Firewall on the DataPower appliance to schema-validate the XML document provided in the response from a custom software application.

### About this task

If desired, an XML Firewall on the DataPower appliance can validate the XML document that the custom software application sends. Most often, this would be done during initial testing of the application. Once it is proven that the application responds with a valid XML document, remove the XML Firewall from the flow to optimize performance.

### Procedure

1. Follow the procedures to create an XML Firewall.
2. Configure a processing policy with a validate action.
3. In the **Schema Validation Method** field, select **Validate Document via Schema URL**.
4. In the **Schema URL** field, specify store: ///ODCInfo.xsd for the schema file.
5. Complete configuration of the processing policy.
6. Click **Apply** to save the changes to the running configuration information.
7. Optional: Click **Save Config** to save the changes to the startup configuration.

## What to do next

Create a WebSphere Cell to act as an intermediary between the custom software application and the load balancer group.

## Creating a WebSphere Cell for non-WebSphere application servers

Create a WebSphere Cell on the DataPower appliance to act as an intermediary between a custom software application and the load balancer group on the DataPower appliance.

### Before you begin

If you created a DataPower XML Firewall for schema validation of the XML data from a custom software application, you must know the address and port number of the XML Firewall.

### About this task

When not using the ODCInfo application, add and configure a WebSphere Cell to query the custom software application. If there is an information update, the WebSphere Cell sends the updated information to the load balancer group.

**Note:** Poll is the only supported update method in this configuration.

### Procedure

1. Follow the procedures to create a WebSphere Cell.

2. In the **Deployment Manager Host** field, if you are not using an XML Firewall for schema validation, enter either the host name or the IP address of the custom software application. If you are using an XML Firewall for schema validation, enter the address used to access the XML Firewall.
3. In the **Deployment Manager Port number** field, if you are not using an XML Firewall for schema validation, enter the port number associated with the specified host name. If you are using an XML Firewall for schema validation, enter the port number associated with the XML Firewall.
4. In the **Update Method** field, select poll. This is the only supported update method in this configuration.
5. Click **Apply** to save the changes to the running configuration information.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

## What to do next

Create or modify a load balancer group to reference the WebSphere Cell.

## Modifying a load balancing group to use workload management information for non-WebSphere application servers

Modify the configuration of a load balancer group to request workload management information from the independent software vendor application.

## Before you begin

Configure a WebSphere cell and a load balancer group.

## About this task

Configure the load balancer group to request workload management information from the independent software vendor application. The load balancer group uses the WebSphere Cell configuration to gather information about the member application servers.

## Procedure

1. Click **Objects** **Network Settings** **Load Balancer Group**.
2. Click the name of the load balancer group to modify.
3. Modify the load balancer group to use the workload management information from the WebSphere cell.
  - a. Set **Retrieve Workload Management Information** to **on**. The WebGUI refreshes to display additional properties.
  - b. From **Workload Management Retrieval** list, select **WebSphere Cell**.
  - c. From **WebSphere Cell Subscription** list, select the WebSphere Cell configuration that references the independent software vendor application.
  - d. In **Workload Management Group Name** field, enter the name of the application server cluster as it is specified in the cluster attribute of the response XML document.
4. Set **Enable Application Routing** to **off**. This is the only supported option in this configuration.
5. Review the session affinity information on the **Session Affinity** tab to ensure that session affinity is correctly configured.
6. Click **Apply** to save the changes to the running configuration information.
7. Click **Save Config** to save the changes to the startup configuration.

## Results

The load balancer group begins to request information (through the WebSphere cell) from the custom software application.

---

## Defining cryptographic profiles

A Crypto Profile identifies a collection of SSL resources that support SSL connections with remote peer appliances.

To create and configure a Crypto Profile:

1. Click **Objects** **Crypto** **Crypto Profile**.
2. Click **Add**.
3. Provide the following inputs:

### **Name**

Specify the name of the object.

### **Administrative State**

Identifies the administrative state of the configuration.

- To make inactive, click **disabled**.
- To make active, click **enabled**.

### **Identification Credentials**

Select the Identification Credentials to assign to this Profile object, or retain the default value, **none**, when no Identification Credentials is needed.

The Identification Credentials provides the PKI certificate-key pair that will be used to authenticate the appliance during the SSL handshake.

Refer to “Defining Identification Credentials objects” on page 188 for more information.

### **Validation Credentials**

Select the Validation Credentials for this Profile object, or retain the default value, **none**, when no Validation Credentials is needed. Refer to “Validation credentials” on page 221 for more information.

### **Ciphers**

Use the field to identify the symmetric key-encryption algorithms for this Profile object. Common cipher values are as follows:

**ALL** Includes all cipher suites, except the eNULL ciphers.

#### **DEFAULT**

Includes all cipher suites, except for the following ciphers and cipher suites:

- eNULL ciphers
- Cipher suites that use DH authentication
- Cipher suites that contain the RC4, RSA, and SSL version 2 ciphers

**HIGH** Includes all “high” encryption cipher suites. These ciphers support a key length in excess of 128 bits.

#### **MEDIUM**

Includes all “medium” encryption cipher suites. These ciphers support a key length of 128 bits.



**LOW** Includes all “low” encryption cipher suites. These ciphers support a key length of 56 or 64 bits, but exclude EXPORT cipher suites.

**EXPORT**

Includes all cipher suites that support a key length of 40 or 56 bits and are eligible for export outside of the United States.

For a detailed list of ciphers, refer to the **profile** command in the product-specific version of the *Command Reference*.

**Options**

Use the check boxes to disable support for SSL versions and variants. By default, SSL Version 2, SSL Version 3, and Transaction Level Security (TLS) Version 1 are enabled.

- To disable SSL Versions 2, click **Disable-SSLv2**.
- To disable SSL Version 3, click **Disable-SSLv3**.
- To disable TLS Version 1, click **Disable-TLSv1**.
- To allow SSL and TLS renegotiation, which is vulnerable to a man-in-the-middle (MITM) attack documented in CVE-2009-3555, click **Permit insecure SSL renegotiation**.

**Send Client CA List**

Enable or disable the transmission of a Client CA List during the SSL handshake.

**Note:** Transmission of a Client CA List is meaningful only when this Profile object supports a reverse (or server) proxy and when this Profile object has an assigned Validation Credentials.

A Client CA List consists of a listing of the CA certificates in the Validation Credentials for this Profile object. A Client CA List can be sent by an SSL server as part of the request for a client certificate. The Client CA list provides the client with a list of approved CAs whose signatures are acceptable for authentication purposes.

**Note:** SSL servers are *not* required by the protocol to send a Client CA List. Generally, SSL servers do *not* send a Client CA list.

Some implementations or local policies, however, might mandate the use of Client CA lists.

4. Click **Apply** to save the changes to the running configuration.
5. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## RADIUS Settings

RADIUS settings define RADIUS servers. RADIUS settings can be defined in the default domain only.

Within the DataPower appliance, RADIUS servers can be used for the following purposes:

- On any appliance, to authenticate access using RBM.
- On all appliances except XML Accelerator XA35, to authenticate access in AAA Policy objects.

Each RADIUS server has a positional value that the DataPower appliance uses to determine the order in which to contact the servers. The appliances contacts the

servers from most preferred (lowest number) to least preferred (highest number). The appliance sends the request to the next server based on the global timeout value and the global retry value.

If the configuration defines three RADIUS servers with positional values of 10, 20, and 30, the appliance contacts the servers in the following sequence:

1. Requests are always first sent to server 10.
2. If the request times out, it is sent to server 20.
3. If the request times out, it is sent to server 30.

## NAS-identifier

The DataPower appliance is a client to RADIUS servers. The *NAS-identifier* is a RADIUS attribute that the client uses to identify itself to a RADIUS server. The NAS-Identifier, as defined in Section 5.32 of RFC 2865, can be used instead of an IP address to identify the client. The NAS-identifier consists of one or more octets and must be unique in the scope of the RADIUS server. The NAS-identifier is often the fully qualified domain name (FQDN) of the RADIUS client.

## Configuring RADIUS Settings

To configure RADIUS settings, use the following procedure:

1. Select **Administration** **Access** **RADIUS Settings**.
2. Configure global settings for all RADIUS servers.
  - a. Set **Administrative State** to identify the administrative state of the configuration.
    - To make inactive, click **disabled**.
    - To make active, click **enabled**.
  - b. Optional: In the **Comments** field, enter a descriptive summary.
  - c. Specify the NAS-identifier in the **Identifier** field.
  - d. Specify the interval in milliseconds that the appliance waits for a reply from a RADIUS server before retransmitting the outstanding request in the **Timeout** field. Use an integer in the range of 1 through 5000. The default is 1000.
  - e. Specify the number of times that the appliance retransmits an unanswered request to a RADIUS server before contacting another server in the list in the **Retries** field.
3. Do not define RADIUS servers to authentication CLI access without the use of RBM. In other words, do not define any RADIUS servers on the **CLI Servers** tab. This functionality is deprecated. If using RADIUS for authentication, define RADIUS as the RBM method and define the appropriate RADIUS servers on the **AAA/RBM Servers** tab.
4. Define RADIUS servers for use by AAA Policy objects or by the RBM policy.
  - a. Click the **AAA/RBM Servers** tab.
  - b. Define a server.
    - 1) Click **Add**.
    - 2) Specify the relative position of this server in the list in the **Number** field.
    - 3) Specify the IP address or domain name of the server in the **Server Address** field,
    - 4) Specify the listening port on the remote server in the **Server Port** field. The default is 1812.

- 5) Specify the password to log in to the server in the **Secret** field.
- 6) Reenter the password in the **Confirm Secret** field.
- 7) Click **Save**.
- c. Repeat the previous step to add additional servers to the list.
5. Click **Apply** to save the changes to the running configuration.
6. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Adding SSH known hosts

Use the SSH Known Host page to create a list of SSH known hosts.

You do not need to define hosts as a known hosts to use SCP or SFTP. On rare occasions, you might need to change an entry when the server key for an SSH server changes. The server key generally changes only after you reinstall the firmware. If this happens, delete or edit that entry to make SCP or SFTP work again.

To add an SSH peer as an SSH known host, use the following procedure:

1. Select **Administration** **Miscellaneous** **Crypto Tools** to display the Crypto Tools screen.
2. Click the **Add SSH Known Host** tab.
3. Provide the following information:
 

<b>Host</b>	Specify the fully-qualified host name or IP address for the peer. For example: ragnarok.datapower.com 10.97.111.108
<b>Type</b>	Retain <b>ssh-rsa</b> . This is the only selection.
<b>Key</b>	Specify the host public key for the peer. For example: AAAAB3NzaC1yc2EAAAABIwAAAIEA1J/99rRvdZmVvkaKvcG2a+PeCm25 p80Jl87SA6mtFxudA2ME6n3lcXEakpQ8KFTpPbBXt+yDKNFR9gNHI fRl UDho1HAN/a0gEsvrnDY5wKrTcRHrqDc/x0buPzbsEmXi 0l ud5Pl 7+BXQ VpPhyVuj oHI NCrx0k/z7Qpkobz4qZd8==
4. Click **Add SSH Known Host**.

---

## SSL Proxy Profile objects

An SSL Proxy Profile defines a level of SSL service when operating as an SSL proxy. The SSL proxy has the following modes:

### forward

The SSL proxy acts as an SSL client (or acts in the forward direction). In client proxy mode, SSL is used over the appliance-to-server connection.

### reverse

The SSL proxy acts as an SSL server (or acts in the reverse direction). In server proxy mode, SSL is used over the appliance-to-client connection.

### two-way

The SSL proxy acts as both an SSL client and SSL server (or acts in both directions). In two-way mode, SSL is used over the appliance-to-server connection and the appliance-to-client-connection.

## Creating a forward (or client) proxy

To create a forward SSL Proxy Profile, use the following procedure:

1. Select **Objects** **Crypto** **SSL Proxy Profile** to display the SSL Proxy Profile catalog.
2. Click **Add** to display the SSL Proxy Profile Configuration screen.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Select **Forward** from the **SSL Direction** list.
6. Select the profile that defines SSL service to the backend server from the **Forward (Client) Crypto Profile** list.
7. Set **Client-side Session Caching** to enable or disable client side caching.
8. Click **Apply** to save the changes to the running configuration.
9. Optional: Click **Save Config** to save the changes to the startup configuration.

## Creating a reverse (or server) proxy

To create a reverse SSL Proxy Profile, use the following procedure:

1. Select **Objects** **Crypto** **SSL Proxy Profile** to display the SSL Proxy Profile catalog.
2. Click **Add** to display the SSL Proxy Profile Configuration screen.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Select **Reverse** from the **SSL Direction** list.
6. Select the profile that defines SSL service to frontend clients from the **Reverse (Server) Crypto Profile** list.
7. Set **Server-side Session Caching** to enable or disable server side caching.
8. Specify the time that session-specific state data is maintained in the server cache in the **Server-side Session Cache Timeout** field.
9. Specify the maximum size of the server-side cache in the **Server-side Session Cache Size** field.
10. Set **Client Authentication is optional** to control when SSL client authentication is optional.
  - on** Client authentication is not required. When there is no client certificate, the request does not fail.
  - off** (Default) Requires client authentication only when the server cryptographic profile has an assigned Validation Credentials.
11. Set **Always Request Client Authentication** to control when to request SSL client authentication.
  - on** Always requests client authentication.
  - off** (Default) Requests client authentication only when the server cryptographic profile has an assigned Validation Credentials.
12. Click **Apply** to save the changes to the running configuration.

13. Optional: Click **Save Config** to save the changes to the startup configuration.

## Creating a two-way proxy

To create an SSL Proxy Profile, use the following procedure:

1. Select **Objects** **Crypto** **SSL Proxy Profile** to display the SSL Proxy Profile catalog.
2. Click **Add** to display the SSL Proxy Profile Configuration screen.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Select **Two Way** from the **SSL Direction** list.
6. Select the profile that defines SSL service to the backend server from the **Forward (Client) Crypto Profile** list.
7. Select the profile that defines SSL service to frontend clients from the **Reverse (Server) Crypto Profile** list.
8. Set **Server-side Session Caching** to enable or disable server side caching.
9. Specify the time that session-specific state data is maintained in the server cache in the **Server-side Session Cache Timeout** field.
10. Specify the maximum size of the server-side cache in the **Server-side Session Cache Size** field.
11. Set **Client-side Session Caching** to enable or disable client side caching.
12. Set **Client Authentication is optional** to control when SSL client authentication is optional.
  - on** Client authentication is not required. When there is no client certificate, the request does not fail.
  - off** (Default) Requires client authentication only when the server cryptographic profile has an assigned Validation Credentials.
13. Set **Always Request Client Authentication** to control when to request SSL client authentication.
  - on** Always requests client authentication.
  - off** (Default) Requests client authentication only when the server cryptographic profile has an assigned Validation Credentials.
14. Click **Apply** to save the changes to the running configuration.
15. Optional: Click **Save Config** to save the changes to the startup configuration.

---

## Validation credentials

Validation credentials consists of a set of certificates. Validation credentials validate the authenticity of received certificates and digital signatures. You can create validation credentials from the following types of certificates:

- All non-expiring, non-password-protected certificates
- Specific certificates

## Creating for non-expiring, non-password-protected certificates

You can create a validation credentials for all valid, non-expired, non-password-protected certificates in the pubcert: directory. The process silently creates a Certificate object for each valid certificate file in the pubcert: directory.

To create the pubcert validation credentials for non-expiring, non-password-protected certificates:

1. Click **Objects** **Crypto Configuration** **Crypto Validation Credentials**.
2. Click **Create Validation Credential from pubcert:**.
3. Follow the prompts.
4. Optional: Click **Save Config** to save the changes to the startup configuration.

If the validation credentials is in the **down** operational state, one or more certificates might be expired or otherwise unusable. If this occurs, access the pubcert validation credentials and click **View Status**.

## Validation methods

When creating a validation credentials from specific certificates, you must define the validation method. Validation can use one of the following methods:

### Match to an exact certificate or immediate issuer

Validates uses the certificates in the validation credentials. The validation credential contains either the exact peer certificate to match or the certificate of the immediate issuer. The certificate could be an intermediate CA or a root CA. This mode is useful to match the peer certificate exactly, but that certificate is not a self-signed (root) certificate.

### Full certificate chain checking, or PKIX

Validation checks the complete certificate chain from subject to root. Validation succeeds only if the chain ends with a root certificate in the validation credentials. Nonroot certificates in the validation credentials are used as untrusted intermediate certificates. Additional untrusted intermediate certificates will be obtained dynamically from the context at hand (SSL handshake messages, PKCS#7 tokens, PKIPath tokens, and so forth).

When using this validation method, self-signed certificates are considered to be trusted roots assuming that they are correctly designated as CA certificates by their Basic Constraints extension and Key Usage extension, if present. Non-self-signed certificates are considered untrusted intermediates.

The validation credentials must not contain more than one certificate with a given subject name. During client certificate validation, the client can present a set of *other* certificates to be considered when building the certification chain. Only non-self-signed CA certificates are used from this set and are treated as candidate untrusted intermediate certificates.

## PKIX validation

When the validation method is PKIX, the following extensions for CA certificates can be marked as critical. A certificate that contains any other critical extension causes the certificate to be rejected. When a certificate contains other noncritical extensions, these extensions are ignored.

- Key Usage – This extension is not required to be present. If present, it must indicate that the key is suitable for certificate signing.

- Subject Alternative Name – This extension is not used. Regardless of its criticality, validation does not reject a certificate if it contains the extension.
- Basic Constraints – This extension is required in a CA certificate. There is an exception for X509 V1 root certificates. However, all V3 CA certificates must have the extension. Only V3 certificates can be used as intermediates. Fully implemented in accordance to RFC 3280.
- Certificate Policies – Fully implemented in accordance to RFC 3280.
- Authority Information Access – This extension is used for only Online Certificate Status Protocol (OCSP).
- Policy Constraints – Fully implemented in accordance to RFC 3280.
- Inhibit Any-Policy – Fully implemented in accordance to RFC 3280.

## Creating for specific certificates

You can create a validation credentials for existing Certificate objects.

To create a validation credentials for existing certificates:

1. Click **Objects** **Crypto Configuration** **Crypto Validation Credentials**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. From the **Certificates** list, add select certificates to the validation credentials.
6. From the **Certificate Validation Mode** list, select the method for certificate validation.
7. Set **Use CRLs** to control whether each Certificate Revocation List (CRL) is checked during the processing of the certificate chain.
8. When CRLs are checked during certificate chain processing, define controls.
  - a. Set **Require CRLs** to control whether processing fails when CRLs are unavailable.
  - b. From the **CRL Distribution Points Handling** list, select how to handle X.509 extensions.
9. For PKIX validation, define policy sets.
  - a. In the **Initial Certificate Policy Set** field, specify the unique object identifiers for the certificate policy. RFC 3280 refers to the certificate chain validation input variable as the “user-initial-policy-set”. This set of object identifiers specifies the allowable values of certificate policies at the end of chain processing.  
The default is 2.5.29.32.0, which is the object identifier for anyPolicy.
  - b. If you defined an initial policy set, enable **Require Explicit Certificate Policy**. Otherwise, these policy sets will be used only when there are Policy Constraints extensions in the certificate chain.
10. Click **Apply** to save the changes to the running configuration.
11. Optional: Click **Save Config** to save the changes to the startup configuration.



---

## WebSphere Cell

The WebSphere Cell object is responsible for retrieving the configuration information from the WebSphere Network Deployment or the WebSphere Virtual Enterprise back end.

The WebSphere Cell object initiates requests to the ODCInfo application and receives the results as an XML representation of membership, weights, and session affinity information. When the WebSphere Cell object receives the response, it notifies each Load Balancer Group of the new information. The Load Balancer Group then updates its membership, weights, and session affinity information accordingly.

### Selecting the update method

The update method specifies how to retrieve the information from the ODCInfo application on the WebSphere Application Server Network Deployment or WebSphere Virtual Enterprise.

Use one of the following update methods:

- Poll
- Subscribe

The poll update method uses a static polling interval. The poll to retrieve the WebSphere Cell information occurs every interval regardless of whether the WebSphere Cell configuration has changed.

The subscribe update method specifies that the request to retrieve the WebSphere Cell information waits for either the duration of the time interval to expire or for the WebSphere Cell information to change, whichever occurs first. If the ODCInfo application has any new information, the application immediately responds with an XML document. If there is no new information, the ODCInfo application delays for the specified time interval number of seconds before returning with the current, unchanged XML document.

The subscribe method results in more responsive updates by the appliance to changes in the cell. Using this method might result in several updates within a short amount of time. As a result, the subscribe method consumes more resources on the appliance and on the server that is running the ODCInfo application. The subscribe method is more appropriate when application routing is enabled, and must be used if application edition (group and atomic rollout) functions are used.

**Note:** To use the subscribe update method, the version of the ODCInfo application must match the firmware version. A back-level ODCInfo application is not supported.

### Creating a WebSphere Cell

Create a WebSphere Cell on the DataPower appliance to act as an intermediary between the ODCInfo application on the WebSphere deployment manager and the load balancer group on the DataPower appliance.



## Before you begin

The ODCInfo application must be installed, and you need to know the host and port of the WebSphere deployment manager where this application is installed. To find the port number

1. From the WebSphere Administrative Console, click **System Administration Deployment Manager ports**.
2. Select the port name:
  - Click the **WC\_adminhost** port name for HTTP.
  - Click the **WC\_adminhost\_secure** port name for HTTPS.

To create this configuration, the DataPower appliances require the Option for Application Optimization feature.

## About this task

Add and configure a WebSphere Cell to query the ODCInfo application for current information about the host weights or if a new host has been added or removed from the cluster. If there is an information update, the WebSphere Cell sends the updated information to the load balancer group.

## Procedure

1. Click **Objects Configuration Management WebSphere Cell**.
2. Click **Add**.
3. In the **Name** field, enter a name.
4. Retain the default setting for **Admin State**. To place in an inactive administrative state, click **disabled**.
5. Optional: In the **Comments** field, enter a brief descriptive summary.
6. In the **Deployment Manager Host** field, enter the host name or IP address of the deployment manager with the installation of the ODCInfo application.
7. In the **Deployment Manager Port number** field, enter the port of the deployment manager.
8. Optional: From the **SSL Proxy Profile** list, select the SSL proxy profile for a secured connection.
9. In the **Update Method** field, indicate whether to use a static polling interval or to subscribe to the WebSphere cell information.
10. In the **Time Interval** field, if the update method is poll, specify the amount of time in seconds between poll requests. If the update method is subscribe, specify the maximum duration of the request in seconds. The recommended value is 10 seconds.
11. Click **Apply** to save the changes to the running configuration information.
12. Optional: Click **Save Config** to save the changes to the startup configuration.

## What to do next

Create or modify a load balancer group to reference the WebSphere Cell.

---

## NSS Client

The NSS client enables integration with RACF® on the z/OS Communications Server. The NSS Client object specifies the authentication information required to allow the DataPower appliance to function as an NSS client. The NSS Client object specifies the following properties:

- **Remote Address**
- **Remote Port**
- **SSL Proxy Profile**
- **Client ID**
- **System Name**
- **User Name**
- **Password**

Based on these properties and the request type, the following actions occur:

- DataPower requests a secure connection to the z/OS Communications Server
- RACF performs authentication of users
- RACF performs authorization to resources
- RACF logs authorized and unauthorized attempts to access RACF-protected resources
- z/OS Communications Server NSS protocol provides return codes and reason codes for connectivity requests

To support this functionality, the NSS server must be configured to support the NSS client. See the following z/OS Communications Server documentation for these configuration steps:

- Enable the **XMLAppliance** discipline support. For further information, refer to the section on network security services server in the *z/OS Communications Server: IP Configuration Reference*.
- Authorize the client userid to SAF profiles representing security services and resources. For further information, refer to the section on preparing to provide network security services in the *z/OS Communications Server: IP Configuration Guide*.
- Configure SSL for the TCP connection between the client and server. For further information, refer to the section on configuring the NSS server in the *z/OS Communications Server: IP Configuration Guide*.

Only one physical connection per **Remote Address**, **Remote Port**, and **Client ID** is allowed. Additional NSS Client objects might be configured, but if more than one client with the same tuple try to connect, the connection will fail. If the connection is not established or the provided parameters are not valid, the object operational state is **down** and shows one of the following event codes:

- Invalid registration parameters
- TCP connection retry (interval is 1 minute)
- TCP connection in progress
- Communication failed
- Cannot connect to host

For additional information on logged NSS protocol return codes and reason codes, refer to <http://www.ibm.com/support/docview.wss?rs=852&uid=swg21329236> for *z/OS Communications Server: IP Diagnosis Guide* updates.

**Contact NSS for SAF Authentication** is selected as the Authenticate method in the AAA policy configuration and **Contact NSS for SAF Authorization** is selected for the Authorization method.

## Creating the NSS Client

To configure an NSS client:

1. Click **OBJECTS   z/OS Configurations   NSS Client**.
2. Click **Add**.
3. In the **Name** field, enter the name for the object.
4. Set **Administrative State** to identify the administrative state of the configuration.
  - To make inactive, click **disabled**.
  - To make active, click **enabled**.
5. Optional: In the **Comments** field, enter a descriptive summary.
6. In the **Remote Address** field, specify the IP address or hostname of the NSS server.
7. In the **Remote Port** field, specify the port on which the NSS server listens.
8. From the **SSL Proxy** list, select an SSL Proxy Profile to provide a secured connection to the remote authentication server.
9. In the **Client ID** field, specify the client ID to use for registration with the NSS server.
10. In the **System Name** field, specify the system name to identify the NSS client to the NSS server.
11. In the **User Name** field, specify the user name to use to authenticate with the SAF.
12. In the **Password** field, specify the password to use to authenticate with the SAF.
13. Reenter the password in the **Confirm Password** field.
14. Click **Apply** to save the changes to the running configuration.
15. Optional: Click **Save Config** to save the changes to the startup configuration.



---

## Appendix. User interface customization

This appendix contains information about creating an XML file that defines aspects of the command line interface and the WebGUI user interface that you can customize. By using these custom interface extensions, the DataPower interfaces can display business and IT-centric information to users on each DataPower appliance.

Each DataPower appliance can have a different custom user interface file, and all customized aspects of the interfaces apply to all users in all application domains.

To customize the user interfaces and to adhere to best practices, complete the following high-level procedures:

1. Build an XML that defines the aspects of the user interfaces to customize.
2. Validate the conformance of the file against its schema.

The remaining sections of this appendix detail the markup that is necessary to custom-tailor this XML file.

Using any text editor to create the XML file, you must cut and paste the markup, and then specify the content of each customized message within the markup.

After the XML file is complete, validate the conformance of the file against its schema with the **test schema** command. For information about the **test schema** command, refer to the product-specific version of the *Command Reference*.

---

### Aspects that can be customized

You can custom-tailor the following aspects of the user interfaces:

- The command line prompt extension to include the appliance identifier.
- Pre-login, post-login, and appliance messages in command line sessions.
- Pre-login, post-login, and appliance messages in WebGUI sessions, and the text color and background color for these messages.

---

### Markup supported for the XML file

When creating an XML file that defines the custom aspects of the user interface, the schema supports the following case-sensitive elements:

#### <User-Interface>

The <User-Interface> element is the root element of the XML file and defines the required namespace statements. The XML file must contain this element from the template without modification.

#### <CustomPrompt>

The <CustomPrompt> element indicates whether to extend the command line prompt with the appliance identifier. To enable this aspect, add this element from the template without modification.

#### <MarkupBanner>

The <MarkupBanner> element identifies the messages to display to users in WebGUI sessions. The file can contain up to four <MarkupBanner> elements, based on a combination of the `type` attribute and `location` attribute.

The element supports the following attributes:

`type="message-type"`

The `type` attribute identifies the type of message. This attribute supports the following keywords:

`pre-login`

Displays the message before users log in to the WebGUI. You can define one pre-login message.

`post-login`

Displays the message in a popup window immediately after users log in to the WebGUI. You can define one post-login message.

`system-banner`

Displays the message on each WebGUI screen. You can define two appliance messages depending on the keyword associated with the `location` attribute. Use the `location` attribute to define where on the WebGUI screen to display the message.

`location="location"`

The `location` attribute indicates the location on the WebGUI screen to display the message. This attribute is relevant only when used with `type="system-banner"`. The `location` attribute supports the following keywords:

`header` Displays the message at the top of each WebGUI screen. You can define one message with this keyword. You cannot define a message with this keyword and another with the both keyword.

`footer` Displays the message at the bottom of each WebGUI screen. You can define one message with this keyword. You cannot define a message with this keyword and another with the both keyword.

`both` (Default) Displays the message at the top and the bottom of each WebGUI screen. You can define one message with this keyword. You cannot define a message with this keyword and another with the header keyword or with the footer keyword.

`foreground-color="color"`

The `foreground-color` attribute identifies the color of the text in the WebGUI message. This attribute supports the following keywords:

- none (Default)
- blue
- green
- orange
- red
- yellow

The none keyword displays the text of a message in black.

`background-color="color"`

The `background-color` attribute identifies the color of the background in the WebGUI message. This attribute supports the following keywords:

- none (Default)
- blue
- green
- orange
- red
- yellow

The `none` keyword removes any color from the message background.

For WebGUI messages, the contents of the `<MarkupBanner>` element can include the following standard HTML tags:

- `<p>` Defines individual paragraphs.
- `<em>` Defines text to display in italics.
- `<strong>` Defines text to display in bold.
- `<tt>` Defines text to display in monospace.

#### `<TextBanner>`

The `<TextBanner>` element identifies the messages to display to users in command line sessions. The file can contain up to three `<TextBanner>` elements, one for each keyword associated with the `type` attribute.

This element supports the following attribute:

`type="message-type"`

The `type` attribute identifies the type of message. This attribute supports the following keywords:

#### `pre-login`

Displays the message before users log in from the command line.

#### `post-login`

Displays the message immediately after users log in from the command line.

#### `system-banner`

Displays the message immediately after completing each command invocation from the command line.

For command line messages, the content of the `<TextBanner>` element cannot include other HTML or XML elements.

---

## Structure of the XML file

The following excerpts display the structure of the XML file that defines aspects of the command line interface and the WebGUI interface that you can customize. For a complete sample, refer to “Template of the custom user interface file” on page 234.

```
<User-Interface
  xmlns="http://www.datapower.com/schemas/user-interface/1.0">
  <CustomPrompt>%s</CustomPrompt>
  <MarkupBanner ... > ... </MarkupBanner>
  <TextBanner ... > ... </TextBanner>
</User-Interface>
```

---

## Command line prompt extension definition

To custom-tailor the command line prompt, you must add the following markup without modification to the XML file:

```
<CustomPrompt>%s</CustomPrompt>
```

The %s indicates a variable that represents the appliance identifier, as defined with the **System Identifier** field in System Settings (**Administration Device System Settings**).

For example, if the **System Identifier** field is **IDD**, the generic **xi50#** prompt would change to the custom **IDD: xi50#** prompt.

---

## Example messages for WebGUI sessions

Messages for WebGUI sessions include the pre-login message, the post-login message, and the appliance message. WebGUI messages can be an unlimited number of characters in length.

### Example pre-login message

The following example shows the markup for a pre-login message that displays before users log in. In this example, the color behind the message is blue.

```
<MarkupBanner type="pre-login" background-color="blue">
  XYZ LLC - London
</MarkupBanner>
```

### Example post-login message

The following example shows the markup for a post-login message that displays in a popup window immediately after users log in. In this example, the text color is red, and the word “refreshed” is in italics.

```
<MarkupBanner type="post-login" foreground-color="red">
  XYZ cycles after-hour servers each day. Use a <em>refreshed</em>
  server number at all times.
</MarkupBanner>
```

### Example appliance messages

System messages for WebGUI sessions can be displayed on the top of the screen (location= "header"), the bottom of the screen (location= "footer"), or in both locations (location= "both").

The following example shows the markup for an appliance message that displays on the top of the screen. In this example, the text color is green on a red background.

```
<MarkupBanner type="system-banner" location="header"
  foreground-color="green" background-color="red">
  Use a supervisor console to access a public Internet Web site.
</MarkupBanner>
```



The following example shows the markup for an appliance message that displays on the bottom of the screen. In this example, the text color is blue on a yellow background.

```
<MarkupBanner type="system-banner" location="footer"
  foreground-color="blue" background-color="yellow">
  Use a supervisor console to access a public Internet Web site.
</MarkupBanner>
```

---

## Example messages for command line sessions

Messages for command line sessions include the pre-login message, the post-login message, and the appliance message. Pre-login and post-login messages can be an unlimited number of characters in length, but appliance messages are limited to 255 characters in length.

### Example pre-login message

The following example shows the markup for a pre-login message that displays before users log in.

```
<TextBanner type="pre-login">
  Use XYZ access codes for all external requests.
</TextBanner>
```

### Example post-login message

The following example shows the markup for a post-login message that displays immediately after users log in.

```
<TextBanner type="post-login">
  Only XYZ employees are authorized to use this station.
</TextBanner>
```

### Example appliance message

The following example shows the markup for an appliance message that displays after each command invocation.

```
<TextBanner type="system-banner">
  XYZ NA
</TextBanner>
```

---

## Template of the custom user interface file

The following template is an XML file to help you create the custom user interface file for your DataPower appliance. This template conforms to the schema (store:///schemas/dp-user-interface.xsd).

```
<User-Interface
  xmlns="http://www.datapower.com/schemas/user-interface/1.0">

  <!-- Markup for the prompt extension to command line interface -->
  <CustomPrompt>%s</CustomPrompt>

  <!-- Markup for custom messages for the WebGUI interface -->
  <MarkupBanner type="pre-login" foreground-color="red" background-color="blue">
    WebGUI pre-login message
  </MarkupBanner>
  <MarkupBanner type="post-login" foreground-color="blue" background-color="yellow">
    WebGUI post-login pop up message
  </MarkupBanner>
  <MarkupBanner type="system-banner" location="header" foreground-color="green"
    background-color="red">
    WebGUI system message - header
  </MarkupBanner>
  <MarkupBanner type="system-banner" location="footer" foreground-color="blue"
    background-color="yellow">
    WebGUI system message - footer
  </MarkupBanner>

  <!-- If the following markup was outside of comments, the file would not
    conform to the schema. Cannot define multiple system messages as the
    header or footer. -->
  <MarkupBanner type="system-banner">
    WebGUI system message - header and footer
  </MarkupBanner>

  <!-- Markup for custom messages for the command line interface -->
  <TextBanner type="pre-login">
    Command line pre-login message
  </TextBanner>
  <TextBanner type="post-login">
    Command line post-login message
  </TextBanner>
  <TextBanner type="system-banner">
    Command line system message
  </TextBanner>
</User-Interface>
```

---

## Notices and trademarks

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements or changes in the product(s) or the program(s) described in this publication at any time without notice.

---

## Trademarks

IBM, the IBM logo, DataPower, and WebSphere are registered trademarks of the International Business Machines Corporation in the United States or other countries. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (<sup>®</sup> or <sup>™</sup>), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

---

# Index

## Special characters

- ... button
  - list of referenced object 9
  - referenced object 8
- .java.policy file 135
- + button
  - list of referenced object 9
  - referenced object 8

## Numerics

- 9235 features
  - auxiliary data storage 139

## A

- AAA
  - authentication
    - search parameters 34
    - search parameters 34
- AAA Policy
  - NSS Client 226
- accepted configuration
  - deployment policy 163
- Access Control List
  - clause sequence 185
  - configuring 186
  - creating 186
  - IPv6 185
  - object pages 186
  - overview 185
  - ssh instance 185
  - SSH service 185
  - Web Management Service 185
  - web-mgmt instance 185
  - XML Management Interface 185
  - xml-mgmt instance 185
- access management 17
- access policy
  - adding 50
  - editing access profile 52
  - elements 49
  - examples
    - granting full access 51
    - granting user management permissions 51
    - using wildcards 51
  - removing access profile 52
- Access Policy builder 49
- access profile
  - editing access policy 52
  - removing from access policy 52
- access rights for CLI
  - defined on user groups 47
- access rights for WebGUI
  - defined on group account 46
- accounts
  - See also* group-defined accounts
  - See also* privileged accounts
  - See also* user accounts

- accounts (*continued*)
  - accessing MIB 55
  - changing passwords 55
  - creating SNMP users 56
  - forcing password change 54
  - group-defined access level 53
  - managing 53
  - privileged access level 53
  - RBM policy 35
  - user access level 53
- ACL
  - See* Access Control List
- Add button
  - list of referenced object 9
- Address Resolution Protocol (ARP)
  - See* ARP
- admin account
  - exporting configuration data 149
- Administration menu 7
- administrative interfaces
  - command line 112
  - WebGUI 111
- administrative states, objects 12
- administrators
  - network access 111
- allow clauses, ACL 185
- AMP endpoint 116
- AP-REQ message, Kerberos 189
- appliance
  - generating appliance certificate 91
  - quiescing 109
  - rebooting 90
  - reloading firmware 90
  - rolling back firmware 129
  - selecting reboot configuration 88
  - setting time 86
  - shutting down 90
  - unquiescing 109
  - upgrading firmware 129
- appliance certificate 91
- appliance configuration
  - backing up 149
  - comparing 158
  - configuration checkpoints 154
  - copying
    - files 152
    - objects 152
  - disaster recovery 159
  - end-of-life management 159
  - exporting 149
    - select objects and files 150
  - importing configuration 156
  - managing configuration changes 157
  - moving
    - files 152
    - objects 152
  - reading change report 158
  - restoring from secure backup 161
  - reverting changes 159
  - secure backup 161
  - undoing changes 159

- appliance configuration (*continued*)
  - validating a secure backup 162
- appliance management 69
- appliance settings
  - audit log space 93
  - contacts 92
  - customizing interfaces 92
  - identifier 92
  - location 92
  - purpose 91
  - read-only properties 93
  - replacement appliance 92
  - SNMP system table 93
  - updating serial number 92
  - viewing system information 93
- appliance-wide log
  - location 132
- Application Domain
  - object pages 144
- application domains
  - See also* domains
  - backing up configuration 150
  - catalog 144
  - creating 144
  - quiesce 146
  - restarting
    - from catalog 145, 146
    - from System Control pane 146
    - from System Control panel 145
  - unquiesce 146
- Apply button 11
- ARP
  - defining retries 81
  - defining retry intervals 81
- aspects of
  - customizing the interface 229
- au-method of authentication
  - RBM policy file 39
- audit log
  - location 131
  - reserving space 93
  - viewing 131
- audit: directory 131
- authenticate users
  - RBM 18
- authentication
  - configuring RADIUS settings 217
  - custom RBM method 21
  - LDAP 34
  - LDAP RBM method 22
  - local user RBM method 24
  - RADIUS RBM method 25
  - RBM 18
  - SAF RBM method 27
  - search parameters 34
  - SPNEGO RBM method 28
  - SSL user certificate RBM method 30
  - XML file RBM method 31
- authfile.xml file 39
- authorization
  - RBM 19

- authorize access to users
  - RBM 19
- auto-config.cfg file 11
- auxiliary data storage 139

## B

- backupmanifest.xml file 160
- bold typeface 4
- builder
  - access policy 49
  - deployment policy 164
  - RBM policy file 39
- buttons
  - ... 8
  - + 8
  - Apply 11
  - Cancel 11
  - Delete 11
  - Edit 9
  - Logout 7
  - Save Config 7, 11
  - Undo 11
  - View 9

## C

- caches
  - DNS hosts 82
  - flushing 84
  - status provider 84
- Cancel button 11
- capabilities
  - RBM 18
- capture.pcap file 80
- cert: directory 131
- certificate files
  - location 131
- Certificate objects
  - export packages 149
- Certificate Revocation List
  - See CRL
- certificates
  - converting 65
  - DER 61
  - exporting 63
  - generating 62
  - importing 64
  - PEM 61
  - PKCS #12 61
  - PKCS #8 61
  - security
    - location, shared 132
    - location, Web browsers 132
  - supported formats 61
  - uploading 135
- checkpoint configuration files
  - location 131
- chkpoints: directory 131
- CLI
  - removing access to a command group 47
- CLI access rights
  - defined on user groups 47
- command groups
  - controlling access 47

- command line
  - access 112
  - customizing the interface 229
  - enabling custom prompt 92
  - RBM
    - changing admin-state 37
    - restoring access 36
- commands
  - See also utilities
  - unknown 19
  - web-mgmt 7, 128
- communities, SNMP 103
- compact flash
  - configuring 139
  - file system
    - initializing 139
    - managing 139
    - repairing 140
- config: directory 131
- configuration
  - managing appliance configuration 143
- configuration checkpoints
  - defining number to allow 154
  - deleting 155
  - listing 155
  - loading 155
  - overwriting 154
  - rolling back 155
  - saving 154
- configuration data
  - applying 11
  - backing up
    - SOAP Interface 120
    - WebGUI 149
  - backing up application domains 150
  - comparing
    - SOAP Interface 119
    - WebGUI 158
  - configuration checkpoints 154
  - copying
    - files 152
    - objects 152
  - different release level 149
  - exchanging 149
  - exporting
    - location of files 131
    - select objects and files 150
    - SOAP Interface 120
    - WebGUI 149
  - files not included 149
  - importing
    - SOAP Interface 120
    - WebGUI 149, 156
  - managing changes 157
  - moving
    - files 152
    - objects 152
  - objects not included 149
  - reading change report 158
  - reading changes 159
  - restoring
    - SOAP Interface 120
  - saving 11
  - undoing changes 159
- configuration files
  - exported, location 131

- configuration files (*continued*)
  - location 131
- configuration states, objects 12
- Conformance Report
  - generating
    - SOAP Interface 120
- contexts, SNMP 104
- Control Panel
  - File Management 133
- credentials
  - identification
    - configuring 188
    - creating 188
- credentials mapping
  - LDAP 34
  - search parameters 34
- CRL
  - enabling update policy 65
  - update policy 65
- CRL Retrieval
  - object pages 65
- Crypto Certificate
  - configuring 186
  - creating 186
  - object pages 186
- Crypto Certificate Monitor
  - configuring 67
  - creating 67
  - object pages 67
- Crypto Identification Credentials
  - object pages 188
- Crypto Key
  - configuring 192
  - creating 192
  - object pages 192
- Crypto Profile
  - configuring 216
  - creating 216
- Crypto Tools
  - adding SSH known hosts 219
  - converting certificates 65
  - converting keys 64
  - exporting certificates 63
  - exporting keys 63
  - generating certificates 62
  - generating keys 62
  - importing certificates 64
  - importing keys 64
- customizing the interface
  - aspects of 229
  - defining messages for CLI 233
  - defining messages for WebGUI 232
  - defining the CLI prompt 232
  - structure of XML file 231
  - supported markup 229

## D

- dashboard 7
- data storage
  - 9235 only 139
  - auxiliary 139
  - compact flash
    - configuring 139
  - file system, initializing 139
  - file system, managing 139
  - file system, repairing 140

- data storage (*continued*)
  - hard disk array
    - configuring 140
    - file system, initializing 140
    - file system, managing 140
    - file system, repairing 140
    - RAID volume, activating 141
    - RAID volume, deleting 141
    - RAID volume, initializing 141
    - RAID volume, managing 141
    - RAID volume, rebuilding 141
- date
  - setting 86
- default log
  - location 132
- defining messages for CLI
  - customizing the interface 233
- defining messages for WebGUI
  - customizing the interface 232
- defining the CLI prompt
  - customizing the interface 232
- del-config element 121
- Delete button 11
  - list of referenced object 9
- deny clauses, ACL 185
- deployment policy
  - accepted configuration 163
  - creating 163
  - filtered configuration 163
  - modified configuration 163
  - using the builder 164
- Deployment Policy
  - object pages 163
- deployment policy builder
  - creating matching statements 164
- DER
  - certificate format 61
  - key format 61
- destination based routing, managing 81
- directories
  - audit: 131
  - available 131
  - cert: 131
  - chkpoints: 131
  - config: 131
  - displaying contents 133
  - dpcert: 131
  - export: 131
  - hiding contents 133
  - image: 131
  - local: 131
  - logstore: 131
  - logtemp: 132
  - managing 131
  - pubcert: 132
  - refreshing contents 134
  - sharedcert: 132
  - store: 132
  - tasktemplates: 133
  - temporary: 133
- disabled administrative state 12
- disaster recovery
  - conditions 160
  - creating a secure backup 161
  - managing configuration 159
  - manifest 160
  - restoring from a secure backup 161

- disaster recovery (*continued*)
  - validating secure backup 162
- DNS hosts cache
  - flushing 84
  - purpose 82
  - status provider 84
- DNS Settings
  - configuring name resolution 84
  - hosts cache 82
  - IPv6 82
  - load balancing 82
  - purpose 82
  - search domains 84
  - static hosts 84
- do-action element 120
- do-backup element 120
- do-export element 120
- do-import element 120
- do-restore element 120
- documentation conventions, typefaces 4
- Domain list 7
- domains
  - application domains 143
  - default domain 143
  - managing 143
  - visible domains 144
- down operation state 12
- dpcert: directory 131

## E

- e-mail pager
  - configuring 174
- ECN
  - disabling TCP sessions 81
- Edit button 9
- enabled administrative state 12
- end-of-life, managing configuration 159
- endpoints
  - AMP 116
  - SLM 116
  - UDDI Subscription 116
- enterprise MIBs
  - See* MIBs
- ethereal utility 80
- Ethernet Interface
  - configuring 76
  - managing 76
  - object pages
    - Main 76
    - Standby Control 78
    - Static Routes 78
- Ethernet interfaces
  - failover 70
  - IPv6 69
  - overview 69
  - packet capture 80
  - removing from network 80
  - self-balancing 70, 73
  - standby configuration 69
  - standby groups 70
  - static routes 78
- EUI
  - format 99
  - iSCSI Initiator 99
  - iSCSI Target 99

- evaluate access profile
  - RBM 18
- event logging 167
- event subscription filters
  - setting 169
- event subscriptions
  - setting 171
- event suppression filters
  - setting 169
- event triggers
  - setting 170
- Event triggers
  - example
    - Log Target 175
- examples
  - access policy
    - granting full access 51
    - granting user management permissions 51
    - using wildcards 51
  - SOAP Interface
    - comparing configurations 122
    - sample request, compare configurations 123
    - sample request, status 122
    - sample response, compare configurations 123
    - sample response, status 122
    - viewing status 121
- Explicit Congestion Notification (ECN) in TCP
  - See* ECN
- Export link 12
- export packages
  - admin account 149
  - files not included 149
  - objects not included 149
  - permission 149
- export: directory 131
- Extended Unique Identifier
  - See* EUI

## F

- failover
  - Ethernet interfaces 70
  - VLAN interfaces 70
- failover mode
  - Ethernet interfaces 70
  - VLAN interfaces 70
- file formats
  - pcap 80
- file management
  - iSCSI
    - repairing volume 100
- File Management utility, launching 133
- file space
  - throttle 88
- file system
  - See* directories
- files
  - .java.policy 135
  - authfile.xml 39
  - auto-config.cfg 11
  - backupmanifest.xml 160
  - capture.pcap 80

## files (*continued*)

- certificates
  - location 131
- checkpoint configurations
  - location 131
- configurations
  - location 131
- copying 136
  - remote URL 136
- creating custom user interface 234
- deleting 138
- downloading
  - SOAP Interface 120
- editing
  - during configuration 10
  - File Management utility 138
- exported, location 131
- fetching 136
- listing
  - SOAP Interface 120
- logs
  - filtering 172
  - sorting 173
  - viewing 172
- managing 131
- moving 137
- not in export packages
  - firmware files 149
  - log files 149
- packet captures (pcap) 80
- private keys
  - location 131
- RBMInfo.xml 39
- renaming 137
- uploading
  - JKS 135
  - remote 136
  - SOAP Interface 120
  - workstation 134
- viewing
  - during configuration 10
  - File Management utility 138
- XML Management Interface
  - schema 118
  - WSDL 118
- xml-mgmt-base.xsd 118
- xml-mgmt-ops.xsd 118
- xml-mgmt.wsdl 118
- xml-mgmt.xsd 118

filtered configuration

- deployment policy 163

firmware

- applying 129
- rolling back 129
- upgrading 129

firmware files

- between release levels 149
- export packages 149

firmware images

- location 131

flash drive

- See* directories

flush RBM cache

- RBM 37

## G

- get-config element 121
- get-conformance-report element 120
- get-diff element 119
- get-file element 120
- get-filestore element 120
- get-log element 120
- get-samlart element 119
- get-status element 119
- group account
  - defining access rights for WebGUI 46

## H

hard disk array

- configuring 140
- file system
  - initializing 140
  - managing 140
  - repairing 140
- RAID volume
  - activating 141
  - deleting 141
  - initializing 141
  - managing 141
  - rebuilding 141

HELO exchange, (unknown) 92

Host Alias

- object pages 84

host aliases

- using local aliases 84

hosts

- adding known (SSH) 219

hosts cache

- DNS
  - flushing 84
  - purpose 82
  - status provider 84

HTTP Service

- configuring HTTP Service
  - objects 181
- creating HTTP Service objects 181
- object pages 181
- service description 181

## I

ICMP

- disabling 81
- managing requests 81

Identification Credentials

- configuring 188
- creating 188

image: directory 131

Import Package

- creating 148

Include Configuration File

- creating 147

installation images

- See* firmware images

intellectual property 235

interface isolation

- enforcing 81
- relaxing 81

IP address filters

- setting 171

## IPv6

- DNS 82
- Ethernet interfaces 69
- VLAN interfaces 69

## IQN

- format 99
- iSCSI Initiator 99

iSCSI CHAP

- configuring 102
- object pages 102

iSCSI HBA

- See* iSCSI Initiator

iSCSI Host Bus Adapter

- See* iSCSI Initiator

iSCSI Initiator

- configuring 101
- IQN 99
- object pages 101

iSCSI qualified name

- See* IQN

iSCSI Target

- configuring 101
- EUI 99
- IQN 99
- object pages 101

iSCSI volume

- configuring 99
- initializing 100
- managing 99
- repairing 100

iSCSI, support 98

italics typeface 4

## J

J2RE (j2re1.4.2) 135

j2re1.4.2 (J2RE) 135

j2sdk1.4.2 (SDK) 135

Java Crypto Extension

- See* SunJCE

Java Crypto Extension Key Store

- See* JCEKS

Java Key Store

- See* JKS

java.security package 135

JCE

- See* SunJCE

JCEKS 135

JKS

- crypto extension 135
- granting permissions 135
- java.security package 135
- keytool utility 135
- managing 135
- required software 135
- uploading certificates 135
- working with 135

## K

KDC, Kerberos 189

Kerberos

- AP-REQ message 189
- configuring KDC server 190
- KDC 189
- keytab 189



- Kerberos (*continued*)
  - principal 189
- Kerberos KDC server
  - configuring 190
  - creating 190
  - object pages 190
- Kerberos keytab
  - configuring 191
  - definition 189
- Kerberos Keytab File
  - object pages 191
- Key Distribution Center
  - See* KDC
- Key objects
  - export packages 149
- key-certificate pairs
  - creating 61
- keys
  - converting 64
  - DER 61
  - exporting 63
  - generating 62
  - importing 64
  - PEM 61
  - PKCS #12 61
  - PKCS #7 61
  - supported formats 61

**L**

- LDAP
  - authentication
    - search parameters 34
  - credentials mapping
    - search parameters 34
  - RBM authentication 22
  - search parameters 34
- LED lights
  - locate LED
    - activating 91
    - controlling 91
    - deactivating 91
- licensing
  - sending inquiries 235
- limitations
  - RBM account policy 35
- links
  - Export 12
  - View Logs 12
  - View Status 12
- load balancer group
  - adding members 204
  - basic configuration 203
  - creating 194, 202
  - health
    - convalescent (down) 200
    - healthy (up) 200
    - quarantined (softdown) 200
  - health checks
    - enabling 205
    - overriding port 203
  - health of members 200
  - members
    - assigning weight 207
    - disabling members 207
  - server state 194

- Load Balancer Group
  - example
    - Log Target 174
- load balancing
  - DNS 82
- local: directory 131
- locate LED
  - activating 91
  - controlling 91
  - deactivating 91
- log categories
  - configuring 168
- log files
  - export packages 149
  - filtering 172
  - understanding 173
  - viewing 172
- Log Target
  - Event triggers 175
  - Load Balancer Group 174
  - XML Manager 174
- log targets
  - configuring 168
  - event subscription filters 169
  - event suppression filters 169
  - event triggers 170
  - IP address filters 171
  - managing 168
  - object filters 169
  - types 167
- login token, retrieving 119
- Logout button 7
- logs
  - appliance-wide
    - location 132
  - audit
    - location 131
    - viewing 131
  - default
    - location 132
  - retrieving
    - SOAP interface 120
  - viewing configuration-specific
    - logs 12
  - viewing from catalog 12
  - viewing from configuration pane 12
- logstore: directory 131
- logtemp: directory 132

**M**

- macros, unknown 19
- Management Information Base
  - See* MIB
- manifests
  - secure backup 160
- matching statements
  - deployment policy builder 164
  - deployment policy, manual 165
- mc-method of authorization
  - RBM policy file 39
- memory
  - throttle 88
- message catalogs 132
- MIB
  - configuring access 55

- MIBs
  - viewing 105
- modified configuration
  - deployment policy 163
- Modified configuration state 12
- modify-config element 121
- monospaced typeface 4

**N**

- NAS-identifier 218
- navigation
  - Administration menu 7
  - Network menu 7
  - Objects menu 7
  - Services menu 7
  - Status menu 7
- network
  - removing Ethernet interfaces 80
- network access
  - administrators 111
  - command line 112
  - serial port 112, 113
  - SSH 114
  - SSL proxy profile 127
  - WebGUI 111
- Network menu 7
- network setting
  - ARP retries 81
  - ECN in TCP 81
  - ICMP 81
  - interface isolation 81
  - routing 81
  - source address 82
  - TCP retries 81
  - TCP segmentation offload 81
  - TCP Window Scaling 82
- network settings
  - object pages 80
- New configuration state 12
- NFS Dynamic Mounts
  - object pages 94
- NFS Static Mounts
  - object pages 96
- notices 235
- notification recipients
  - SNMP 104
- NSS Client
  - creating 227
  - overview 226
- NTP Service
  - object pages 86

**O**

- object filters
  - setting 169
- object pages
  - Access Control List 186
  - Application Domain 144
  - CRL Retrieval 65
  - Crypto Certificate 186
  - Crypto Certificate Monitor 67
  - Crypto Identification Credentials 188
  - Crypto Key 192
  - Deployment Policy 163

object pages (*continued*)

- Ethernet Interface
  - Main 76
  - Standby Control 78
  - Static Routes 78
- Host Alias 84
- HTTP Service 181
- iSCSI CHAP 102
- iSCSI Initiator 101
- iSCSI Target 101
- Kerberos KDC server 190
- Kerberos Keytab File 191
- NFS Dynamic Mounts 94
- NFS Static Mounts 96
- NTP Service 86
- SSL Proxy Profile 219
- VLAN Sub-Interface
  - Main 77
  - Standby Control 78
  - Static Routes 78
- XML Management Interface
  - Advanced 118
  - Main 117

objects

- administrative state 12
- configuration state 12
- creating
  - SOAP Interface 121
- deleting
  - SOAP Interface 121
- modifying
  - SOAP Interface 121
- not in export packages
  - Certificate 149
  - Key 149
  - User 149
- operational state 12
- referenced
  - ... button 8
  - + button 8
  - creating 8
  - modifying 8
  - selecting 8
- retrieving
  - SOAP Interface 121
- status 12

Objects menu 7

objects pages

- Network setting 80
- operational states, objects 12

## P

- packet captures
  - initiating 80
- pager, e-mail
  - configuring 174
- passwords
  - changing 55
  - forcing change 54
  - RBM policy 33
- patents 235
- pcap files 80
- PEM
  - certificate format 61
  - key format 61

- PKCS #12
  - certificate format 61
  - key format 61
- PKCS #7
  - certificate format 61
- PKCS #8
  - key format 61
- principal, Kerberos 189
- private key files
  - location 131
- private keys
  - uploading 135
- pubcert validation credentials 222
- pubcert: directory 132

## Q

- quiesce
  - application domains 146
- quiescing
  - appliance 109
  - overview 107
  - status 109

## R

- RADIUS
  - NAS-identifier 218
  - purpose 217
  - RBM authentication 25
- RBM
  - account policy 35
  - authenticate users 18
  - authorizing access to resources 19
  - builder 39
  - capabilities 18
  - changing admin-state 37
  - configuration steps 19
  - custom authentication 21
  - defining access credentials 45
  - defining credential mapping 39
  - defining user authentication 39
  - defining user groups accounts for 45
  - evaluate access profile 18
  - extending RBM access to WebGUI
    - only 36
  - flushing RBM cache 37
  - LDAP authentication 22
  - local user authentication 24
  - password policy 33
  - RADIUS authentication 25
  - restoring access from command line 36
  - retrieving credentials 18
  - SAF authentication 27
  - settings 17
  - SPNEGO authentication 28
  - SSL user certificate authentication 30
  - XML file authentication 31
- RBM policy file
  - au-method of authentication 39
  - mc-method of authorization 39
- RBMInfo.xml file 39
- reboot configuration, selecting 88
- referenced objects
  - ... button 8

referenced objects (*continued*)

- + button 8
- creating 8
- modifying 8
- selecting 8
- referenced objects, lists
  - ... button 9
  - + button 9
  - Add button 9
  - adding 9
  - creating 9
  - Delete button 9
  - deleting 9
  - modifying 9
  - selecting 9
- remote file management
  - iSCSI volume
    - configuring 99
    - initializing 100
    - managing 99
- removing access to a command group
  - CLI 47
- retrieving credentials
  - RBM 18
- role-based management
  - See RBM
- routing
  - destination based 81

## S

- SAML artifact, retrieving 119
- Save Config button 7, 11
- Saved configuration state 12
- schema files
  - XML Management Interface 118
- schemas
  - location 132
- SDK (j2sdk1.4.2) 135
- search domains
  - configuring 84
  - DNS 84
- search parameters, LDAP 34
- secure backup
  - conditions 161
  - creating 161
  - restoring 161
  - validating 162
- secure backup-restore
  - See disaster recovery
- secure restore
  - conditions 161
  - running 161
- security certificates
  - shared
    - location 132
  - Web browsers
    - location 132
- self-balancing
  - Ethernet interfaces 73
  - VLAN interfaces 73
- self-balancing mode
  - Ethernet interfaces 70
  - VLAN interfaces 70
- serial port
  - connection 112, 113

servits  
Access Control Lice  
11(104) TJT\*IPv6ice  
SlePro11018(Pr)17eatiewins 120r18(Pr)77.8(o110)17,onligruri.7(18(Pr)17eatiewins)-1020(120) TJT\*m (r)17. (ve,ent)-332p8(Pr)77.8(o110)17,onligr

## V

- validation credentials
  - non expiring, non-password-protected certificates 222
  - pubcert 222
  - specific certificates 223
  - supported extensions 222
  - types 221
  - validation methods 222
- View button 9
- View Logs link 12
- View Status link 12
- virtual LAN interface
  - See VLAN interface
- visible domains 144
- VLAN interfaces
  - configuring 77
  - failover 70
  - IPv6 69
  - managing 77
  - overview 69
  - packet capture 80
  - self-balancing 70, 73
  - standby configuration 69
  - standby groups 70
  - static routes 78
- VLAN Sub-Interface
  - object pages
    - Main 77
    - Standby Control 78
    - Static Routes 78

## W

- Web Management Interface 7
- Web Management Service
  - See also WebGUI
  - Access Control List 185
  - IPv6 185
- Web Services Distributed Management
  - See WSDM
- web-mgmt command 7, 128
- WebGUI
  - access 111
  - accessing 7
  - Administration menu 7
  - applying configuration changes 11
  - canceling changes 11
  - common tasks 11
  - customizing the interface 229
  - dashboard 7
  - deleting objects 11
  - Domain list 7
  - enabling custom messages 92
  - exporting objects 12
  - extending RBM access to WebGUI
    - only 36
  - logging in 7
  - Logout button 7
  - Network menu 7
  - Objects menu 7
  - resetting configuration 11
  - reverting changes 11
  - Save Config button 7
  - saving configuration changes 11
  - Services menu 7

- WebGUI (*continued*)
  - SSL proxy profile
    - cryptographic material 128
    - default settings 127
    - generating custom 127
    - removing 128
  - Status menu 7
  - viewing configuration-specific logs 12
  - viewing object status 12
  - Welcome screen 7
- WebGUI access rights
  - defined on user groups 47
- WebSphere Cell
  - purpose 224
- Welcome screen 7
- workstation
  - uploading files 134
- WSDL files
  - XML Management Interface 118
- WSDM
  - endpoint 116
- WSDM interface
  - accessing configuration data 123
  - XML Management Interface 123

## X

- XML Management Interface
  - Access Control List 185
  - changing default security 118
  - changing HTTP settings 118
  - endpoints
    - AMP 116
    - SLM 116
    - UDDI Subscription 116
    - WS-Management 116
    - WSDM 116
  - IPv6 185
  - object pages
    - Advanced 118
    - Main 117
  - overview 115
  - Services
    - available 116
    - enabling 117
  - SOAP interface 118
  - SSL proxy profile
    - default settings 127
    - removing 128
  - WSDM interface 123
- XML Manager
  - Load Balancer Group
    - Log Target 174
- XML Names
  - throttle 88
- xml-mgmt-base.xsd schema file 118
- xml-mgmt-ops.xsd schema file 118
- xml-mgmt.wsdl WSDL file 118
- xml-mgmt.xsd schema file 118





Printed in USA