Server Setup

*BAE Version 4.3 Release BAE-SQ-M-20180213*

Boardwalktech Inc.

10050 N Wolfe Rd, Cupertino,

CA 95014

Phone: +1-650-618-6100

Email: support@boardwalktech.com

Optimal Configuration

***Client Machine***

1. Server: OS Version / License : Windows 7 or higher
2. Office Version : 2007 32 bit or higher
3. Memory : 4GB or higher

***Application Servers***

1. Server: OS Version / License : Windows Server 2012 R2 Standard Edition 64 bit
2. Processor : Dual Processor Quad-Core Intel or AMD 1.9 Gigahertz
3. Memory : 32GB
4. Drive Configuration : 200 GB
5. Network : 1000 Mbps
6. Java : JDK 1.7 or higher
7. Tomcat : Version 7 or higher
8. Text File editor : Like Notepad++
9. External Storage Connection : Private Backup Network Connection
10. Managed Backup : Unmetered Backups

Weekly Full and Daily Differential

1. Redundant Power : Yes

***Database Servers***

1. Server: OS Version / License : Windows Server 2012 Standard Edition 64 bit
2. Processor :  Dual Processor Quad or Hex-Core Intel or AMD 2.5Gh
3. Memory : 64 GB
4. Drive Configuration : 4 Raid 10 100 GB

The drive space is dependent on the level of data in the application

If we bring in transactional data then the drive space will need re-evaluation

1. Network : 1000 Mbps
2. Standard Drive Partitioning : As recommended
3. External Storage Connection : Private Backup Network Connection
4. Managed Backup : Unmetered Backups

Weekly Full and Daily Differential

1. Microsoft Windows Server Standard Edition 2008 or higher

* SQL Server Database Engine
* SQL Server Integration Services
* SQL Server Management Studio
* Business Intelligence Development Studio or Data Tools

Pre-requisite

* Microsoft SQL Server is installed on the database server
* Java is installed on Application server
* Apache Tomcat is installed on Application server

Installation Package

Installation package consist of following files:

1. BAE\_4\_3.war
2. BAE\_4\_3.zip

Assumptions:

1. Database Machine
   1. Microsoft SQL Server is installed
   2. Microsoft SQL Server Management Studio (SSMS) is installed
2. Application Machine
   1. Apache Tomcat is installed
   2. Java JDK is installed
3. Admin rights on Database and Application Servers
4. Installation files have been downloaded on both the machines

Installation Steps:

1. **Boardwalk Database Installation**

Unzip the file **BAE\_4\_3.zip** in which there will be 8 SQL files like below.

Execute the extracted files in the following order.

1. **01\_Create\_Login.sql**
2. **02\_Create\_Database.sql**

**Note**: Replace the string ‘BAE\_4\_3’ with desired database name and change the path for MDF and LDF file creation.

1. **03\_Create\_Tables.sql**

**Note:** Replace ‘BAE\_4\_3’ with desired database name.

1. **04\_Create\_Table\_Types.sql**

**Note:** Replace ‘BAE\_4\_3’ with desired database name.

1. **05\_Create\_Procedures.sql**

**Note:** Replace ‘BAE\_4\_3’ with desired database name.

1. **06\_Create\_Functions.sql**

**Note:** Replace ‘BAE\_4\_3’ with desired database name.

1. **07\_Default\_Values.sql**

**Note:** Replace ‘BAE\_4\_3’ with desired database name.

1. **08\_Create\_Objects.sql**

**Note:** Replace ‘BAE\_4\_3’ with desired database name.

1. **Boardwalk Application Installation**
2. Copy the file **BAE\_4\_3.war** in <Tomcat>/webapps folder.
3. **BAE\_4\_3.war** file will extract automatically under the webapps folder.
4. Rename the extracted folder with desired name.
5. Make the following changes to Tomcat configuration (**web.xml** file).
6. Delete **BAE\_4\_3.war** from Webapps folder.
7. Restart Tomcat.

**Tomcat Path Changes**

Replace the string **BAE\_4\_3** with the newly created application name.

**Database Parameters Configuration**

<init-param>

<param-name>databasename</param-name>

<param-value>BAE\_4\_3</param-value>

</init-param>

<init-param>

<param-name>databasetype</param-name>

<param-value>SQLSERVER</param-value>

</init-param>

<init-param>

<param-name>InstanceName</param-name>

<param-value>DEFAULT</param-value>

</init-param>

<init-param>

<param-name>user</param-name>

<param-value>BOARDWALK\_APPLICATION\_USER</param-value>

</init-param>

<init-param>

<param-name>password</param-name>

<param-value>BOARDWALK\_APPLICATION\_USER</param-value>

</init-param>

<init-param>

<param-name>server</param-name>

<param-value>localhost</param-value>

</init-param>

<init-param>

<param-name>port</param-name>

<param-value>1433</param-value>

</init-param>

**SMTP Parameters Configuration**

<init-param>

<param-name>smptserver</param-name>

<param-value>secure.emailsrvr.com</param-value>

</init-param>

<init-param>

<param-name>smtpport</param-name>

<param-value>80</param-value>

</init-param>

<init-param>

<param-name>username</param-name>

<param-value>password@boardwalktech.com</param-value>

</init-param>

<init-param>

<param-name>password</param-name>

<param-value>boardwalk</param-value>

</init-param>

</servlet>

1. Verify Boardwalk Application from browser.

Ex: <http://localhost:8080/BAE_4_3/MyCollaborations>

1. There is an Administrator user already created with User Name ‘admin’. Use this User Name and default Boardwalk password to login to the system.
2. The ‘ROOT’ Neighborhood is already existing in the application and the default members in this Neighborhood are
   1. admin
   2. BOARDWALK\_INTEGRATION (Integration User)
3. Below ROOT folder, there is a default Collaboration with name ‘SYSTEM’ which should be used strictly for product level Whiteboards and Cuboids.

*Note: Please don’t use this Collaboration for project specific Whiteboards and Cuboids and please create a new Collaboration for the same.*

1. The SYSTEM Collaboration will have the below default Whiteboards and Cuboids.

|  |  |  |
| --- | --- | --- |
| **Cuboid Id** | **Whiteboard Name** | **Cuboid Name** |
| 1000002 | BRect | BRectDefinition |
| 1000009 | Configuration | SystemConfiguration |
| 1000003 | KeyStore | KeyStore |
| 1000010 | Manifest | TemplateManifest\_ProcessManagement |
| 1000001 | TemplateManifest\_SuperMerge |
| 1000008 | PerformanceCapture | PerformanceCapture |
| 1000006 | SuperMerge | C2C\_SuperMerge\_Rules |
| 1000005 | C2S\_SuperMerge\_Rules |
| 1000007 | Multi\_C2C\_SuperMerge\_Rules |
| 1000004 | S2C\_SuperMerge\_Rules |

1. Configure Boardwalk Template to connect with newly installed Boardwalk Server.

User Authentication Setup

Once all the above setup is done, User Authentication Setup should be configured if needed.

To configure the User Authentication Setup, please follow the below steps

1. Download and Save the Process Management template with version 3.1 to the local hard disk.
2. Go to System\_Properties sheet to connect the template with the Webapp by providing the URL.
3. From WELCOME sheet and Download the data.
4. Go to SystemConfiguration sheet with the below data

|  |  |  |
| --- | --- | --- |
| **Type** | **Parameter** | **Value** |
| Security | Minimum Password Length | 0 |
| Security | Special Character Required | N |
| Security | Number Required | N |
| Security | Upper Case Required | N |
| Security | Lower Case Required | N |
| Security | Restrict Repeat Characters | N |
| Authentication | Change Password On Next Login | N |
| Authentication | Number of Unsuccessful Login Attempts Allowed | 0 |
| Authentication | Temp Lockout Time (Mins) | 0 |
| Authentication | Inactivity Lockout (Days) | 0 |
| Authentication | Password Validity (Days) | 0 |

1. There will be 2 different Types named as Security and Authentication. The items which belong to Security Type are the ones to set up the Password Complexity whereas the items belong to Authentication Type are to configure the User Authentication Set up.
2. All the data in the Value column is the default data and all the functionalities are in disabled state. The values should be changed in order to implement the behavior of Parameter column.
3. Below is the explanation about each item
4. **Minimum Password Length**

Password with less than this value will not be accepted while resetting the password. The minimum value which can be set to this value will be equal to the number of YES flags(Y) of the remaining items of the Security type.

For Example, if 2 values are Y for the items of Security Type, the minimum value which we can set for ‘Minimum Password Length’ is 2.

Set the value to 0 to disable this feature.

1. **Special Character Required**

If Y, the password without at least one special keyboard character will not be accepted while resetting the password.

Set the value to N to disable this feature.

1. **Number Required**

If Y, the password without at least one numeric character will not be accepted while resetting the password.

Set the value to N to disable this feature.

1. **Upper Case Required**

If Y, the password without at least one upper case character will not be accepted while resetting the password.

Set the value to N to disable this feature.

1. **Lower Case Required**

If Y, the password without at least one lower case character will not be accepted while resetting the password.

Set the value to N to disable this feature.

1. **Restrict Repeat Characters**

If Y, the password with repeated characters will not be accepted while resetting the password.

Set the value to N to disable this feature.

1. **Change Password On Next Login**

If Y, user should change his password to login to the system for the first time.

Set the value to N to disable this feature.

1. **Number of Unsuccessful Login Attempts Allowed**

This is the maximum number of times the user can try to login to the system with invalid credentials.

The counter will increase by 1 with every unsuccessful attempt and the user account will be temporarily locked once it reaches this value.

Once the user account is locked, user needs to wait for some time to login again. This wait time needs to be set for the next item ‘Temp Lockout Time (Mins)’

Set the value to 0 to disable this feature.

1. **Temp Lockout Time (Mins)**

This is the number of minutes the user needs to wait to login to the system once the user account is temporarily locked. The account will be unlocked automatically after this many minutes.

Set the value to 0 to disable this feature.

1. **Inactivity Lockout (Days)**

The user account will be permanently locked if user hasn’t performed any operation on the system. The administrator has to unlock once the user account is permanently locked.

Set the value to 0 to disable this feature.

1. **Password Validity (Days)**

User cannot use the password for more than these many days and the user is not allowed to login to the system once the validity is over. User will be prompted an option automatically to reset the password.

Set the value to 0 to disable this feature.