

Deployit Upgrade Manual

Version 3.7.5

Table of Contents

| | |
|--|---|
| Table of Contents | 2 |
| The upgrade process | 3 |
| Upgrade notes | 3 |
| Performing the upgrade | 3 |
| Upgrading the Server | 3 |
| Upgrading the CLI | 4 |
| Specific upgrade notes | 4 |
| Upgrading from Deployit 3.0 or earlier | 4 |
| Upgrading from Deployit 3.5 to Deployit 3.6 | 4 |
| Upgrading from Deployit 3.5 or 3.6 to Deployit 3.7 | 4 |
| Security upgrade | 4 |
| Additional upgrade steps | 6 |
| Completing the migration | 6 |

The upgrade process

Overall, the upgrade process consists of the following steps:

- Obtain a new version of the Deployit software (the main product and/or plugins) from XebiaLabs.
- Read the new version's **release notes** so you are aware of the new functionality and possible upgrade considerations.
- Read the new version's **upgrade manual** (this document) so you are aware of possible upgrade considerations.
- Stop the current version of Deployit if it is still running.
- Create a brand-new installation directory for the new version of Deployit so the existing version is still available in case of problems.
- Extract the new Deployit software release into the new installation directory.
- Copy the data from the previous Deployit installation directory into the new installation directory.
- Start the new version of Deployit.

See the section **Performing the Upgrade** below for a detailed explanation of these steps.

Upgrade notes

- It is possible to skip Deployit versions when upgrading. Deployit will sequentially apply any upgrades for the intermediate (skipped) versions. **Please read the specific upgrade instructions for each of the versions carefully.**
- The new version of Deployit may not be compatible with the existing version of your plugins. If this is the case, you'll need to download an updated version of your plugin as well. **Please read the specific upgrade instructions for each of the versions carefully.**
- If a repository upgrade is required, Deployit will detect that it is running against an old repository and will automatically execute an upgrade when it is first started. The server log will contain extensive logging of the repository upgrade process.
- Plugin versions are related to the version of Deployit that they are compatible with. For instance, WAS plugin version 3.6.0 requires **at least** Deployit server version 3.6.0. This version of the WAS plugin should also work in Deployit 3.7.0 unless stated otherwise in this document.

Performing the upgrade

To begin upgrading Deployit, first unpack the distribution archive. The distribution archive contains the following:

- A server archive.
- A CLI archive.

The release notes are stored in the server's **doc** directory. Please read them carefully before performing the upgrade.

Upgrading the Server

To upgrade an existing Deployit server installation, do the following:

1. Create a directory for the new Deployit server installation, including the new Deployit server version number in the directory name.
2. Extract the server archive in this directory.
3. Copy the contents of the **conf** directory from the previous installation into the new installation directory.
4. Copy the entire **repository** directory from the previous installation into the new installation directory.
5. Copy the contents of the **importablePackages** directory from the previous installation into the new installation directory.
6. Unless new versions of your plugins were provided with the new Deployit version, copy the contents of the **plugins** directory from the previous installation into the new installation directory.
7. Copy the contents of the **ext** directory from the previous installation into the new installation directory.
8. **DO NOT** copy the contents of the **hotfix** directory (unless instructed) because hotfixes are version specific.
9. If you added libraries to Deployit's **lib** directory (for instance, database drivers), copy

the additional libraries from the previous installation into the new installation directory.

10. If you have made any changes to the Deployit server startup scripts (*server.sh* or *server.cmd*), manually re-do these changes in the new installation directory.

Note: please make sure that the plugins and extensions in the old Deployit installation are compatible with the new Deployit server version.

This completes upgrading of the Deployit server.

Upgrading the CLI

To upgrade an existing Deployit CLI installation, do the following:

1. Create a directory for the new Deployit CLI installation, including the new Deployit CLI version number in the directory name.
2. Extract the CLI archive in this directory.
3. Copy the contents of the **plugins**, **ext** and **hotfix** directories from the previous installation into the new installation directory.
4. If you have made any changes to the Deployit CLI startup scripts (*cli.sh* or *cli.cmd*), copy these from the **bin** directory in the previous installation into the new installation directory.

This completes upgrading of the Deployit CLI.

Specific upgrade notes

This section describes specific considerations for migrating from or to a particular Deployit version.

Upgrading from Deployit 3.0 or earlier

Deployit and the plugins were changed extensively in version 3.5. As a consequence, it is **not** possible to automatically migrate from a 3.0 or earlier version to version 3.5 or later. If you want to perform this type of upgrade, please contact the XebiaLabs support team.

Upgrading from Deployit 3.5 to Deployit 3.6

- Deployit 3.6 is a drop-in replacement for Deployit 3.5. No repository migration is needed.
- New versions of the following plugins are needed:
 - WAS plugin
 - WLS plugin

Upgrading from Deployit 3.5 or 3.6 to Deployit 3.7

- Deployit 3.7 contains an updated security implementation. Data from a pre-3.7 repository will automatically be converted to the new security model. See the section below for a complete description of the security upgrade.
- New versions of the following plugins are needed:
 - WAS
 - WLS
 - Tomcat
 - JBoss

Security upgrade

Permissions and repository

Starting with Deployit 3.7, Deployit needs to know the admin user's password to access the repository. This must be entered in the `deployit.conf` file prior to starting the new Deployit server. Note that the password in the configuration file is encrypted by the Deployit server when it starts.

The main change in the Deployit 3.7 security model is that local security permissions are stored only on root nodes and *core.Directory* CIs. During the upgrade, Deployit will convert pre-3.7-style permissions to the new permission system and automatically create directories to attach the relevant permissions to. The server log contains a description of the old security information that was found and how this was translated to the new permission system.

Permissions in Deployit are now assigned to **roles** instead of directly to principals. Deployit itself contains the definitions of roles and the principals they map to. Deployit will create a role for every user it finds during the upgrade.

It is also no longer possible to globally grant certain permissions. Permissions *deploy#initial*, *deploy#upgrade*, *deploy#undeploy*, *import#initial*, *import#upgrade*, *task#skip_step*, *task#move_step* can now only be granted on a directory CI. Deployit will convert these

global permissions into directory permissions during the upgrade.

Deployit 3.7 no longer allows *deny* permissions. Instead, permissions should be segregated using the new *core.Directory* grouping CIs. The *deny* permissions are not migrated by Deployit and an equivalent configuration must be created manually.

Permission *repo#edit* no longer allows deleting of packages. From 3.7 onwards, new permission *import#remove* is required to be allowed to delete packages.

In summary, these are the security changes in Deployit 3.7:

| Feature | Pre-3.7 | 3.7 | Conversion |
|---|--|---|--|
| Admin password | Deployit did not need the administrator password. | Deployit needs the administrator password. | The administrator password must be set manually in the <code>deployit.conf</code> file before starting Deployit 3.7. |
| Local permissions defined per CI | Local permissions can be defined on any CI, if the permission is applicable. | Local permissions can only be defined on root nodes or core.Directory CIs. | Deployit automatically migrates permissions from pre-3.7 repositories to 3.7, creating new directory CIs as needed. |
| Permission assignment | Permissions are assigned to users (when using the repository as user store) or LDAP principals (users or groups). | Permissions are assigned to roles managed within Deployit. | Deployit automatically migrates principals from pre-3.7 repositories to 3.7, creating new roles as needed. |
| Permissions that are both global as well as local | Several permissions (<code>deploy#initial</code> , <code>deploy#upgrade</code> , <code>deploy#undeploy</code> , <code>import#initial</code> , <code>import#upgrade</code> , <code>task#skip_step</code> , <code>task#move_step</code>) can be assigned both globally as well as locally. | These permissions can only be assigned locally on root nodes or directory CIs. | Deployit automatically migrates these permissions from pre-3.7 repositories to 3.7. |
| deny permissions | Permissions can explicitly be denied on any level. | Denying permissions is no longer possible. | Deployit does not migrate deny permissions. An equivalent security configuration must be created manually after the upgrade. |
| Permission to delete packages | <code>repo#edit</code> permission allowed deleting of packages. | New permission import#remove is introduced to allow deleting of packages. Permission <code>repo#edit</code> is still required to edit CIs. | Deployit automatically assigns <code>import#remove</code> to roles that had <code>repo#edit</code> permission in the pre-3.7 repository. |

LDAP

Configuration of LDAP security has also changed. The configuration in 3.7 is specified in a file called *deployit-security.xml*. The 3.6-style LDAP configuration in the *jackrabbit-jaas.config* file can be migrated easily to the 3.7 format. The following table describes the mapping of the 3.6-style LDAP setup to the new 3.7 setup:

| 3.6 example | 3.7 XML element | 3.7 XML properties | 3.7 example |
|--|--|-------------------------|--|
| <code>userProvider="ldap://localhost:389/ou=system"</code> | <code>security:ldap-server</code> | url and root properties | <code><security:ldap-server id="ldapServer" url="ldap://localhost:389/" root="ou=system"/></code> |
| <code>userFilter="(&(uid={USERNAME}))(objectClass=inetOrgPerson)"</code> | <code>security:ldap-authentication-provider</code> | user-search-filter | <code>user-search-filter="(&(uid={0}))(objectClass=inetOrgPerson)"</code> |
| <code>userSearchBase="dc=example,dc=com"</code> | <code>security:ldap-authentication-provider</code> | user-search-base | <code>user-search-base="dc=example,dc=com"</code> |
| <code>groupFilter="(memberUid={USERNAME})"</code> | <code>security:ldap-authentication-provider</code> | group-search-filter | <code>group-search-filter="(memberUid={0})"</code> |
| <code>groupSearchBase="ou=groups,dc=example,dc=com"</code> | <code>security:ldap-authentication-provider</code> | group-search-base | <code>group-search-base="ou=groups,dc=example,dc=com"</code> |
| <code>java.naming.security.principal="cn=admin,dc=example,dc=com"</code> | <code>security:ldap-server</code> | manager-dn | <code><security:ldap-server id="ldapServer" url="ldap://localhost:389/" manager-dn="cn=admin,dc=example,dc=com" manager-password="secret"/></code> |
| <code>java.naming.security.credentials="secret"</code> | <code>security:ldap-server</code> | manager-password | <code><security:ldap-server id="ldapServer" url="ldap://localhost:389/" manager-dn="cn=admin,dc=example,dc=com" manager-password="secret"/></code> |
| <code>useSSL</code> | <code>security:ldap-server</code> | url | Use the LDAPS protocol in the url, for example: <code><security:ldap-server id="ldapServer" url="ldaps://localhost:686/"></code> |
| <code>principalProvider=com.xebialabs.deployit.security.LdapPrincipalProvider</code> | n/a | n/a | This element is no longer required. |

See the **System Administration manual** for more details on the available LDAP configuration options.

If you used Deployit 3.6 with LDAP, you will have modified the **conf/jackrabbit-repository.xml** file. For 3.7, the *Security* snippet must be:

```
<security>
  <ldap/>
</security>
```

```
<Security appName="Jackrabbit">
  <SecurityManager
class="org.apache.jackrabbit.core.DefaultSecurityManager"
workspaceName="security" />
  <AccessManager
class="org.apache.jackrabbit.core.security.DefaultAccessManager" />
  <LoginModule
class="org.apache.jackrabbit.core.security.authentication.DefaultLoginModule">
    <param name="anonymousId" value="anonymous" />
    <param name="adminId" value="admin" />
  </LoginModule>
</Security>
```

Additional upgrade steps

After completing the upgrade procedure described in **Upgrading the Server** above, perform the following additional steps:

1. Edit the `deployit.conf` file and enter the admin password to property `admin.password`.
2. If you use LDAP, migrate the LDAP configuration to the `deployit-security.xml` configuration file.
3. Create a backup of your repository.
4. Start the Deployit server. When the server starts, Deployit will migrate the security information from the 3.6 repository to the 3.7 structure. In this process, Deployit will automatically create a role for each user in Deployit as well as special `core.Directory` CIs to assign permissions to.
5. Log into Deployit as the admin user and inspect the changes to the repository.
6. Open the Admin tab to create meaningful role assignments.
7. Open the Repository tab to create meaningful directory names.

Completing the migration

After the Deployit automated upgrade completes, log in to the Deployit GUI with various credentials to ensure that the security setup was correctly migrated. It is now possible to see the security permissions on `directory` CIs in the Repository Browser.