

Classification	Strictly Confidential	
	Confidential	
	Restricted	✘
	Unrestricted	
Access list		

# sDWP

## Frequently Asked Questions

---

This document contains confidential information of Siemens. Except with the express prior written permission of Siemens, this document and the information contained herein may not be published, disclosed, or used for any other purpose

## Table of Contents

sDWP and Services.....	1
How do I avail these services?.....	3
How to use EMAIL + OTP option to authenticate?.....	4
How to use VMware Horizon Client.....	9
Support & FAQ.....	12

## **sDWP and Services**

### **What is sDWP and what are its usage benefits?**

sDWP stands for Secure Digital Workspace. sDWP is a Virtual Desktop Infrastructure that has been built from the ground-up as part of the Siemens IT transformation. Virtual desktop infrastructure (**VDI**) is the technology for providing and managing virtual desktops. **VDI** hosts desktop environments on a centralized server and deploys them to end clients on request which allows users working from home using their Personal Systems or Official Laptops to consume IT services in much faster way.

### **What is the Coverage of Services?**

sDWP current services span across:

1. Multiple Siemens sites
  - Keonics (KEO)
  - Salarpuria (SAL)
2. Siemens networks
  - Production (SNX)
3. Hypervisor platforms
  - VMware
4. Operating Systems
  - Windows 10 DWP Images

**What services are offered through the sDWP platform?**

The current services offerings can be summarized as follows:

1. **sDWP** Virtual Machines for Laptop and Personal System users who are working from home.
  - a. Laptop users are basically using the **sDWP** virtual machines due to heavy operations such as copying build from URA network, which takes lot of time to copy due to personal network limitations. For such users we provide **sDWP** virtual machines as well as required software's like Visual Studio\*, Clearcase client etc.
  - b. Virtual Machines are assigned through Dynamic assignment that means users will not have their dedicated Virtual machines. Once you logout and connect back you get a new Virtual machine which is free in that pool.
2. Physical Desktops users can also directly access their desktops from personal system by just installing a Client on the Physical Desktop's.
  - a. Physical desktops will be assigned manually as the assets is owned by a specific user, so dynamic assignment of Physical desktop is not available.
  - b. For installation and configuration of client on Desktops, kindly raise a IT ticket and respective engineers will help you on the same.

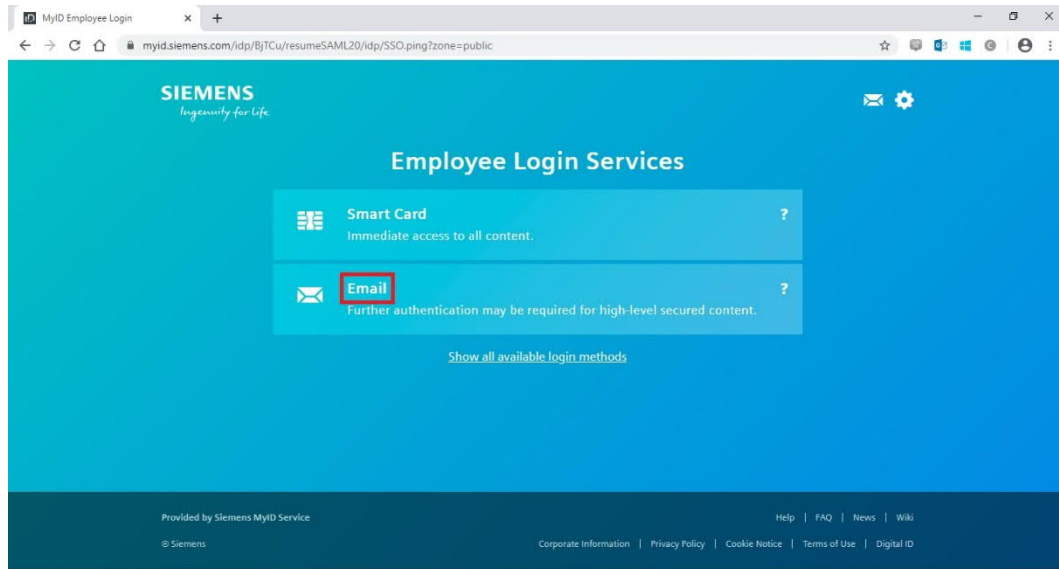
**How do I avail these services?**

Visit <https://digitalworkspace.siemens.com>

- From open internet you will be able to browse the above-mentioned website.
- Once browse the site you will by default be redirected to smart card authentication page.
  - There are multiple ways to authenticate.
    - Smart Card authentication.
    - Email + OTP
      - For Email + OTP option you need to install an APP on your Mobile handsets in which you are using your official Siemens Mobile Numbers.
      - How to use Email + OTP option to authenticate is demonstrated below.

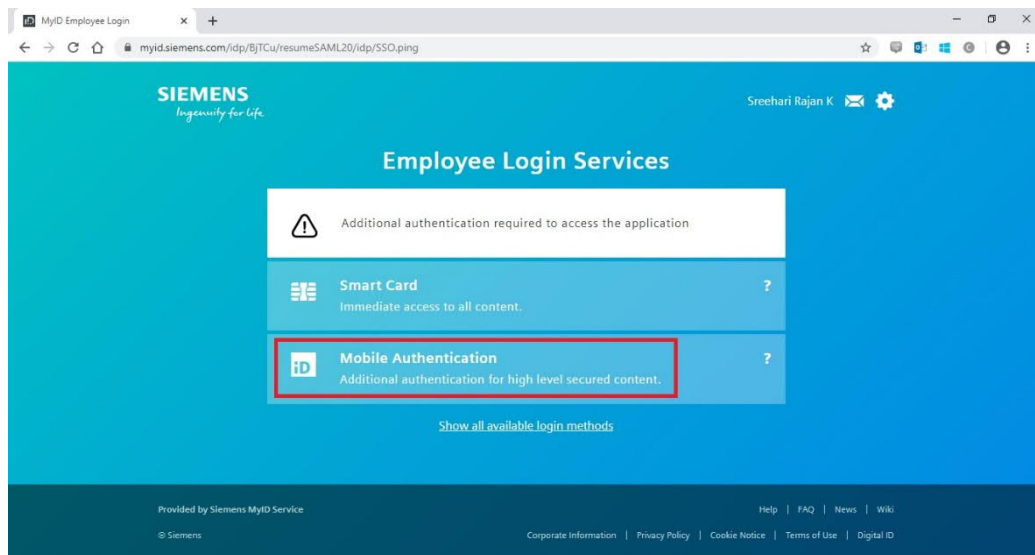
## How to use EMAIL + OTP option to authenticate?

1. Go to Play Store (For Apple mobiles please chose app store), search PingID.
2. Install PingID.
3. Now Browse <https://digitalworkspace.siemens.com> from your personal systems. You will be redirected back to Smart card authentication page.
4. Select Email option as shown in the below screenshot.
5. Enter your email id and windows login password.

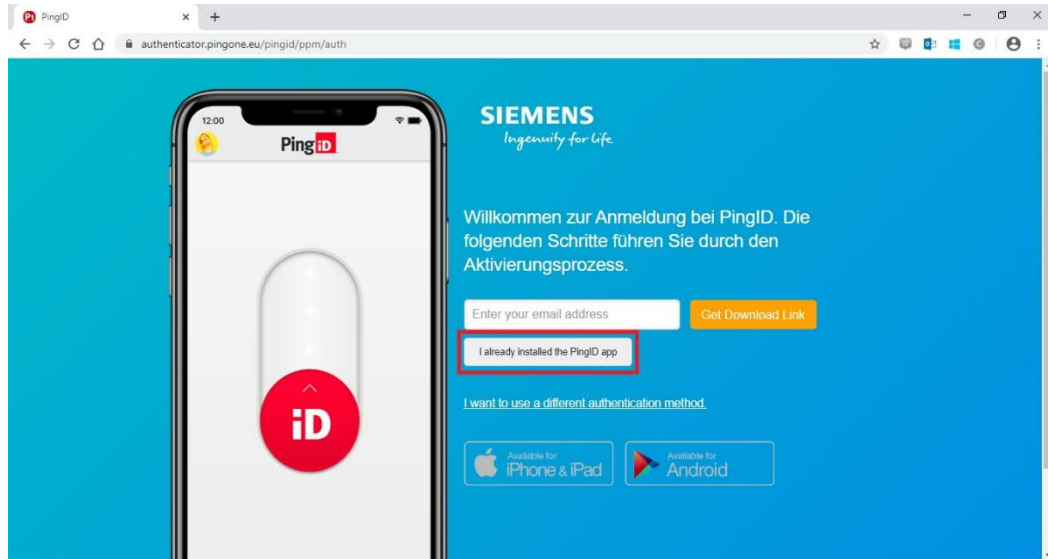


6. Once you login using Email ID and Password you will be redirected to additional authentication page as shown in the below screenshot.

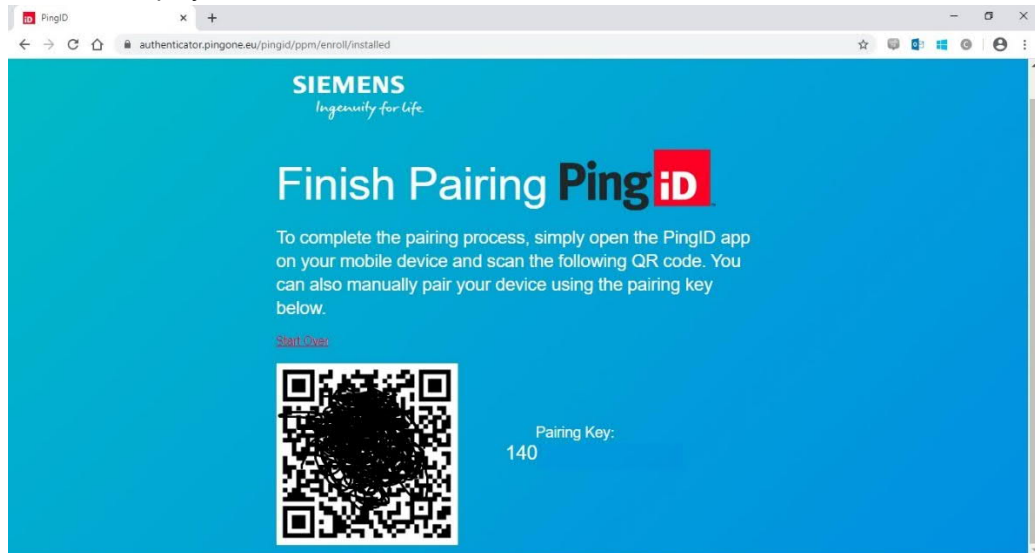
### a. Select Mobile authentication



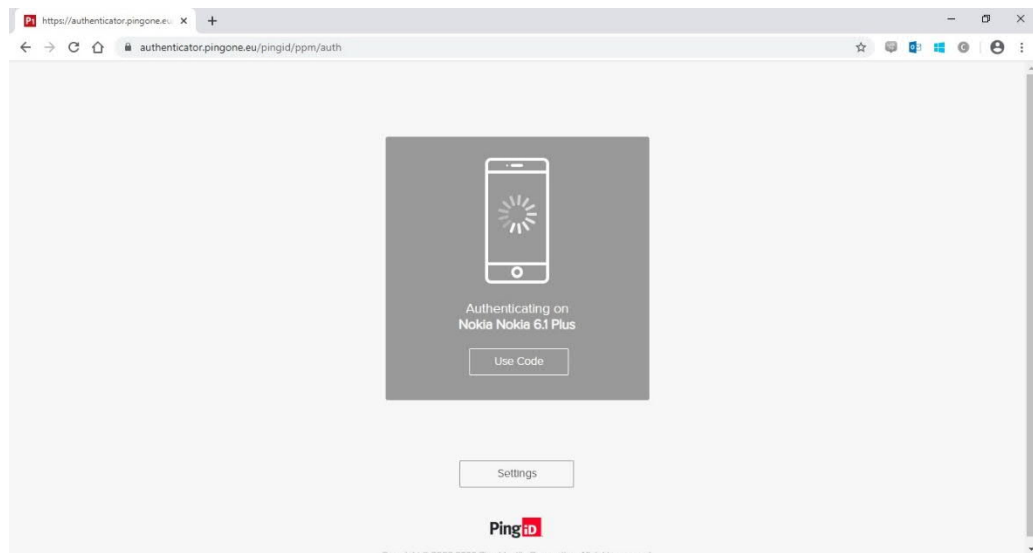
7. Open PingID app on your mobile and select Accept the License Agreement.
8. Select I Understand option from the Important notification page on your Mobile.
9. App on your mobile will open a Barcode Scanner and there will be a prompt "Allow PingID to take pictures and record video?"
  - a. Select Allow
10. Now from the webpage on your personal system select "I already installed the PingID app"
  - a. You will now be redirected to a webpage where you will see a Barcode to scan using your PingID mobile App.



11. Scan the barcode shown on your webpage from your mobile app. Barcode webpage would be displayed as shown in the below screenshot.

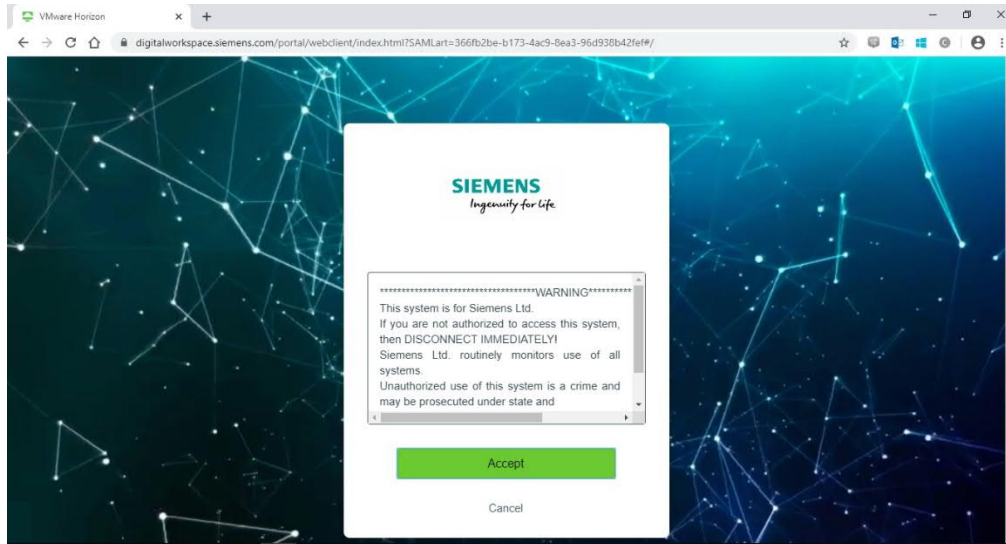


12. Once authenticated on your mobile App you will be prompted by PingID app to "Allow PingID to access this device's location?"
  - a. Select ALLOW ALL THE TIME
13. Enter a Nickname on your mobile PingID app, you can additionally also upload your Photograph which is not mandatory.
14. Select "Done" from PingID App.
15. You will get a popup on mobile for authentication of PingID App from the website shown below.
  - a. If you have Mobile Finger Print security enabled just keep your finger on the Finger print sensor you will be now authenticated.
  - b. You can use Enter Passcode manually and enter the passcode shown in your PingID app on your mobile.
    - i. Kindly note, Passcodes will be changed every minute and the same passcode cannot be used multiple times to authenticate as that becomes invalid.

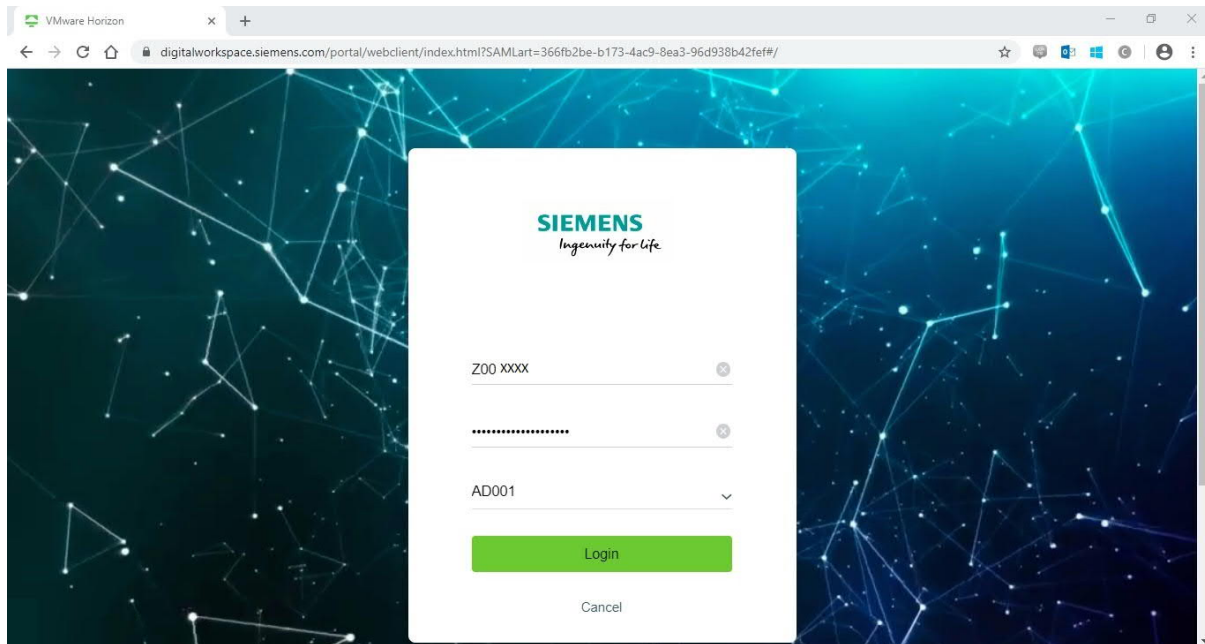


16. Once authenticated you will be redirected back to the **sDWP** Authentication page as shown in the below screenshot.
  - a. Select Accept

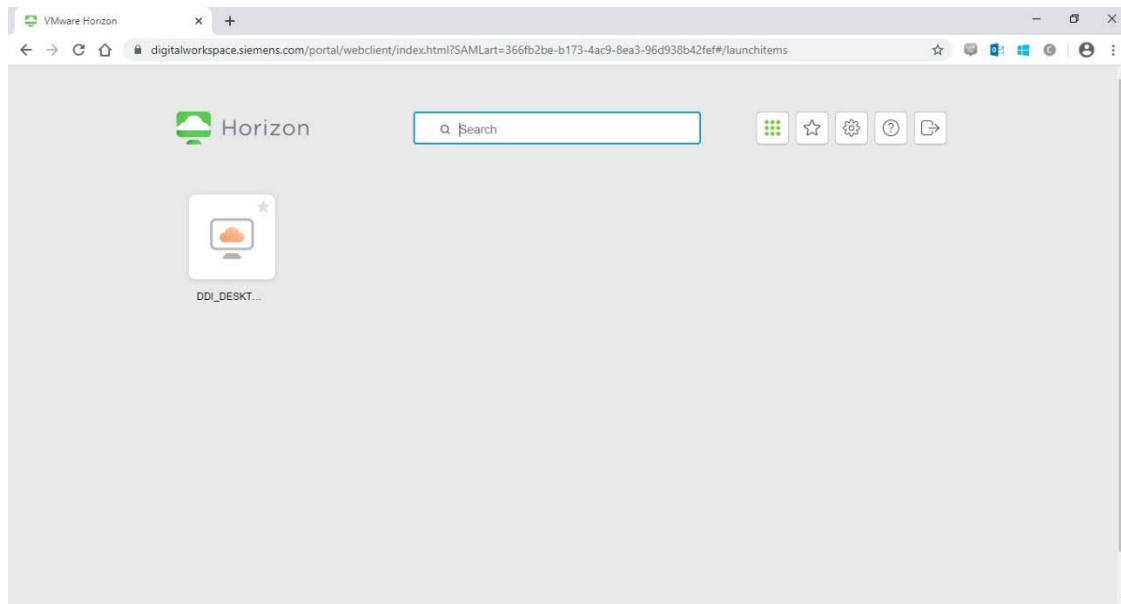




17. Now Enter your Windows Login ID (GID), Enter your Password as shown in the below screenshot and select Login.



18. Once you are logged in, you will see the **sDWP** machine entitled for you. Select the machine as shown in the below screenshot and it will launch.

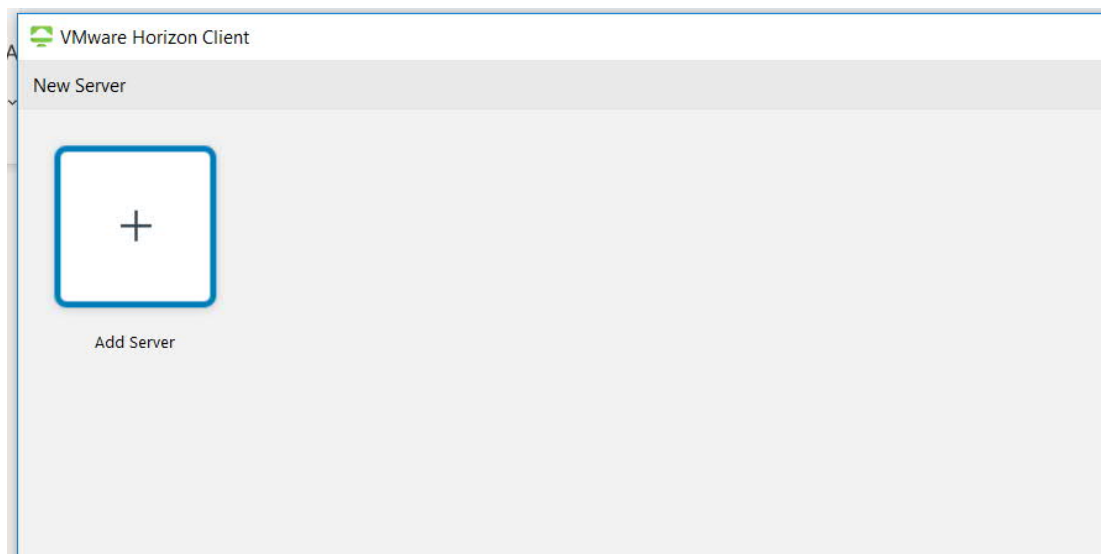


## How to use VMware Horizon Client:

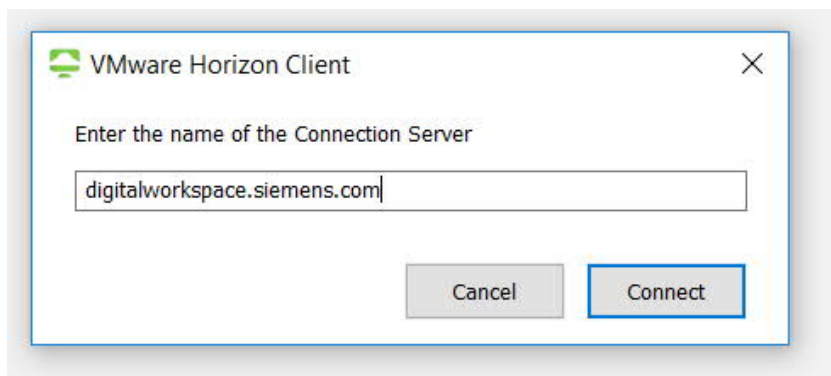
1. From the below link kindly download the Horizon client to your personal system.

[https://my.vmware.com/web/vmware/details?downloadGroup=CART21FQ1\\_WIN\\_542&productId=863&rPId=44970](https://my.vmware.com/web/vmware/details?downloadGroup=CART21FQ1_WIN_542&productId=863&rPId=44970)

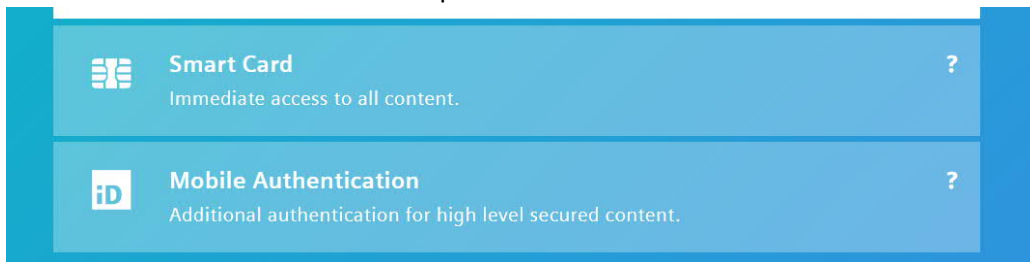
2. Once download is completed, please install it with default options, restart the machine after installation is completed.
3. Once installation is completed and once you launch the Horizon Client you will see the below screen. Double click on ADD server option, there will be a dialogue box opened.



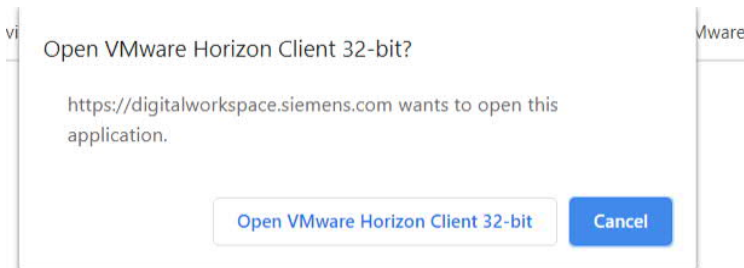
4. Enter the name of the connection server as “**digitalworkspace.siemens.com**” and select Connect.



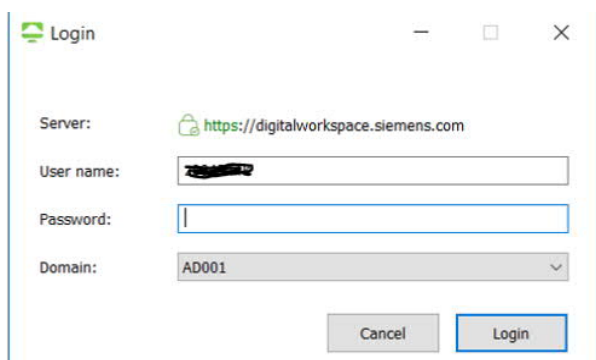
5. Once you click on Connect you will be redirected to a Browser for the Smartard Authentication. You can refer the “How to use EMAIL + OTP option to authenticate?” from this document to use EMAIL + OTP option for authentication.



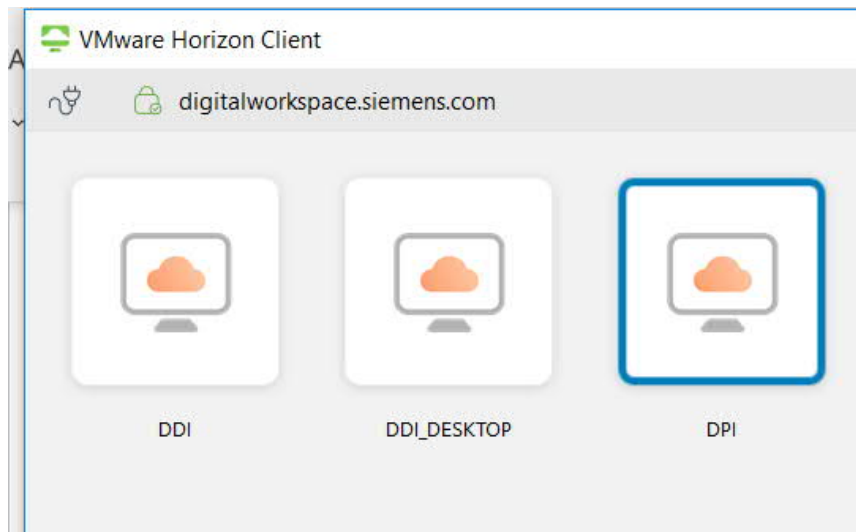
6. Once you are authenticated you will see an popup windows on Browser as shown in the below screenshot. Select “**open VMware Horizon Client 32-bit**”.



7. After Selecting the Open VMware Horizon Client 32-bit from the last step you will be prompted with the below authentication as shown in the below screenshot.
  - a. Enter your GID as the Username
  - b. Enter your password
  - c. Domain should by default be “**AD001**”



8. Once you are authenticated from the last step you will be able to see your entitled sDWP Desktop. Double click on the same and it will launch your Desktop.



**SUPPORT**

- For any issues with respect to accessing the **sDWP** machine kindly raise an MyIT ticket and share us ticket number on “RG IN STS Siecloud Escalation”

**FAQ :**

- Where is the **sDWP** machine hosted?
  - This is a on premises solution, so we have **sDWP** machines deployed at Bangalore Salarpuria, and Bangalore Keonics. We will shortly extend these services to other locations of STSPL.
- How to request?
  - You can get in touch with your BU IT Managers.
  - While requesting please specify your work location, as you may also require connectivity to your Test Labs / Test Network Machines.
- In which network is the **sDWP** Machine hosted?
  - **sDWP** machines are basically hosted on the Siemens SNX Network.
- Is Siemens CERT Guidelines applicable for these machines?
  - Yes. This is just like your development machine.
- Can other location users request for the **sDWP** Machine which is hosted in Bangalore?
  - Yes, unless and until you don't have any dependencies over your Test Network.