

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 User1
2	Configure the Management Portal to Accept Password Authentication3

1 Create a New User

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

ers															
					er: Admin	Li Li	censed!	o: Dallasi	Il Field Offi	ce Instan	ce: CACHE			by InterSy	sterns
reate New Use	r .														
	a list of user definiti	0.000										.705 🕅 Auto	_		
e totowing is	a list of user definiti	0115.							case abo	10. 2015-02	-10 10005:33	.705 E Ano			
Filter:	Page siz	20 •	tems found:	8											
User F	ull Name	Enabled	Namespace	Routine	Туре		_								
PUBLIC (I	internal use - not for login)	No			Cache password	user Edit		Profile.							
SYSTEM S	QL System Manager	Yes			Cache password	user Edit		Profile.							
Admin S	ystem Administrator	Yes			Cache password	user Edit	Delete	Profile.							
	SP Gateway user	Yes			Cache password										
	ystem Super user	Yes			Cache password										
UnknownUser U	inauthenticated user	Yes	VISTA	*%PMODE	Cache password	user Edt		Profile.							

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 VHAxxxnnnnn 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.)

C C V trap/focablest57772/craftystore/bit D - 2 C X V Editor X
File Edit View Favorites Tools Help 💁 🖸 My Dictribution Groups 📓 BMC Remedy (Search) 🕂 webTA Log In 📓 BMC Remedy Mid Tier 76 🔯 U.S. Department of Vetera 🆓 👻 🔝 🖉 Safety 💌 Tools + 😥 = "
Memo Herms Alexel Help Logical Spitlam > Socially Banagement > Less > Lettil Management > Secially Banagement > Less > Lettil Management > Secially Banagement > Less > Lettil Banagement > Less > Les
Potes Edit definition for user COWNEK General [Bole] SQL Privileges SQL Tables SQL Views [SQL Procedures]
COMMEX is avaigned to the Following Roles Grant Option
Assgn user COWNIEK to one or more roles: Available Selected
Salet Over Norm → Term Salete1 → Assign Assign with Grant Option
Hard He (Shiff or (Shiff or White dialog) is a land multiple.

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 <mark>%Service_Bindings</mark>, under the 'Allowed Authentication Methods' definition, uncheck *Unauthenticated* and ensure that **Password <u>IS</u> checked**. Click <u>SAVE</u>.

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 Calln	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
<u>%Service Mirror</u>	No	N/A		Unrestricted	Controls Mirroring	No
%Service Monitor	No	N/A		Unrestricted	Controls SNMP 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.

	age size: 20	that are curr				Last update: 2015-02-18 10:10:01.109 📗 Auto
		Resource	Authentication Methods	_		
Yes	CSP	no anna ce	Unauthenticated		Delete	
Yes	CSP		Unauthenticated		Delete	
Yes	CSP					
Yes	CSP					
Yes	System CSP		Unauthenticated	Edit		
Yes	System.CSP		Unauthenticated	Edit		
Yes	System.CSP	%Development	Password Unauthenticated	Edt		
Yes	System,CSP		Password	Edt		
Yes	System,CSP		Password, Unauthenticated	Edt		
Yes	System,CSP	%Development	Password, Unauthenticated	Edt		
Yes	System,CSP	%Admin_Manage	Password, Unauthenticated	Edit		
Yes	System,CSP	%Admin_Operate	Password, Unauthenticated	Edt		
Yes	System,CSP	%Admin_Secure	Password, Unauthenticated	Edt.		
Yes	System,CSP		Password, Unauthenticated	Edt		
Yes	System,CSP	%Development	Password, Unauthenticated	Edit		
	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Yes CSP Yes System,CSP Yes System,CSP Yes System,CSP Yes System,CSP Yes System,CSP Yes System,CSP Yes System,CSP Yes System,CSP Yes System,CSP	Yes CSP Yes System,CSP Yes System,CSP	Yes CP Paraver Unabletedad Yes Syber.CP Daward Unabletedad Yes Syber.CP Uradiverticidad Yes Syber.CP Daward Unabletedad Yes Syber.CP Daward Unabletedad Yes Syber.CP Paraver Unabletedad	Yes OP Parametrical control of end VI 629 Reserved Standardset Ed Reserved Standardset Ed VI Reserved Standardset Ed Reserved Standardset Ed Reserved Standardset Ed VI Reserved Standardset Ed Reserved Standardset Ed Reserved Standardset Ed VI Reserved Standardset Ed Reserved Standardset Ed Reserved Standardset Ed VI Reserved Standardset Ed Reserved Standardset Ed Reserved Standardset Ed VI Reserved Standardset Ed Reserved Standardset Ed Reserved Standardset Ed VI Reserved Standardset Ed Reserved Standardset Ed Reserved Standardset Ed VI Reserved Standardset Ed Reserved Standardset Ed Reserved Standardset Ed VI Reserved Standardset Ed Reserved Standardset Ed Reserved Standardset Ed	Yet CB Person (Standard) (Standard) Molecular (Standard) <

4. On the **Web Applications** page, the <u>/csp/sys</u> 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 <u>NOT</u> checked and enable **Password** access by ensuring it <u>IS</u> checked. Click Save, then Close.

Configure the Management Portal to Accept Password Authentication

Μ	enu Home About Help Logo	ut System > Security Managem	ent > Web Application	s > Edit Web Application	Caché
E	dit Web Application		er: ISD-LTEASONL7	Namespace: %SYS Licensed to: Dallas OI Field Office	
E	it definition for Web application /csp/sy:	s:			
	[General] Application Roles	Matching Roles			
	Web Application Name*:	/csp/sys			
	Description:	System Management Portal			
	Enabled:	only Password			
	Resource required to run the application:	should be checked			
	Allowed Authentication Methods:				
		Password			
		Login Cookie			
	Group By Id:	%ISCMgtPortal			
	Two Factor Enabled:				
	CSP/ZEN Enabled:				
	Inbound Web Services Enabled:				
	Namespace:	%SYS 🔻			
	CSP Files Physical Path :	c:\intersystems\cache\csp\sys\		Browse	
	Recurse:				
	Auto Compile:				
	E 0				

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	Туре	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	<u>Edit</u>	-
/isc/studio/templates	Yes	System,CSP	%Development	Unauthenticated	<u>Edit</u>	-

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.