



**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

Date	Revision	Description	Author
4/2015	PSB*3*84	New document.	REDACTED

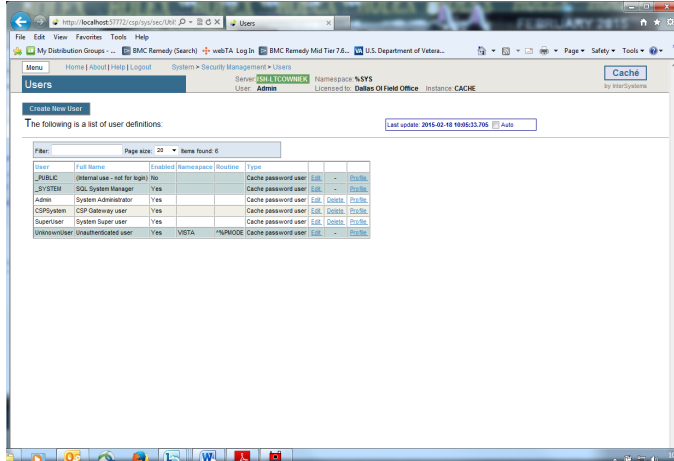
Revision History

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]).



- B. On the 'Users' page, select **Create New User**.

This displays the **[General]** tab of the **Edit User** page for creating and configuring users.

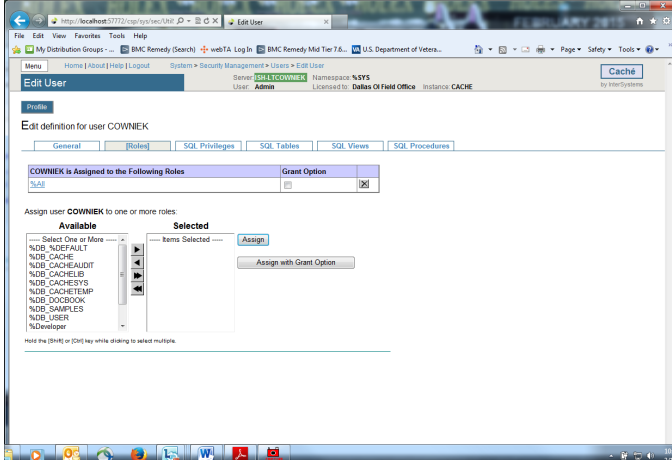
- C. On the **Edit User** page, set values for only the following user properties. (Fill out the required fields below.) The other fields are optional.
- **Name** (required) — Unique user identifier (suggest using your VHxxxxnnnnnn ID).
 - **Password** (required) — New password value. (Remember this 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.

Authentication

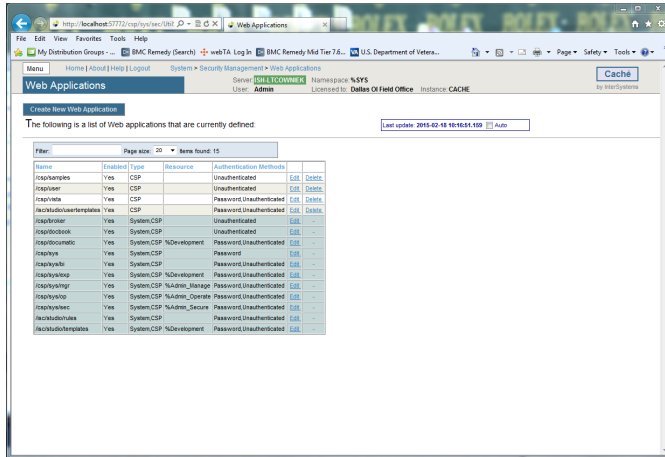
2 Configure the Management Portal to Accept Password Authentication

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 Bindings**, 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.

Name	Enabled	Public	Authentication Methods	Allowed Connections	Description	Two-Factor Enabled
%Service_Bindings	Yes	N/A	Password	Unrestricted	Controls SQL or Objects	No
%Service_CSP	Yes	Yes	Password Unauthenticated	Unrestricted	Controls CSP Gateway access	No
%Service_CacheDirect	Yes	Yes	Unauthenticated	Unrestricted	Controls Cache Direct	No
%Service_CallIn	Yes	Yes	Unauthenticated	Unrestricted	Controls the Call-in Interface	No
%Service_ComPort	No	Yes	Unauthenticated	Unrestricted	Controls COMM ports attached to a Windows system	No
%Service_Console	Yes	Yes	Unauthenticated	Unrestricted	Controls CTERM (TRM.pid) and the Windows Console	No
%Service_DataCheck	No	N/A		Unrestricted	Controls this system as a DataCheck source	No
%Service_ECP	No	N/A		Unrestricted	Controls Enterprise Cache Protocol (ECP)	No
%Service_Login	Yes	No	Password	Unrestricted	Controls SYSTEM.Security.Login	No
%Service_MSMActivate	No	N/A	Unauthenticated	Unrestricted	Controls MSM Activate Protocol	No
%Service_Mirror	No	N/A		Unrestricted	Controls Mirroring	No
%Service_Monitor	No	N/A		Unrestricted	Controls SHMP and remote Monitor commands	No
%Service_Shadow	No	N/A		Unrestricted	Controls if this system can be the source of a shadow	No
%Service_Telnet	Yes	Yes	Unauthenticated	Unrestricted	Controls Telnet sessions on a Windows server	No
%Service_WebLink	No	N/A	Unauthenticated	Unrestricted	Controls Weblink	No

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]).



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

Menu Home | About | Help | Logout System > Security Management > Web Applications > Edit Web Application Caché

Edit Web Application Server: **ISD-L-TEASONL7** Namespace: **%SYS**
 User: **vhaisdeasonl** Licensed to: **Dallas OI Field Office** Instance: **CACHE** InterSystems

Edit definition for Web application /csp/sys:

[General] Application Roles Matching Roles

Web Application Name: /csp/sys
 Description: System Management Portal
 Enabled:
 Resource required to run the application:
 Allowed Authentication Methods:
 Unauthenticated
 Password
 Login Cookie
 Group By Id: %SCMgtPortal
 Two Factor Enabled:
 CSP/ZEN Enabled:
 Inbound Web Services Enabled:
 Namespace: %SYS
 CSP Files Physical Path: c:\intersystems\cache\csp\sys
 Recurse: Yes
 Auto Compile: No

only Password should be checked

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.

Name	Enabled	Type	Resource	Authentication Methods		
/csp/samples	Yes	CSP		Unauthenticated	Edit	Delete
/csp/user	Yes	CSP		Unauthenticated	Edit	Delete
/csp/vista	Yes	CSP		Unauthenticated	Edit	Delete
/isc/studio/usertemplates	Yes	CSP		Unauthenticated	Edit	Delete
/csp/broker	Yes	System,CSP		Unauthenticated	Edit	-
/csp/docbook	Yes	System,CSP		Unauthenticated	Edit	-
/csp/documatic	Yes	System,CSP	%Development	Unauthenticated	Edit	-
/csp/sys	Yes	System,CSP		Password	Edit	-
/csp/sys/bi	Yes	System,CSP		Unauthenticated	Edit	-
/csp/sys/exp	Yes	System,CSP	%Development	Unauthenticated	Edit	-
/csp/sys/mgr	Yes	System,CSP	%Admin_Manage	Unauthenticated	Edit	-
/csp/sys/op	Yes	System,CSP	%Admin_Operate	Unauthenticated	Edit	-
/csp/sys/sec	Yes	System,CSP	%Admin_Secure	Unauthenticated	Edit	-
/isc/studio/rules	Yes	System,CSP		Unauthenticated	Edit	-
/isc/studio/templates	Yes	System,CSP	%Development	Unauthenticated	Edit	-

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.