

Predict | Protect | Prevent

ARCON|PAM

Application Gateway Server

Table of Contents

1	Overview	4
2	Advantages	5
3	Prerequisites	6
4	Privileges	7
5	AGW Configuration	8
5.1	AGW to Service Mapping.....	11
6	Service Access using AGW	14
6.1	AGW to Service UnMapping	17
7	Application Path Settings over AGW	21
8	Vault Broker	23
9	Session Collaboration.....	26
10	Using AGW through PAM API	29
10.1	Getting the User Details.....	29
10.2	Getting the Service Details of the User	30
10.3	Starting the Session.....	32

Disclaimer

The handbook of ARCON PAM solution is being published to guide stakeholders and users. If any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON through the support team. Wherever appropriate, references have been made to facilitate a better understanding of the PAM solution. ARCON team has made every effort to ensure that the information contained in it was correct at the time of publishing.

Nothing in this document constitutes a guarantee, warranty, or license, expressed or implied. ARCON disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON.

Copyright Notice

Copyright © 2022 ARCON All rights reserved.

ARCON retains the right to make changes to this document at any time without notice. ARCON makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Sales Contact

You can directly contact us with sales-related topics at the email address <sales@arconnet.com>, or leave us your contact information and we will call you back.

1 Overview

Every organization has multiple access requirements for a different set of devices. Some prefer to have a traditional approach wherein the application would be installed on an end-user machine for a particular user to access it. For this, organizations need to keep certain required ports open from the end-user machine.

Another better approach would be to connect to a Streaming server and access all the applications from there itself. Application Gateway server (AGW) is a solution that controls all the entry points into your environment. With AGW one can allow taking remote sessions to one particular machine (AGW Server) that is placed in a very controlled environment and is monitored, from the AGW Server users can connect to other applications and machines.

Application Gateway server (AGW) completely eliminates the need for downloads and installations on end-user machines and allows them to connect to the target device via a terminal server using Secure HTTPS Protocol. Since it is a Streaming application, it is atypical from a Jump server. It only streams the required data and does not launch the application there.

2 Advantages

- **Enhanced security:**
 - With privileged based access rights, organizations can control the level of access to granting to individual users.
 - When the End User takes a connection to Target Device via ARCON PAM Solution, Session is initiated on the AGW Server and is streamed to the End User Machine on Secure HTTPS Protocol.
 - AGW supports command line credential injection during the SSH session. Whereas, Telnet session uses command and response mechanism through automation DLL and RDP uses the RDP offered credential injection methodologies. The HTTP or HTTPS session uses user interface credential injection and keystroke automation.
- **Enhanced Performance:** The organizational network load is reduced to minimum usage as the users will be accessing everything on the centralized AGW server instead of the individual user machine.
- **Cost-Effective:** With a centralized AGW server, organizations don't have to purchase multiple licenses for third party applications and the organizations can go for a lesser bandwidth package.
- **Time Management:** Installation and configurations on individual systems are not required and so about the updates, thus, in the long run, a lot of time and money can be saved.
- **Access Control:** AGW Server can be monitored and every single activity on the server is tracked and thus ensuring data security, lowering the risk of data loss and breaching.
- **Administration:** Complete administration of ARCON PAM (Server Manager) such as User Access Review, Password Management, Real-Time Session Monitoring, Command Profiling and other, can be easily managed and accessed through the web interface.
- **Session Management:** Session management in AGW is browser-based supporting HTML5, SSH, Telnet connections to the target systems. Moreover, we can carry out session management through a proxy. ARCON Streaming Server (AGW) also allows us to record and isolate connections.
- **Vault Broker:** ARCON Application Gateway Server also acts as a secret less broker where any user/client sends a request to the VaultBroker service (ARWH) hosted on the application streaming server which in turn makes a call to ARCON PAM Vault or any other third-party Vault provider.
- **Session Monitoring:** Whenever the user wants to monitor an end-users session in AGW, he can use smart session monitoring. Smart session monitoring allows enhanced filtering to capture commands, texts, process tabs, keystrokes, and mouse clicks.

3 Prerequisites

- For AGW connection, **Use AGW for Open Connection** configuration should be **enabled** under **Settings**.
- It is recommended to install AGW on an independent server other than the app server.
- To launch the Server Manager on a particular AGW, **Use AGW to Open Server Manager** configuration should be **enabled** under **Settings**.

4 Privileges

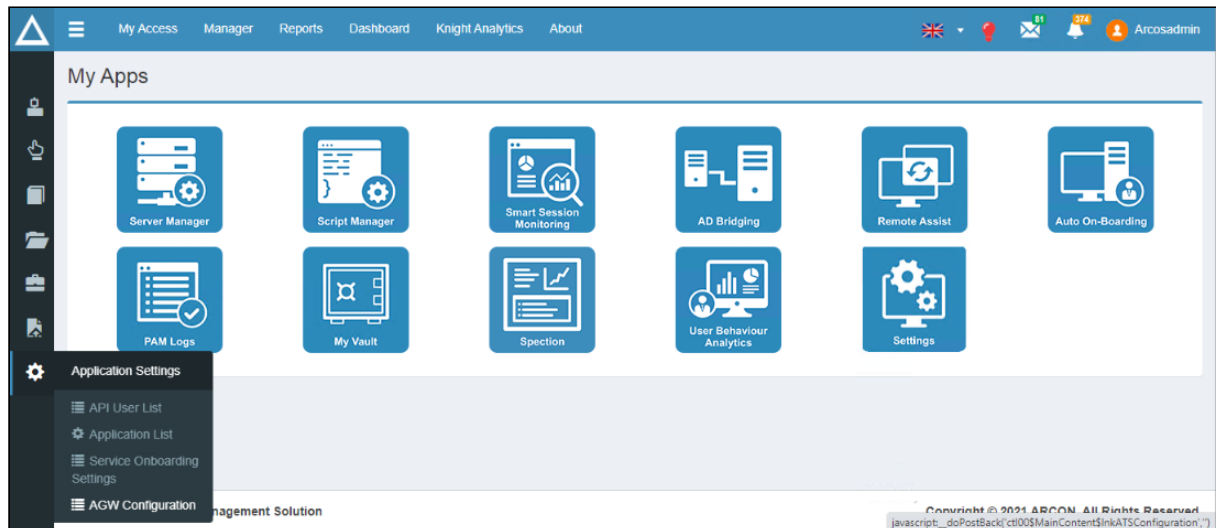
- Global Configuration **Use AGW for Open Connection** value should be set to **1** to enable AGW Connection.
- Users with the privilege **Application Gateway server** can only do AGW configurations.
- It is recommended to install AGW on an independent server other than the app server.

Before using the AGW server for streaming, the following are the major steps of configuration in ARCON PAM:

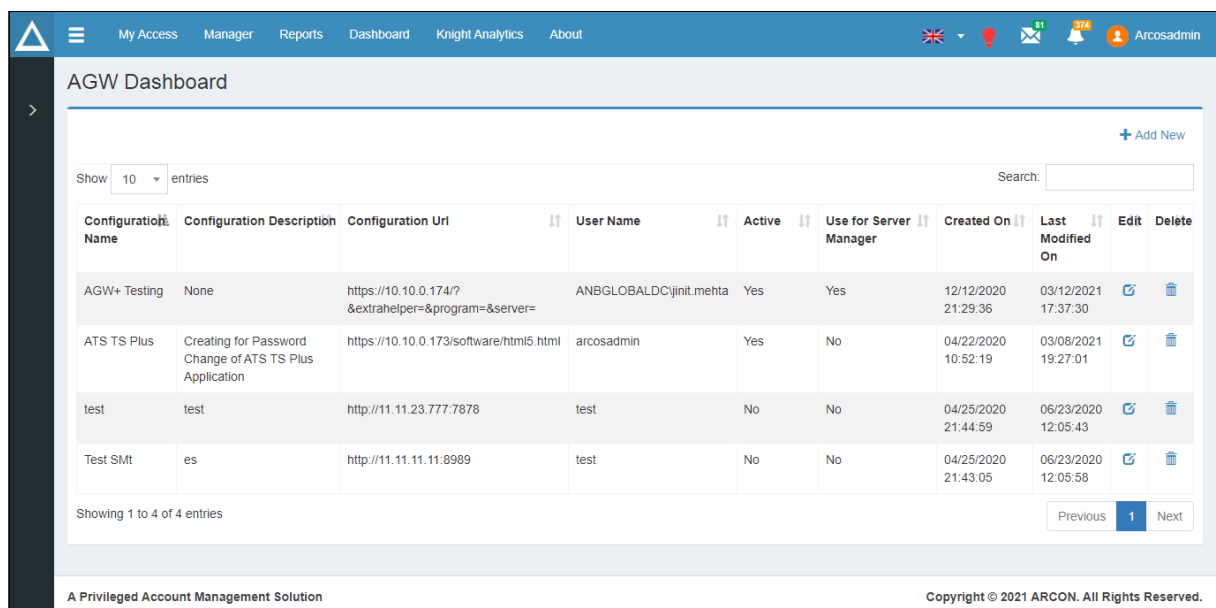
1. Allow the above-mentioned privileges to the Administrator who can configure AGW Servers.
2. AGW Server Configurations for allowing streaming through ARCON PAM.
3. AGW Service Mapping to map streaming services to AGW.
4. Service Access through AGW.

5 AGW Configuration

1. **AGW Configuration** will be displayed under Application Settings as in the below image for users with the Privilege of Application Gateway Server.



2. Click AGW Configuration, AGW Dashboard will be displayed and here we can add multiple AGW Servers.



3. Click **Add New**, the following ADD Configuration screen will be displayed.

Add Configuration ✕

All Fields are mandatory, can keep config active or inactive

Configuration Name

Configuration Description

Configuration Url i

Exe Path

Exe Directory Path

User Name

Password

Pin

☐ Use for Server Manager

☐ Is Active

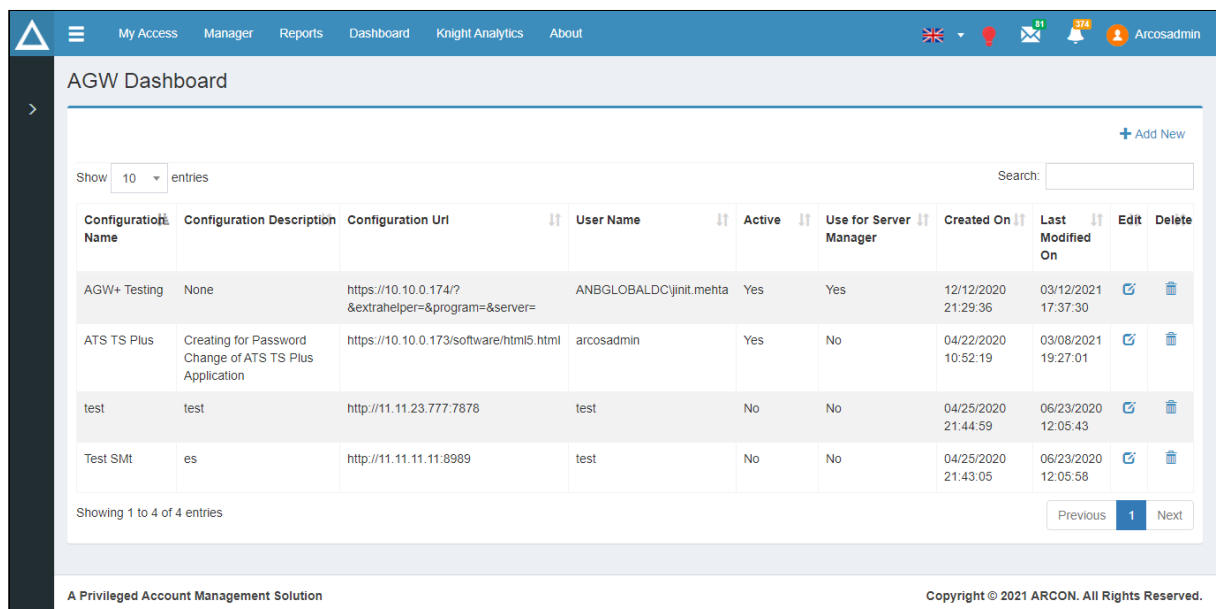
Add

The **AGW Dashboard** screen contains the following fields:

Field	Description
Configuration Name	Name of AGW Server
Configuration Description	Description of AGW Server
Configuration URL	Enter the URL of the AGW Server where TS Plus is configured

Field	Description
EXE Path	Full Path of ARWH executable is placed
Exe Directory Path	Directory path of the ARWH Executable file
User Name	Local user of the AGW Server
Password	Password of the above username
PIN	Enter the PIN configured in TS Plus Web Credential
Use of Server Manager	<p>Select this checkbox to launch server manager on a particular AGW Server.</p> <div> <p>i</p> <ul style="list-style-type: none"> If one AGW server is hosted and this checkbox is enabled then the server manager will be hosted on that particular AGW server. If there are multiple AGW Servers hosted and this checkbox is enabled then the server manager will be hosted on one of the AGW servers randomly. </div>
Is Active	Select this checkbox if this AGW server is supposed to be kept active

- Enter all the descriptions as in the above table and click Add.
- Once the AGW configuration is done, it will be displayed as follows on the AGW Dashboard. (Users can add multiple AGW Servers)



The screenshot shows the AGW Dashboard with a table of configurations. The table has columns for Configuration Name, Configuration Description, Configuration Url, User Name, Active status, Use for Server Manager, Created On, Last Modified On, Edit, and Delete. There are 4 entries listed.

Configuration Name	Configuration Description	Configuration Url	User Name	Active	Use for Server Manager	Created On	Last Modified On	Edit	Delete
AGW+ Testing	None	https://10.10.0.174/?extrahelper=&program=&server=	ANBGLOBALDCjini.mehta	Yes	Yes	12/12/2020 21:29:36	03/12/2021 17:37:30		
ATS TS Plus	Creating for Password Change of ATS TS Plus Application	https://10.10.0.173/software/html5.html	arcosadmin	Yes	No	04/22/2020 10:52:19	03/08/2021 19:27:01		
test	test	http://11.11.23.777.7878	test	No	No	04/25/2020 21:44:59	06/23/2020 12:05:43		
Test Smt	es	http://11.11.11.11:8989	test	No	No	04/25/2020 21:43:05	06/23/2020 12:05:58		

Showing 1 to 4 of 4 entries

Previous 1 Next

A Privileged Account Management Solution

Copyright © 2021 ARCON. All Rights Reserved.

- Once AGW is configured, users can map services to AGW Server.

5.1 AGW to Service Mapping

This option will allow users to map services to AGW servers so that users can make connections through AGW.

My Access

Manager

Reports

Dashboard

Knight Analytics

About

g1

374

Arcosadmin

AGW Dashboard

Back

AGW to Service Mapping

AGW to Service Unmapping

AGW Preference Path

Manager

Search:

Configuration Description	Configuration Url	User Name	Active	Use for Server Manager	Created On	Last Modified On	Edit	Delete	
	https://10.10.0.174/?&extrahelper=&program=&server=	ANBGLOALDC\jinit.mehta	Yes	Yes	12/12/2020 21:29:36	03/12/2021 17:37:30			
ATS TS Plus	Creating for Password Change of ATS TS Plus Application	https://10.10.0.173/software/html5.html	arcosadmin	Yes	No	04/22/2020 10:52:19	03/08/2021 19:27:01		
test	test	http://11.11.23.777-7878	test	No	No	04/25/2020 21:44:59	06/23/2020 12:05:43		
Test SMT	es	http://11.11.11.11:8989	test	No	No	04/25/2020 21:43:05	06/23/2020 12:05:58		

Showing 1 to 4 of 4 entries

10.10.0.91:16521/ATS/frmATSMapping.aspx

Panel to activate Windows

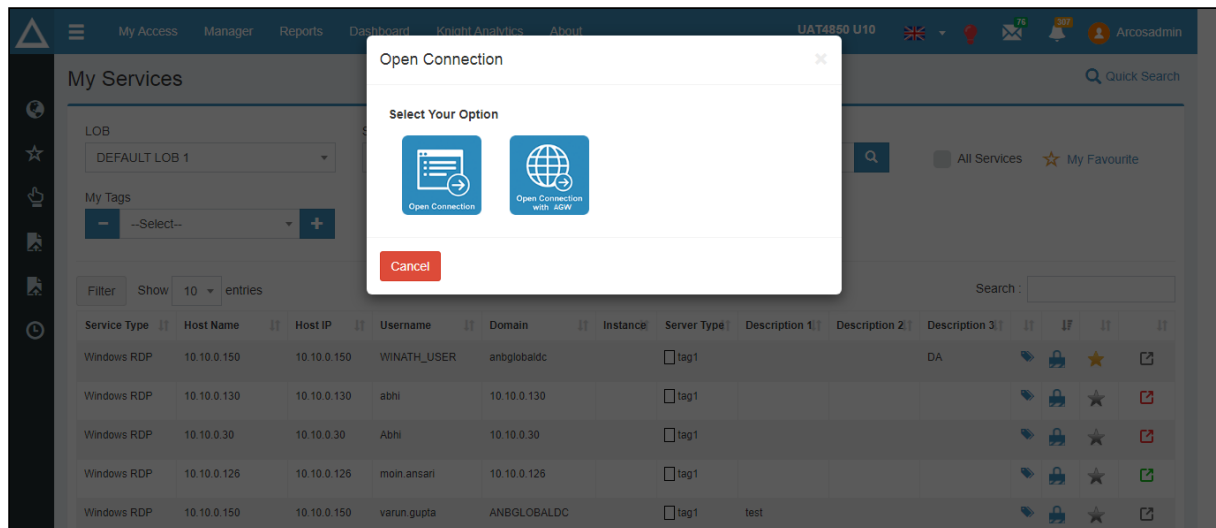
Previous

1

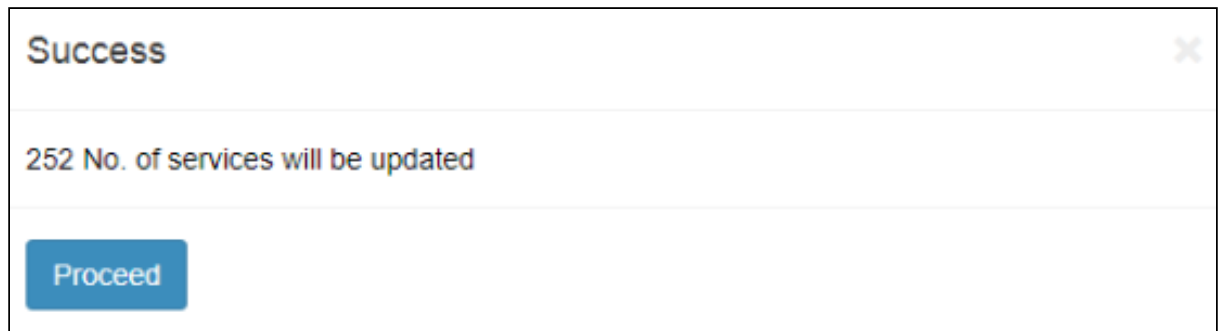
Next

Following are the steps for AGW to Service Mapping:

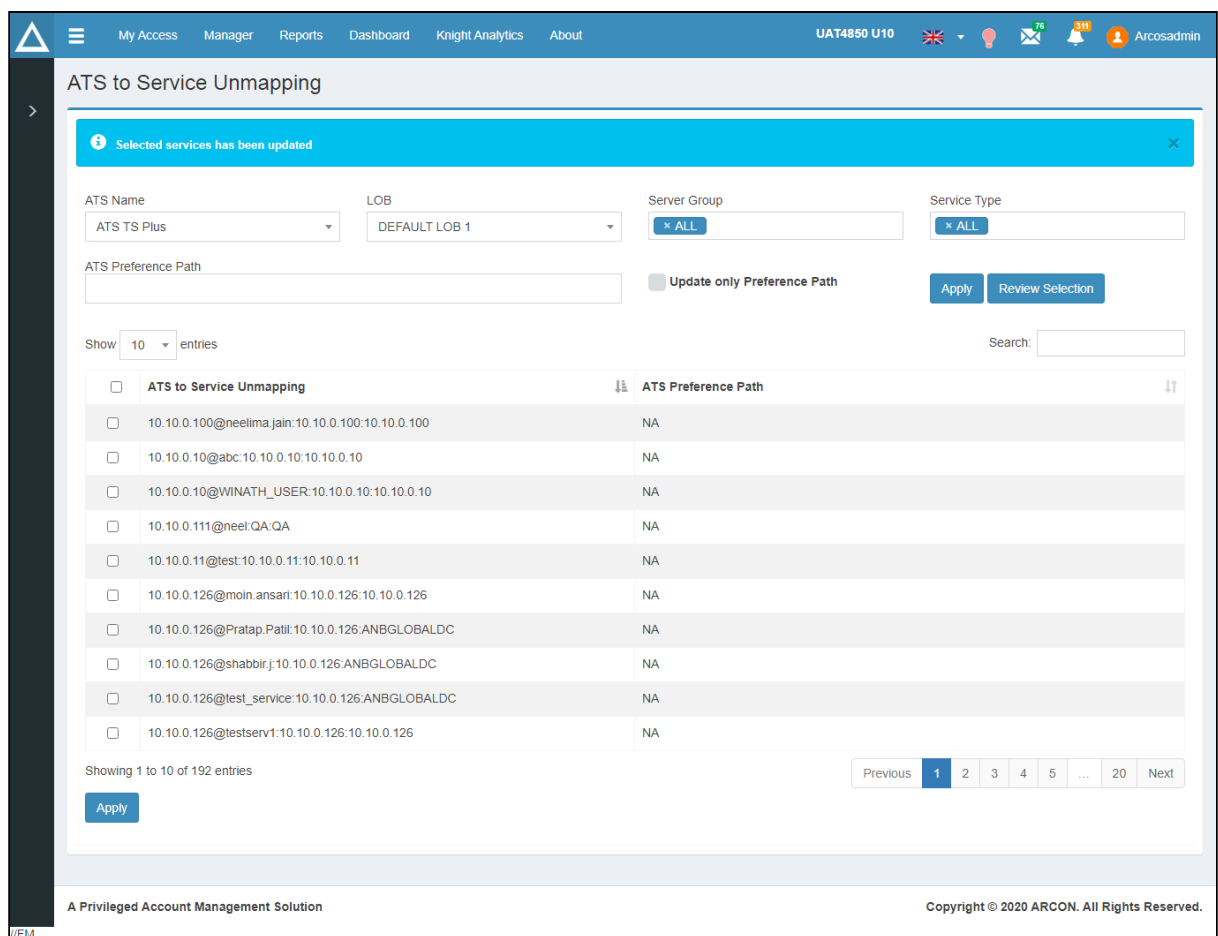
1. Click AGW to Service Mapping



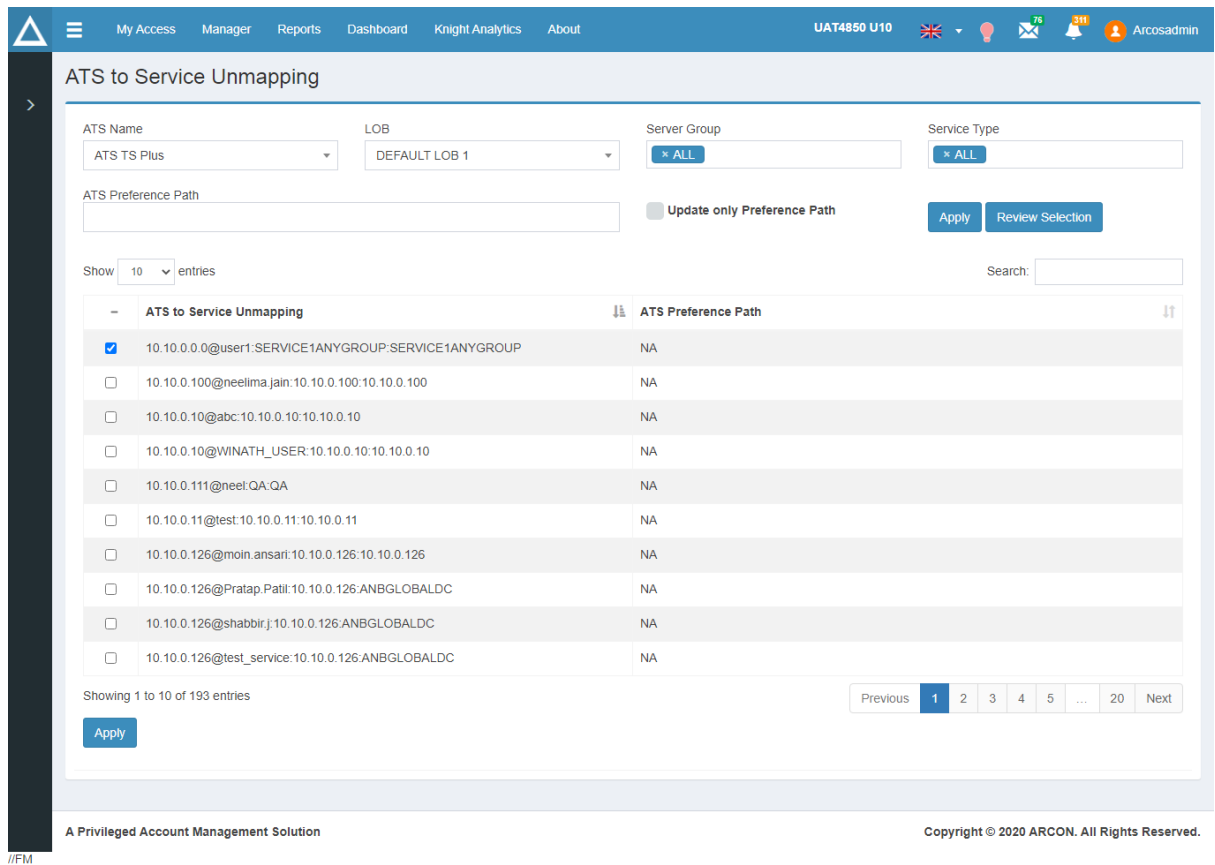
2. Select AGW Server Name, LOB, Server Group, Service Type, and AGW preference path.
3. On clicking **Use only AGW** checkbox, the connection for that service will **always** take place via **AGW**.
4. Click Apply to enable/ allow AGW for all the listed services.
5. A pop-up message will be displayed with the total number of services that will be mapped.



6. Click **Proceed** to continue with mapping all the services in the selected category with the AGW Server.
7. Click **Review Selection** and it will list all the services in the selected category and users can select the services for which AGW has to be enabled and click Apply.



8. A pop-up message will displayed with the total number of services that will be mapped.



ATS to Service Unmapping

ATS Name: LOB: Server Group: Service Type:

ATS Preference Path: ☐ Update only Preference Path

Show: entries Search:

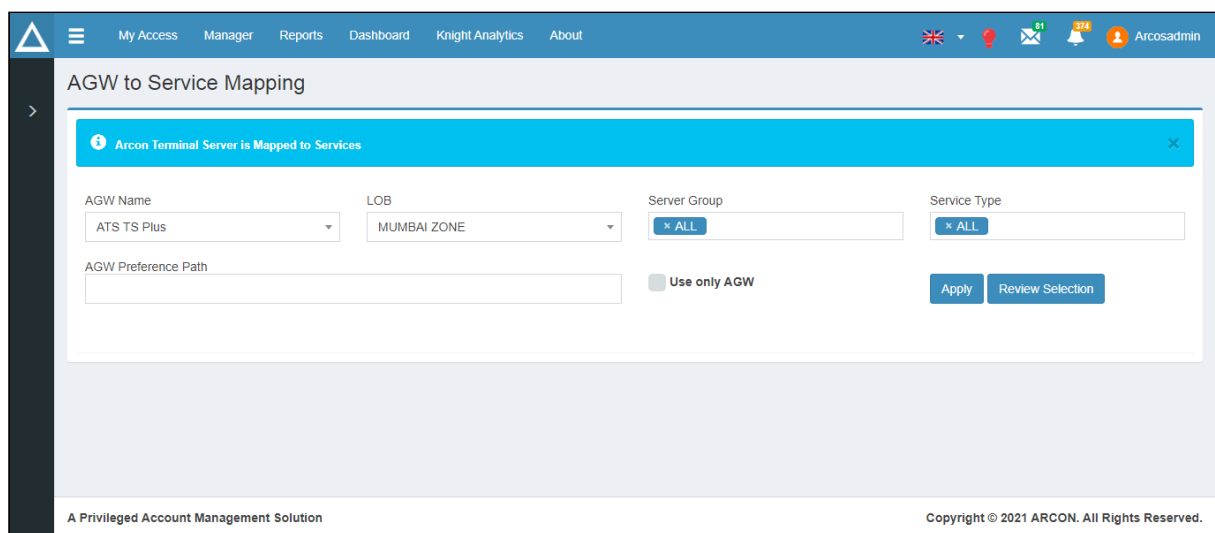
	ATS to Service Unmapping	ATS Preference Path
<input checked="" type="checkbox"/>	10.10.0.0.0@user1:SERVICE1ANYGROUP:SERVICE1ANYGROUP	NA
<input type="checkbox"/>	10.10.0.100@neelima.jain:10.10.0.100:10.10.0.100	NA
<input type="checkbox"/>	10.10.0.10@abc:10.10.0.10:10.10.0.10	NA
<input type="checkbox"/>	10.10.0.10@WINATH_USER:10.10.0.10:10.10.0.10	NA
<input type="checkbox"/>	10.10.0.111@neet:QA:QA	NA
<input type="checkbox"/>	10.10.0.11@test:10.10.0.11:10.10.0.11	NA
<input type="checkbox"/>	10.10.0.126@moin.ansari:10.10.0.126:10.10.0.126	NA
<input type="checkbox"/>	10.10.0.126@Pratap.Patil:10.10.0.126:ANBGLOALDC	NA
<input type="checkbox"/>	10.10.0.126@shabbir.j:10.10.0.126:ANBGLOALDC	NA
<input type="checkbox"/>	10.10.0.126@test_service:10.10.0.126:ANBGLOALDC	NA

Showing 1 to 10 of 193 entries Previous 1 2 3 4 5 ... 20 Next

A Privileged Account Management Solution Copyright © 2020 ARCON. All Rights Reserved.

9. Click Proceed to continue with the mapping process.

10. On successful mapping of AGW to the services, the following message will be displayed on the screen.



AGW to Service Mapping

Arcon Terminal Server is Mapped to Services

AGW Name: LOB: Server Group: Service Type:

AGW Preference Path: ☐ Use only AGW

A Privileged Account Management Solution Copyright © 2021 ARCON. All Rights Reserved.

6 Service Access using AGW

The process to use AGW, Select services and open the connection for the server are as follows:

1. Select My Services from the navigation bar on the left, the below screen will be displayed.

2. Select the **LOB** and **Service Type** from the drop-down list. It will list down all the services assigned to the user.

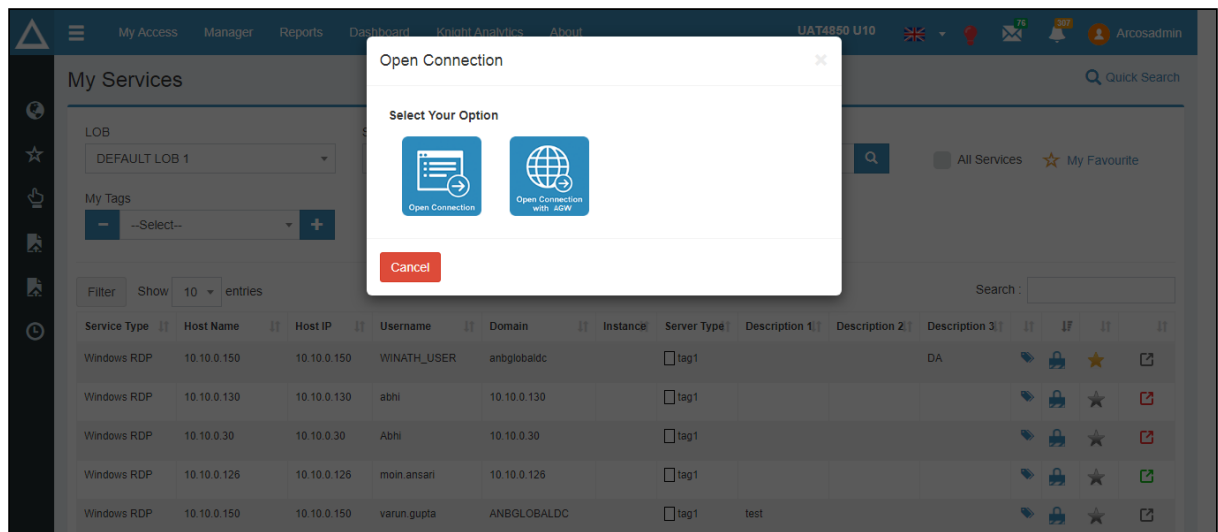


If the user knows the IP Address/Host Name, then the services will be displayed according to the IP address selected. However, according to the selected LOB, the IP address should be entered.

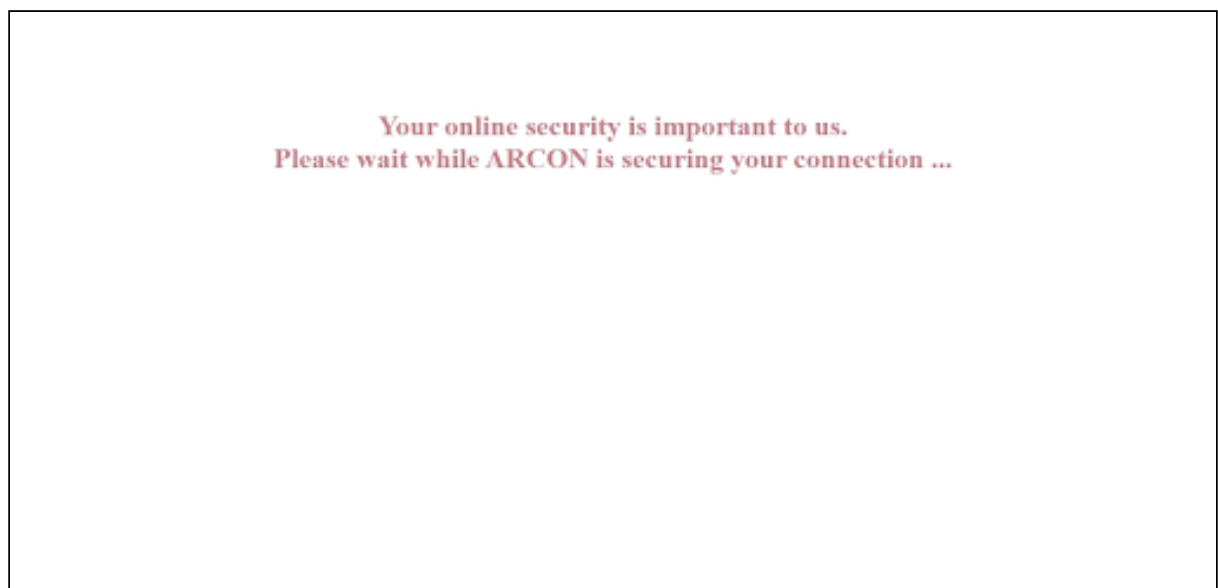
3. Check **ALL Services** checkbox, to display all the services that are assigned to the user.
4. User has two choices to make a connection. One is either via AGW and the other is the normal open connection. ARCON PAM supports Multiple sessions wherein a user can access multiple services at a time. All the sessions opened are recorded and stored in different files.



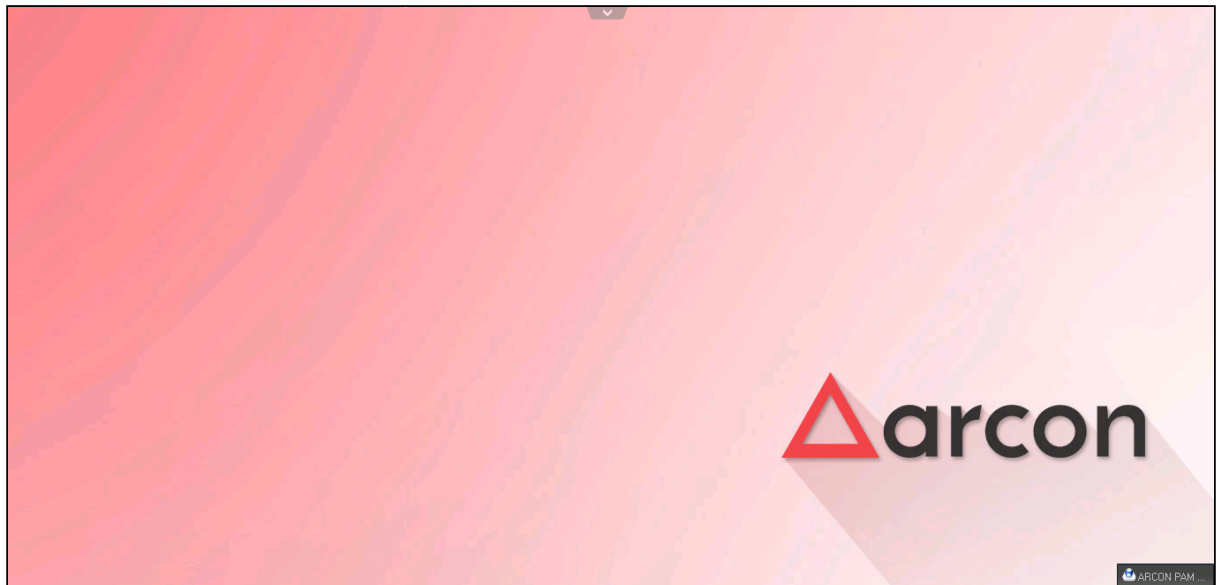
- If for a particular service AGW is not configured, User will not see have this open connection option. It will directly take a normal connection.
- If **Use only AGW** checkbox is selected on the **AGW to Service Mapping** the connection for that service will **always** take place via **AGW**. In this case, also, User will not see have this open connection option.



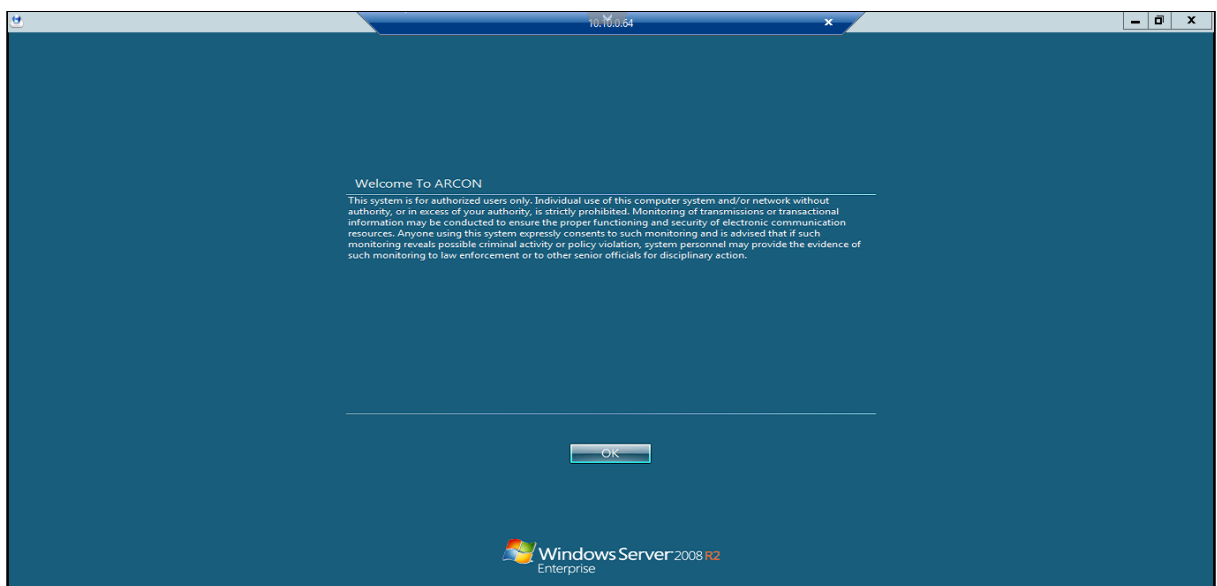
5. After selecting the **Open Terminal with AGW** option it will open a new tab in the browser, it will display a message while it loads: **Your Security is important to us. Please wait while ARCON is securing your connection.**



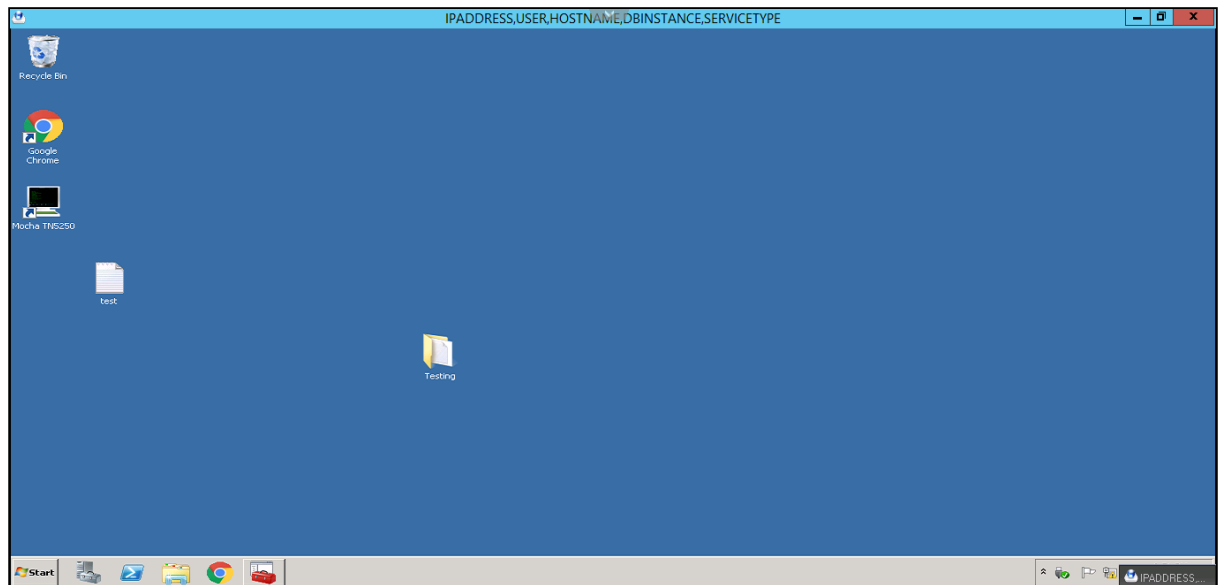
6. It will display the following screen while it loads and connects to the service.



7. It will later open the AGW and display the welcome message.



8. The user will finally be able to gain remote access through the service after the connection has been established.



6.1 AGW to Service UnMapping

This option will allow users to unmap services to AGW servers so that AGW permissions are revoked for the particular services.

Configuration Description	Configuration Uri	User Name	Active	Use for Server Manager	Created On	Last Modified On	Edit	Delete
ANBGLOBALDC\jinit.mehta	https://10.10.0.174/?&extrahelper=&program=&server=	ANBGLOBALDC\jinit.mehta	Yes	Yes	12/12/2020 21:29:36	03/12/2021 17:37:30		
ATS TS Plus Creating for Password Change of ATS TS Plus Application	https://10.10.0.173/software/html5.html	arcosadmin	Yes	No	04/22/2020 10:52:19	03/08/2021 19:27:01		
test	http://11.11.23.777:7878	test	No	No	04/25/2020 21:44:59	06/23/2020 12:05:43		
Test SMT	http://11.11.11.11:8969	test	No	No	04/25/2020 21:43:05	06/23/2020 12:05:58		

Following are the steps for AGW to Service UnMapping:

1. Click AGW to Service UnMapping.

AGW to Service Unmapping

AGW Name: SELECT LOB: SELECT Server Group: x ALL Service Type: x ALL

Preference Path:

☐ Update only Preference Path

Apply Review Selection

A Privileged Account Management Solution Copyright © 2021 ARCON. All Rights Reserved.

2. Select AGW Server Name, LOB, Server Group and Service Type.
3. Click Apply to unmap AGW for all the listed services in the selected category.
4. A pop-up message will be displayed with the total number of services that will be unmapped.

Success

252 No. of services will be updated

Proceed

5. Click **Proceed** to continue with the unmapping process. On successful unmapping, it will display the message AGW server is unmapped to services.
6. Click **Review Selection** and it will list all the services in the selected category and users can select the services to be unmapped from the list and click Apply.

ATS to Service Unmapping

Selected services has been updated

ATS Name: ATS TS Plus | LOB: DEFAULT LOB 1 | Server Group: * ALL | Service Type: * ALL

ATS Preference Path: | Update only Preference Path: ☐

Apply | Review Selection

Show: 10 entries | Search:

	ATS to Service Unmapping	ATS Preference Path
<input type="checkbox"/>	10.10.0.100@neelima.jain:10.10.0.100:10.10.0.100	NA
<input type="checkbox"/>	10.10.0.10@abc:10.10.0.10:10.10.0.10	NA
<input type="checkbox"/>	10.10.0.10@WINATH_USER:10.10.0.10:10.10.0.10	NA
<input type="checkbox"/>	10.10.0.111@neel:QA:QA	NA
<input type="checkbox"/>	10.10.0.11@test:10.10.0.11:10.10.0.11	NA
<input type="checkbox"/>	10.10.0.126@moin.ansari:10.10.0.126:10.10.0.126	NA
<input type="checkbox"/>	10.10.0.126@Pratap.Patil:10.10.0.126:ANBGLOBALDC	NA
<input type="checkbox"/>	10.10.0.126@shabbir.j:10.10.0.126:ANBGLOBALDC	NA
<input type="checkbox"/>	10.10.0.126@test_service:10.10.0.126:ANBGLOBALDC	NA
<input type="checkbox"/>	10.10.0.126@testserv1:10.10.0.126:10.10.0.126	NA

Showing 1 to 10 of 192 entries | Previous | 1 | 2 | 3 | 4 | 5 | ... | 20 | Next

Apply

A Privileged Account Management Solution | Copyright © 2020 ARCON. All Rights Reserved.

7. A pop-up message will be displayed with the total number of services that will be unmapped.

Success

252 No. of services will be updated

Proceed

8. Click Proceed to continue with the unmapping process. On successful unmapping, a message will be displayed Application Gateway Server is unmapped to Servers.

My Access

Manager

Reports

Dashboard

Knight Analytics

About

81

274

Arcosadmin

AGW to Service Unmapping

Selected services has been updated

AGW Name

LOB

Server Group

Service Type

Preference Path

Show

10

entries

ATS to Service Unmapping

Preference Path

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

Apply

ATS TS Plus

DEFAULT LOB 1

* ALL

* ALL

Update only Preference Path

Apply

Review Selection

Search:

A Privileged Account Management Solution

Copyright © 2021 ARCON. All Rights Reserved.



7 Application Path Settings over AGW

AGW Preference Path option will allow users to map the preferred path of the thick clients installed on the Application Gateway server. Enter all the below details and click Update.

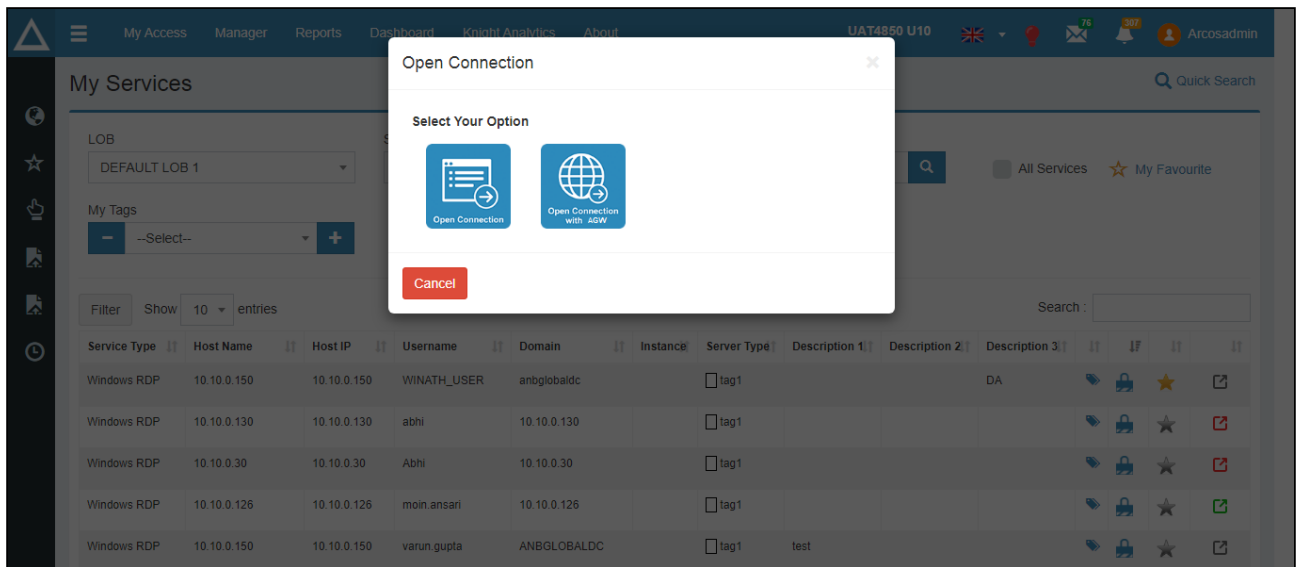
Field	Description
AGW Name	Name of the AGW Server
LOB	Select the LOB name from the drop-down
Service Type	Select the service type from the drop-down
Preference Path	Enter the integrated third-party application's exe path.

Final Connection

Once the above configurations are done, the user has two choices to make a connection. One is either via AGW and the other is a normal open connection. ARCON PAM supports Multiple sessions wherein a user can access multiple services at a time. All the sessions opened are recorded and stored in different files.

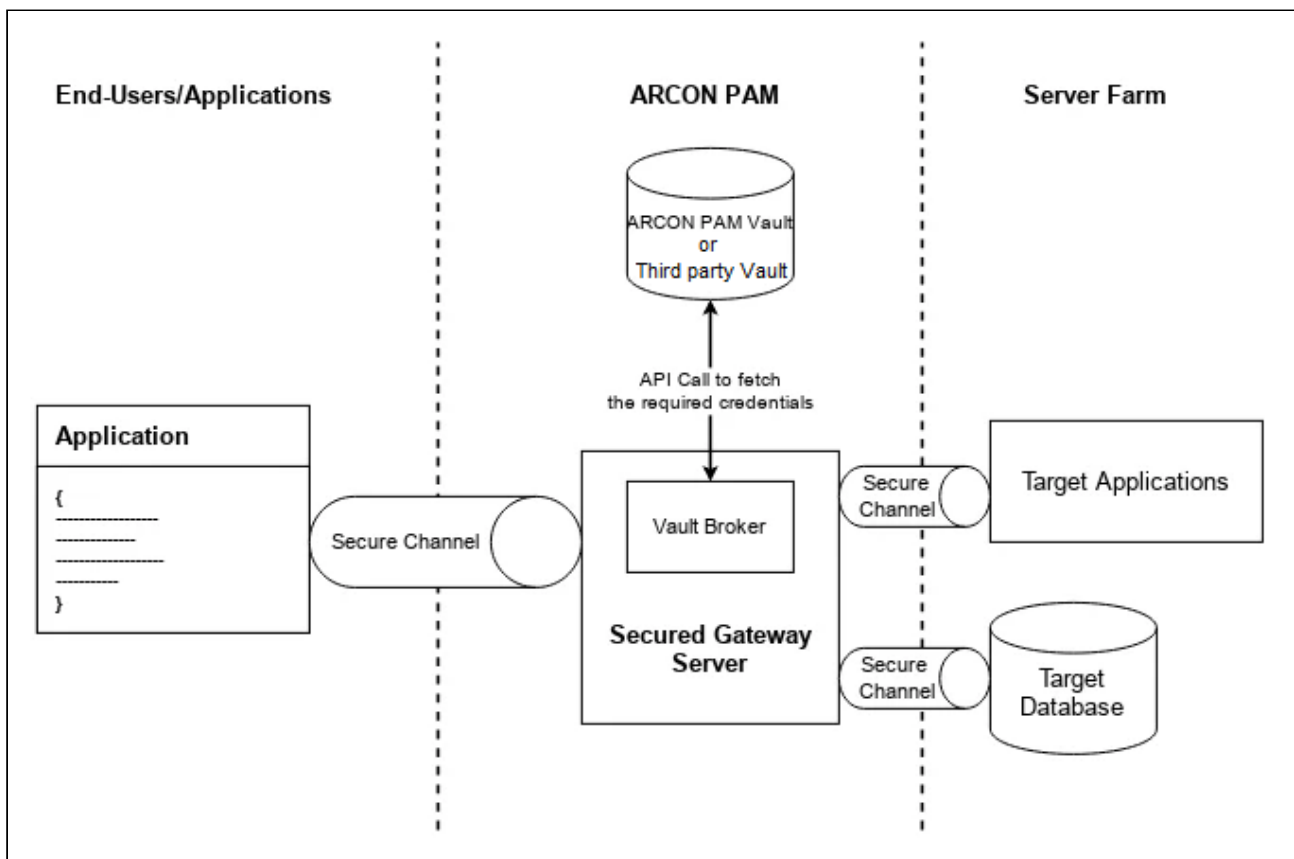


- If for a particular service AGW is not configured, User will not see have this open connection option. It will directly take a normal connection.
- If **Use only AGW** checkbox is selected on the **AGW to Service Mapping** the connection for that service will **always** take place via **AGW**. In this case, also, User will not see have this open connection option.



8 Vault Broker

Applications which require the privileged passwords and as well as channel to connect to the various systems. The channel request is mainly if the target applications are not able to make a direct connection to the target systems. ARCON PAM not only provides the privileged password through the "ARCON PAM Vault API" but also helps in creating a secured connection via the "Vault Broker" running on the ARCON PAM secured server to the target systems. The "Vault Broker" not only can securely connect to the ARCON PAM Vault but also third-party vaults. Moreover, it can act as a credential broker to third party secret store.



1. End-user/Applications web call to "Vault Broker" running on "ARCON PAM Secure Gateway Server"

GetServicePassword has 2 parameters which are as follows:

Parameter Name	Description
ARCONWebAPIURL	Web URL of ARCON Vault Broker.

Parameter Name	Description
ARCONSharedKey	<p>Shared Key / Identification No / Token / Certificate</p> <p>ARCON PAM Vault API incorporates authentication using a shared key generated using the Application Fingerprint, IP Address and MAC Address of the machine on which the application resides. This information must be registered inside ARCON PAM to securely access ARCON PAM Vault.</p> <p>This parameter indicates, the request coming from the End-User/ Application is from a valid server and can connect with ARCON PAM Vault via ARCON Application Server. Also, this parameter helps the ARCON PAM Vault to identify which password is requested by calling the application. This reduces the risk of knowing of application Privilege ID, Server IP Address and Database Instance (in case the password gets compromised outside of ARCON).</p> <p>ARCON PAM will enable SAML for certificate-based authentication. Any application that uses certificate-based authentication will have to login via their enterprise identity provider. ARCON PAM being the service provider will validate the certificate across the application user from the database and return a token with the refresh token. For further access to ARCON PAM Vault, this application can call using the access token returned after authentication.</p> <p>ARCON PAM has incorporated OAuth2.0 and OpenID Connect for JWT Token-based authentication. Applications that use JWT Token-based authentication will have to provide username and password in the request to generate a JWT Token and Refresh Token for accessing ARCON PAM Vault. Since the decoder of JWT token is available open-source ARCON PAM sends an encrypted token with a proprietary key which is decrypted when the application sends the request.</p>
Target Application	Specify the target application name.

2. Vault Broker calls to "ARCON PAM Vault API Online"

ARCON PAM Vault API Online - GetServicePassword has 9 parameters which are as follows:

Parameter Name	Description
ARCOSWebAPIURL	Web URL of ARCON PAM Vault API Online.
ARCOSSharedKey	Shared Key / Identification No / Token / Certificate
LOBProfile	Profile of Service
Server IP	IP Address of Server
ServiceType	Service Type of Server in ARCON PAM
UserName	Privilege ID of Server
DBInstanceName	Database Instance Name of Server

Parameter Name	Description
Target Application	Specifies the target application name.
IsUseCustomPort	Is Use Custom Port
CustomPort	Custom Port

Return data of **ARCON PAM Vault API Online** is an array of JSON string that contains the following 6 values.

- String [0] = Dynamic IP Address
- String [1] = Dynamic Port No.
- String [2] = Username
- String [3] = Password of the requested target application
- String [4] = Session ID
- String [5] = Other Configurations (Custom configurations as per the application's requirement)

3. End-User/Application Call to function "CloseARCONSecureServer"

CloseARCOSGateway has 1 parameter which is as follows:

Parameter Name	Description
pSessionID	Returned session ID by OpenARCONSecureServer function

ARCON PAM Vault API Online can be installed as a separate module on a different application server or on the ARCON PAM application server.

9 Session Collaboration

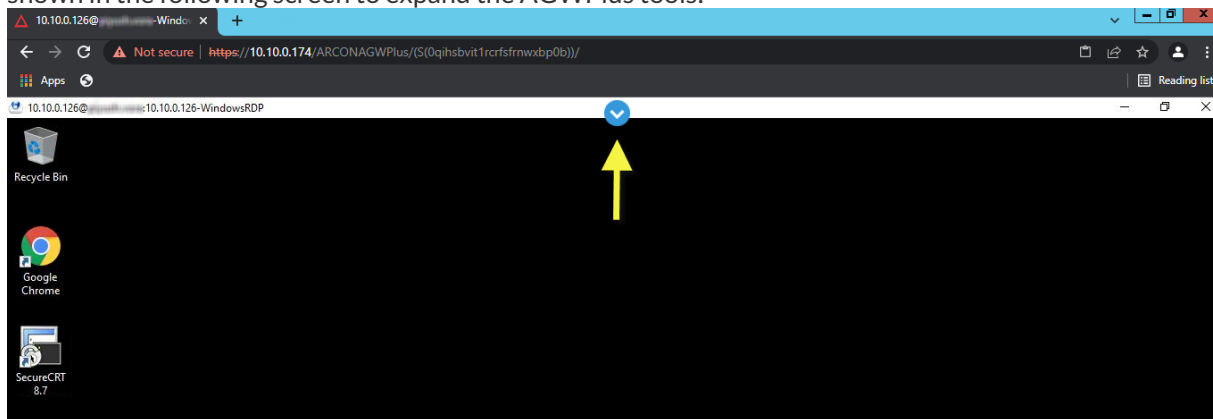
The **Session Collaboration** is a tool available in AGW Plus (Application Gateway Server), which helps the user to establish a session between two systems to provide remote access.

The user can generate a URL for Session Collaboration and send it to the endpoint user. This URL will be a one-time use, and it will be sent to the respective endpoint user's email ID. The endpoint user can browse the URL on the same network on a browser and access the AGW Plus session.

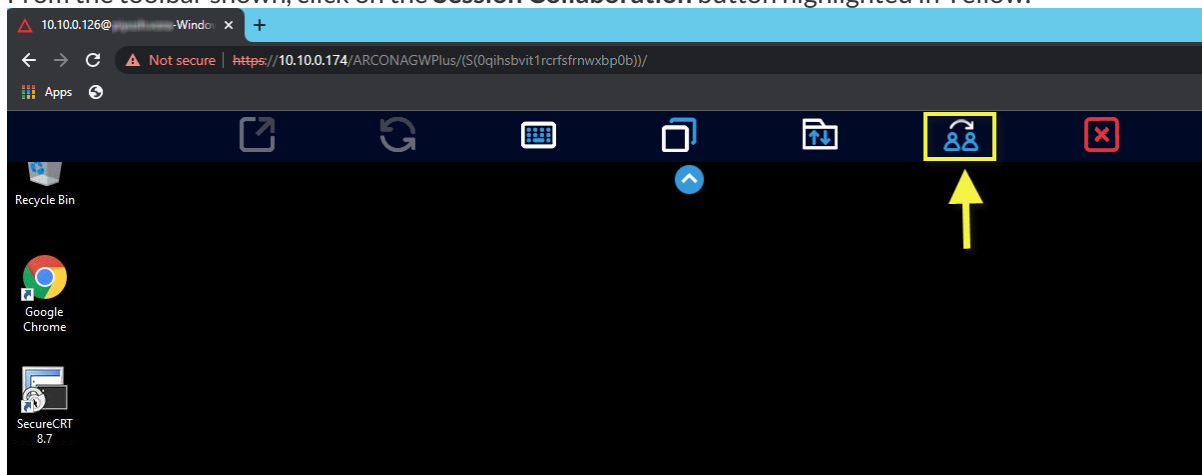
Once the session is established, the remote screen can be shared to the endpoint user in such a way that the endpoint user can view or even control the remote screen depending upon the privileges granted by the user (sender).

To initiate the Session Collaboration, user will need to perform the following steps:

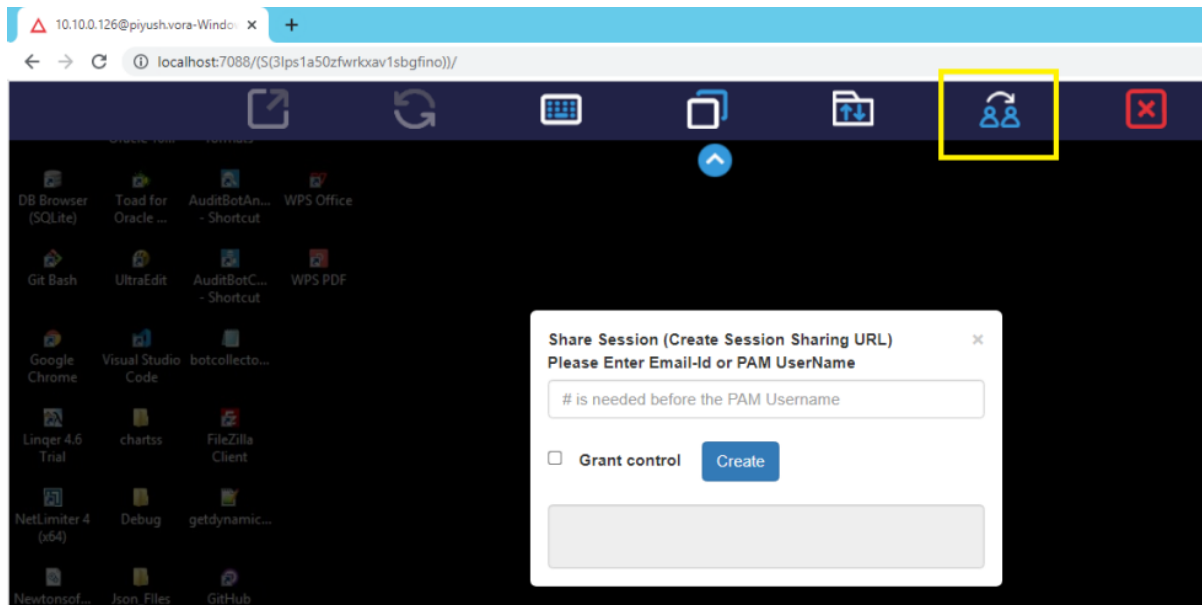
1. Considering the user has logged-in to the AGWPlus system, open the browser and click on the icon shown in the following screen to expand the AGWPlus tools:



2. From the toolbar shown, click on the **Session Collaboration** button highlighted in Yellow:



3. The Share Session pop-up will be displayed where user can specify the endpoint user details:



4. The user can either specify the endpoint user's PAM username or email ID. If the user wish to provide the endpoint user to control the remote session, user can tick the **Grant control** checkbox.
- a. If the user is specifying endpoint user's PAM username, it needs to be started with the hash (#) as shown in the following screen:

A screenshot of the "Share Session (Create Session Sharing URL)" modal. The text input field contains "#arcos.admin". A tooltip "Enter Email id or PAM Userid" is visible above the input field. The "Grant control" checkbox is checked, and the "Create" button is highlighted.

- b. If the user is specifying endpoint user's email ID, it will look like the following screen:

A screenshot of the "Share Session (Create Session Sharing URL)" modal. The text input field contains "jnit.mehta@arconnet.com". A tooltip "Enter Email id or PAM Userid" is visible above the input field. The "Grant control" checkbox is checked, and the "Create" button is highlighted.

- Once the endpoint user's details are entered, click on **Create** button. The email containing the session sharing URL will be sent to the endpoint user and the same confirmation message will be shown below the **Create** button:

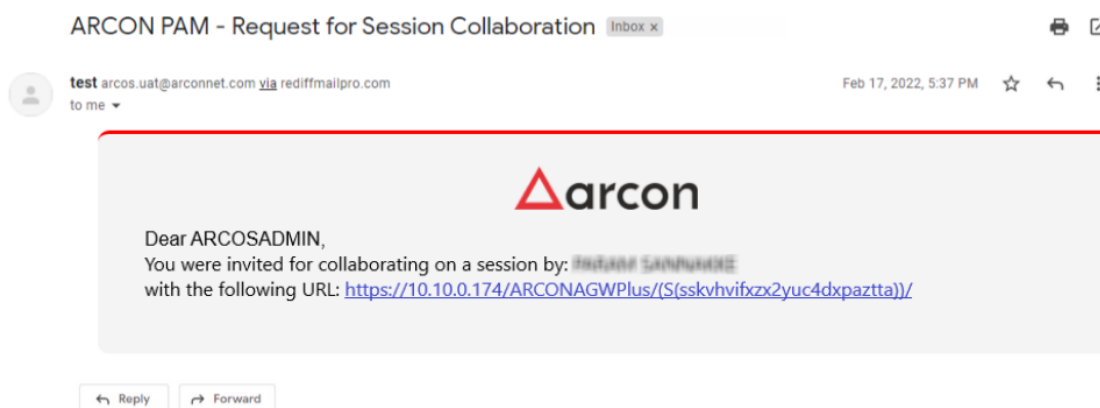
Share Session (Create Session Sharing URL) ×

Please Enter Email-Id or PAM UserName

☒ **Grant control** **Create**

Email containing the session sharing url was sent to the requested user

- The sample of email received from the endpoint user's side will look like the following:



- Once the endpoint user clicks on the URL given, the session will be established and remote connection screen will be shared between the user (sender) and the endpoint user (receiver).

10 Using AGW through PAM API

In this section, we will cover how user can access AGW (Application Gateway Server) through an external platform. This ARCON PAM functionality will help the user to connect to the target server without logging into PAM.

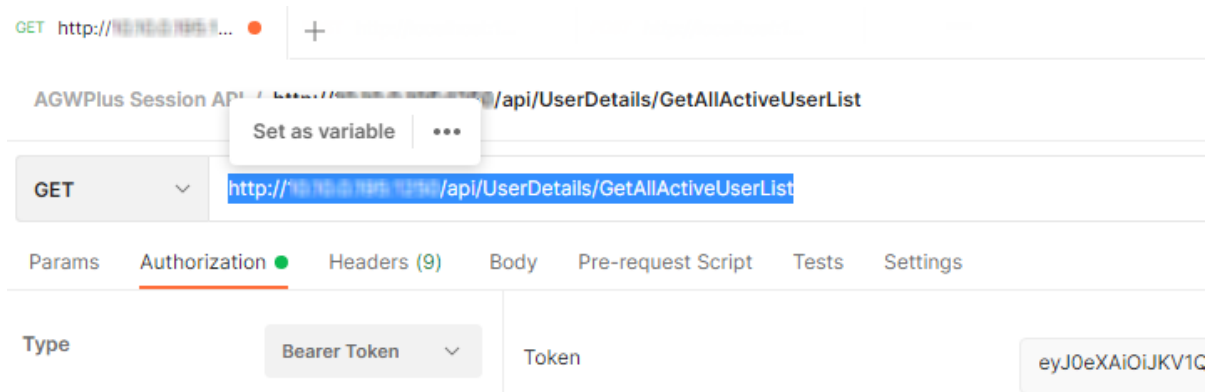
The end user can use their own ITSM portal to raise a ticket request, the request will go through the workflow process. Once the request is approved, a URL will be generated via ARCON PAM API. This URL will be one-time use and will be provided to the end user. The end user then can launch a session through this URL on any web browser in a controlled environment via ARCON PAM.

All the activities performed throughout this session will be recorded and stored as PAM Session Monitoring Capabilities.

10.1 Getting the User Details

To get the list of all the active users, follow the steps below:

1. Get the ARCOMPAM token generated.
2. The following API would be called to get the active users list from the ITSM tool or any third-party application with the token as authorization as bearer token:
http://ip-address:port/api/UserDetails/GetAllActiveUserList;
3. Replace **ip-address:port** with the desired API URL.
4. The sample for API call used in the POSTMAN is shown below:



5. Get the User ID of the user for which, the session needs to be established:

```

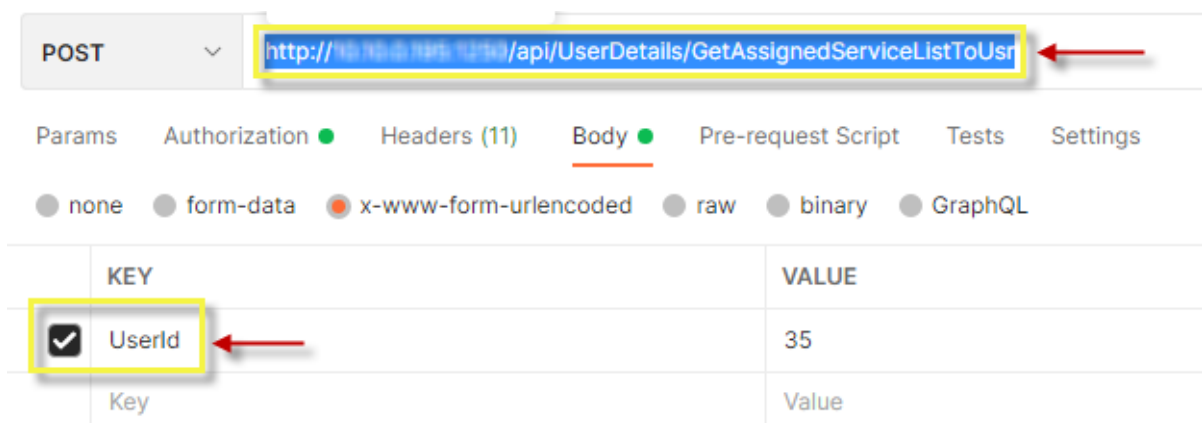
6      "ErrorCode": null,
7      "ErrorMessage": null,
8      "Message": "10494 Records Found",
9      "Result": [
10         {
11             "UserId": 35,
12             "UserName": "ARCOSADMIN",
13             "UserDisplayName": "ARCOSADMIN",
14             "DomainName": "ARCOSADMIN",
15             "ValidTill": "Jan 1 2025 11:59PM",
16             "ARCOSUserType": "Admin",
17             "Status": "Password Level OK",

```

10.2 Getting the Service Details of the User

Now, the User ID of the user has been received, the services details assigned to that respective user needs to be fetched. To get the list of all the service details of the respective user, the following POSTMAN Testing configuration will be required:

- Add the User ID of the user (received from the previous API response) in the body of the request, and hit the following API to get the service details of the specified user ID from the ITSM tool or any third-party application with the token as authorization as bearer token:
http://ip-address:port/api/UserDetails/GetAssignedServiceListToUser
- The sample output for API call in POSTMAN is shown as follows:



- Once the list of services have been fetched, get the Service ID of the service that is mapped to AGW in PAM:

Body Cookies (1) Headers (3) Test Results Statu

Pretty Raw Preview Visualize JSON 150

```

17      "ServiceDomain": "ANBGLOBALDC"
18    },
19    {
20      "ServiceId": "114331",
21      "IpAddress": "10.10.0.10",
22      "HostName": "10.10.0.10",
23      "ServiceUserName": "PamServiceUser",
24      "Port": "3389",
25      "ServiceType": "Windows RDP",
26      "ServiceDomain": "ANBGLOBALDC"

```

- The combination of the UserID & the PAMServiceID from the previous API responses will be used to create a URL.
- Add the User ID & Pam Service ID in the body of the request and hit the following API to get the URL from the ITSM tool or any third-party application with the token as authorization as bearer token:
<http://ip-address:port/api/AGWPlus/GetConnectionURL>
- The sample output for API call in POSTMAN is shown as follows:

POST ▼ <http://10.10.0.10:3389/api/AGWPlus/GetConnectionURL>

Params Authorization ● Headers (11) Body ● Pre-request Script Tests Settings

● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL

KEY	VALUE
<input checked="" type="checkbox"/> PAMServiceID	114331
<input checked="" type="checkbox"/> UserID	35

- The result output will be displayed as follows:

```

{
  "Program": "ARCON PAM API",
  "Version": "1.0",
  "DateTime": "19/Jan/2022 05:29:54",
  "Success": true,
  "ErrorCode": null,
  "ErrorMessage": null,
  "Message": null,
  "Result": "https://10.10.0.10/ARCONAGWPlus/apicall/apicallsupport.aspx?&cuid=hNbPFM4NXEVzf4qiKD5WfQ%3d%3d"
}

```

10.3 Starting the Session

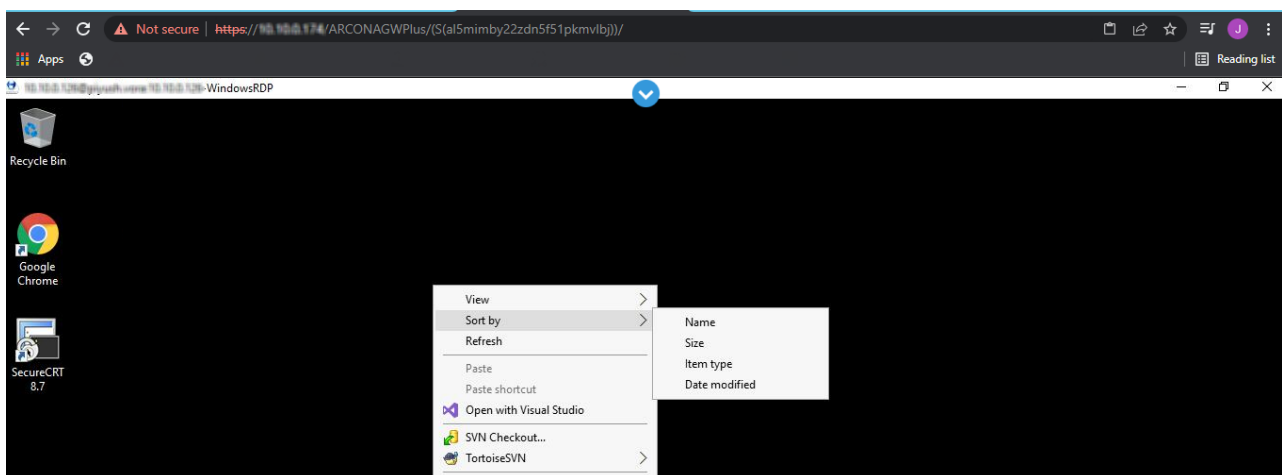
Once the result is fetched from the **GetConnectionURL** API, copy the URL from the result without the quotes and browse it:

```
1  "Program": "ARCON PAM API",  
   "Version": "1.0",  
   "DateTime": "2022/01/27 06:29:54",  
   "Success": true,  
   "ErrorCode": null,  
   "ErrorMessage": null,  
   "Message": null,  
   "Result": "https://10.10.10.174/ARCONAGWPlus/apicall/apicallsupport.aspx?&cuid=hNbPFM4NXEVzf4qiKD5WfQ%3d%3d"
```



If an ITSM tool is being used, this URL can be stored for future use for the same day.

The user will be able to take a connection to the target server as shown in the following screen:



Privileged Access Management Suite



No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means such as electronic, mechanical, photocopying, recording, or otherwise without permission.