

VA



U.S. Department
of Veterans Affairs

U.S. DEPARTMENT OF VETERANS
AFFAIRS CEIAESA (EA)

STANDARD OPERATING PROCEDURES (SOP)

Version 2.4 May 2026 OY1

Table of Contents

- Section 1 | Purpose 3
- Section 2 | Asset Management Portal 3
- Appendix A | How to create a user ID for the Iron Bow portal 5
- Appendix B | Portal request/submissions and request types defined 9
- Appendix C | Abbreviations and Definitions 9

Section 1 | Purpose

This document provides the standard operating procedures for the *Department of Veterans Affairs Smartnet Enterprise Agreement*. This and many other resources are found at Iron Bow's Resource website. For any questions or concerns, please email VAsmartnetEA@ironbow.com for a prompt reply.

Section 2 | Asset Management Portal

This portal is intended to assist the VA during the lifecycle of the Enterprise Agreement procured through Iron Bow. The portal will assist you in managing your assets, provide you with a documentation database, and ease of access to Iron Bow advanced Services. This document will show you how to navigate the portal.

2.1 View My Assets

By Selecting the “View My Assets” button, a new page will be opened to the asset list. The assets listed in this page are already added to the contract and can be viewed by clicking the serial number on the left-hand side of the table. Additionally, you can filter by any of the fields listed in this table at the top of the page by selecting the half hourglass icon. If the information listed for the asset is not correct, please see **Appendix B** on how to open a request.

2.2 Submitting a Request

The “Submit A Request” button will navigate you to a second page consisting of fields to be completed. Select what type of request you are submitting and complete the fields to the best of your knowledge. The more information provided will result in a faster resolution from the XR team.

Request types:

- 2.2.1 MACD Requests (Moves, Adds, Change, Delete)
- 2.2.2 Reporting requests
- 2.2.3 Other

2.3 Reports

The “Reports” button will populate multiple reports regarding your enterprise agreement. This is sorted by report type, year, and month. The reports will be created by the XR team and uploaded to the tool on a scheduled basis.

2.4 Resources

The “Resources” section is managed by the XR team to provide you with important documentation regarding the enterprise agreement. IE: SOP, FAQs, Quick Reference Guides, contact sheets, Recorded trainings, and Process documentation.

2.5 Gaining Access to the asset management portal

The asset management portal is a role-based system that allows the VA and Iron Bow to better manage the assets in the VAs install base. To gain access to the portal start at this page [Click Here](#) and follow the process outlined in Appendix A.

2.6 Asset update process defined

The data reflected in the tool is what is listed in the Cisco system as covered under the contract. Iron Bow works hand in hand with Cisco and the VA to ensure the data is as accurate as possible. If there is a change that needs to be made, please submit a case for a MACD request type and define what action should be taken on the devices. Once a request is received in the Iron Bow system the XR team will acknowledge the request and take it to VA leadership for approval. Once approved by VA leadership the XR team will notify Cisco asset management to ensure the update is made in their end as well as the Iron Bow tool. Please note, that the XR team will keep the case as up to date as possible during this time to ensure the requestor is kept in the loop. If the change is denied by VA leadership the XR team will notify the requestor with the reason for the decision and close the case.

2.7 User Roles Defined

The VA portal has a role-based access privileges as mandated and assigned by the VA

- 1.) Admin: Admin users are defined as Iron Bow System admins. This role is not designed for VA use as it is a level of access reserved for the system hosts and backend support.
- 2.) Super Users: Super users are VA employees that have been designated by VA leadership to be trusted approvers of requests that come through the system from regular users. This user type has elevated privileges from the normal users to see all cases and requests in the system as well as approve new users and download the asset list.
- 3.) Users: Can see assets Submit requests and see ONLY their tickets.

***Please note this is a living document that will be updated with the progression of the contract. If there is something you feel is not accurate or should be added, please email vasmartnetea@ironbow.com.


Appendix A | How to create a user ID for the Iron Bow portal

- 1.) For first time login please go to: <https://ironbow.servicenowservices.com/va> and select New User Registration.



- 2.) From there it will direct you to a page to fill out the needed information. Please note you must use your official VA email address to gain access to the tool. Any access requests that do not use their VA email will be automatically rejected from the system.

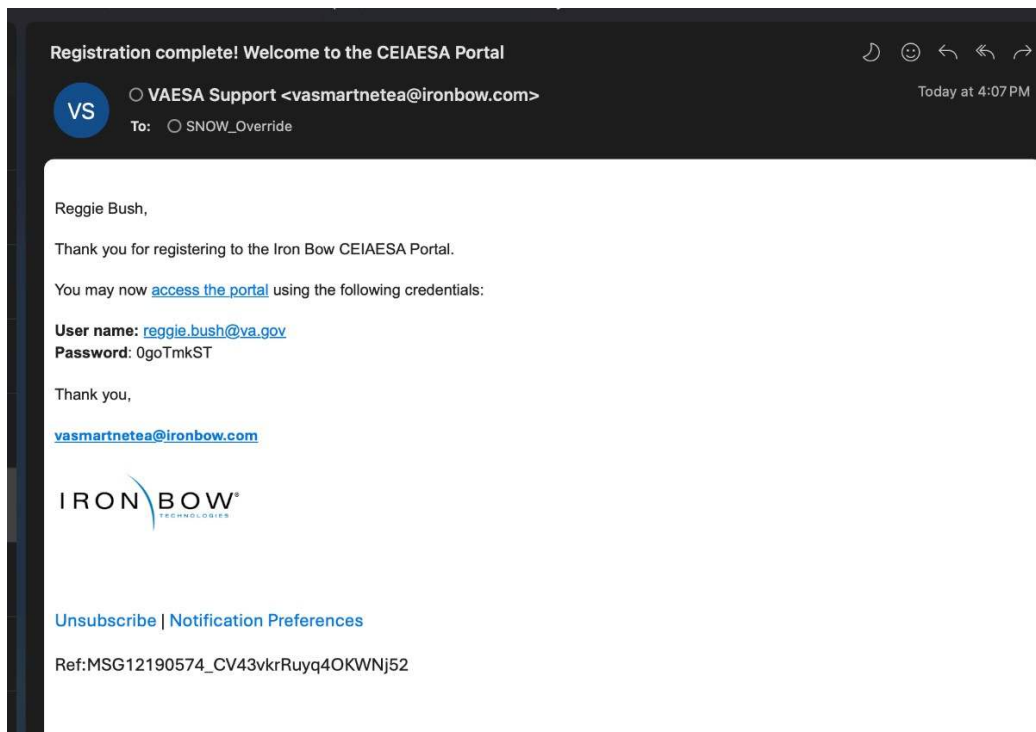
Customer Registration

First Name	<input type="text" value="first name"/>
Last Name	<input type="text" value="last name"/>
Business Email	<input type="text" value="business email"/>
Phone number	<input type="text" value="Business Phone +1(###)###-####"/>
	<input type="checkbox"/> I agree to the Privacy Policy and Community Terms and Conditions
Security Code	<input type="checkbox"/> I'm not a robot  <small>reCAPTCHA Privacy - Terms</small>

- 3.) Once submitted the system will automatically push you to the login screen with a confirmation message as seen below. Your access request must be approved by a VA superuser before you can continue.



- 4.) The system will send an automated email to the super users and portal administrators to approve or deny the request. If approved, you will receive an email with your username and temporary password. Example below. (If your request is denied you will receive a different message. If this is the case, please follow up with your leader for direction.)



- 5.) Once approved, on your first login to the system, you will be prompted to update/change your password to ensure the system stays secure.

The screenshot shows a web interface for changing a password. At the top, a light blue banner contains the text: "System administrator requires you to change your password". Below this is a white box titled "Change Password". Inside the box, the "User name:" is pre-filled with "john.doe@va.gov". There is a text input field for "Current Password:" with a toggle icon to its right. Below this, the "Password Requirements:" are listed: "- Minimum 8 characters", "- Maximum 40 characters", "- At least 1 lowercase letter(s)", "- At least 1 uppercase letter(s)", and "- At least 1 digit(s)". There are two more text input fields: "New password:" and "Confirm New Password:", each with a toggle icon. A green "Submit" button is located at the bottom right of the form box.


- 6.) After changing your password, you will be prompted to register with an MFA tool for two factor authentication. The INITIAL authentication will require registration via a mobile app of your choice. (The VA preferred MFA tool is Microsoft Authenticator. You can also use any other authenticator such as Google Authenticator or Cisco Duo). Please note for initial authentication, the profile MUST be associated with your official VA Email address to register properly. After that, you will be able to obtain the authentication code via your mobile app or your registered VA email for authentication.

Enable multi-factor authentication(MFA)

[Learn more](#) [Postpone Setup](#)
Number of times MFA setup can be postponed is: 3

1. Download an authenticator app that supports Time Based One-Time Password(TOTP) on your mobile device. For more details, view our documentation.

2. Open the app and scan this QR code to pair your mobile device



Or type in

3. Enter the 6-digit code generated by your authenticator app in the text field

Pair device and login

Verify your identity

Select one of the following methods to complete authentication.

Get a verification code from your authenticator app

Get a verification code sent to caXXXXXXXX@va.gov

Continue

***Once above steps have been finished your registration for the portal is complete. For any escalations or problems, please reach out to vasmartnetea@ironbow.com.

Appendix B | Portal request/submissions and request types defined

Contract Move, Add, Change, Delete (MACD)

- 1.) Contract Move – This should be used for existing devices that are within the VA environment on a different contract/expired contract. For this type, please provide the old Contract Number the device serial number.
- 2.) Add – This should be used for Net New devices to the VA environment. For this request type please provide the device serial number instance number and the address where the new device will be installed. If this device is replacing a device currently active in the VA network, please provide the serial number of the device being replaced in the notes section of the case.
- 3.) Change – this action will be used for updating current devices on the CEIAESA Contract. These actions can be defined as address changes/updates/service level.
- 4.) Delete – This action type should be used for a device that’s being decommissioned/replaced.

Please note if this asset is being replaced, please ensure the new serial number is provided and note if the address will be different then what is listed on the legacy device.

All Change types will be subject to portal super user approval and case will be updated with notes for information requests and notification will be sent once approved.

Once approved by portal admin please allow up to 7 days for changes to be reflected in the portal.

Appendix C | Abbreviations and Definitions

CCO ID	Cisco Connection Online Identification. The user credentials created at Cisco.com to access device details from the Cisco Software Central website.
LDOS	Last Day of Support. Cisco’s term that defines a date when a device will no longer be supported, replace, or create software updates for.
MCE	My Cisco Entitlements. A section of the Cisco Software Central website that provides the user access to details like what devices are assigned to their unit, cost of devices owned, and what date the device will enter LDOS status.
SDWAN	Software Defined Wide Area Network