

Guide to deploying  
ADSelfService Plus in  
**Amazon Web Services**



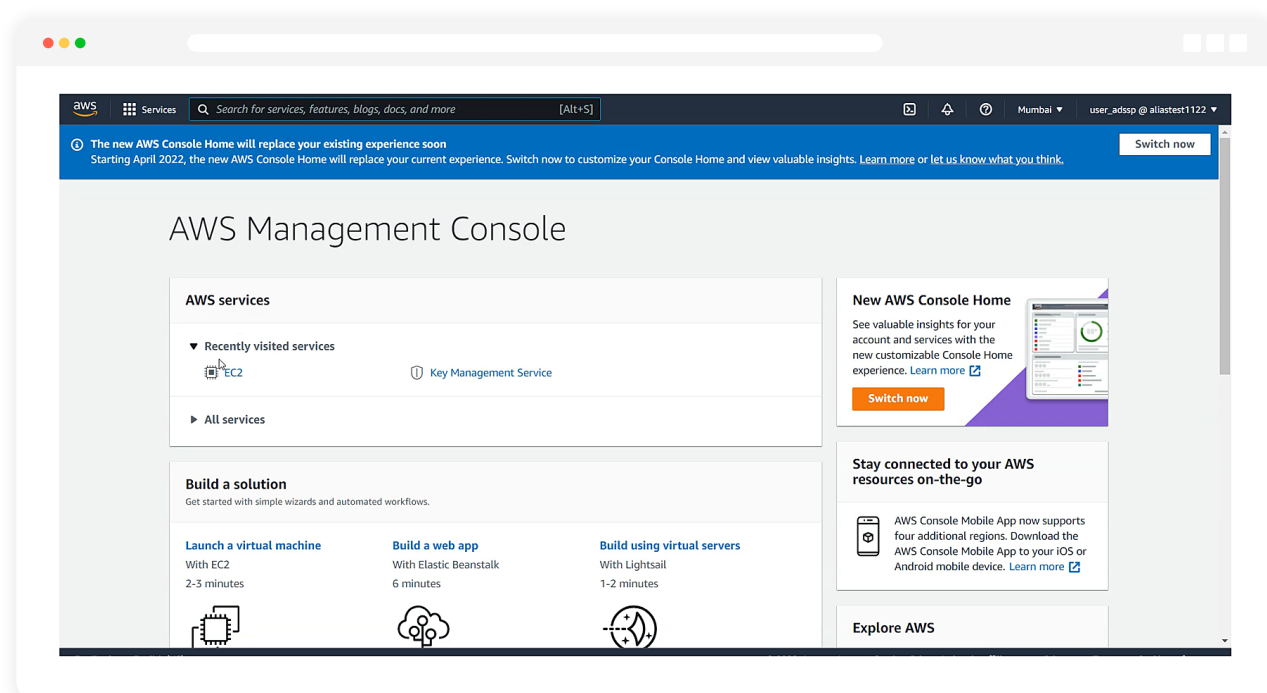
# How to deploy ADSelfService Plus in AWS

This document provides the steps to deploy ManageEngine ADSelfService Plus in the Amazon cloud via Amazon Web Services (AWS). These steps have been drafted for system administrators with knowledge of Microsoft Windows, Microsoft Remote Desktop Protocol, and AWS.

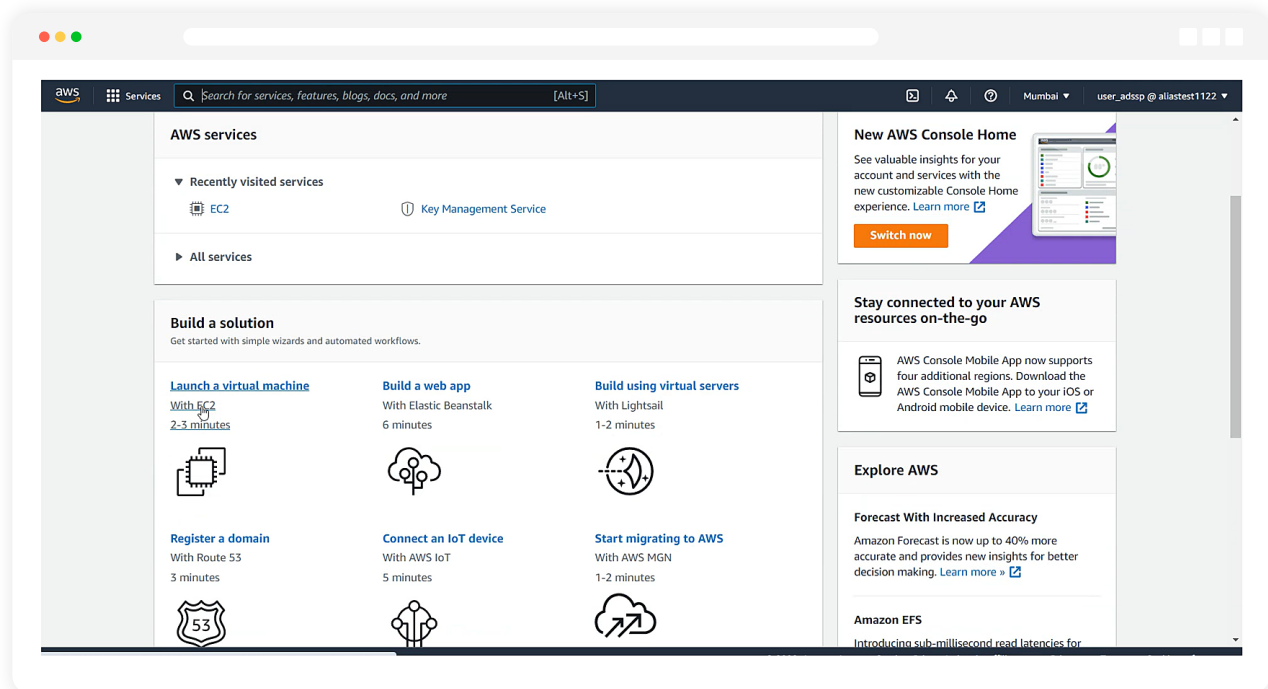
**Note:** You can also subscribe to the EC2 instance with ManageEngine ADSelfService Plus already deployed in it. You can find this instance in the AWS Marketplace.

**Note:** Steps 1 through 14 can be skipped if your organization has an AWS EC2 instance (Windows Server 2019) available that can be used to deploy ADSelfService Plus.

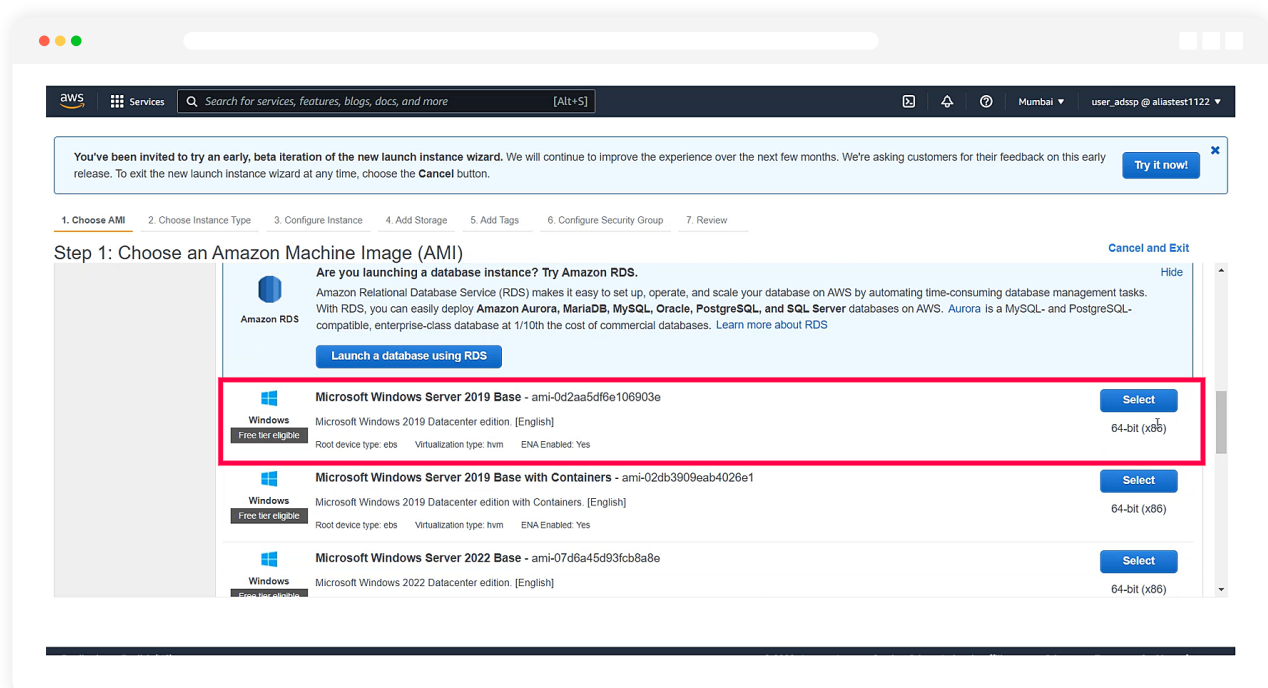
1. Log in to **AWS** as an IAM user. The AWS Management Console will open.



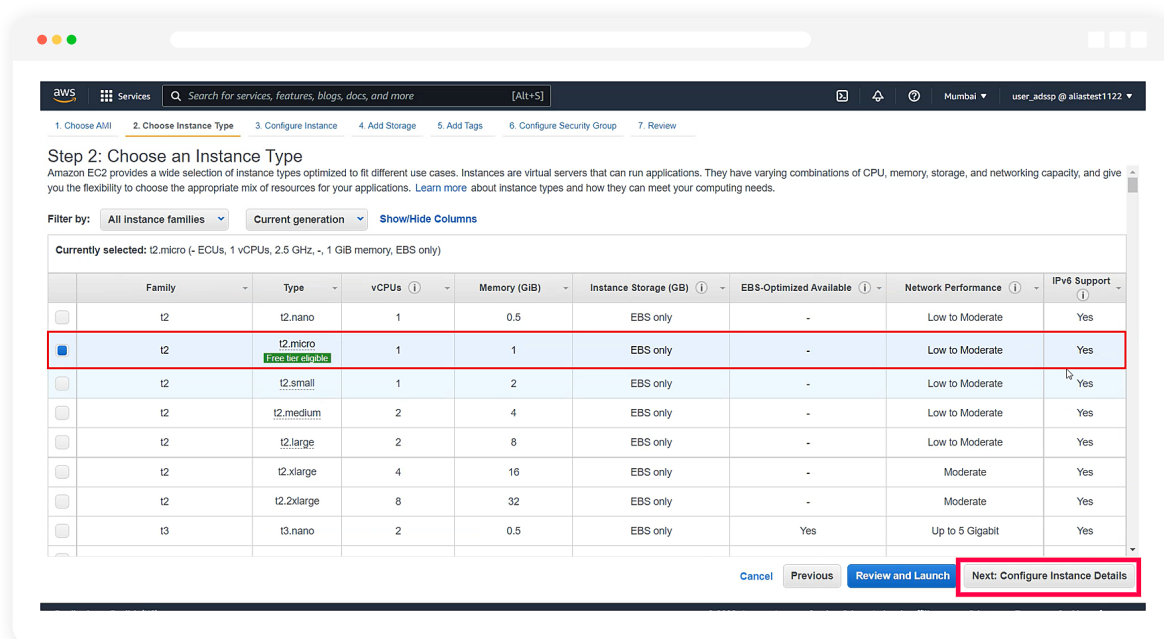
2. Under *Build a solution*, click **Launch a virtual machine With EC2**.



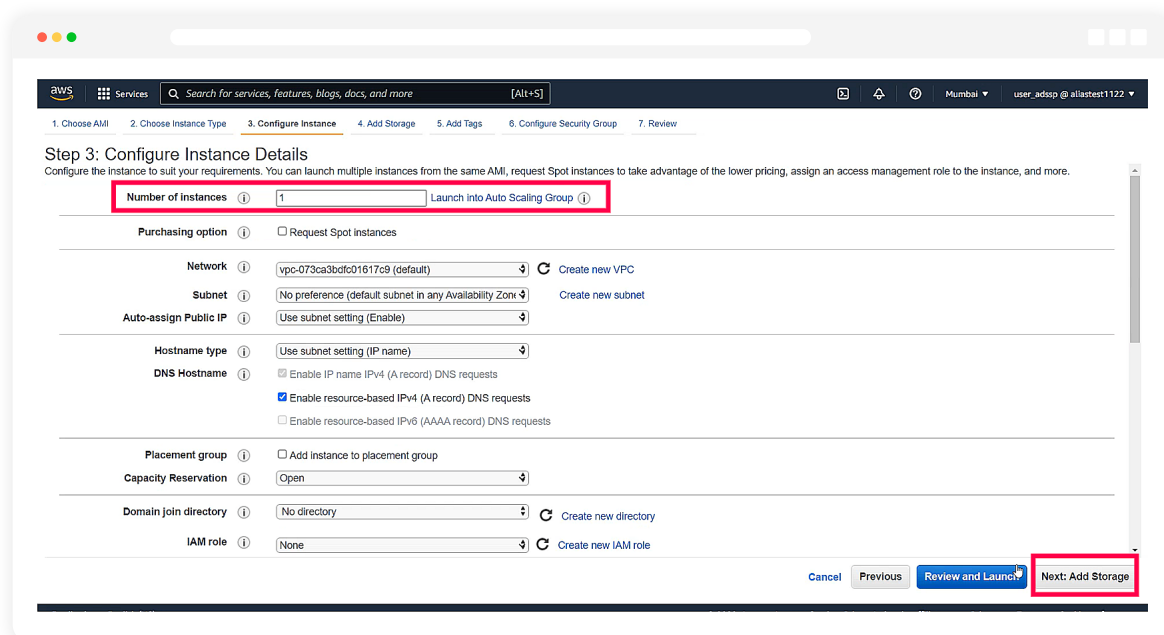
3. In the *Step 1: Choose an Amazon Machine Image (AMI)* tab that opens, navigate to **Microsoft Windows Server 2019 Base**, and click **Select**.



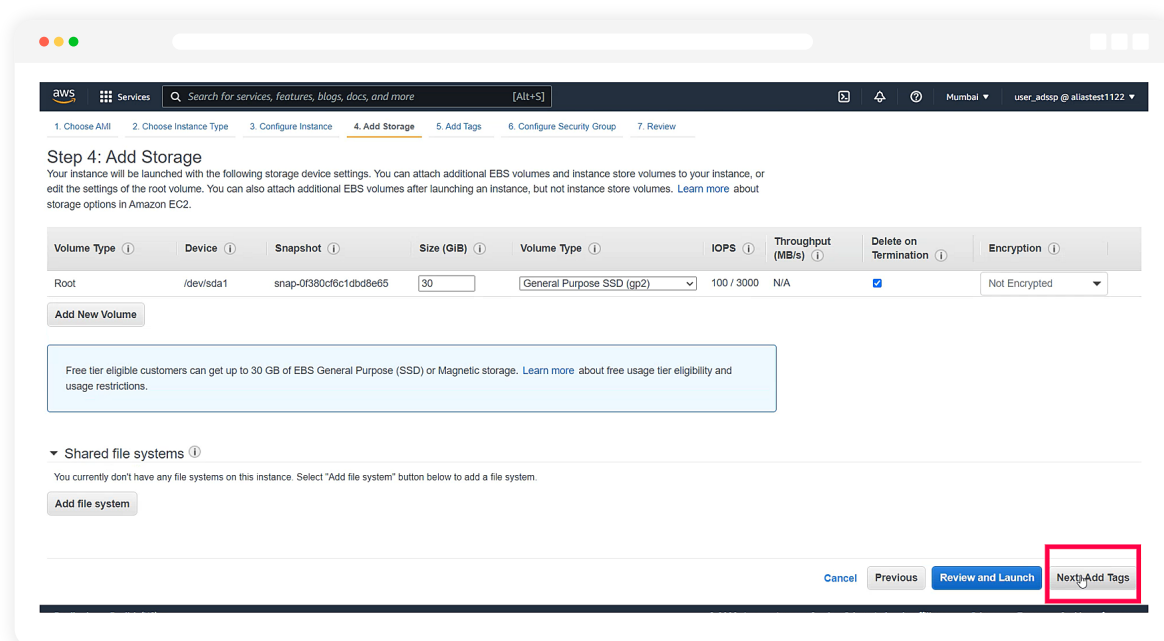
- In the *Step 2: Choose Instance Type* tab that opens, select **t2.micro** as the instance type, and click **Next: Configure Instance Details**.



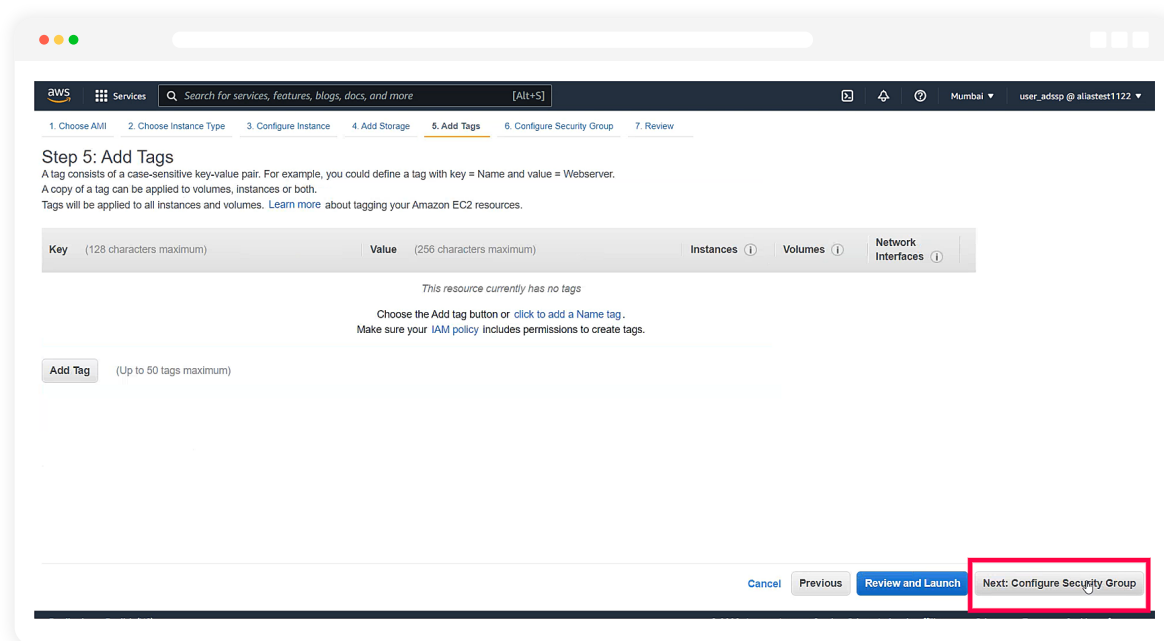
- The *Step 3: Configure Instance Details* tab will open. Enter **1** in the *Number of instances* field. Create and set a new **Amazon Virtual Private Cloud (VPC)** as the Network or select an existing network.
- Enter other details such as **Subnet**, **Hostname type**, and **DNS Hostname** according to your organization's preferences. Click **Next: Add Storage**.



7. In the *Step 4: Add Storage* tab that opens, edit the **settings** of the root storage device if needed. Click **Next: Add Tags**.



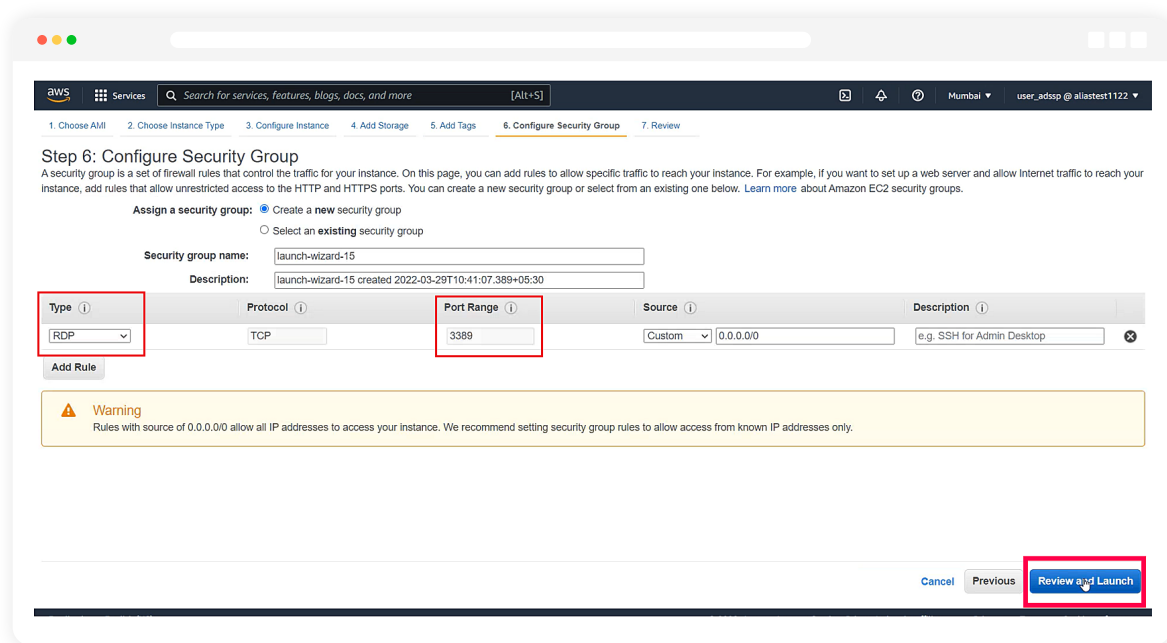
8. The *Step 5. Add Tags* tab will open. Click **Next: Configure Security Group**.



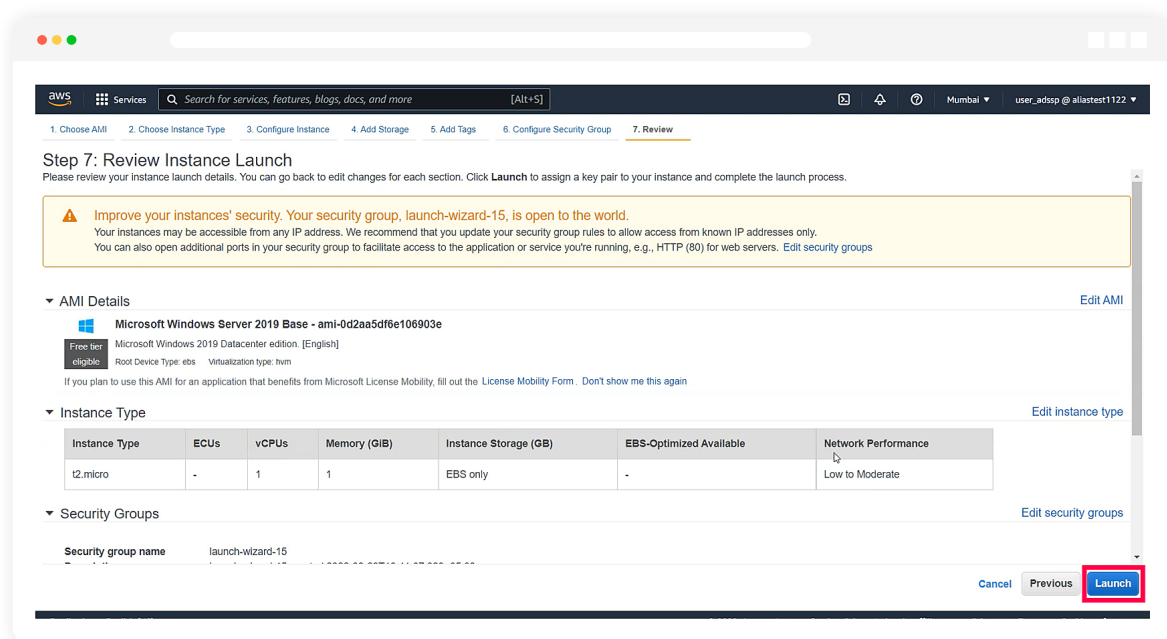
9. In the *Step 6. Configure Security Group* tab, you can choose to create a new security group or use an existing one. Ensure that the *Type* is set as **RDP** and the *Port Range* is **3389** for the security group.

**Note:** To ensure that users can access the EC2 instance and that the product deployed in it, the security group must have an inbound traffic rule that allows the IP address range of the user machines.

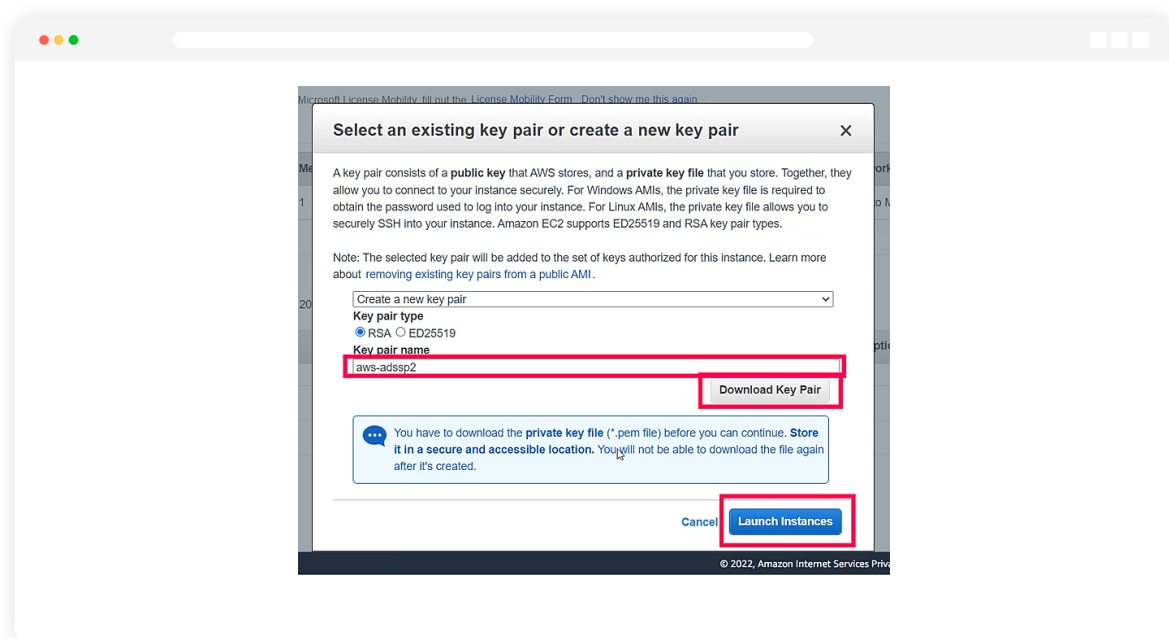
10. Click **Review and Launch**.



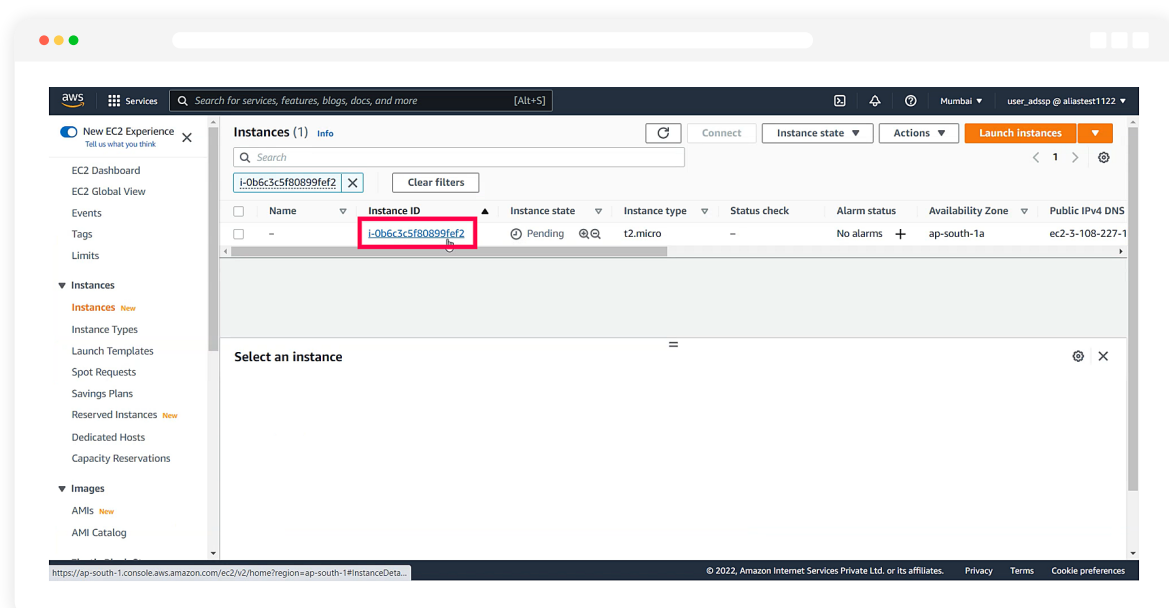
11. In the **Step 7: Review Instance Launch** tab, click **Launch**.



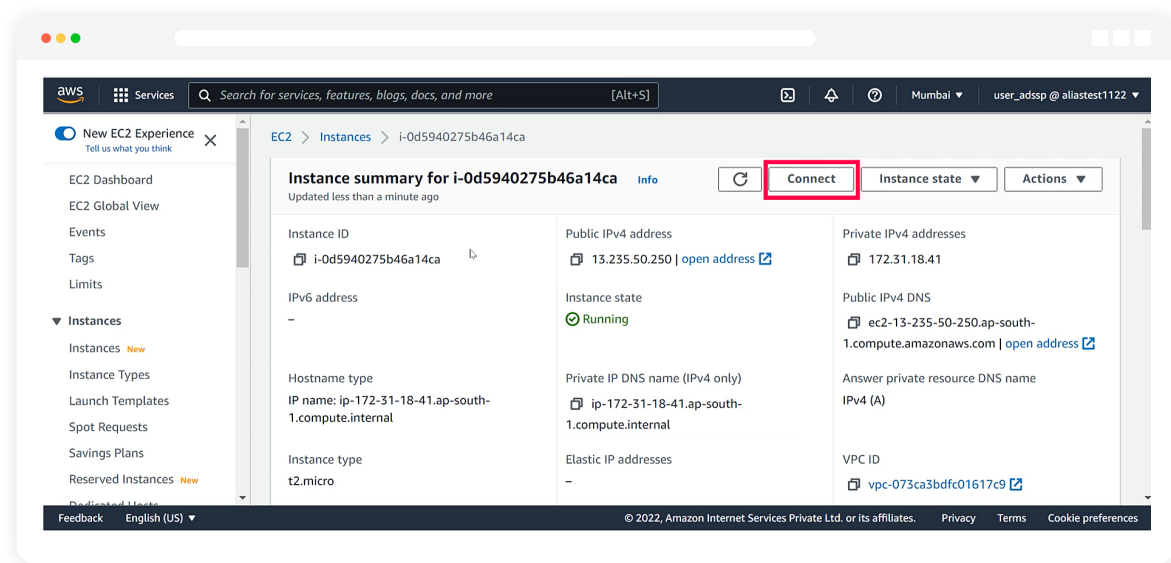
12. The *Select an existing key pair or create a new key pair* pop-up will open. Here, select **Create a new key pair**.
13. Select **RSA** as the *Key pair type* and enter a **Key pair name**. Click **Download Key Pair**.
14. Once the key pair file is downloaded, click **Launch Instances**.



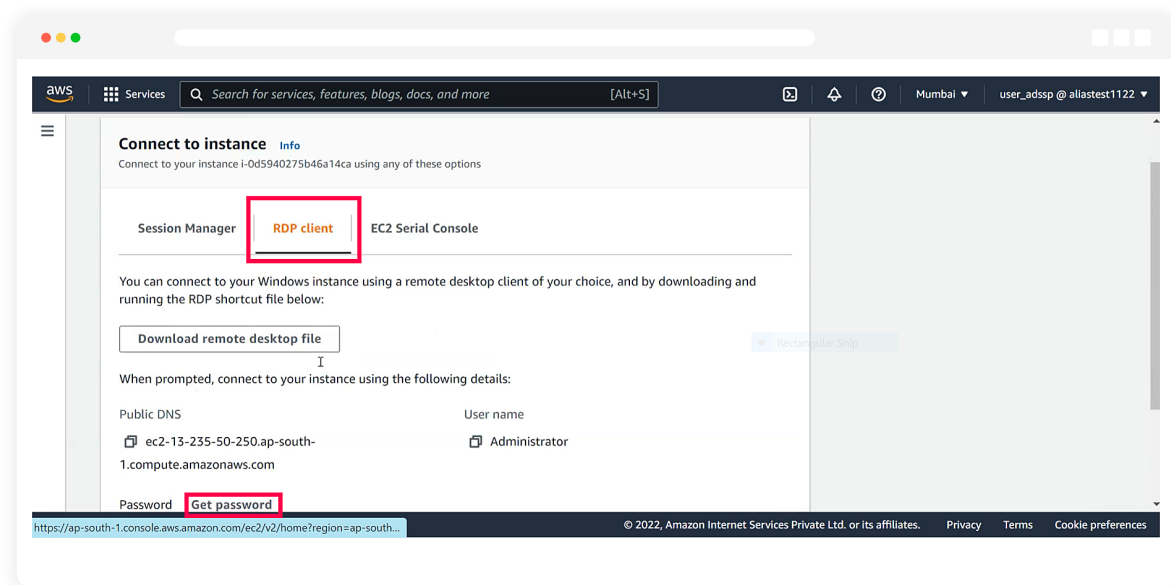
15. On the *Launch Status* page that opens, click the **instance name**.
16. On the table that appears, click the **instance name** once again.



17. The instance summary will appear. Click **Connect**.

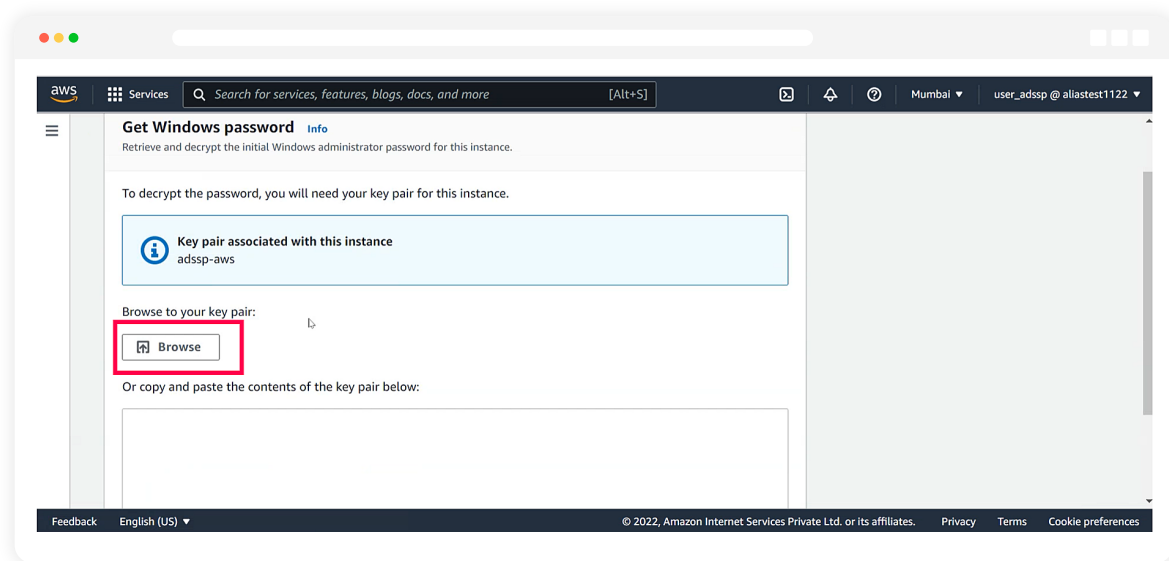


18. On the page that opens, click the **RDP client** tab and then click **Get password**.

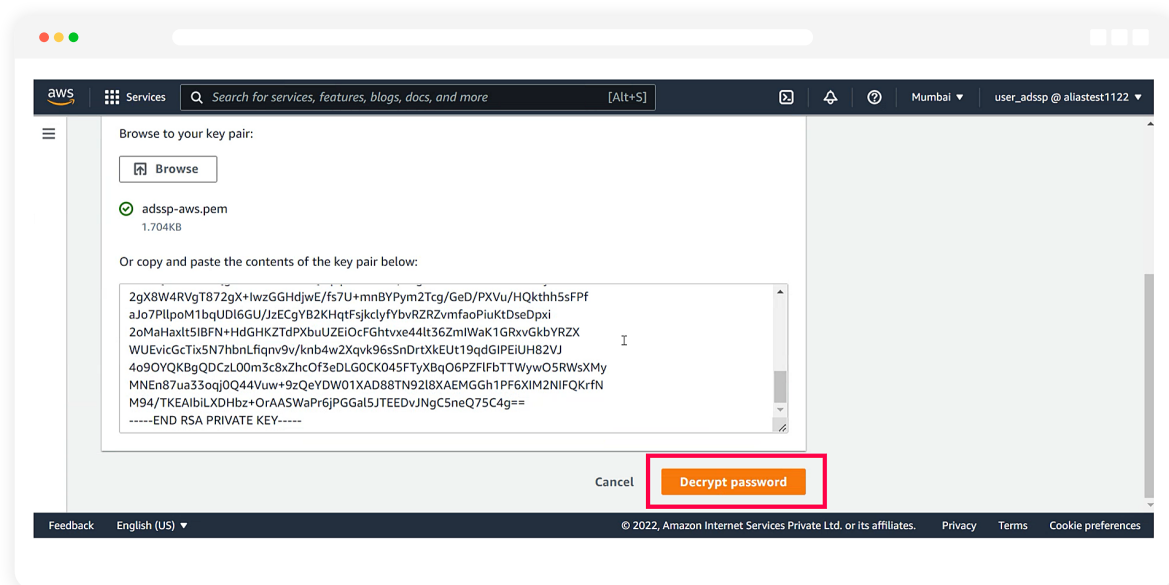


19. Click **Browse** and select the key pair file downloaded in step 12.



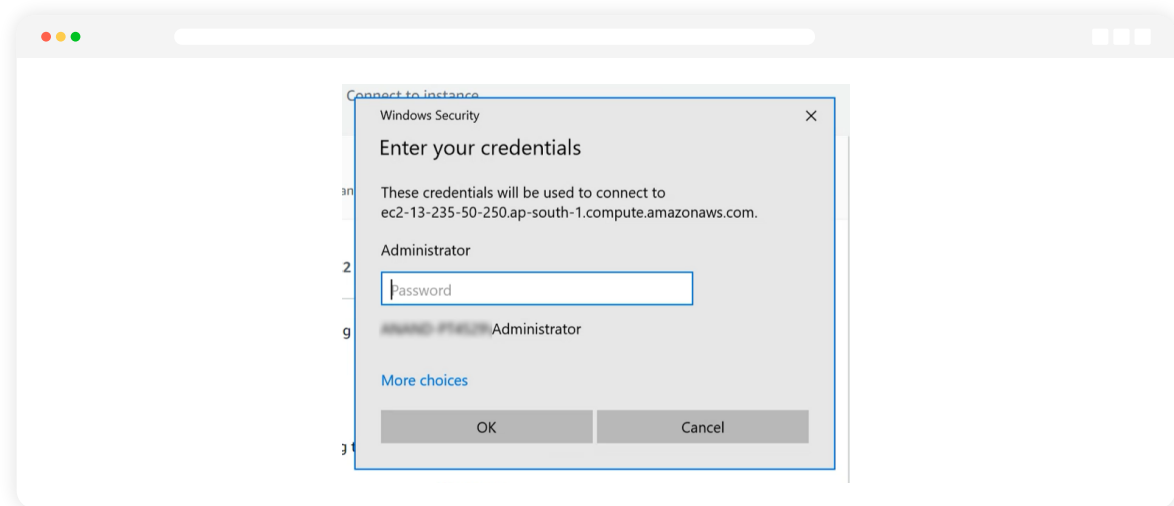
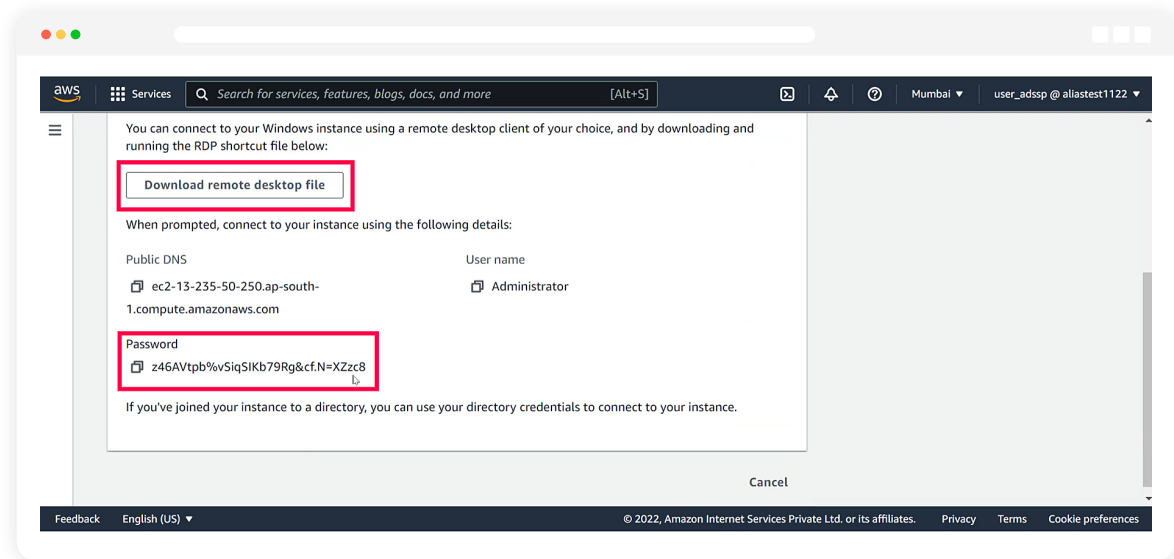


20. Scroll down, and click **Decrypt password**.



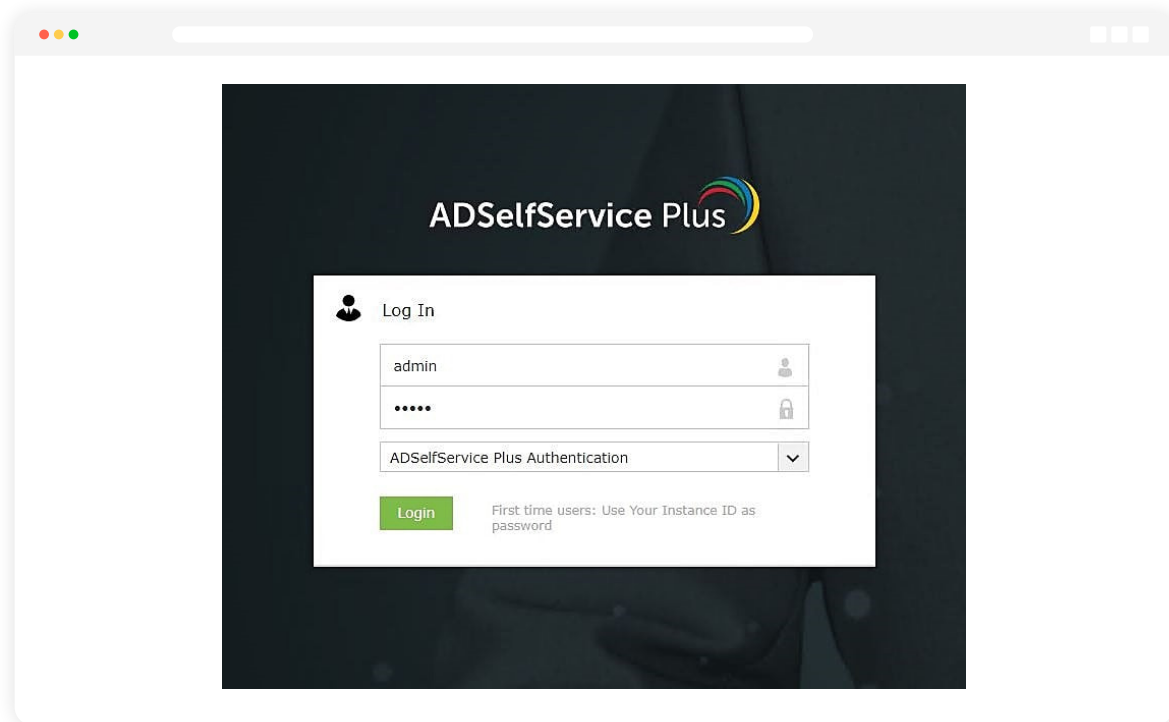
21. The **RDP client** tab will open again. Here, click **Download remote desktop file**.

22. Open the **remote desktop file** once downloaded. Copy the **Password** from the *RDP* client tab and use it to authenticate the remote desktop connection.



23. Once the remote desktop connection is established with the EC2 instance, open a web browser in the instance and [download](#) and [install](#) **ADSelfService Plus**.

24. Users can now access the product on the cloud from anywhere using AWS.



**Note:** The ADSelfService Plus access URL will have to be configured as a trusted webpage according to the web browser instructions.

ManageEngine  
**ADSelfService Plus**

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces. For more information about ADSelfService Plus, visit <https://www.manageengine.com/products/self-service-password>.

\$ Get Quote

↓ Download