Common Security Services (CSS) Development Support

VBA BEP Web Application 2FA Login Page User Manual



Department of Veterans Affairs

January 2017

Version 1.0

Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 2017/01/20 | 1.0 | Initial version | Ivan Vanegas |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 1: Revision History

**Table of Contents**

[List of Figures iii](#_Toc472688389)

[1 Introduction 4](#_Toc472688390)

[1.1 Scope 4](#_Toc472688391)

[1.2 Audience 4](#_Toc472688392)

[2 VBA BEP CA SiteMinder Two Factor (PIV) Authentication and CSS Authorization 5](#_Toc472688393)

[2.1 Login Page 5](#_Toc472688400)

[2.1.1 VA Active Directory User/Password authentication 5](#_Toc472688401)

[2.1.2 PIV/PIN Authentication 6](#_Toc472688402)

[2.2 CSS Profile overload for Test Environments 7](#_Toc472688403)

[2.2.1 VA Active Directory User/Password authentication 8](#_Toc472688404)

[2.2.2 PIV/PIN Authentication 9](#_Toc472688405)

# List of Figures

[Figure 1. Login Page 5](#_Toc472942895)

[Figure 2 Login Page - PIV/PIN Authentication 7](#_Toc472942896)

[Figure 3. PIV/PIN Dialogs 8](#_Toc472942897)

[Figure 4 Login Page with optional Test User ID 9](#_Toc472942898)

[Figure 5 Login page with PIV/PIN authentication 10](#_Toc472942899)

[Figure 6 PIV/PIN Dialogs 11](#_Toc472942900)

# Introduction

The goal of the project is to move VBA BEP Web Applications from the current authentication to a Two Factor Authentication (2FA) using PIV Cards. By using 2FA the user’s identity will be confirmed when a combination of a physical PIV card and a Personal Identification Number (PIN) is presented to the system.

All applications that use VBA BEP Web Authentication Services are redirected to a single Login Page. Examples of these applications are: VBMS-\*, CaseFlow, WSMS, WEAMS, FOCAS and QaWeb.

This document describes the Login Page features from the user’s perspective.

## Scope

The scope of this document includes the Login Pages for Production and Test Environments.

## Audience

The audience for this document consists of:

* Users of VBA Web Applications in the Benefits Enterprise Platform like WEAMS, WSMS, FOCAS and QaWeb.
* Users of the VBA BEP Federation Authentication Services like VBMS-\* and CaseFlow.

# VBA BEP CA SiteMinder Two Factor (PIV) Authentication and CSS Authorization

## Login Page

Both, VBA Applications hosted inside or outside of the BEP WebLogic Internal Domain will be redirected to the same Login Page for authentication. This Login Page will provide the user the option of authentication into the applications using either Windows/CAG credentials or PIV/PIN.



Figure 1. Login Page

### VA Active Directory User/Password authentication

The Active Directory User/Password authentication form is located in the right panel of the Login Page. To be able to use this method of authentication the user should have been granted an exemption from PIV Login previously, normally from the National Service Desk.

The user should provide the following information:

* Station ID: A three-digit number that identifies the Station that the user will use for this session.
* User ID: VA Active Directory Username. This is the Windows/CAG username. NOTE: The domain should not be provided in this field.
* Password: The password provided by NSD when the exception was granted or the current VA Active Directory password if the user has already changed it.

Once the user has provided all the Login Credentials and after pressing the “Login” button in the right panel of the Login Page, the system will authenticate the user and a session will be created with all the Common Security Service (CSS) profile information associated to the user for that station and application. The user will then be redirected to the application that was originally trying to be accessed.

### PIV/PIN Authentication

The PIV/PIN authentication form is in the left panel of the Login Page. To be able to use this method of authentication the user will need the following information:

* PIV Card Reader: The user should insert the PIV Card into the Card Reader of the PC/equipment assigned to the user.



Figure 2 Login Page - PIV/PIN Authentication

* Station ID: A three-digit number that identifies the Station that the user will use for this session.

Once the user has provided all the Login Credentials and after pressing the “Login with PIV” button in the left panel of the Login Page, the system will access the PIV card in the reader and will load the stored certificates and prompt the user to select one.

* Select Certificate: The user should select the certificate used for PIV/PIN authentication and press OK. Then a Pop-Up Window asking for the PIN will be displayed.
* PIN: The user should provide the PIN and press OK.

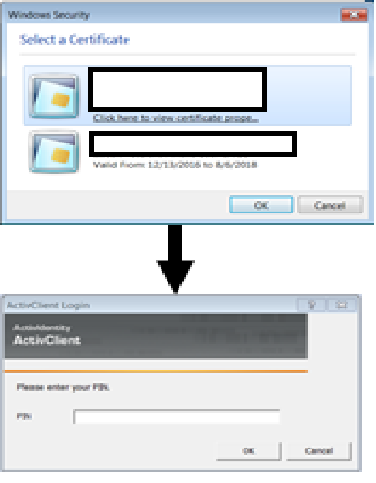


Figure 3. PIV/PIN Dialogs

If the PIV/PIN match correctly and the user has access to the application for the station entered, a session will be created with all the Common Security Service (CSS) profile information associated to the user in the PIV certificate for that station and application.

The user will then be redirected to the application that was originally trying to be accessed.

## CSS Profile overload for Test Environments

VBA BEP CA SiteMinder Two Factor (PIV) will load the CSS Profile of the Active Directory user associated to the PIV card. This poses a challenge for testers in Lower Level Testing Environments since only one PIV can be assigned to a user preventing them to test multiple CSS Profiles.

To facilitate testing work in Lower Level Testing Environments the system let the users use AD credentials or PIV card to authenticate and then load a different Testing CSS Profile (previously created in CSS) for subsequent applications to use instead of the CSS Profile associated to the Active Directory account.

In Lower Level Testing Environments, the Login Page will optionally offer the possibility of override the CSS Profile associated to the AD account with the CSS Profile introduce in the **Test User Id** field.



Figure 4 Login Page with optional Test User ID

### VA Active Directory User/Password authentication

The Active Directory User/Password authentication form is located in the right panel of the Login Page. To be able to use this method of authentication the user should have been granted an exemption from PIV Login previously, normally from the National Service Desk.

The user should provide the following information:

* Station ID: A three-digit number that identifies the Station that the user will use for this session.
* User ID: VA Active Directory Username. This is the Windows/CAG username. NOTE 1: The CSS Profile associated to this Active Directory user will be loaded into the session if the **Test User ID** filed is left blank. NOTE 2: Not domain should be provided in this field.
* Password: The password provided by NSD when the exception was granted or the current VA Active Directory password if the user has already changed it.
* Test User ID: CSS Username associated to the profile that will be loaded into the session instead of the originally associated to the AD user.

Once the user has provided all the Login Credentials and after pressing the Login button in the right panel of the Login Page, the system will authenticate the user and a session will be created with all the Common Security Service (CSS) profile information.

The CSS profile loaded will be:

* The associated to the AD user, if Test User ID field is left blank
* The one specified in the Test User ID field, if Test User ID field is fill out.

The user will then be redirected to the application that was originally trying to be accessed.

### PIV/PIN Authentication

The PIV/PIN authentication form is in the left panel of the Login Page. To be able to use this method of authentication the user will need the following information:

* PIV Card Reader: The user should insert the PIV card into the card reader of the PC/equipment assigned to the user.

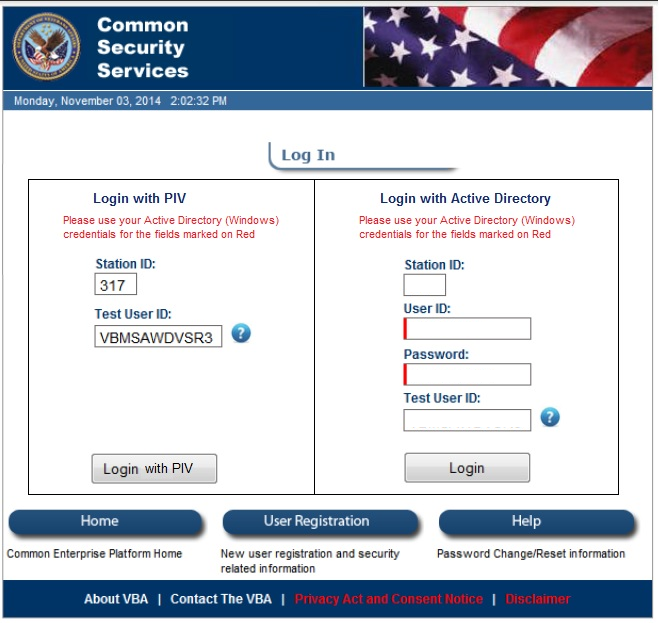


Figure 5 Login page with PIV/PIN authentication

* Station ID: A three-digit number that identifies the Station that the user will use for this session.
* Test User ID: CSS Username associated to the profile that will be loaded into the session instead of the originally associated to the AD user in PIV. NOTE: If left blank, the CSS Profile associated to the AD user in the PIV will be loaded into the session.

Once the user has provided all the Login Credentials and after pressing the PIV Login button in the left panel of the Login Page, the system will access the PIV card in the reader and will load the certificates stored in it asking the user to select one.

* Select Certificate: The user should select the certificate used for PIV/PIN authentication and press OK. Then a Pop-Up Window asking for the PIN will be displayed.
* PIN: The user should provide the PIN and press OK.

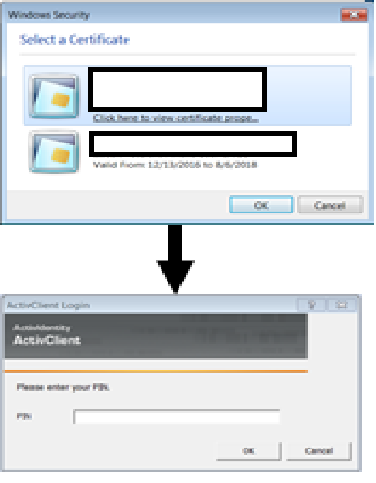


Figure 6 PIV/PIN Dialogs

If the PIV/PIN match correctly the user is authenticated, and session will be created with all the Common Security Service (CSS) profile information:

* The associated to the AD user, if Test User ID field is left blank
* The one specified in the Test User ID field, if Test User ID field is fill out.

The user will then be redirected to the application that was originally trying to be accessed.