



Securing Borland Enterprise Server

February 2005



Copyright © 2005 by Dolphin Data Development Ltd. All rights reserved. Dolphin Development Ltd. reserves the right to make changes in the information contained in this publication without prior notice. No part of this work may be reproduced or transmitted in any form or by any means without prior written permission by the Publisher.

Borland Enterprise Server is a registered trademark of Borland Corporation. Other brands or product names are trademarks or service marks of their respective owners, should be treated as such, and may be registered in various jurisdictions.

Contributors

Author	Kevin Dean	Application Services Manager	kdean@datadevelopment.com
Editor	Tim White	Documentation Services Manager	twhite@datadevelopment.com

Version History

1.0	February 14, 2005	Initial Release
-----	-------------------	-----------------

Securing Borland Enterprise Server

Introduction

Upon installation, the default user name and password for managing a Borland Enterprise Server instance are both *admin*. While this is suitable for a development environment, it is not suitable for a production environment.

Unfortunately, the task here is not as simple as changing a single password. Borland Enterprise Server comes bundled with several users in the management domain and each of them has a default password that matches the user name. Even if you secure the *admin* user with a password that will take years to crack, you can still login to Borland Enterprise Server with user name *scu* or *partition* and with the password equal to the user name.

This whitepaper outlines the steps necessary to change the default *admin* password, to create additional roles and users, and to secure other required users. Note that references to path names use the UNIX '/' rather than the Windows '\' path separator.

This document has been developed with Borland Enterprise Server 6.5; it may apply to version 6.0 as well but it does not apply to any earlier version. It is assumed that the reader is already familiar with the installation and configuration of Borland Enterprise Server.

Management Hub Configuration

All of the security parameters other than the users may be configured through the management console. To configure security:

1. Start the **Borland Management Agent**;
2. Start the **Management Console**;
3. When prompted for security credentials, enter **admin** for the user name and **admin** for the password;
4. Expand the **Management Hubs** node;
5. Expand the **node** of the management hub you would like to configure;
6. Expand the **Agents** node;
7. Expand the **node** of the agent you would like to configure;
8. Expand the **Security Profiles** node;
9. Right-click on **management** and select **Properties...**;



10. If you want to enable SSL, check **Secure Sockets Enabled** (note that, as most hubs will be on local subnets, SSL should not be required and may incur a performance penalty);
11. Press **Authorization...**;
12. Add the line ***GROUP=operators** to the “**AdministratorViewers**” section in the management rolemap;

```
#
# Map user identities to the administration
roles.
#
AdministratorUpdaters {
    *GROUP=administrators
}
AdministratorViewers {
    *GROUP=operators
    ROLE = AdministratorUpdaters
}
ServerProcess {
    *GROUP=administrators
}
```

13. Press **Verify** to verify that the file is correct;
14. Press **OK**;
15. Press **Yes** to save the changes;
16. Press **OK**;
17. Expand the **Configurations** node;
18. For every configuration, right-click and select **Delete...** to delete the configuration, and press **Yes** to confirm;
19. Stop the **Management Console**; and
20. Stop the **Borland Management Agent**.



User configuration

To configure users you will need to work from the command prompt. The BES bin directory needs to be in the PATH for the command-line utilities to work. Under Windows, select **BES AppServer Edition Command Prompt** from the *BES AppServer Edition* program group to open a command prompt with the appropriate PATH setting.

Before starting, make sure that you have new passwords in mind for the *admin*, *scu*, and *partition* users. The latter two especially can have passwords as cryptic as you want as you will only ever have to use the passwords once.

To configure users:

1. Open a **command prompt** or add the **BES bin directory** to the current PATH;
2. Stop the **Management Console**;
3. Stop the **Borland Management Agent**;
4. Change to the **directory**
`"BES_installation/var/security/profiles/management"`;
5. Start an **interactive user database administration session** as follows:
`userdbadmin -db jdbc:borland:dslocal:mgmtdb.jds -user
admin -password admin -interactive`
6. Add the **operators group** as follows:
`addgroups operators`
7. Change the password for each of the **admin**, **scu**, and **partition** users as follows:
`updateuser existing_user new_password`
8. Remove the unused **borland** user as follows:
`removeuser borland`
9. Add a new **administrator user** as follows:
`adduser new_user new_password user administrators`
10. Add a new **operator user** as follows:
`adduser new_user new_password user operators
and`
11. Quit the **interactive user database administration session** as follows:
`quit`



Updating the SCU management vault

The SCU process needs to authenticate (essentially with itself) on startup. To do so, it uses credentials stored in a vault; this vault needs to be updated with the new password chosen for the *scu* user as follows:

1. Change to the **directory**
`BES_installation/var;`
2. Delete the **file**
`domains/base/adm/security/scu_mgmt_vault;`
3. Regenerate the **vault** as follows:
`vaultgen -vault domains/base/adm/security/scu_mgmt_vault -config
security/profiles/management/management_config.jaas login
ServerRealm`
 - 3.1. Enter the **scu** user name and the new **password** when prompted.

Creating a template management vault

Many of the processes within configurations need to authenticate with the server on startup. To do so, they use credentials stored in a vault. Unfortunately, Borland Enterprise Server makes multiple copies of the vault and so the only practical time to update it is when a configuration is first created. To create the template:

1. Change to the **directory**
`BES_installation/var;`
2. Generate the **vault** as follows:
`vaultgen -vault management_vault -config
security/profiles/management/management_config.jaas login
ServerRealm`
 - 2.1. Enter the **partition** user name and the new **password** when prompted; and
3. Move the **file** to a safe location.



Securing the management user database

Unfortunately, it is not possible to secure the management user database. While it would be possible to change the password for the database, the password would have to be updated in a plain text file (`management_config.jaas`) in the same directory. Accordingly, anyone who can gain access to the directory can update the database, though they will not be able to read existing passwords which are SHA-encrypted. As long as the host system is secure, the database is as well.

Operators vs. administrators

Users in the group *operators* are granted the *AdministratorViewers* role when they authenticate with the management service. With this role they can view a running installation but cannot configure it or manage it in any way. Such users may be useful for monitoring an operation without being able to change it.

Despite this restriction, the user interface in the management console doesn't prevent the user from accessing configuration dialogs and attempting to make changes until such time as the changes are applied, at which point an exception of type `"org.omg.CORBA.NO_PERMISSION"` is thrown. Furthermore, for these users the management hub will show up as being unlicensed, though this will not affect operation.

Securing the remaining security profiles

Borland Enterprise Server is bundled with four security profiles: default, disabled, management, and `ssl_enabled`. The management security profile is secured as above; of the rest, the default and `ssl_enabled` security profiles have default users in their user databases and the disabled security profile has no user database at all.

While the default users have no access to any application unless it is explicitly granted, it is a good idea to remove anyway; it is very easy to forget about them when configuring application security months after Borland Enterprise Server is installed.

To secure the remaining security profiles:

1. Change to the **directory**
`"BES_installation/var/security/profiles/profile_name"` where the profile name is either **default** or **ssl_enabled**;
2. Start an **interactive user database administration session** as follows:

```
userdbadmin -db jdbc:borland:dslocal:userdb.jds -user  
admin -password admin -interactive
```



3. Remove the **default users** as follows:

```
removeuser admin
removeuser jeeves
removeuser pclare
removeuser borland
removeuser joeshopper
removeuser defaultuser
and
```

4. Quit the **interactive user database administration session** as follows:

```
quit
```

Creating a new configuration

When creating a new configuration, Borland Enterprise Server creates a management vault with the user name and password *partition*. If you start this configuration after having changed the password as above, the configuration won't start correctly.

Before starting the configuration for the first time, replace the **file** `BES_installation/var/domains/base/configurations/new_configuration/mos/standard/adm/security/management_vault` with the template management vault created above.