Bar Code Medication Administration (BCMA)
BCMA Backup System (BCBU)
Securing the Cache Cube for BCMA Backup

Version 3.0
April 2015

Department of Veterans Affairs (VA)
Office of Information and Technology (OIT)
Product Development (PD)
Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/2015</td>
<td>PSB<em>3</em>84</td>
<td>New document.</td>
<td>REDACTED</td>
</tr>
</tbody>
</table>
Contents

1  Create a New User ............................................................................................................................. 1
2  Configure the Management Portal to Accept Password Authentication ............................... 3
1 Create a New User

A. From the Management Portal home page, go to the System Administration, Security, Users menu ([System Administration] > [Security] > [Users]).


C. On the Edit User page, set values for only the following user properties. (Fill out the required fields below.) The other fields are optional.
   - Name (required) — Unique user identifier (suggest using your VHAxxxnnnnnnn ID).
   - Password (required) — New password value. (Remember this password!
   - Confirm Password (required) — Confirmation of new password value.
   - User Enabled (required) — Whether or not the account is available for use.

D. Click the Save button to create the new user.

Once you have created a user account, you then need to edit its characteristics.

1. On the Users page ([System Administration] > [Security] > [Users]), click Edit in the newly created user’s row. This displays the Edit User page for the user being edited.
2. Go to the [Roles] tab at the top of the Edit Page.
3. Move the ‘%All’ from the ‘Available’ column to the ‘Selected’ column by clicking the right arrow and then click ‘Assign’ to assign the user to the role(s).

After doing this, the user’s roles should contain the ‘%All’ role. (See example figure below.)
Create a New User

Return to the [General] tab and click Close.

E. Secure the other user accounts. Do this by editing the characteristics of the _System, Admin, CSPSystem, and SuperUser accounts.

1. On the Users page ([System Administration] > [Security] > [Users]), click Edit in the above mentioned user’s row. This displays the Edit User page for the user being edited.
2. On the Edit User page, set values for only the Password* and Confirm Password* fields for these users. (Remember these passwords.)
3. Click the Save button and Close button after you are finished editing each individual user above.
2 Configure the Management Portal to Accept Password Authentication

1. To set credentials for Studio from the Management Portal home page, go back to the Security level, choose Services page ([System Administration] > [Security] > [Services]).

2. Select the *Service_Callback* under the ‘Allowed Authentication Methods’ definition, uncheck Unauthenticated and ensure that Password IS checked. Click SAVE.

When finished the Services table should look like this.

![Services Table]

3. To set credentials for the Management portal from the Management Portal home page, go back to the Security level, then to the Applications level, then to the Web Applications page. ([System Administration] > [Security] > [Applications] > [Web Applications]).

![Web Applications Page]

4. On the Web Applications page, the /csp/sys application represents the Management Portal home page. Select Edit in this row to edit the application. This displays the Edit Web Application page for the /csp/sys application.

5. Under Allowed Authentication Methods, disable Unauthenticated access by ensuring it is NOT checked and enable Password access by ensuring it IS checked. Click Save, then Close.
Configure the Management Portal to Accept Password Authentication

When finished the Web Application table should look like this.

NOTE: If the Authentication Methods are different than this use the Edit for that name and correct to match this table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enabled</th>
<th>Type</th>
<th>Resource</th>
<th>Authentication Methods</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>/csp/samples</td>
<td>Yes</td>
<td>CSP</td>
<td></td>
<td>Unauthenticated</td>
<td>Edit</td>
<td>Delete</td>
</tr>
<tr>
<td>/csp/user</td>
<td>Yes</td>
<td>CSP</td>
<td></td>
<td>Unauthenticated</td>
<td>Edit</td>
<td>Delete</td>
</tr>
<tr>
<td>/csp/vista</td>
<td>Yes</td>
<td>CSP</td>
<td></td>
<td>Unauthenticated</td>
<td>Edit</td>
<td>Delete</td>
</tr>
<tr>
<td>/isc/studio/ustemplates</td>
<td>Yes</td>
<td>CSP</td>
<td></td>
<td>Unauthenticated</td>
<td>Edit</td>
<td>Delete</td>
</tr>
<tr>
<td>/csp/broker</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>Unauthenticated</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/csp/docbook</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>Unauthenticated</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/csp/documatic</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>%Development</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/csp/sys</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>Unauthenticated</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/csp/sys/exp</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>%Development</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/csp/sys/mg</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>%Admin_Manage</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/csp/sys/cop</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>%Admin_Operate</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/csp/sys/sec</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>%Admin_Secure</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/iac/studio/rules</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>Unauthenticated</td>
<td>Edit</td>
<td></td>
</tr>
<tr>
<td>/iac/studio/templates</td>
<td>Yes</td>
<td>System,CSP</td>
<td></td>
<td>%Development</td>
<td>Edit</td>
<td></td>
</tr>
</tbody>
</table>

This configures the Portal to require password authentication (also known as “Caché login”) and not to allow unauthenticated access, and so that all its parts behave consistently.