

COLLABORATIVE SECURITY TEST ENVIRONMENT

Connection Guide

V1.2

08 October 2022

Table of Contents

<i>Welcome to CSTE</i>	<i>3</i>
Overview	3
<i>Obtaining the VPN Client Software</i>	<i>4</i>
<i>Connecting to CSTE</i>	<i>6</i>
<i>Changing your CSTE AD password</i>	<i>7</i>
<i>Logging into vCenter</i>	<i>11</i>
<i>Confluence</i>	<i>14</i>
<i>CSTE Core Services</i>	<i>17</i>
Offensive Security Lab	17
Cyber Range	17
Jira Ticket System	17
Chat Server	17
<i>Potential OpenVPN issues for Linux Users</i>	<i>18</i>
<i>Requesting Support</i>	<i>19</i>

Welcome to CSTE

Welcome to the Consolidated Security Test Environment!

This Connection Guide will help you get up and running quickly so that you can take advantage of CSTE's offerings.

Overview

CSTE is a private cloud hosted on DND infrastructure and accessible from the Internet. CSTE is only accessible by authorized users. Access is established from a user's host computer by connecting to the CSTE VPN gateway in order to establish a secure VPN tunnel. Users are Authenticated by the CSTE AD, and then Authorized to perform actions based on their CSTE Role.

There are currently two CSTE Roles:

- a. Standard user;
- b. Administrative user.

Once connected to CSTE, the user is free to participate in scheduled exercises, start an individual training event, participate in hacking labs, chat with other users, contribute to the Cyber Wiki, the possibilities are endless.

A major CSTE capability is being able to accessing a range. A 'range' traditionally consists of a defended domain which has been designed to mimic a real-life corporate network, complete with Active Directory, Exchange, subdomains populated with Windows and Linux hosts. There would typically be a Security Enclave which hosts defensive tools such as an IDS, a SIEM, analyst workstations, EDR, UEBA, etc. Ranges are a great place to practice both defensive and offensive tradecraft.

Note: If you have been provided an administrative domain user account, you must always use the standard domain user to log into the VPN, and only use the administrative domain user account to log into vCenter.

Obtaining the VPN Client Software

In order to connect to the CSTE VPN you first need to establish a VPN connection. In order to do this, you require a VPN client application, and an ovpn configuration file.

In order to obtain a VPN client application, browse to the official OpenVPN website and download the appropriate client software for your operating system.

<https://openvpn.net/vpn-client/>

Once you are on the OpenVPN web site you will be presented with the following page:



Image 1 : Open VPN client software download page

Select your operating system and then press the 'Download OpenVPN Connect...' button.

Once the OpenVPN client software is downloaded, install it.

When you have the OpenVPN client software installed, launch the program.

The OpenVPN client software needs to know which VPN service you want to connect to. This is accomplished by importing the ovpn configuration file that was sent to you by the CSTE Range Staff. The OpenVPN configuration should be named 'CSTE_VPN.ovpn'.

Image 2 shows the OpenVPN client software dialog box that will allow you to easily import the CSTE_VPN.ovpn file by simply dragging it onto the dialog box. You can also select 'Browse' and locate the file yourself.

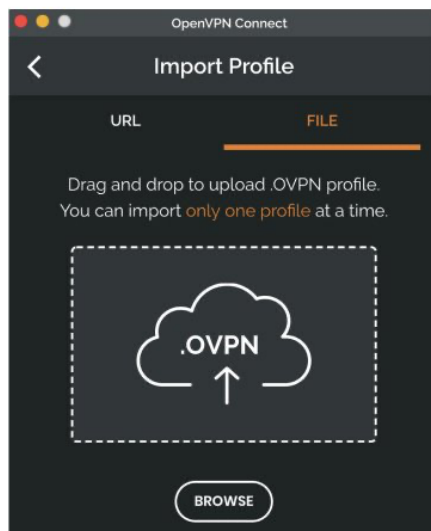


Image 2 : OpenVPN client software Import Profile dialog box

Connecting to CSTE

Now that you have a VPN client application installed, you're ready to connect.

You should have received an email from the CSTE Range Staff identifying your CSTE **username** and **password**. You will need these for this step.

All users will receive a standard domain account, while some users will also receive an A- account. The A- account is required to perform range administration on any ranges you have access to. If you did not receive an A- account that is okay, as you only receive an A- account when its required.

Username Format – Standard user

The username format for standard user is: Lastname.FirstInitial

Example: Sanchez.R

Username Format - Administrator

The username format for an Administrator is: A-Lastname.FirstInitial

Example: A-Sanchez.R

Connection Process

Step 1: Launch the Open VPN client software.

Step 2: Login with your provided CSTE AD credentials.

Changing your CSTE AD password

When your CSTE account was created, you were provided a randomly generated initial password that you used to log into the VPN tunnel.

You must now change your password. This is performed by leveraging the Outlook Web Access (OWA) portal.

Note that if you also received an A- account, you need to change the password for both accounts.

CSTE AD Password Policy

When selecting a new password, take into consideration the following policy:

- At least one uppercase letter
- At least one lowercase letter
- At least one special character
- Password must be greater than seven characters in length
- Password must not have been recently used

Change Password Process

Step 1: Log into CSTE using the provided credentials (See 'Connecting to CSTE' above)

Step 2: Once the VPN is established, browse to the Outlook Web Access web portal.

<https://cste-exchange.cste.mil.ca/owa>

You may receive a warning stating that 'Your connection is not private'.

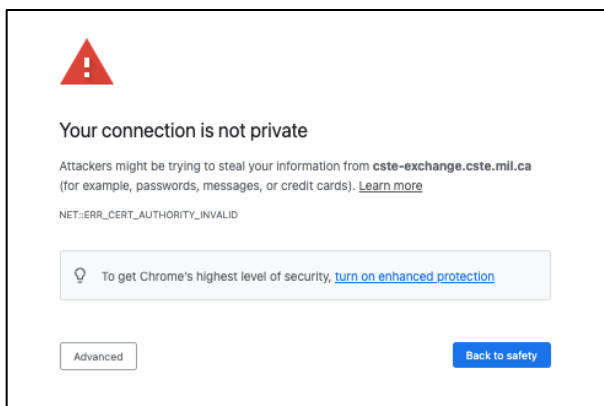


Image 3 : Self-Signed Certificate warning

Accept the Self-Signed Certificate warning by pressing the 'Advanced' button, and then selecting 'Proceed to cste-exchange.cste.mil.ca (unsafe)'

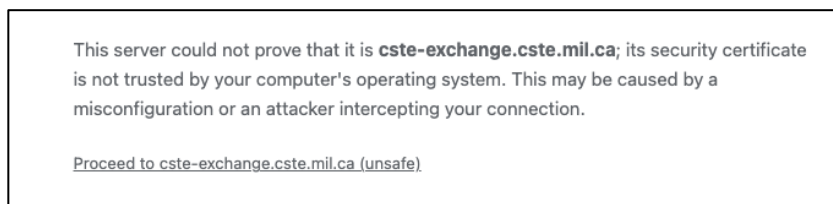


Image 4 : Self-Signed Certificate Warning

Step 3: Log into the Outlook OWA portal by entering your credentials in the following format:

CSTE\USERNAME

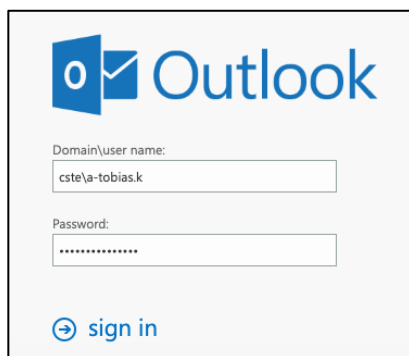


Image 5 : Outlook Web Access login page

Press 'sign in' to complete the sign in process.

Step 4: Once logged into the Outlook OWA, press the gear icon at the top right of the page and select 'Options' from the drop-down menu.

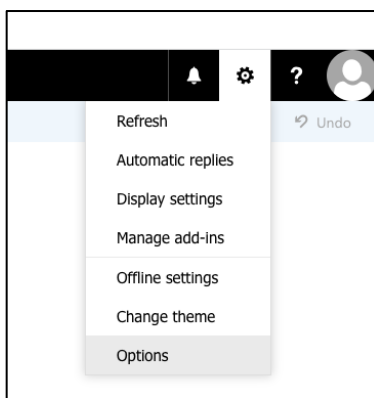


Image 6 : Outlook Web Access options

A new page is displayed with a menu down the left side of the screen.

Expand the 'General' section, and then select 'My Account'

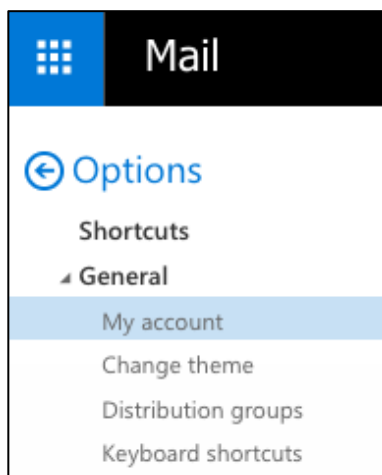


Image 7 : Outlook Web Access password link

Near the bottom right-hand side of the page, press the 'Change your password' link.

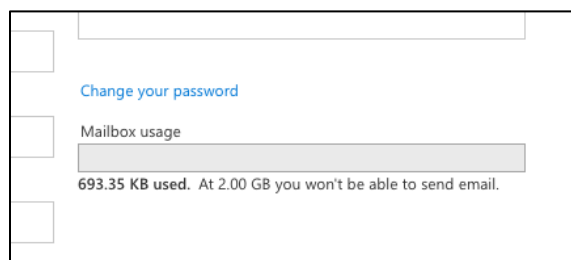


Image 8 : Outlook Web Access password reset

A new pane will open up titled 'Change Password'.

☒ Save
 ☐ Discard

Change password

Enter your current password, type a new password, and then type it again to confirm it.

After saving, you might need to re-enter your username and password and sign in again. You'll be notified when your password has been changed successfully.

Email address: A-Tobias.K@cste.mil.ca

Current password:

New password:

Confirm new password:

Image 9 : Outlook Web Access password reset

Input the current password, and then input your new password. Once complete, press the 'Save' button at the top of the page.

You will be prompted to log back into the Outlook OWA web portal.

Important

Your CSTE AD account is linked to your Outlook account, and changing your Outlook password has also changed your CSTE AD password, and consequently your VPN password.

Logging into vCenter

One of the core features of CSTE is the ability to interact with Virtual Machines on any one of the ranges. Whenever you are required to work with Virtual Machines, you will need to log into the vCenter dashboard. vCenter is a web-based interface developed by vmware specifically used to facilitate working with Virtual Machines running within the ESXi hypervisor.

Process to Log into vCenter

Browse to <https://cste-i10-vc.cste.mil.ca>

Input your CSTE AD credentials into the provided fields.

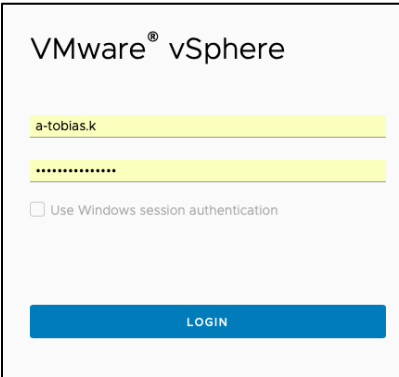
The image shows the VMware vSphere login page. At the top, it says "VMware® vSphere". Below that are two input fields: the first contains the username "a-tobias.k" and the second contains masked characters "*****". There is a checkbox labeled "Use Windows session authentication" which is currently unchecked. At the bottom is a blue button labeled "LOGIN".

Image 10 : vCenter login page

Once you are authenticated, you will be presented with the vmware dashboard.

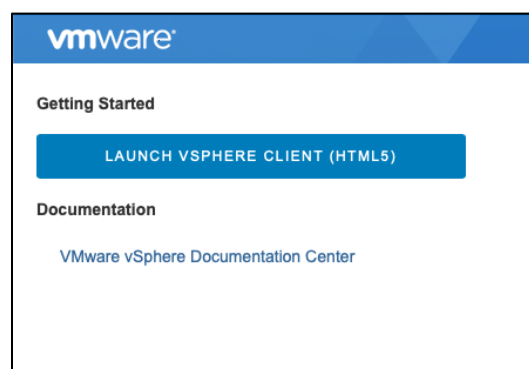


Image 11 : vmware dashboard

Press the 'LAUNCH VSPHERE CLIENT (HTML5)' button.

Note that your account does not enable you to view details about the data center, the cluster or the individual servers that make up the cluster. When you attempt to view these pages will see a page that states ‘You have no privileges to view “CSTE-I10-VC-cste.mil.ca” object’. This is normal.



Image 12 : Error when trying to view privileged objects

The next screen you see will be the vCenter dashboard. Explaining all of the features and functions of vCenter is beyond the scope of this Connection Guide. However, the quickest way to get working is to select the ‘VMs and Templates’ icon located near the top-left of the screen.

The VMs and Templates view is the second icon from the left (see image 12).

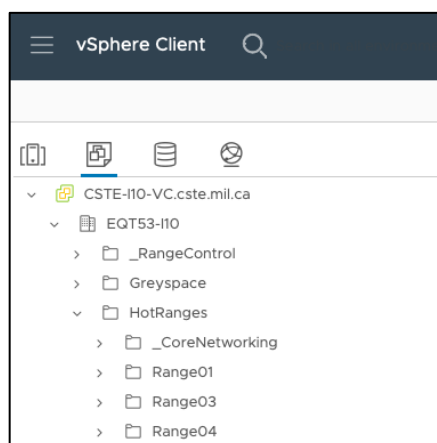


Image 13 : VMs and Templates view

Your view of available folders will vary depending upon the event(s) you have been enrolled into, as well as the role you have been assigned. For example, if you are a member of a Cyber Protection Team (CPT) and are participating in an exercise, you will likely have access to a named range, but will only have access to the Virtual Machines located in the Fly Away Kit (FAK). However, if you are a Local Network Defender (LND) on the same exercise, you would likely have access to the Virtual Machines that make up the defended network, and would not see any of the FAK Virtual Machines. Image 13 below shows what an Administrator would see when viewing the vCenter dashboard for an event hosted on Range08A.

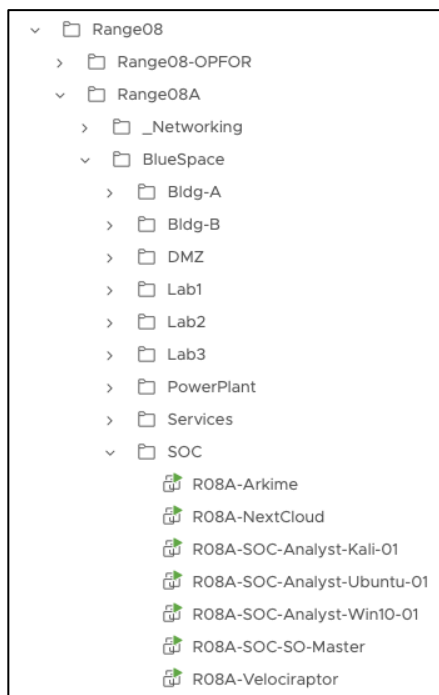


Image 14 : Administrator view of Range08A

In order to interact with a Virtual Machine, simply press the 'LAUNCH WEB CONSOLE' button, or the 'LAUNCH REMOTE CONSOLE' button.

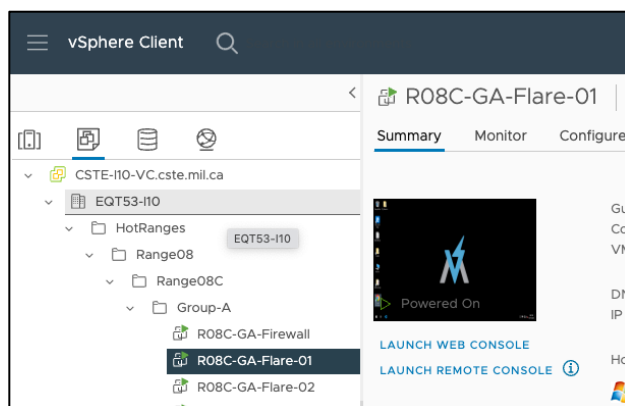


Image 15 : Accessing the Virtual Machine

If you select the 'LAUNCH WEB CONSOLE' option there is a chance that the web page will be blocked because its being displayed as a pop-up tab. If this happens, all you need to do is allow pop-ups. How you do this depends on the web browser you are using.

The choice of which console access option you want to use is entirely up to you. However, COPY-PASTE is only supported when using the vmware remote console. If you want to take advantage of COPY-PASTE, select the 'LAUNCH REMOTE CONSOLE' option and then download the vmware remote console application that is required.

Confluence

CSTE hosts the Atlassian Confluence wiki. There is a separate Confluence Guide. However, here are the basics to get connected to Confluence.

Confluence is a wiki which supports our requirement for a tool that assists with knowledge management and knowledge transfer. Confluence consists of SPACES. A space is a collection of pages that belong to a topic. Spaces can be private, public or anonymous.

- A private space is a space that is hidden from all users who have not been invited to participate in the space.
- A public space is a space that is visible to all Confluence users.
- An anonymous space is a space that is visible to anyone who visits the space – even if not logged into Confluence.

Note that DIMEI 3-2 is in the process of procuring a Data Center license for Confluence which should be delivered before Jan 2023. The Data Center version of Confluence will be fully integrated into CSTE AD, and as such the logon process will be slightly different.

Process to access Confluence

Browse to <http://cste-con.cste.mil.ca:8090>

As an anonymous user you will be granted access to any SPACE which allows anonymous viewing. Specifically, you will see the CSTE SPACE. To view the pages within the CSTE SPACE, simply click on the 'CSTE' link.

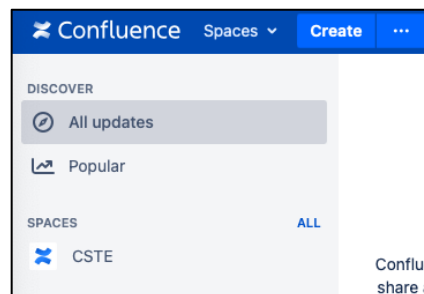


Image 16 : CSTE SPACE on Confluence

Once you click on the CSTE link, the pages associated with the SPACE will become visible.

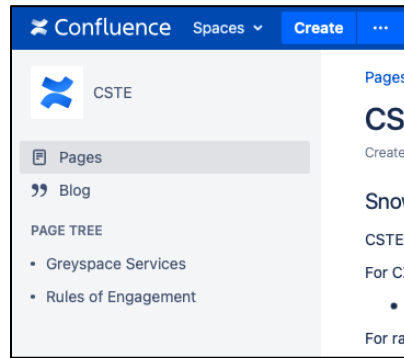


Image 17 : CSTE Pages

As can be seen in Image 15, at the time of drafting this document there are two pages in the CSTE SPACE; Greyspace Services and Rules of Engagement.

We will soon be seeking out volunteers to be moderators for many of the space we plan on creating.

Process to Log into Confluence

Press the 'Log in' link located at the top right-hand side of the page.



Image 18 : Confluence Log in link

Image 19 : Confluence Log in form

Input your CSTE AD credentials and then press the 'Log in' button.

Note: The current version of Confluence does not yet support Active Directory integration, and you will be provided Confluence credentials via your initial welcome email.

CSTE Core Services

CSTE hosts a large number of capabilities, with more being added on a regular basis. Here is a brief summary of some of the key services:

Offensive Security Lab

DIMEI 3-2 has partnered with Offensive Security (OffSec) to deliver a world leading cyber hacking lab. Similar to the labs provided by OffSec for their hacking courses and certifications, the DIMEI hosted OffSec labs come complete with a student control panel which enables users to revert machines and keep track of exploited hosts. The OffSec range will be available Jan 2023.

Please visit <http://cste-con.cste.mil.ca:8090/display/CSTE/Offensive+Security+Labs> for more information.

Cyber Range

DIMEI 3-2 has partnered with Field Effect Software (FES) to deliver a cyber exercise and training environment which enables students to enroll into self-paced training.

Please visit <http://cste-con.cste.mil.ca:8090/display/CSTE/Cyber+Range> for more information.

Jira Ticket System

DIMEI 3-2 has procured Atlassian Jira for our ticketing system, which should be delivered as early as Jan 2023. Coming soon.

Chat Server

Chat server supports text, audio, video and screen sharing. End-to-end encryption. iOS and Android app will enable users to send and receive messages as long as they install an OpenVPN client on their mobile device.

Coming soon.

Potential OpenVPN issues for Linux Users

There seems to be an issue with the way OpenVPN handles the DNS server entries when the OpenVPN configuration file is imported into the Linux version of the OpenVPN client software.

If you are a Linux user and find that the tunnel connects but you receive an error when trying to connect to any of the CSTE core services, the issue is most likely related to DNS.

CSTE has two internal DNS servers:

- a. 133.1.2.10
- b. 133.1.2.11

In order to correct this DNS issue, you will need to manually edit OpenVPN connection and add the two DNS server entries.

```
sudo resolvectl dns tun0 133.1.2.10 133.1.2.11
```

Requesting Support

Should you ever require support while using CSTE, the most effective way is to send an email to the CSTE DWAN distribution email account.

img.cste.etsc@forces.gc.ca

This account is monitored during normal working hours, and during off-hours when CSTE is supporting a special event.