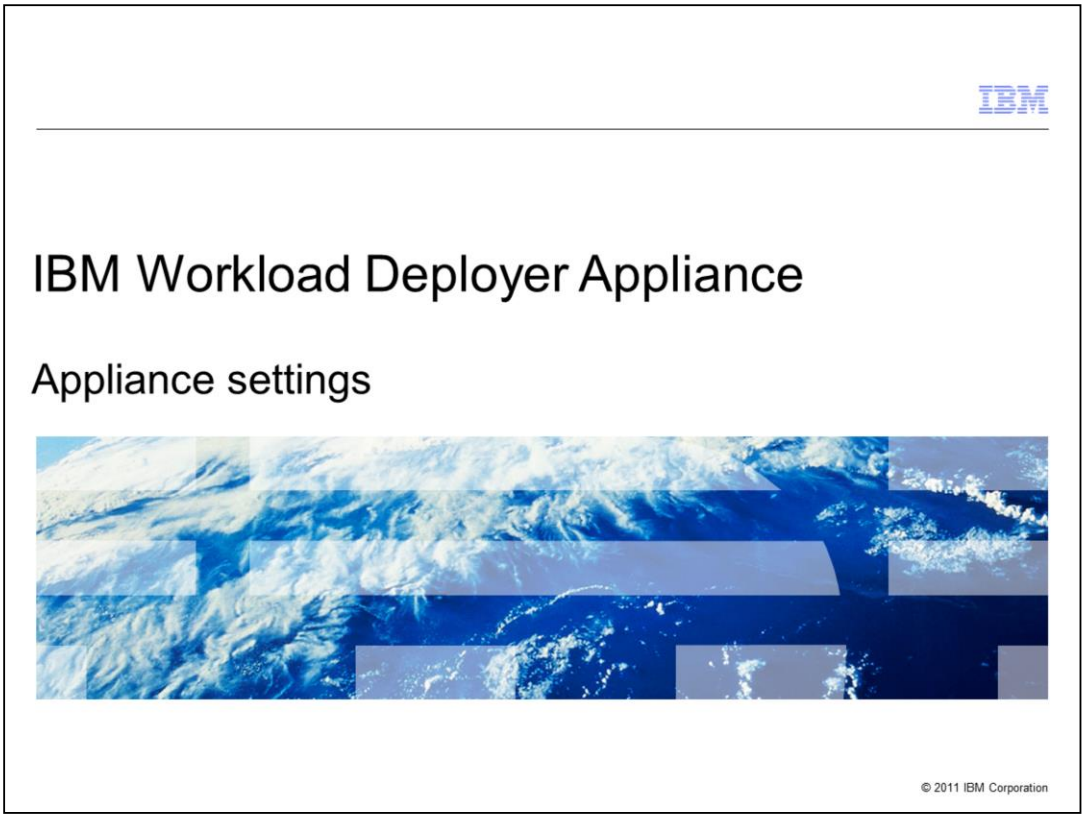


IBM Workload Deployer Appliance

Appliance settings

This presentation will discuss the settings for IBM Workload Deployer appliance.

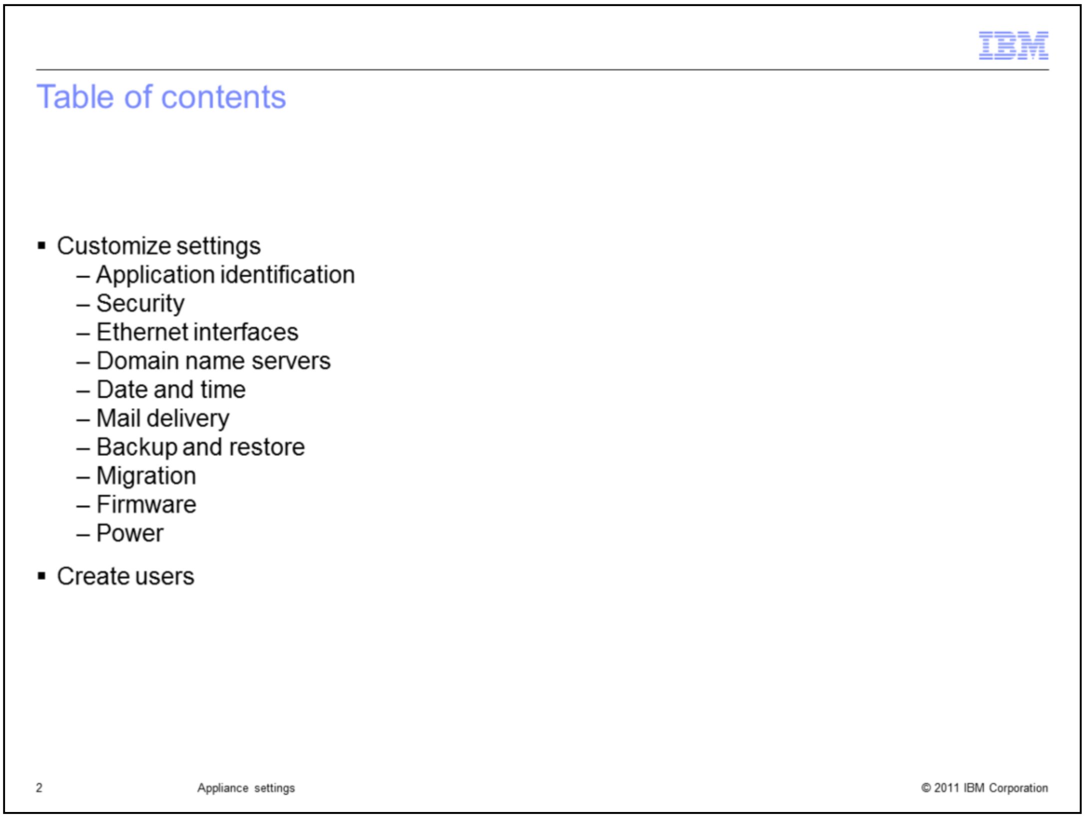


Table of contents

- Customize settings
  - Application identification
  - Security
  - Ethernet interfaces
  - Domain name servers
  - Date and time
  - Mail delivery
  - Backup and restore
  - Migration
  - Firmware
  - Power
- Create users

2 Appliance settings © 2011 IBM Corporation

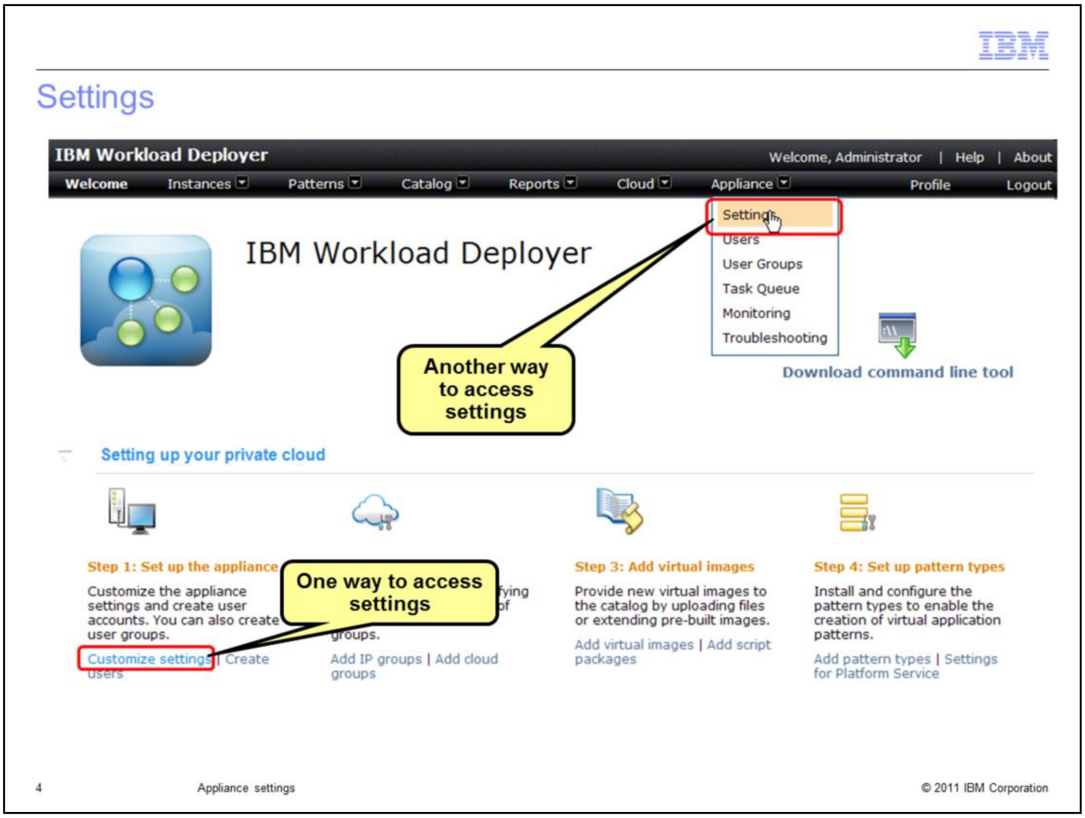
When you are setting up your IBM Workload Deployer Appliance, you will want to modify some of the appliance settings and create new user accounts to perform different operations on the appliance. This presentation will discuss the **Customize settings** and **Create users** functions of the IBM Workload Deployer appliance. The settings include **application identification**, **security, Ethernet interfaces, domain name servers, date and time, mail delivery, backup and restore, migration, firmware,** and **power.** You will see how to create users, review user information, and see what permissions you can set from the user definition screen.

Section

IBM Workload Deployer Appliance settings

3 Appliance settings © 2011 IBM Corporation

This section will discuss a general overview of the IBM Workload Deployer Appliance settings.



Settings

Another way to access settings

Setting up your private cloud

Step 1: Set up the appliance

Customize the appliance settings and create user accounts. You can also create user groups.

Customize settings | Create users

One way to access settings

fying of groups.

Add IP groups | Add cloud groups

Step 3: Add virtual images

Provide new virtual images to the catalog by uploading files or extending pre-built images.

Add virtual images | Add script packages

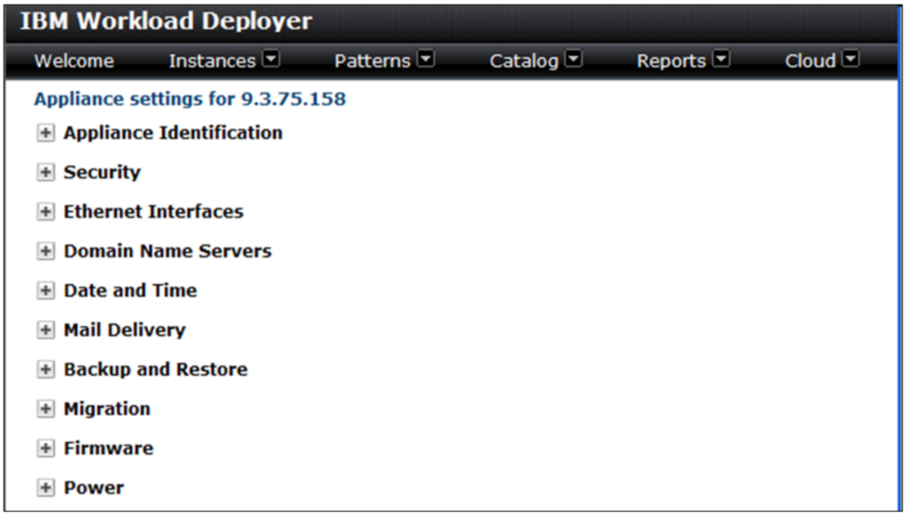
Step 4: Set up pattern types

Install and configure the pattern types to enable the creation of virtual application patterns.

Add pattern types | Settings for Platform Service

After you have logged on to the IBM Workload Deployer appliance, you will see the welcome screen. To set up the appliance, you click **Customize settings** under the topic “Step 1: Set up the appliance” topic. Alternatively you can click **Appliance** within the title bar, and within the pull down that opens, click **Settings.**

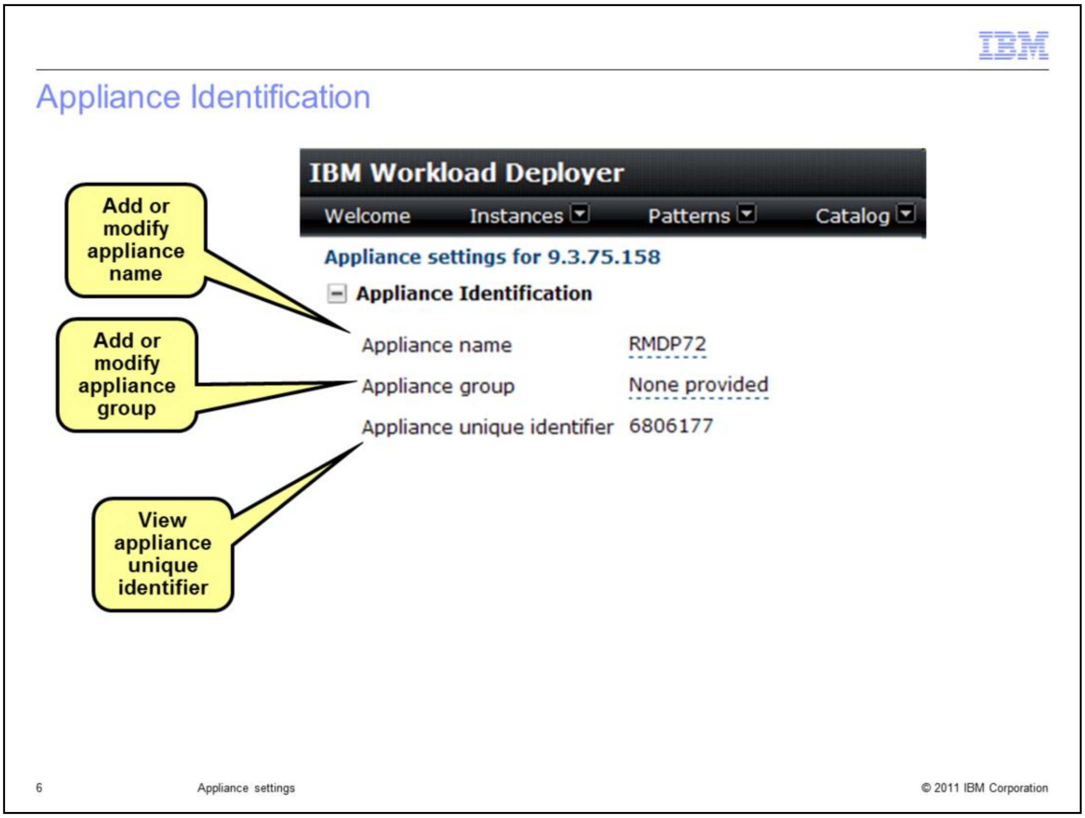
Appliance settings



Appliance settings for 9.3.75.158

- Appliance Identification
- Security
- Ethernet Interfaces
- Domain Name Servers
- Date and Time
- Mail Delivery
- Backup and Restore
- Migration
- Firmware
- Power

Appliance settings will allow you to customize appliance identification, security, Ethernet interfaces, domain name servers, date and time and mail delivery. It provides the ability to backup or restore your appliance, to migrate your appliance, to review and update firmware, and to power off or restart your appliance.



Appliance Identification

IBM Workload Deployer

Appliance settings for 9.3.75.158

Appliance Identification

Appliance name RMDP72

Appliance group None provided

Appliance unique identifier 6806177

Add or modify appliance name

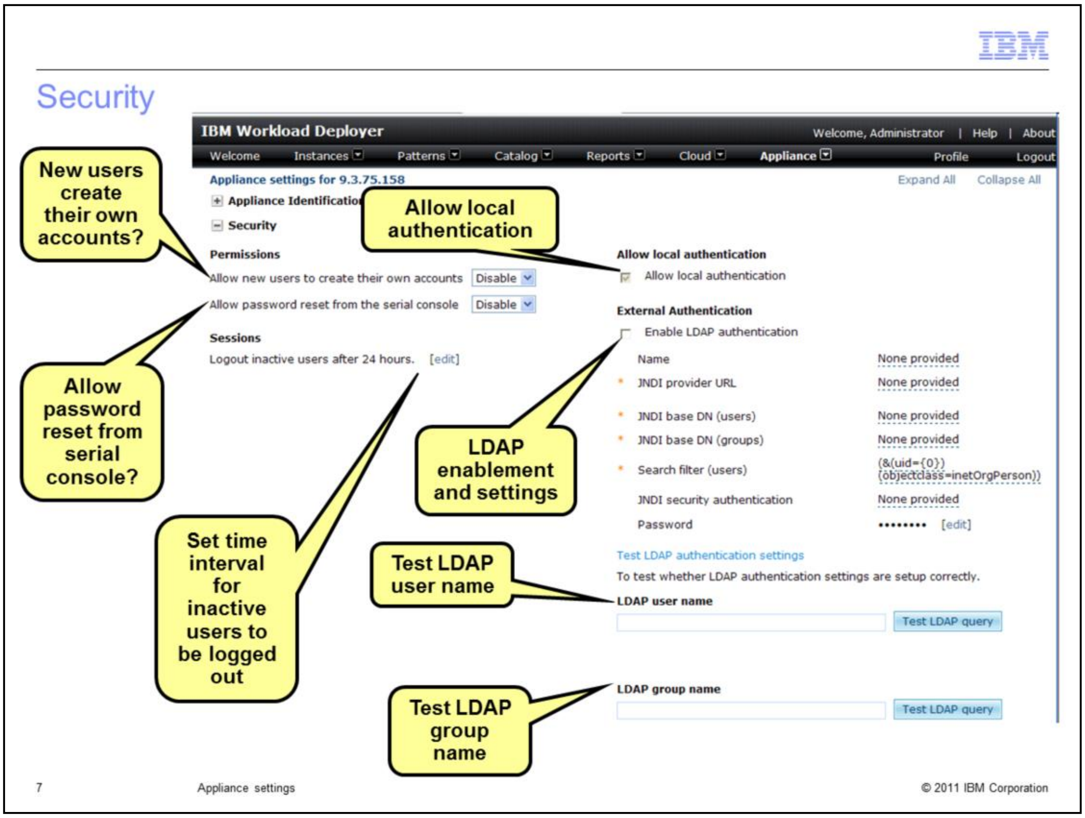
Add or modify appliance group

View appliance unique identifier

6 Appliance settings

IBM Workload Deployer appliances can be named and assigned to appliance groups for easy identification on the network. The appliance unique identifier is the appliance serial number and cannot be changed.

Security



Appliance settings for 9.3.75.158

⊞ Appliance Identification

⊟ Security

Permissions

Allow new users to create their own accounts: Disable

Allow password reset from the serial console: Disable

Sessions

Logout inactive users after 24 hours. [edit]

Allow local authentication

☑ Allow local authentication

External Authentication

□ Enable LDAP authentication

Name	None provided
* JNDI provider URL	None provided
* JNDI base DN (users)	None provided
* JNDI base DN (groups)	None provided
* Search filter (users)	(&(uid={0})(objectclass=inetOrgPerson))
JNDI security authentication	None provided
Password	•••••••• [edit]

Test LDAP authentication settings

To test whether LDAP authentication settings are setup correctly.

LDAP user name

LDAP group name

New users create their own accounts?

Allow local authentication

Allow password reset from serial console?

LDAP enablement and settings

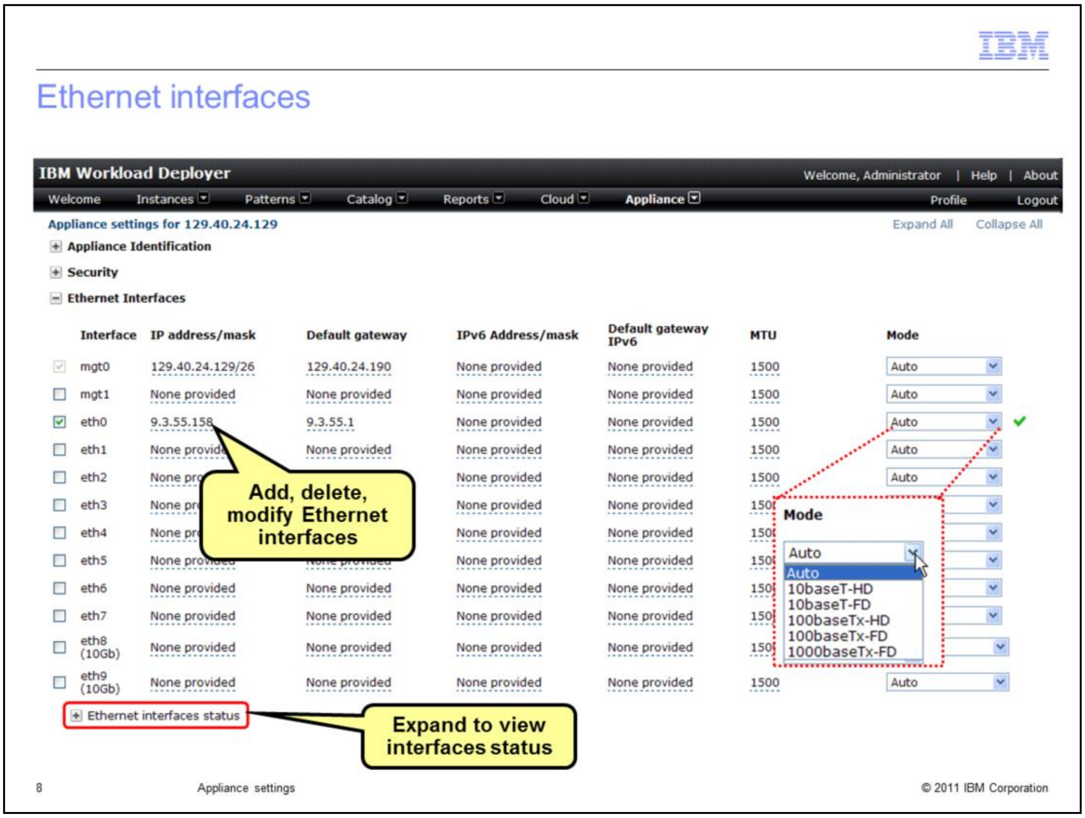
Set time interval for inactive users to be logged out

Test LDAP user name

Test LDAP group name

7 Appliance settings © 2011 IBM Corporation

Within the security settings, you can customize some of the settings for permissions and external authentication. Within permissions, you can allow or disallow new users to create their own accounts within the appliance, and you can allow or disallow a password reset from within the serial console. Under Session, you can set the time interval for inactive users to be logged out. Allow local authentication allows users to be registered within the appliance itself, without using LDAP. External authentication allows you to enable LDAP authentication and provides the capability to test the LDAP user name and group name settings.



Ethernet interfaces

Appliance settings for 129.40.24.129

⊞ Appliance Identification

⊞ Security

⊟ Ethernet Interfaces

	Interface	IP address/mask	Default gateway	IPv6 Address/mask	Default gateway IPv6	MTU	Mode
☑	mgt0	129.40.24.129/26	129.40.24.190	None provided	None provided	1500	Auto
□	mgt1	None provided	None provided	None provided	None provided	1500	Auto
☑	eth0	9.3.55.158	9.3.55.1	None provided	None provided	1500	Auto ✓
□	eth1	None provide	None provided	None provided	None provided	1500	Auto
□	eth2	None pr		None provided	None provided	1500	Auto
□	eth3	None pr		None provided	None provided	150	
□	eth4	None pr		None provided	None provided	150	
□	eth5	None provided	None provided	None provided	None provided	150	
□	eth6	None provided	None provided	None provided	None provided	150	
□	eth7	None provided	None provided	None provided	None provided	150	
□	eth8 (10Gb)	None provided	None provided	None provided	None provided	150	
□	eth9 (10Gb)	None provided	None provided	None provided	None provided	1500	Auto

Mode

Auto

- Auto
- 10baseT-HD
- 10baseT-FD
- 100baseTx-HD
- 100baseTx-FD
- 1000baseTx-FD

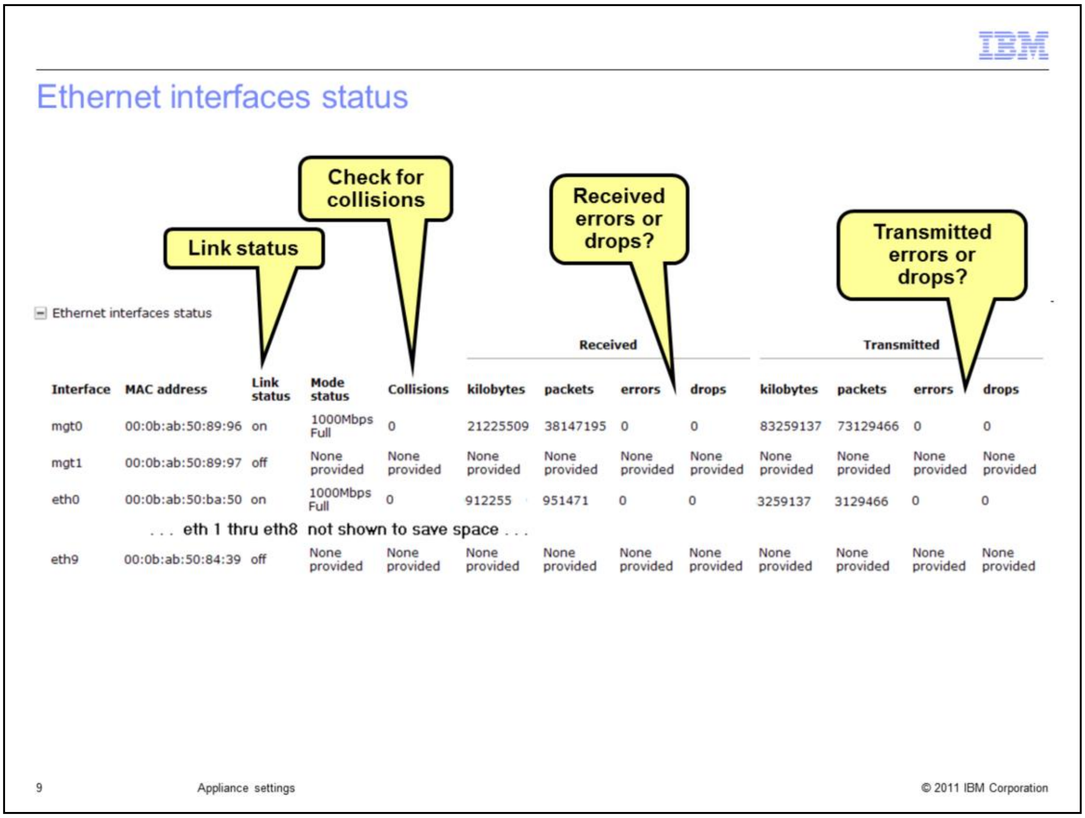
⊞ Ethernet interfaces status

Add, delete, modify Ethernet interfaces

Expand to view interfaces status

8 Appliance settings © 2011 IBM Corporation

The **Ethernet interfaces** settings allow you to review Ethernet definitions and to define or change these definitions. For each entry, you can define the IPV4 or IPV6 address, mask and gateway, the maximum transmission unit (MTU) and the Mode. The entries include the two management interfaces, the eight one-gigabit interfaces and the two ten-gigabit interfaces. The Mode column is a dropdown with the selections you see in this slide example. The **Ethernet interfaces status** portion of the screen allows you to review the individual Ethernet interfaces. The next slide shows you more about that portion of this screen.



Ethernet interfaces status

Check for collisions

Received errors or drops?

Link status

Transmitted errors or drops?

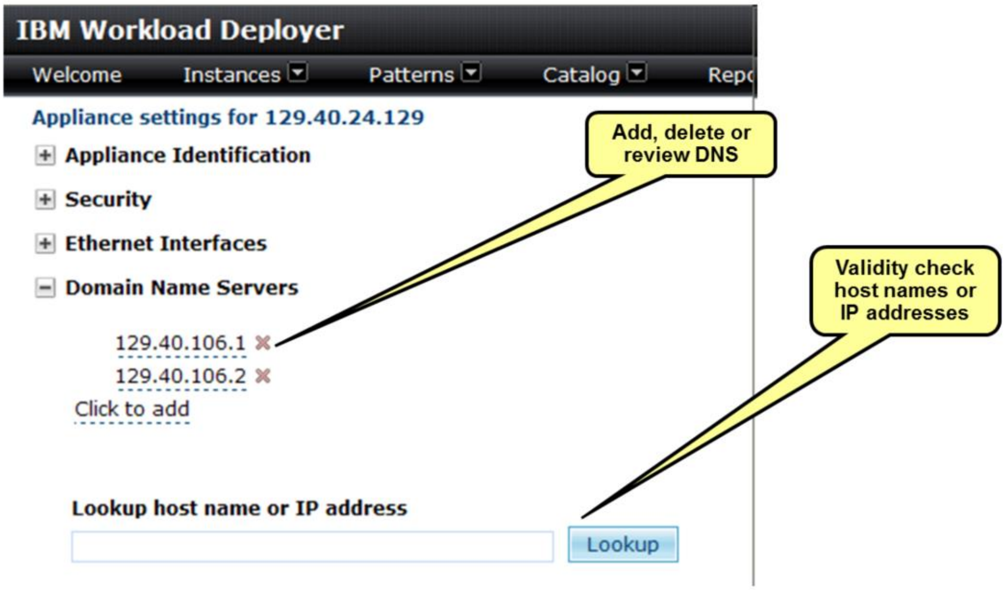
⊟ Ethernet interfaces status

					Received				Transmitted			
Interface	MAC address	Link status	Mode status	Collisions	kilobytes	packets	errors	drops	kilobytes	packets	errors	drops
mgt0	00:0b:ab:50:89:96	on	1000Mbps Full	0	21225509	38147195	0	0	83259137	73129466	0	0
mgt1	00:0b:ab:50:89:97	off	None provided	None provided	None provided	None provided	None provided	None provided	None provided	None provided	None provided	None provided
eth0	00:0b:ab:50:ba:50	on	1000Mbps Full	0	912255	951471	0	0	3259137	3129466	0	0
	. . . eth 1 thru eth8 not shown to save space . . .											
eth9	00:0b:ab:50:84:39	off	None provided	None provided	None provided	None provided	None provided	None provided	None provided	None provided	None provided	None provided

9 Appliance settings © 2011 IBM Corporation

The **Ethernet interface status** portion of the screen allows you to review the individual Ethernet interfaces. This includes MAC address, link status, mode status, number of collisions, the number of kilobytes sent and received, the number of packets sent and received, and the number of errors and dropped packets.

Domain name servers



Appliance settings for 129.40.24.129

⊞ Appliance Identification

⊞ Security

⊞ Ethernet Interfaces

⊟ Domain Name Servers

129.40.106.1 ✖
129.40.106.2 ✖
Click to add

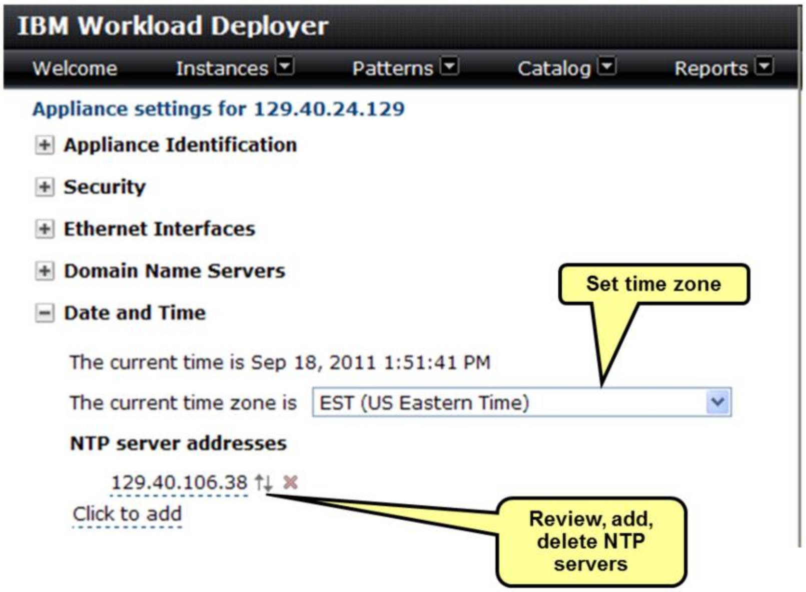
Lookup host name or IP address

Add, delete or review DNS

Validity check host names or IP addresses

The domain name server settings allow you to review, delete, and add domain name servers. It also provides a lookup function to allow you to verify host names or IP addresses, which assists you with validation of the environment.

Date and time



Appliance settings for 129.40.24.129

⊞ Appliance Identification

⊞ Security

⊞ Ethernet Interfaces

⊞ Domain Name Servers

⊟ Date and Time

The current time is Sep 18, 2011 1:51:41 PM

The current time zone is EST (US Eastern Time)

NTP server addresses

129.40.106.38 ↑↓ ✖

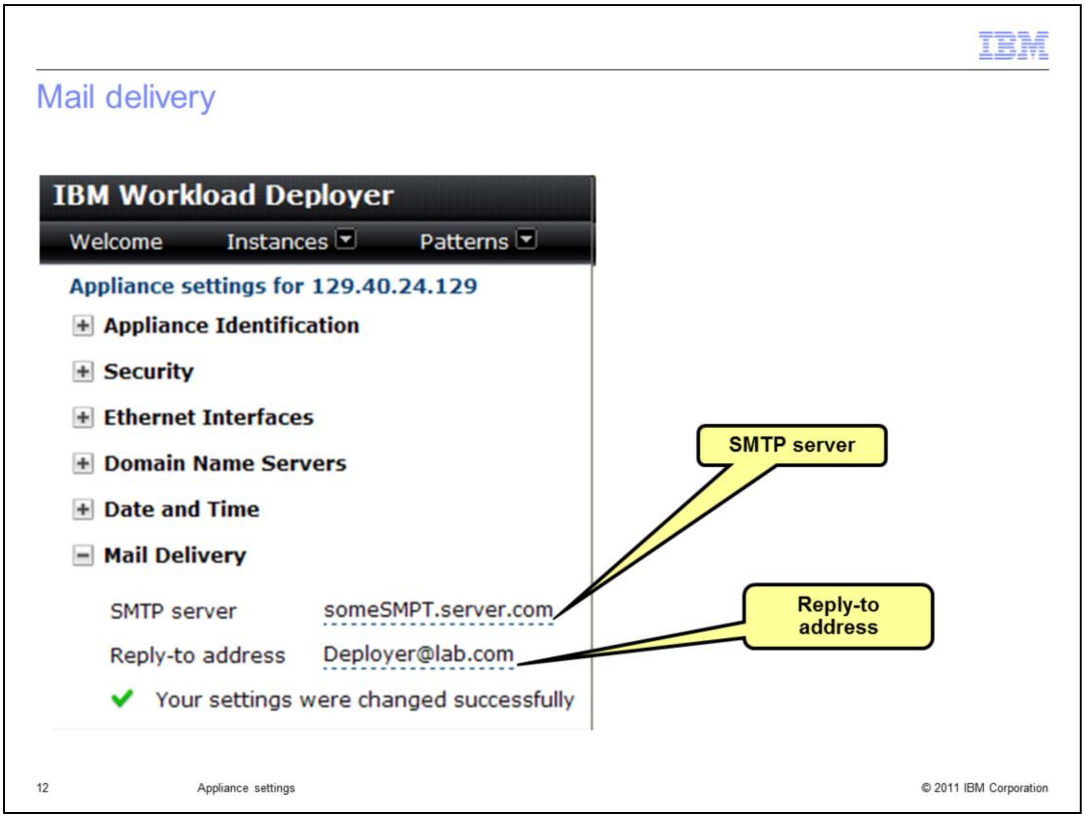
Click to add

Set time zone

Review, add, delete NTP servers

11 Appliance settings

The date and time setting allows you to set the time zone for the appliance and to add, review, and delete network time protocol servers.



Mail delivery

Appliance settings for 129.40.24.129

- ⊞ Appliance Identification
- ⊞ Security
- ⊞ Ethernet Interfaces
- ⊞ Domain Name Servers
- ⊞ Date and Time
- ⊟ Mail Delivery

SMTP server someSMPT.server.com

Reply-to address Deployer@lab.com

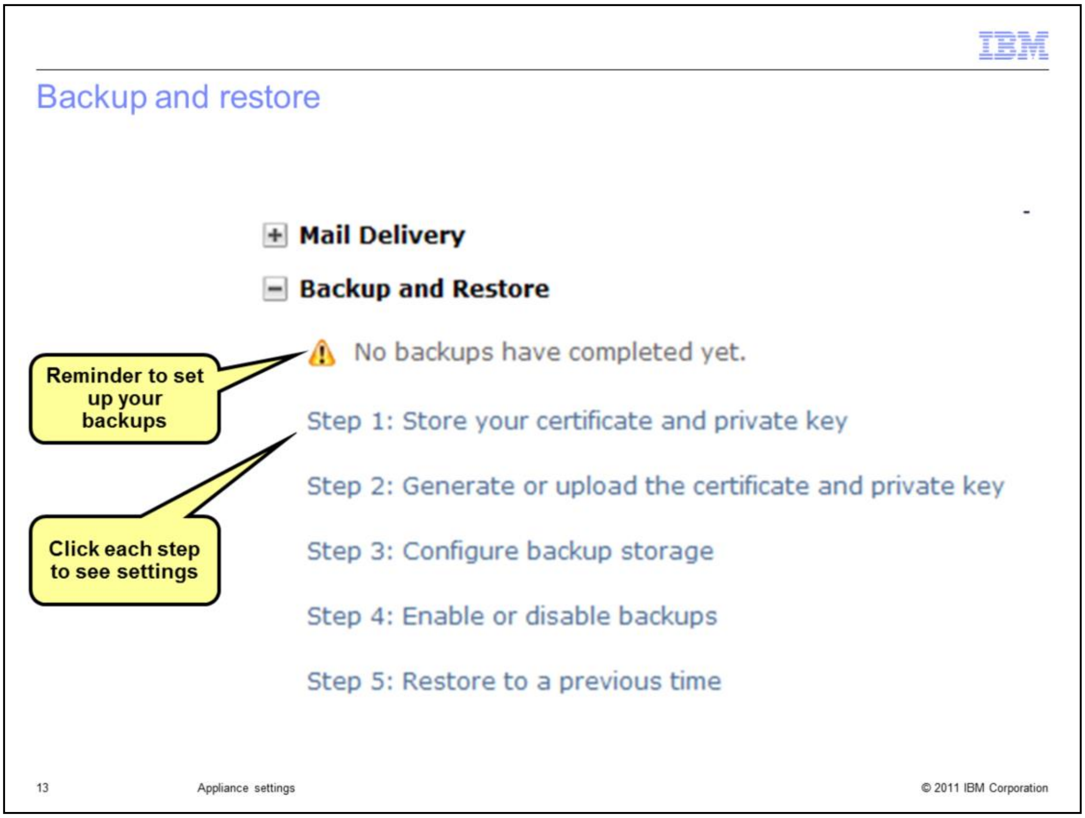
✓ Your settings were changed successfully

SMTP server

Reply-to address

12 Appliance settings © 2011 IBM Corporation

The mail delivery settings allow you to add, delete, or change the SMTP server setting and reply-to address for the appliance. These settings are used by the appliance when it delivers notification messages to users defined within the appliance.



Backup and restore

⊞ **Mail Delivery**

⊟ **Backup and Restore**

⚠ No backups have completed yet.

Step 1: Store your certificate and private key

Step 2: Generate or upload the certificate and private key

Step 3: Configure backup storage

Step 4: Enable or disable backups

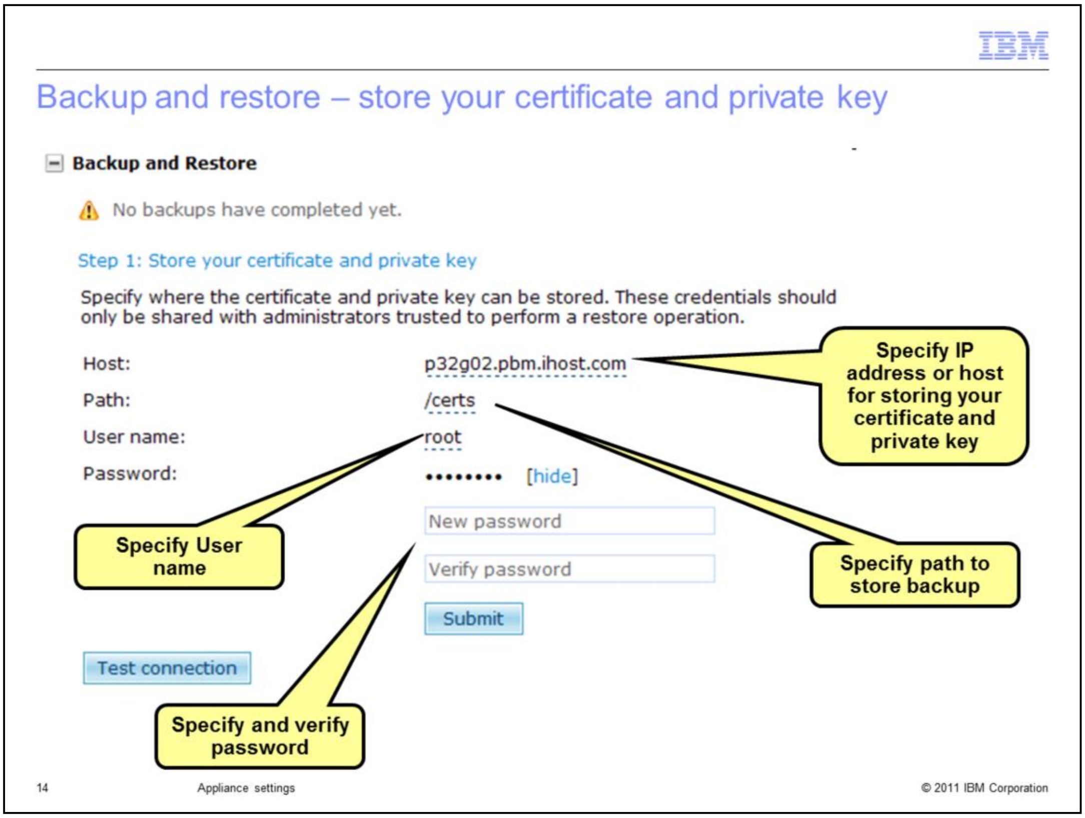
Step 5: Restore to a previous time

Reminder to set up your backups

Click each step to see settings

13 Appliance settings © 2011 IBM Corporation

Using the backup and restore settings, you can ensure that the appliance can be restored when required. If you have never set up for backups, you see a reminder message in this section. Click each step to see the settings. The five steps involved in setting up the backup and restore environment are: Step 1: Store your certificate and private key, Step 2: Generate or upload the certificate and private key, Step 3: Configure backup storage, Step 4: Enable or disable backups, Step 5: Restore to a previous time.



Backup and restore – store your certificate and private key

Backup and Restore

No backups have completed yet.

Step 1: Store your certificate and private key

Specify where the certificate and private key can be stored. These credentials should only be shared with administrators trusted to perform a restore operation.

Host: p32g02.pbm.ihost.com

Path: /certs

User name: root

Password: •••••••• [hide]

New password

Verify password

Specify IP address or host for storing your certificate and private key

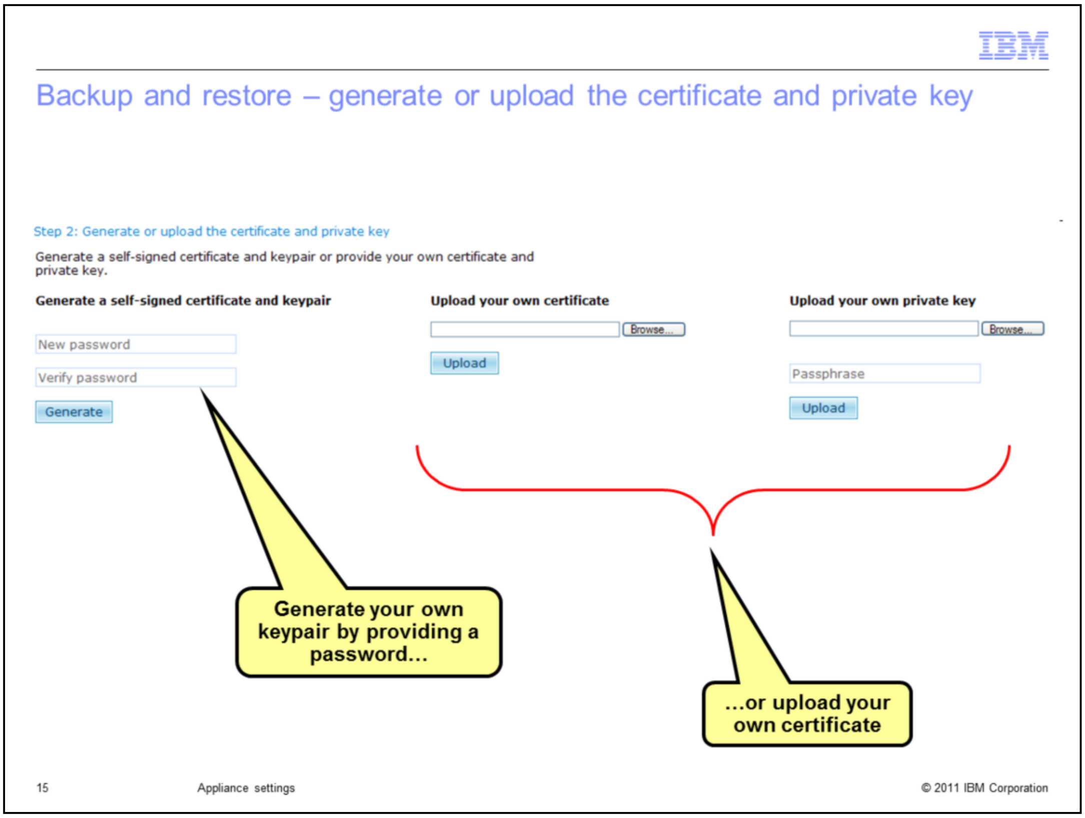
Specify User name

Specify path to store backup

Specify and verify password

14 Appliance settings © 2011 IBM Corporation

Although the certificate containing the public key pair is stored on the Workload Deployer appliance, the certificate and private key must not be stored on the appliance. They must be stored in a safe location. You must specify the safe location in which to store the certificate and private key. In the **Host** field, type the host name or IP address of the SSH host where you want to store the certificate and private key. In the **Path** field type the path to the directory on the SSH server where your certificate and private key are stored. In the **User name** field, type the user that is used to establish a connection with the SSH server. Then click **edit** by the **Password** field to see the password input fields. Type a password in the **New password** field for the user you just identified. Type the password again in the **Verify password** field and click **Submit**.



Backup and restore – generate or upload the certificate and private key

Step 2: Generate or upload the certificate and private key

Generate a self-signed certificate and keypair or provide your own certificate and private key.

Generate a self-signed certificate and keypair

Upload your own certificate

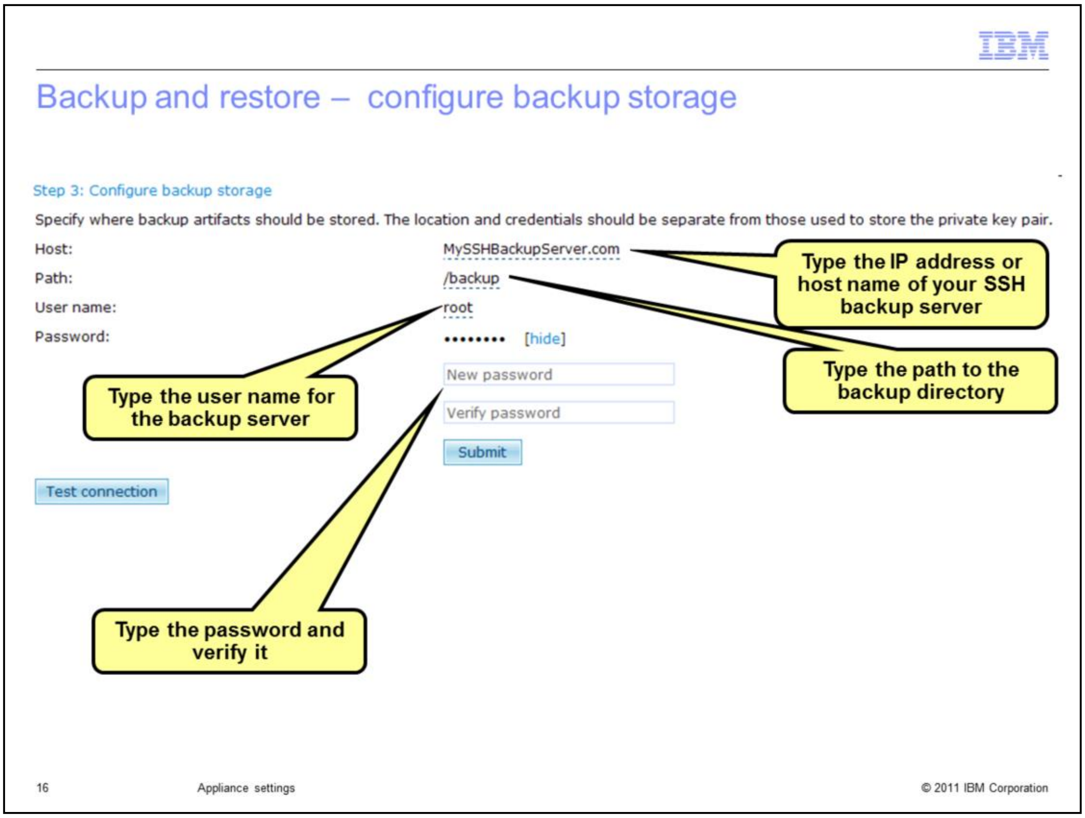
Upload your own private key

Generate your own keypair by providing a password...

...or upload your own certificate

15 Appliance settings © 2011 IBM Corporation

To protect the sensitive information that exists in your backup images, Rivest, Shamir, and Adleman (RSA) encryption is used. The certificate and private key protect your sensitive information as you back it up and restore it. The certificate and private key must either be provided or generated. If you generate your own certificate and keypair, they are stored automatically in the SSH server and path you identified in step one.



Backup and restore – configure backup storage

Step 3: Configure backup storage

Specify where backup artifacts should be stored. The location and credentials should be separate from those used to store the private key pair.

Host: MySSHBackupServer.com

Path: /backup

User name: root

Password: •••••••• [hide]

New password

Verify password

Submit

Test connection

Type the IP address or host name of your SSH backup server

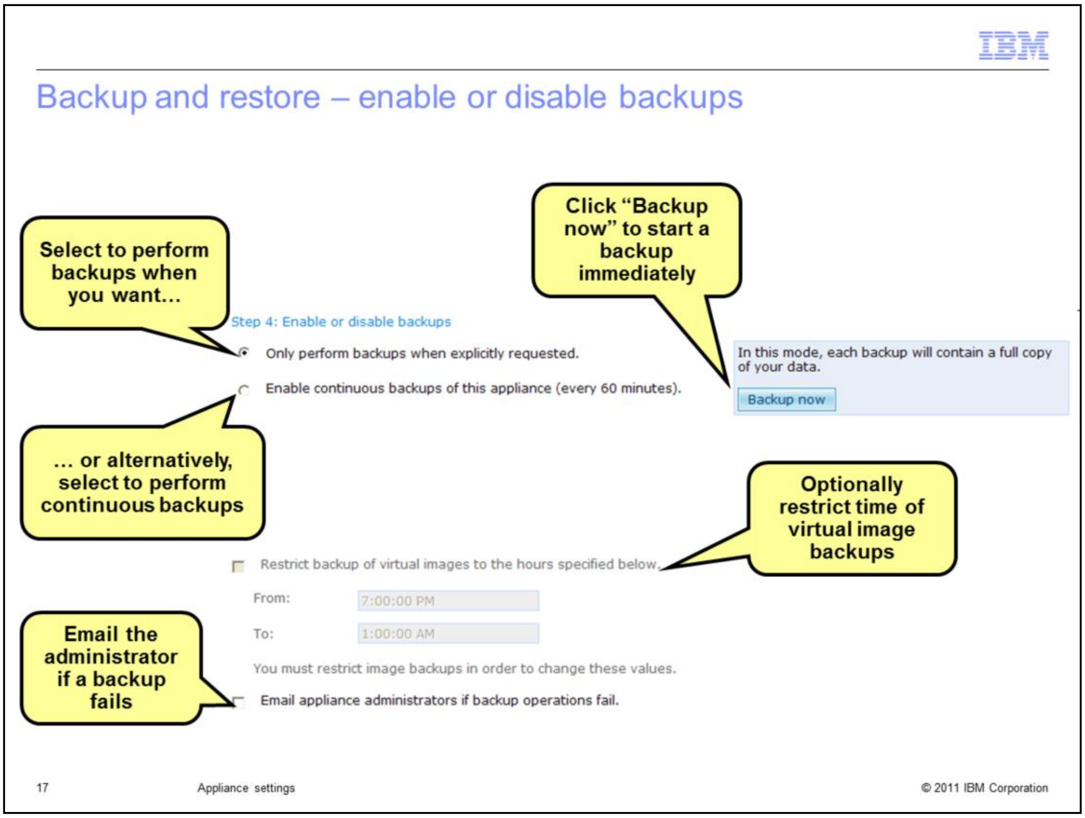
Type the path to the backup directory

Type the user name for the backup server

Type the password and verify it

16 Appliance settings © 2011 IBM Corporation

A backup storage location for the backup artifacts is required before you can schedule a backup image to be taken. This profile also provides the required parameters for establishing authentication to an external server with a Secure Shell (SSH) daemon running. To complete Step 3, type the IP address or host name of your backup server into the **Host** field. Then type the path to the backup directory into the **Path** field. In the **User name** field, type the user name for your backup server. Then in the **Password** field, click **edit** and then type and verify the password for the SSH user name.



Backup and restore – enable or disable backups

Select to perform backups when you want…

Click “Backup now” to start a backup immediately

Step 4: Enable or disable backups

● Only perform backups when explicitly requested.

○ Enable continuous backups of this appliance (every 60 minutes).

In this mode, each backup will contain a full copy of your data.

Backup now

… or alternatively, select to perform continuous backups

Optionally restrict time of virtual image backups

□ Restrict backup of virtual images to the hours specified below.

From: 7:00:00 PM

To: 1:00:00 AM

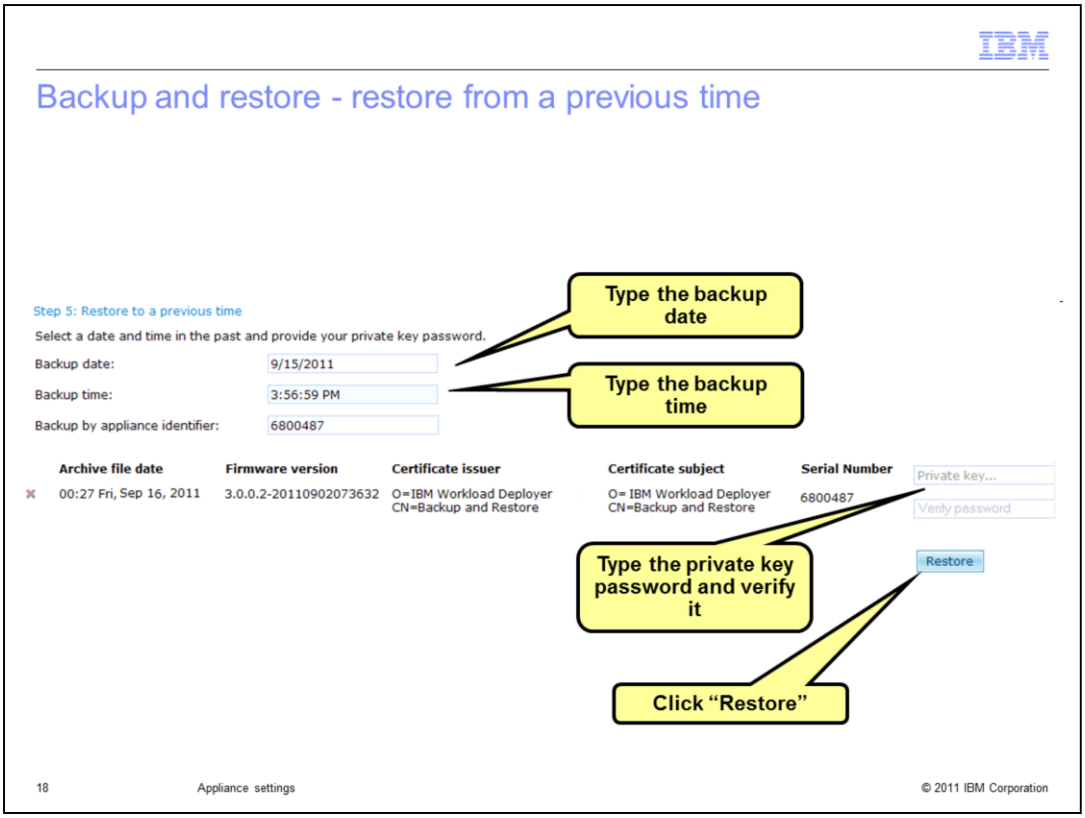
You must restrict image backups in order to change these values.

Email the administrator if a backup fails

□ Email appliance administrators if backup operations fail.

17 Appliance settings © 2011 IBM Corporation

You can schedule backup images of your Workload Deployer environment to begin when you explicitly request a backup or repeatedly at hourly time intervals. You can click **Backup now** to initiate a backup immediately. If you choose continuous backups, you can specify the time period that the backup images are to include the virtual images by checking **Restrict backup of virtual images to the hours specified below** and then specifying the time range when virtual image backups are allowed. Optionally, you can select the check box **Email appliance administrators if backup operations fail.**



Backup and restore - restore from a previous time

Step 5: Restore to a previous time

Select a date and time in the past and provide your private key password.

Backup date:	9/15/2011
Backup time:	3:56:59 PM
Backup by appliance identifier:	6800487

	Archive file date	Firmware version	Certificate issuer	Certificate subject	Serial Number	
✖	00:27 Fri, Sep 16, 2011	3.0.0.2-20110902073632	O=IBM Workload Deployer CN=Backup and Restore	O= IBM Workload Deployer CN=Backup and Restore	6800487	Private key... Verify password

Type the backup date

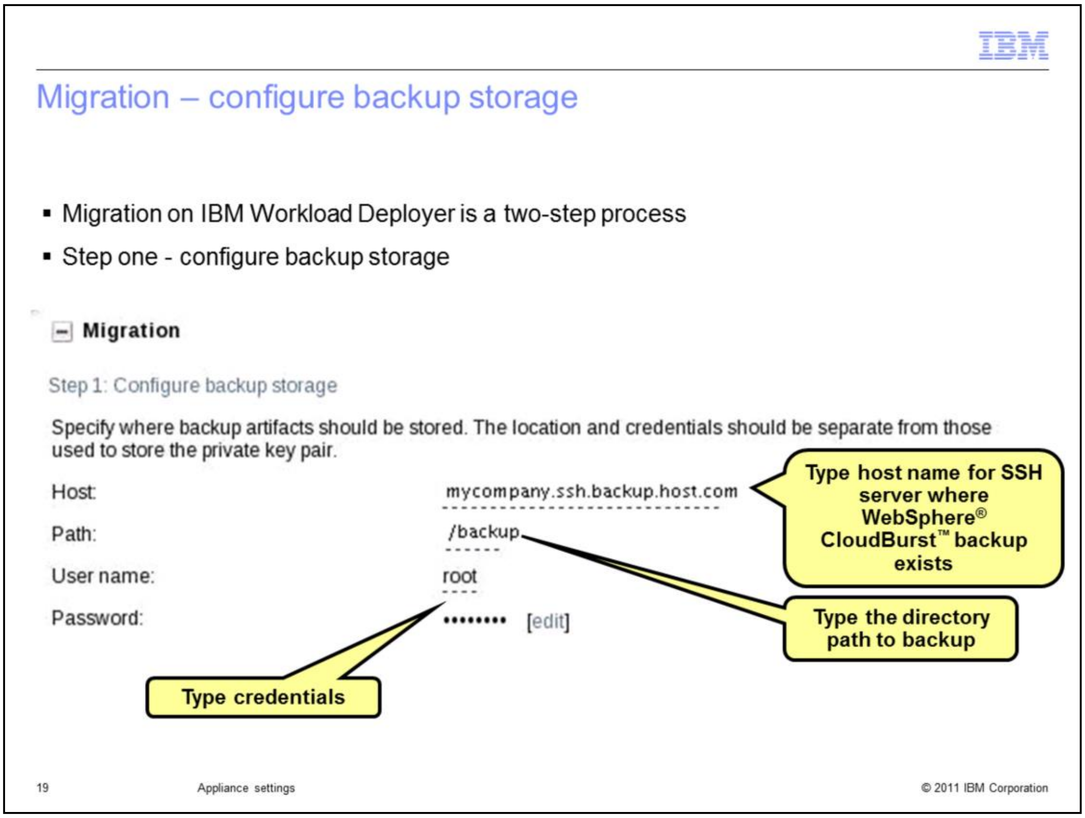
Type the backup time

Type the private key password and verify it

Click “Restore”

18 Appliance settings © 2011 IBM Corporation

The Workload Deployer appliance can be returned to a specific state by restoring from a backup image. The backup image is decrypted and streamed onto the appliance to return Workload Deployer to a previous state. Click the **Backup date** field to select the date of the backup to restore. The backup date does not have to be an exact date because the restore process searches the backup location to find the backup with the timestamp that is equal or less than the date and time that you provide. Click the **Backup time** field to select the time, on the date selected, of the backup to restore. The **backup time** field functions in a similar way as the **backup date** field, in that the time does not have to be an exact time because the restore process searches the backup location to find the backup with the timestamp that is equal or less than the date and time you specified. Change the **Backup by appliance identifier** if the backup was performed by another appliance. Type the password for the private key in the **Private key password** field, and verify it in the **Verify password** field. Then click **Restore.**



Migration – configure backup storage

- Migration on IBM Workload Deployer is a two-step process
- Step one - configure backup storage

⊟ **Migration**

Step 1: Configure backup storage

Specify where backup artifacts should be stored. The location and credentials should be separate from those used to store the private key pair.

Host:	mycompany.ssh.backup.host.com
Path:	/backup
User name:	root
Password:	•••••••• [edit]

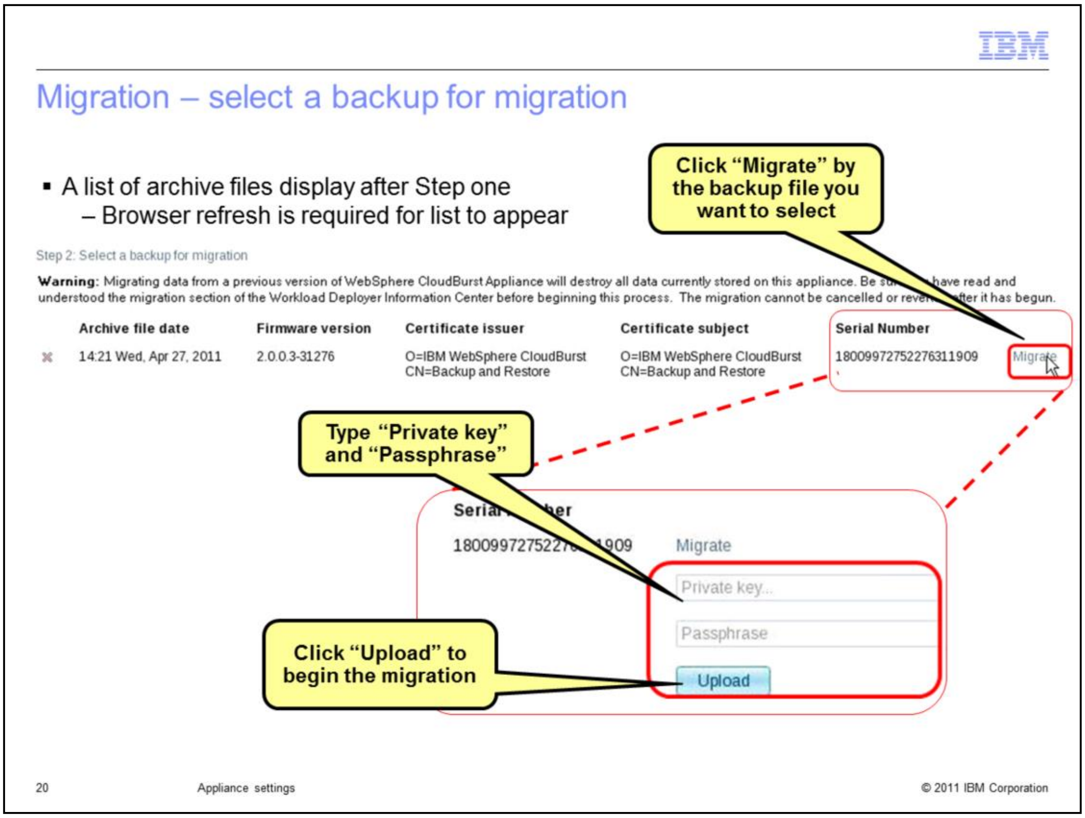
Type host name for SSH server where WebSphere® CloudBurst™ backup exists

Type the directory path to backup

Type credentials

19 Appliance settings © 2011 IBM Corporation

If you have a backup archive from your IBM CloudBurst appliance, you can begin the migration function on the IBM Workload Deployer appliance. You must be logged in as the cbadmin user. Expand the Migration link. The migration function is a two-step process. This slide shows you the information you need for step one. You must provide the Host, Path, User name, and Password for the SSH server where the IBM WebSphere CloudBurst backup exists. In most cases, this is the same server information you used when you performed the backup on the CloudBurst appliance.



Migration – select a backup for migration

- A list of archive files display after Step one
  - Browser refresh is required for list to appear

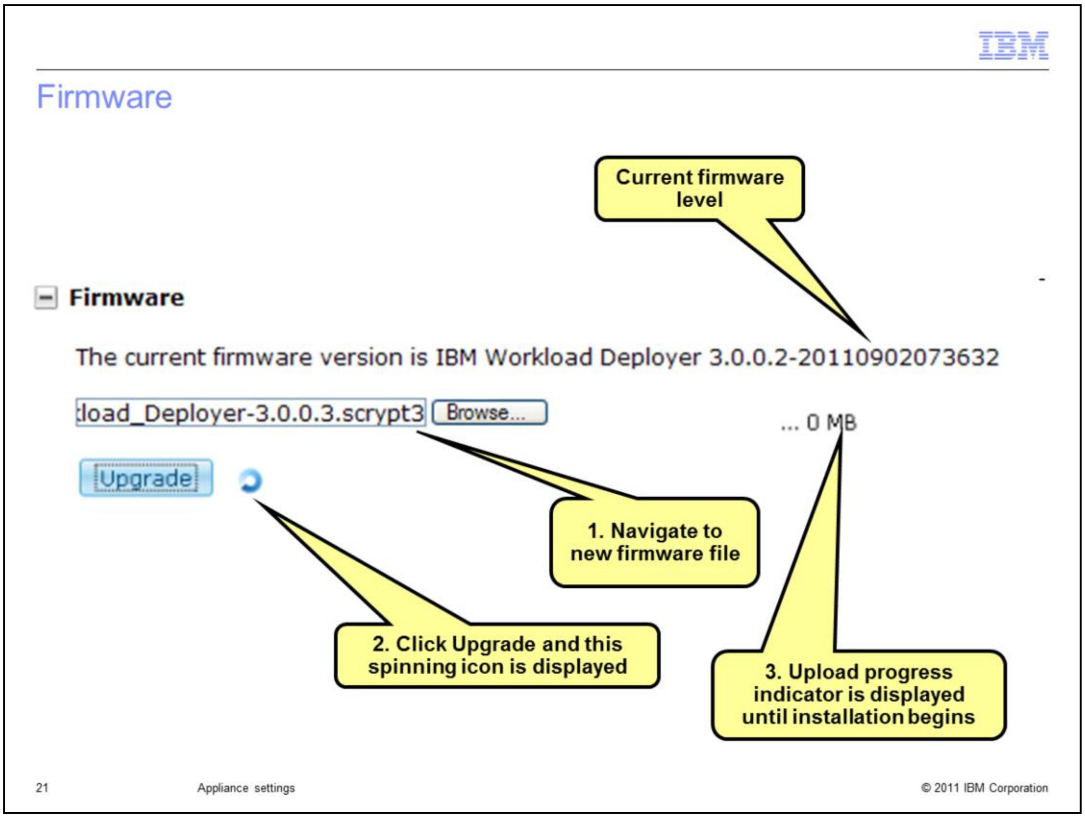
Step 2: Select a backup for migration

Warning: Migrating data from a previous version of WebSphere CloudBurst Appliance will destroy all data currently stored on this appliance. Be su[illegible] have read and understood the migration section of the Workload Deployer Information Center before beginning this process. The migration cannot be cancelled or reve[illegible] after it has begun.

	Archive file date	Firmware version	Certificate issuer	Certificate subject	Serial Number	
✖	14:21 Wed, Apr 27, 2011	2.0.0.3-31276	O=IBM WebSphere CloudBurst CN=Backup and Restore	O=IBM WebSphere CloudBurst CN=Backup and Restore	18009972752276311909	Migrate

Click “Migrate” by the backup file you want to select
Type “Private key” and “Passphrase”
Serial Number
18009972752276311909
Migrate
Private key...
Passphrase
Upload
Click “Upload” to begin the migration

Once you complete step one, refresh the browser screen and the IBM Workload Deployer will list all the available archive files available, listed under **Step 2**. Select the correct backup archive by clicking the Migrate link at the right of the file entry. The prompt displays below the Migrate button for the Private key and Passphrase. After that information is supplied, click the Upload button to start the migration function. Once you click “Upload” you cannot cancel the migration.



Firmware

Current firmware level

Firmware

The current firmware version is IBM Workload Deployer 3.0.0.2-20110902073632

:load_Deployer-3.0.0.3.scrypt3

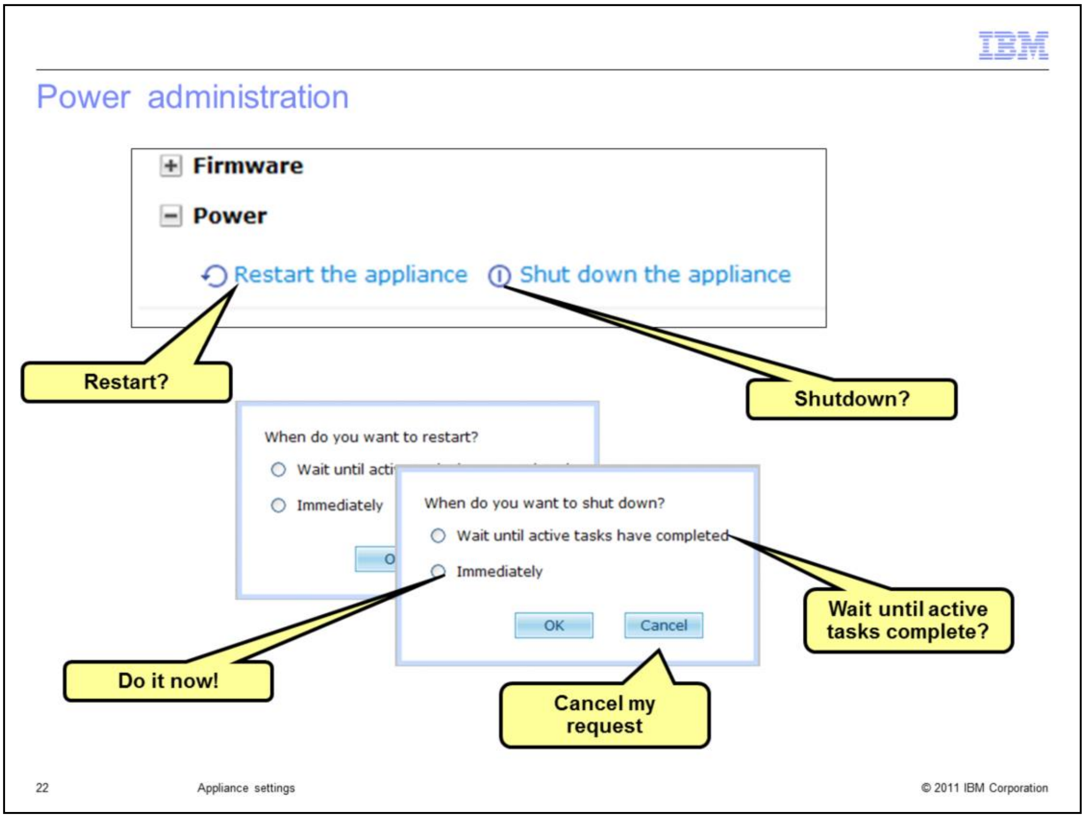
1. Navigate to new firmware file

2. Click Upgrade and this spinning icon is displayed

3. Upload progress indicator is displayed until installation begins

21 Appliance settings © 2011 IBM Corporation

The firmware settings allow you to see the current firmware level that is installed on the appliance and to optionally upgrade the firmware. To upgrade the firmware level, click the **Browse** button to navigate to the firmware upgrade file on your client computer. Then click the **Upgrade** button to begin the upgrade. You will see a spinning activity icon to indicate that the upload of the upgrade image has begun, and you will see an upload progress indicator. Once the upload is completed, you will see a message indicating the upgrade of the appliance has begun.



Power administration

⊞ Firmware

⊟ Power

Restart the appliance Shut down the appliance

Restart?

Shutdown?

When do you want to restart?

○ Wait until acti

○ Immediately

When do you want to shut down?

○ Wait until active tasks have completed

○ Immediately

Wait until active tasks complete?

Do it now!

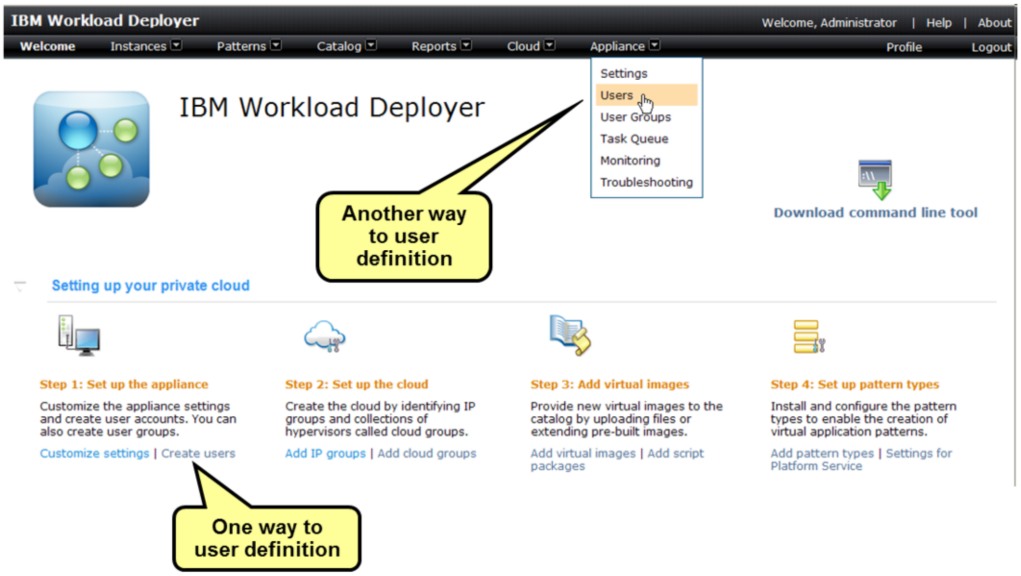
Cancel my request

22 Appliance settings © 2011 IBM Corporation

The power portion of the settings allow you to restart or shutdown the appliance. For both options, you will see a popup that allows you to restart or shutdown only when all active tasks have completed or perform the function immediately, or you can cancel the function.

IBM

Create users



Another way to user definition

Step 1: Set up the appliance
Customize the appliance settings and create user accounts. You can also create user groups.
Customize settings | Create users

Step 2: Set up the cloud
Create the cloud by identifying IP groups and collections of hypervisors called cloud groups.
Add IP groups | Add cloud groups

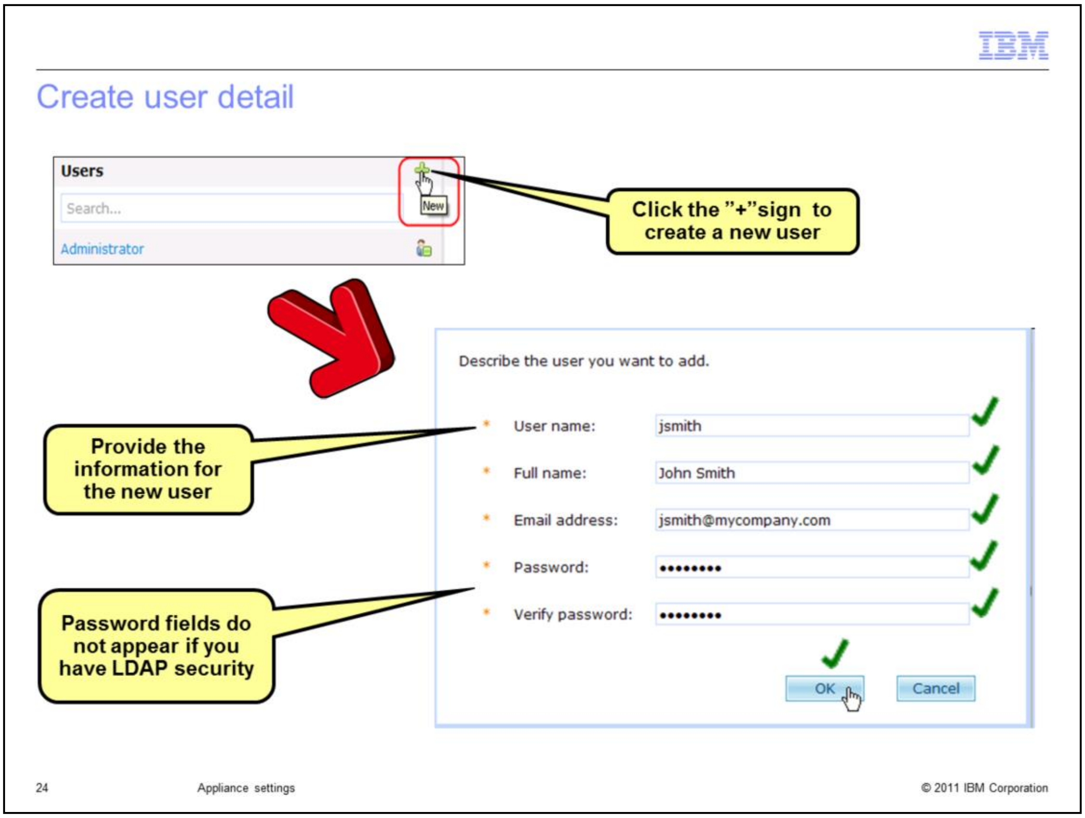
Step 3: Add virtual images
Provide new virtual images to the catalog by uploading files or extending pre-built images.
Add virtual images | Add script packages

Step 4: Set up pattern types
Install and configure the pattern types to enable the creation of virtual application patterns.
Add pattern types | Settings for Platform Service

One way to user definition

23 Appliance settings © 2011 IBM Corporation

As an administrator, you can define the users that access the appliance. To access the user definition screen, click **Create users** under the topic “Step 1: Set up the appliance”. Alternatively you can click **Appliance** within the title bar, and within the pull-down that opens, click **Users.**



Create user detail

Click the "+"sign to create a new user

Provide the information for the new user

Password fields do not appear if you have LDAP security

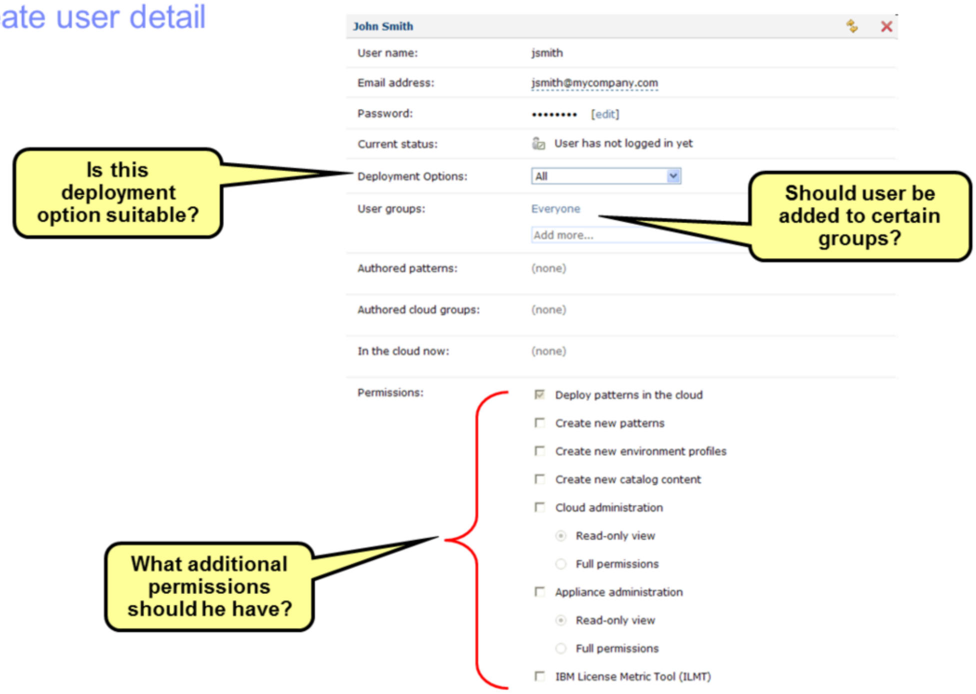
Describe the user you want to add.

- * User name: jsmith
- * Full name: John Smith
- * Email address: jsmith@mycompany.com
- * Password: ••••••••
- * Verify password: ••••••••

24 Appliance settings © 2011 IBM Corporation

Once the **Users** list opens, click the plus sign to define a new user. Then in the right pane supply user name, full name, email address, password, and password verification for the new user. The **Password** and **Verify password** fields do not display if you are using LDAP security.

Create user detail



John Smith

User name:	jsmith
Email address:	jsmith@mycompany.com
Password:	•••••••• [edit]
Current status:	User has not logged in yet
Deployment Options:	All
User groups:	Everyone Add more...
Authored patterns:	(none)
Authored cloud groups:	(none)
In the cloud now:	(none)

Permissions:

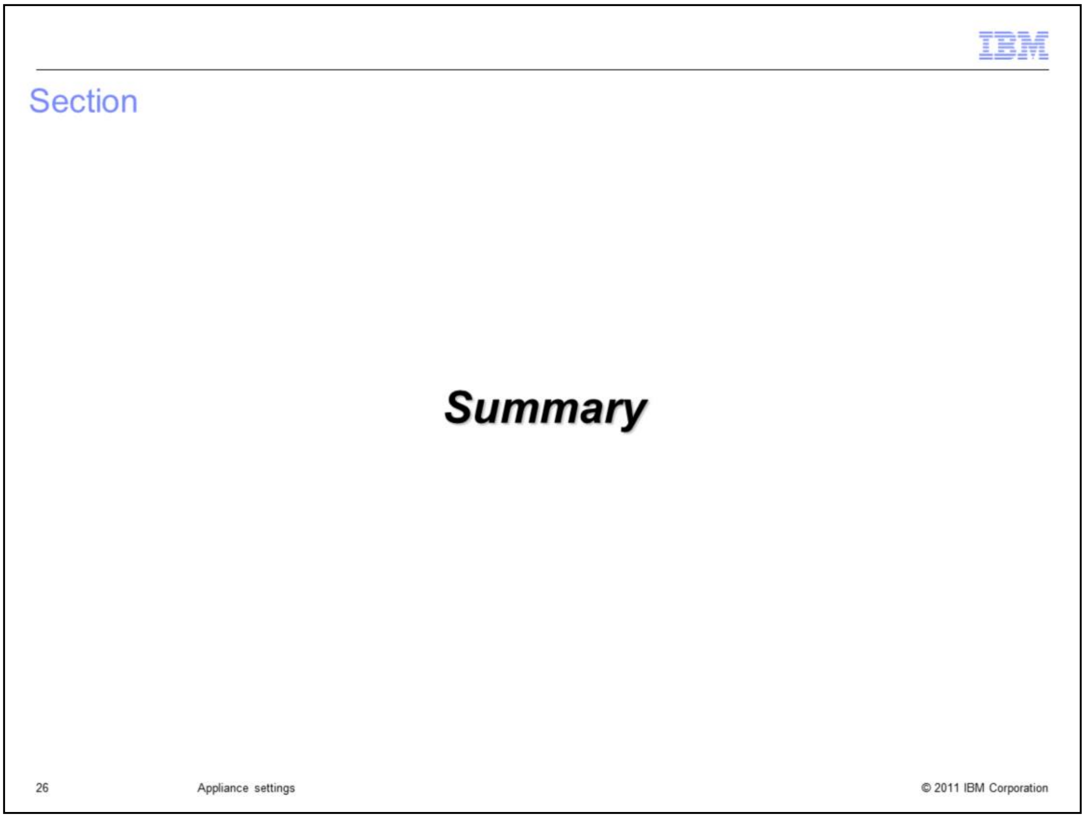
- ☑ Deploy patterns in the cloud
- □ Create new patterns
- □ Create new environment profiles
- □ Create new catalog content
- □ Cloud administration
  - ● Read-only view
  - ○ Full permissions
- □ Appliance administration
  - ● Read-only view
  - ○ Full permissions
- □ IBM License Metric Tool (ILMT)

Is this deployment option suitable?

Should user be added to certain groups?

What additional permissions should he have?

After the new user is initially defined, you will see the user detail panel. You can make changes to the user definition, since the user has only the default settings. Determine if the deployment options are suitable for this user. Consider adding the user to the appropriate groups. Then set specific permissions for the new user as appropriate. User permissions include create new patterns, create new environmental profiles, create new catalog content, cloud administration, appliance administration, and IBM License Metric Tool. The user detail panel also shows you the patterns and cloud groups that the user has created, and the virtual systems that the user has deployed.

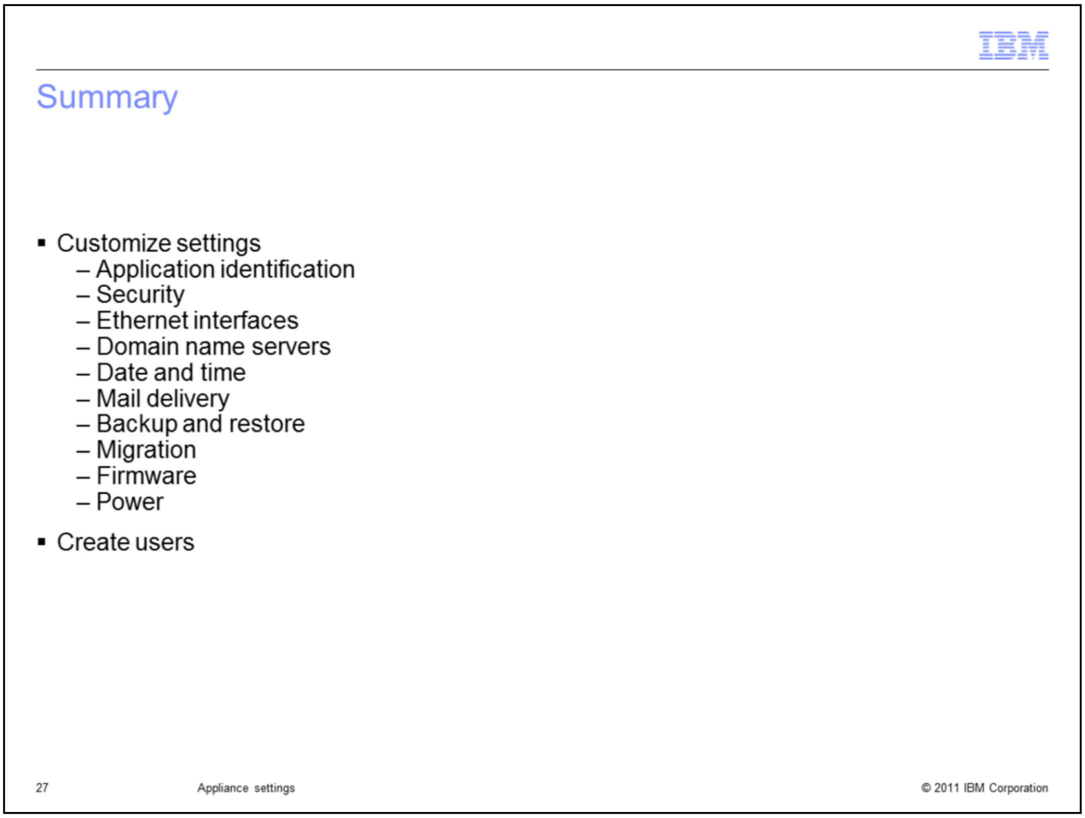


Section

Summary

26 Appliance settings © 2011 IBM Corporation

This section will summarize the settings presentation.

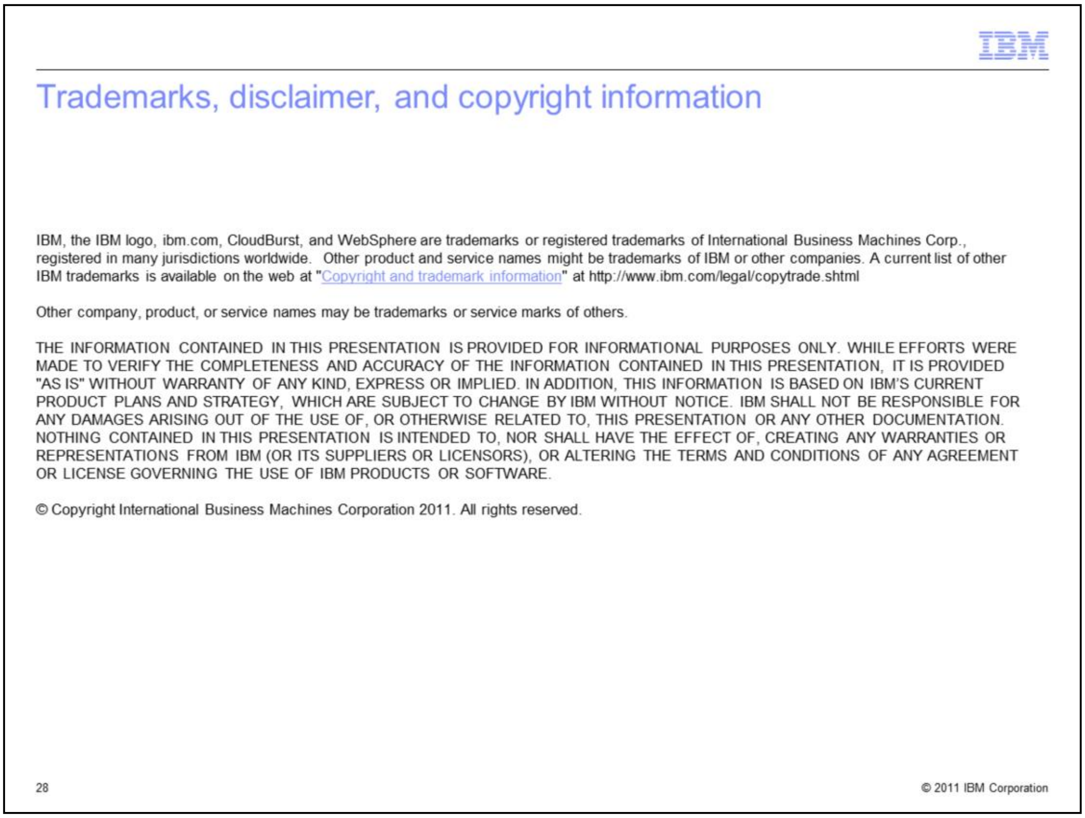


Summary

- Customize settings
  - Application identification
  - Security
  - Ethernet interfaces
  - Domain name servers
  - Date and time
  - Mail delivery
  - Backup and restore
  - Migration
  - Firmware
  - Power
- Create users

This presentation discussed the IBM Workload Deployer appliance settings and creating new users. In the security settings, you can allow or disallow new users to create their own accounts, and set up and test LDAP security. In Ethernet interfaces, you can review, add, change, or delete Ethernet connection definitions and review statistics, including error and drop counts, for the Ethernet connections you have defined. Within the domain name servers setting, you can review, add, or delete domain name servers, and test IP and host names. You use the date and time setting to specify the time zone and to review, add, or delete network time protocol servers. Under mail delivery, you can specify the SMTP server and reply-to address for the appliance to use when sending notification email to registered users. Within the backup and restore settings, you can provide the information needed for taking a backup image of your appliance and for restoring from a backup image. Under migration, you see how to select an IBM WebSphere CloudBurst backup image and initiate your migration. Under firmware settings, you can review the current firmware level settings and upgrade the firmware level. Finally, under power administration, you can restart or shutdown the appliance.

You saw how to create a new user account, how to review user information, and how to specify user permissions.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, CloudBurst, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.