

# Welcome to the JPO Cloud



## We are excited to welcome you into the JPO Cloud environment!

We look forward to welcoming new users into the JPO Cloud and want to ensure the journey is smooth and efficient.

This instruction packet covers everything you need to know to gain access into the environment. Explore all the resources and follow the step-by-step instructions to gain access to your accounts.

#	Topic
2	Important Access Notes
3	Installing AppGate
4	Configuring & Logging into AppGate
6	Changing AppGate Profile Link
7	Device Hardening Error
8	Installing AWS Workspaces
9	Logging into AWS Workspaces
10	JPO Collaboration Tools & Links





## Must Read: Important Notes Regarding Access

- **Password:** You will receive a separate message with your IL5 temporary password. Please copy the contents to a safe place before closing the tab. Once you close the browser tab, you will no longer be able to retrieve this information. You have to wait 24 hours before changing your password.
- **Lock Out:** If you incorrectly input your username, password, or RSA token 3 times, your account will be locked out for 30 minutes
- **RSA Token Attempts:** Please be advised, you can only attempt to login with the token code 1 time per minute. If you attempt to login more than once with the same token code it will begin the process of locking your account. If you fail logins 3 times in a row in less than 15 minutes your account will also be locked
- **Initial AWS Workspaces Access:** Try logging into your account about 1 hour after receiving your welcome email because your accounts are still building in Amazon and it usually takes 40 min to build.
- **Account Inactivity:** After 45 days of inactivity, your AWS Workspaces account and Jira/Confluence account will be disabled.
  - After 90 days of inactivity, AWS Workspaces that are not being used will be deleted. Please ensure you are logging in to all accounts to avoid disablement and deletion. Contact the Help Desk team if your account has been disabled or deleted.





**Overview:** Follow the instructions for installing and connecting the JSF Appgate DMZ Gateway, which will be required to connect to your AWS Workspace. You should be performing these operations from your employer issued workstation. This is not intended for use within the AWS Workspace; instead, it is required to access the AWS Workspace.

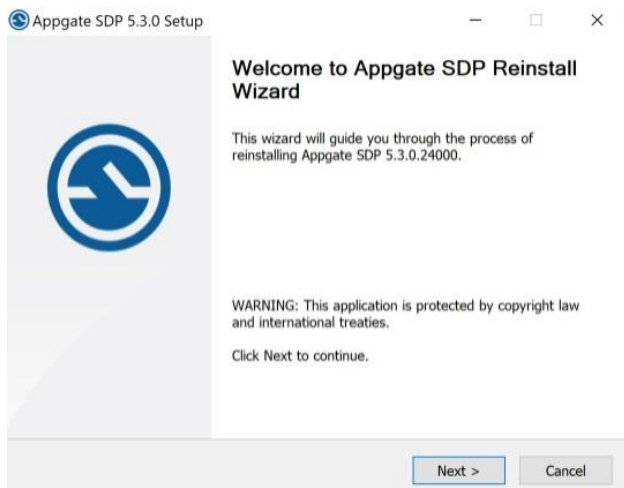
- For a more detailed explanation of Appgate, please reference the [Official User Guide for Appgate](#)
- Please use the FULL VERSION installer and download the latest version for your operating system
  - **Download here:** <https://www.appgate.com/support/software-defined-perimeter-support/>

## Download for Windows

1. Run “Appgate SDP [version] Installer.exe”.
2. After setup has completed the program will automatically start and open the Privacy policy window. If the Client application doesn’t start automatically, launch the “Appgate SDP” application from your applications folder.

## Download for Mac

1. Open “Appgate SDP [version] Installer.dmg”. The dmg file includes programs for installing and uninstalling the client.
2. Open “Appgate SDP Installer.pkg” to start the setup wizard.
3. After setup has completed, the Client application will automatically start and open the Privacy policy window. If the Client application doesn’t start automatically, launch the “Appgate SDP” app in your Applications folder.



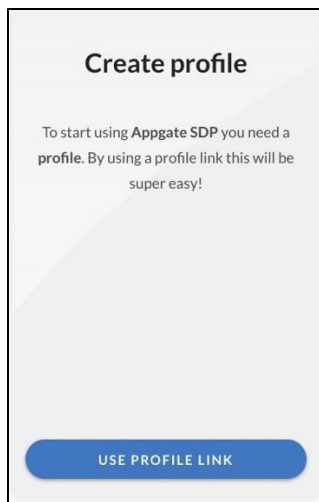




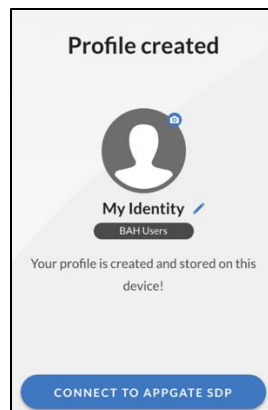
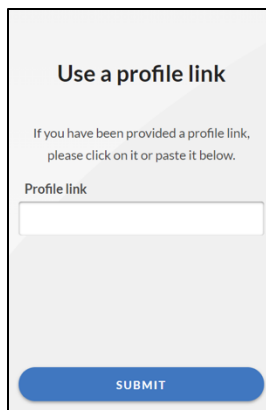
## How to Configure & Login to AppGate

\*Note: Ensure that you're NOT on any external VPNs or you will run into errors accessing AppGate. You must be connected to commercial internet.

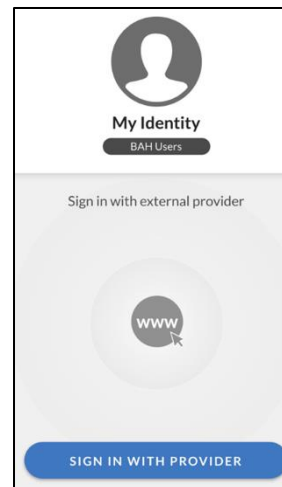
1. Launch the newly installed Appgate SDP client and read the privacy notice, then click **Approve** to continue.
2. Connect to your Appgate Client to the JSF MIDAS environment using the profile link, which was provided in a separate e-mail.



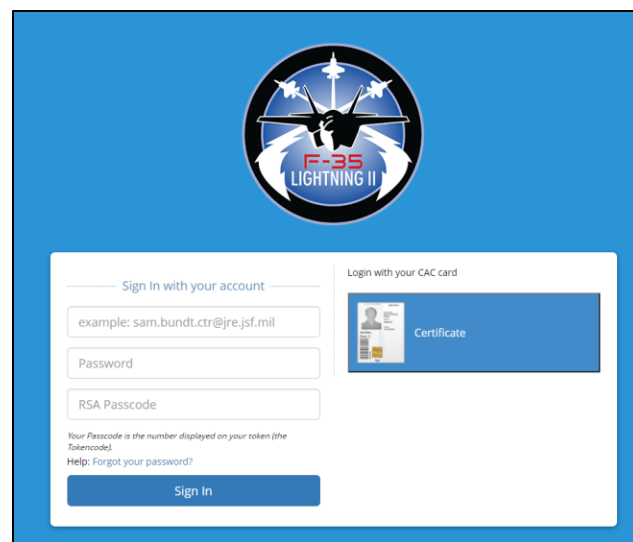
3. Press the **Use Profile Link** to enter the profile link provided in the separate email. Once the profile link is entered, press the **Submit** button. (Note: May fail to connect on the first try)



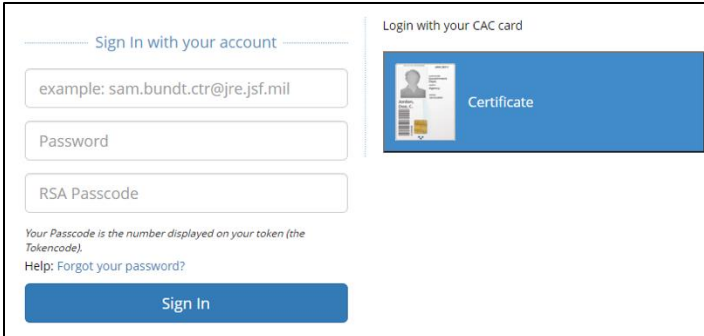
4. To login to the JSF environment, press **Connect To Appgate SDP** and then press the **Sign in with Provider** button. (Note: May fail to connect on the first try)



5. This will launch your default browser and open the Radiant Logic login page located at <https://auth5.jsf.mil/>



6. Enter your credentials that you received in your welcome email. Example:
  - Username, Password, & RSA Passcode
  - SmartCard certificate-based authentication
7. If your login is successful, you'll be redirected to the following page and your Appgate Client should initialize a connection.



Sign In with your account

example: sam.bundt.ctr@jre.jsf.mil

Password

RSA Passcode

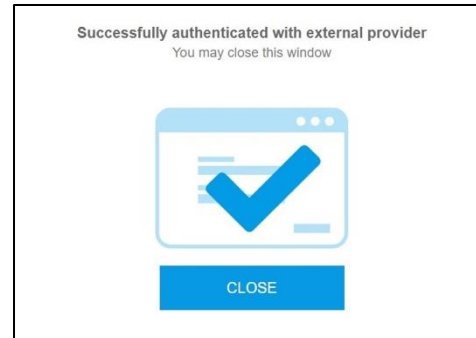
Your Passcode is the number displayed on your token (the Tokencode).

Help: Forgot your password?

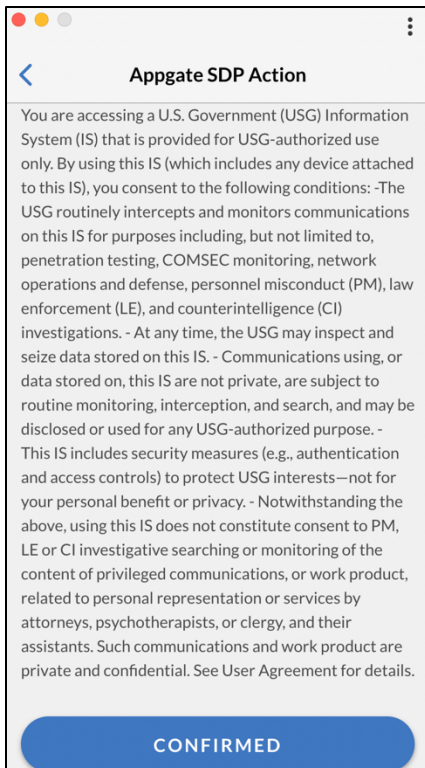
Sign In

Login with your CAC card

Certificate



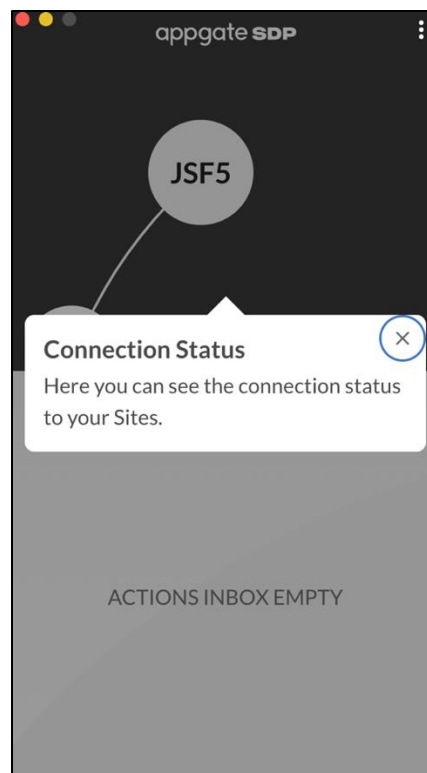
8. A security message will display. Review and click Confirm.



Appgate SDP Action

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. - At any time, the USG may inspect and seize data stored on this IS. - Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. - This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy. - Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

CONFIRMED

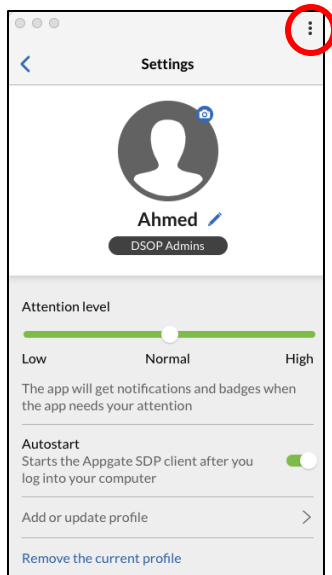




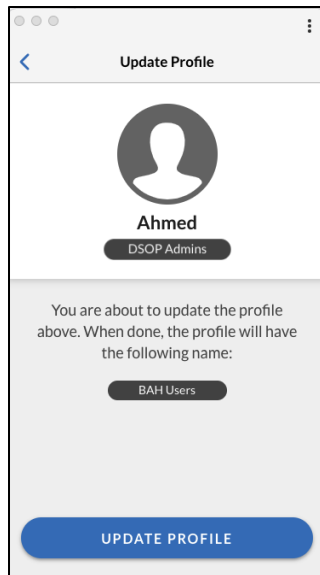
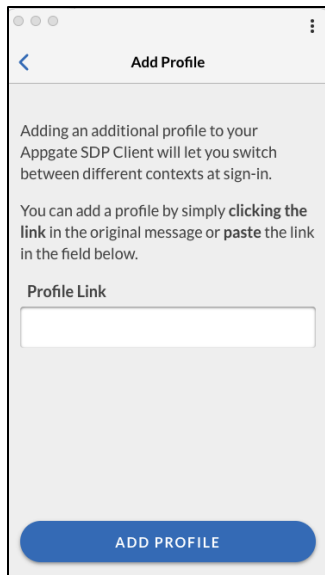
## How to Change Your Profile Link

\*Note: Ensure to engage with your leadership to ensure you have the correct Profile Link. This section is intended for anyone wishing to change/update their AppGate Profile Link.

1. Open AppGate and click the **3 dotted icon** on the top right and select **Settings**.



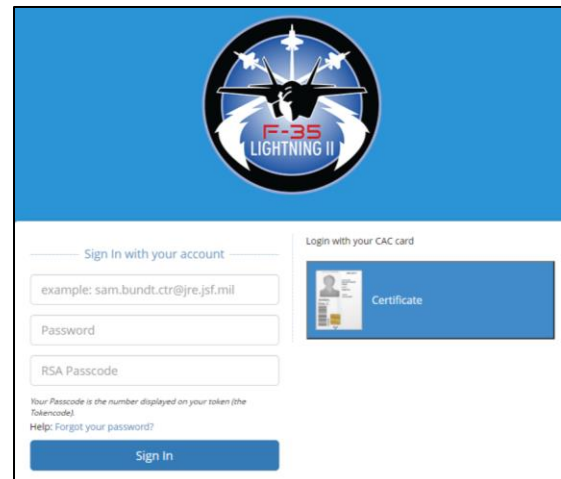
2. Select the **“Add or Update”** profile option. Paste the profile link and press **“Add Profile.”** Your profile link to be provided in a separate email or from your team.



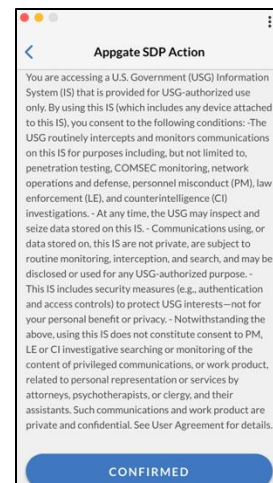
4. Click **“Update Profile”** (\*Note it may fail to connect the first time)

5. This will launch your default browser and open the Radiant Logic login page located at <https://auth5.jsf.mil/>

6. Enter your credentials that you use for AWS Workspaces (either Username, Password, & RSA Passcode or CAC Certificate based authentication). If your login is successful, you'll be redirected to the following page and your Appgate Client should initialize a connection.



7. A security message will display. Review and click **“Confirm.”**

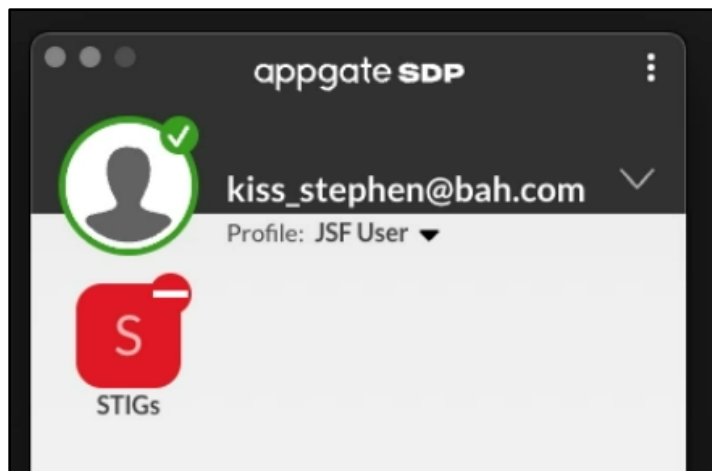




## How to Execute a Device Hardening for MacOS

If you receive and receive a red circle error icon on any of the tiles on your AppGate profile, your computer will need to do a device hardening, to

Please **contact the Help Desk team** ([JPOLCloudHelpDesk@jsf.mil](mailto:JPOLCloudHelpDesk@jsf.mil)) to receive an instructional guide on how to execute the Device Hardening and ensure your device meets the requirements to connect to the Cloud environment.



## Why Am I Getting this Error? Why do I need to Execute a Device Hardening?

Appgate SDP enables organizations to adopt a Zero Trust approach to network security, providing granular, context aware access control for distributed cloud environments. Appgate introduces the concept of the 6-layer trust model with separate verification steps that extend beyond just sign-in allowing further verification to be required at time of use - when an attempt is made to connect to a specific resource.

The Zero Trust Model has been adopted within the Department of Defense and is enforced by the Defense Information Systems Agency (DISA) using the standards defined within NIST SP 800-207 "Zero Trust Architecture".

Information systems, including Windows, Linux & MacOS PCs and servers, tablets and government cellphones, that access government networks must meet government IT security standards. Like their Windows & Linux counterparts, MacOS systems that connect to government networks are required to meet a standard security baseline prior to accessing those networks. Within the DoD, this baseline standard is referred to as the Security Technical Implementation Guide, or **STIG**. DISA requires information systems meet not less than 80% compliance with current STIG requirements in order to access government networks.

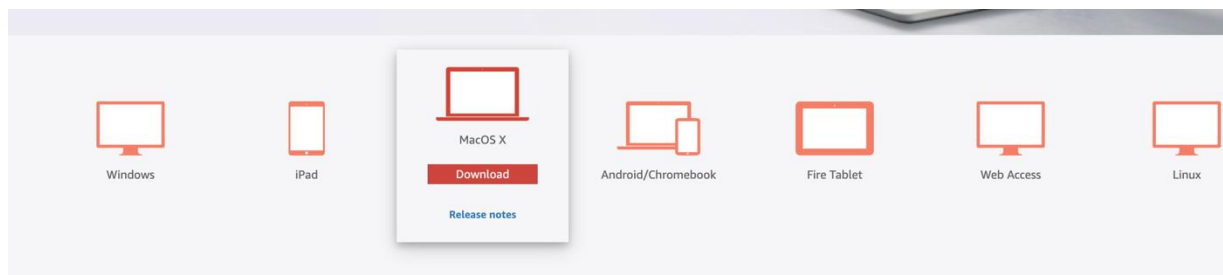
**Overview:** This document provides instructions for installing and connecting to AWS Workspaces.

## Prerequisites:

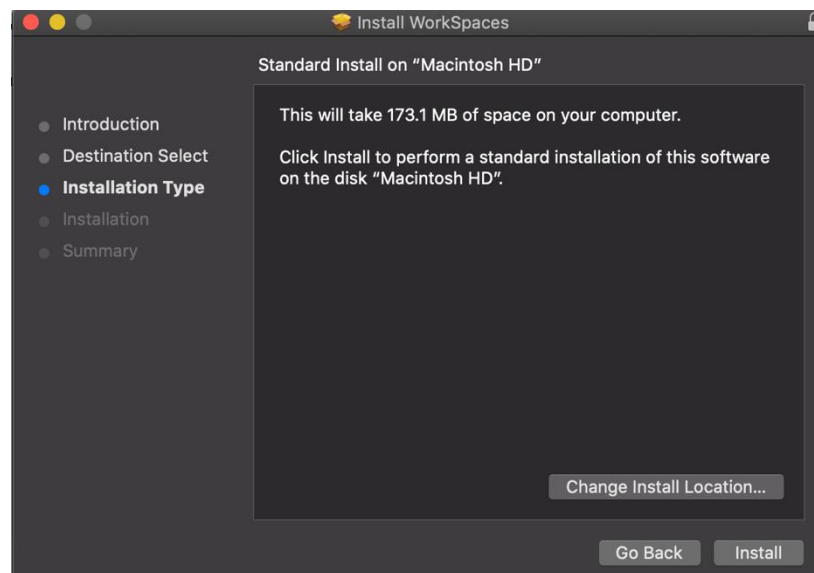
- You must connect to AppGate first. If you do not, you will get a “not authorized” error.
- Ensure you have received your Registration Code which was sent in a separate email.

## How to Download and Install AWS Workspaces

1. Navigate locally in a new browser tab to <https://clients.amazonworkspaces.com/>
2. Download the Workspace Client for your operating system (Mac or Windows)



3. After it downloads, open Workspaces.pkg and click through the prompts to install the package on your device.
  - Note\* If you are asked whether or not to install the driver for USB redirection, you can decline because we will not be using USB accessories for authentication to our Workspaces

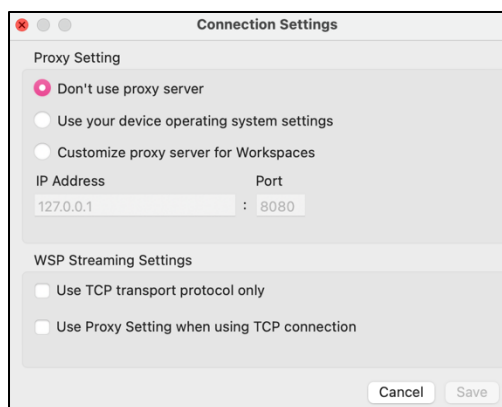
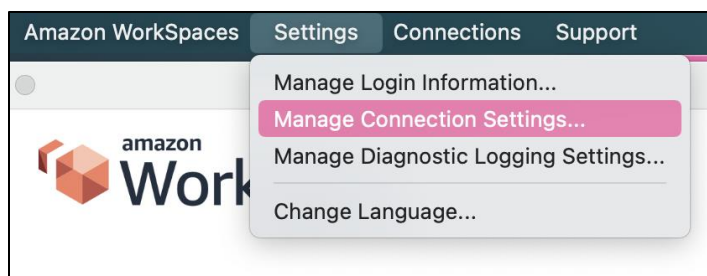


4. AWS Workspaces is successfully installed.



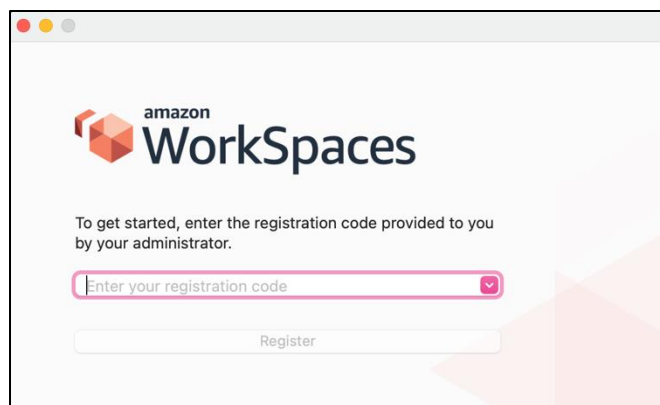
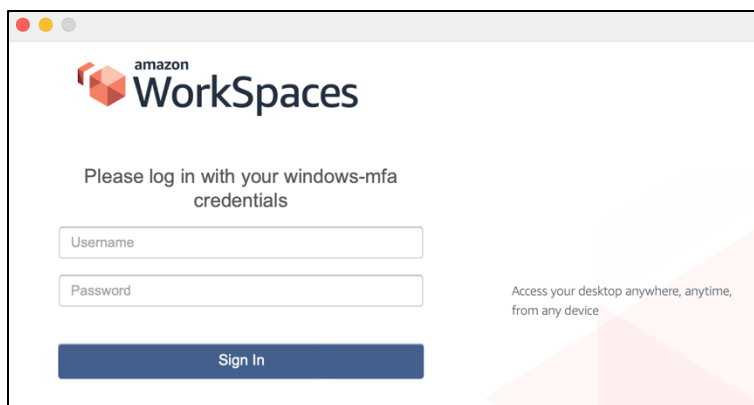
## Logging Into AWS Workspaces

1. Once installed, a shortcut will appear on the desktop. Double click on the icon to open the client.
2. In the **Settings** tab, choose **Manage Connection/Proxy Settings**, and choose **"Don't use proxy server."**



3. Login to your AWS Workspaces by following the below login instructions based on your specific access type.

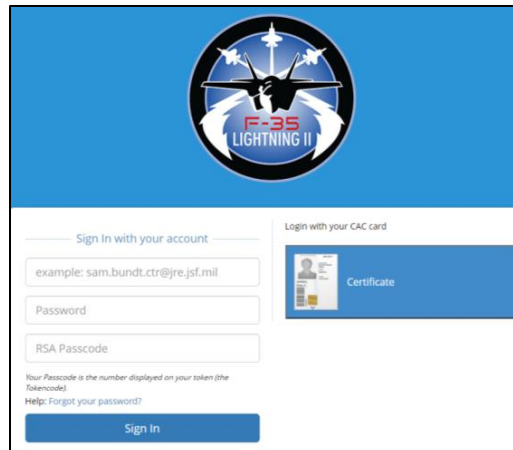
- **For users logging in via IL5 Windows with SmartCard Enablement:**
  - To log in to your workspace, please ensure your CAC is connected and enter in your PIN number.
- **For users logging in via IL5 Windows & IL5 Linux with Username and Password:**
  - To log in to your workspace, please use the username: **first.last.designation** and you will receive in a separate email with your password during onboarding.
  - Note\* you do not need write @jre.jsf.mil for your username
- **For users logging in via Whitelisted Network or MPE Users:**
  - You will receive an RSA token prompt in addition to username and password
  - Note\* you do not need write @jre.jsf.mil for your username



## Instructions for logging into JIRA, Confluence, and MatterMost



When logging into any of the JPO Cloud collaboration tools, you will be taken to the cloud authentication site (AUTH).



The screenshot shows a login interface with a blue header featuring the F-35 Lightning II logo. Below the header, there are two main login sections. The left section, titled 'Sign in with your account', includes input fields for 'example: sam.bundt.ctr@jre.jsf.mil', 'Password', and 'RSA Passcode'. Below these fields is a note: 'Your Passcode is the number displayed on your token (the Tokencode). Help: Forgot your password?'. A 'Sign in' button is at the bottom of this section. The right section, titled 'Login with your CAC card', features a 'Certificate' button with a small icon of a CAC card.

- **For users logging in via SmartCard Enablement:**
  - To login, please ensure your CAC is connected and enter in your PIN number.
- **For users logging in via Username + Password + RSA Token:**
  - To login, please use the username: **first.last.designation@jre.jsf.mil** and you will receive in a separate email with your password during onboarding.
  - Ensure you include @jre.jsf.mil in your username
  - **Password:** Same as your IL5 password
  - **RSA:** You are required to use an RSA hard token in order to gain access.

## Helpful Resources

Explore the Collaboration Suite:

- [JIRA](#)
- [Confluence](#)
- [MatterMost](#)
- [Applications Portal](#)