

Remote Access Guide

Overview

This guide provides instructions on how to remotely access SSH, RDP, Web App and database resources via any standard web browser.

NOTE: If you need to use native clients, then please request native client support from your administrator.

Welcome to secure resource access portal

Access Portal URI: <MAMORI SERVER IP>

Access is authenticated via configured directory and multi-factor providers

This guide covers :

1. Pre-requisites
2. First time portal login – setup 2FA
3. RDP access
4. SSH access
5. Web App access
6. Secret access
7. Database Web SQL access

- Login credentials
- Mobile 2FA App

To follow this guide you will need the following items:

1. A Directory Account

If you don't have one, then contact your administrator.

2. Install the Mamori.io 2FA mobile application

iOS App Store: search for mamori 2FA

Android App Store: search for mamori.io

Note :

When you install the mobile application it will ask you to scan a QR code.
This login QR code is displayed the first time you login to the access portal.

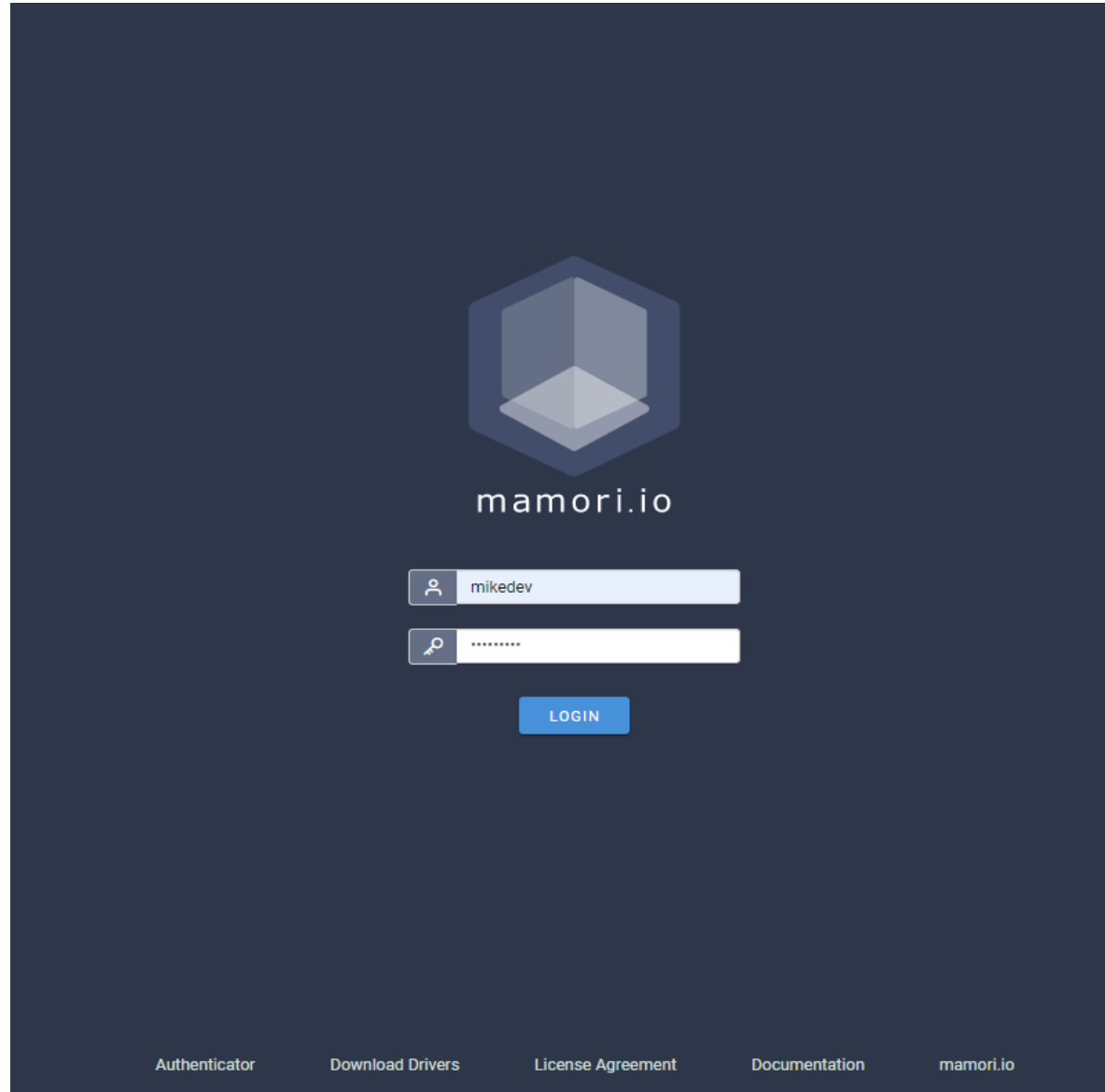
Login to <https://YOUR MAMORI SERVER/>
with your provided credentials

Remote Access Guide

Portal Login


Step 1/3

- 1. Login with your AD credentials**
2. Scan 2FA QR Code
3. Login with AD & 2FA



The screenshot shows the mamori.io login portal. At the top center is the mamori.io logo, a stylized hexagon with a 3D effect. Below the logo is the text "mamori.io". There are two input fields: the first is for the username, containing "mikedev", and the second is for the password, containing ".....". Below the input fields is a blue "LOGIN" button. At the bottom of the page, there are five links: "Authenticator", "Download Drivers", "License Agreement", "Documentation", and "mamori.io".

Scan the displayed QRCode with the mamori.io mobile app


mamori.io


This code will only be shown once.
Please make sure you scan it with your authenticator app on your phone.

Once you have scanned the code above with your authenticator app, click [here](#) to log in to Mamori.

Remote Access Guide

Portal Login

Step 2/3

1. Login with your AD credentials
- 2. Scan 2FA QR Code**
3. Login with AD & 2FA

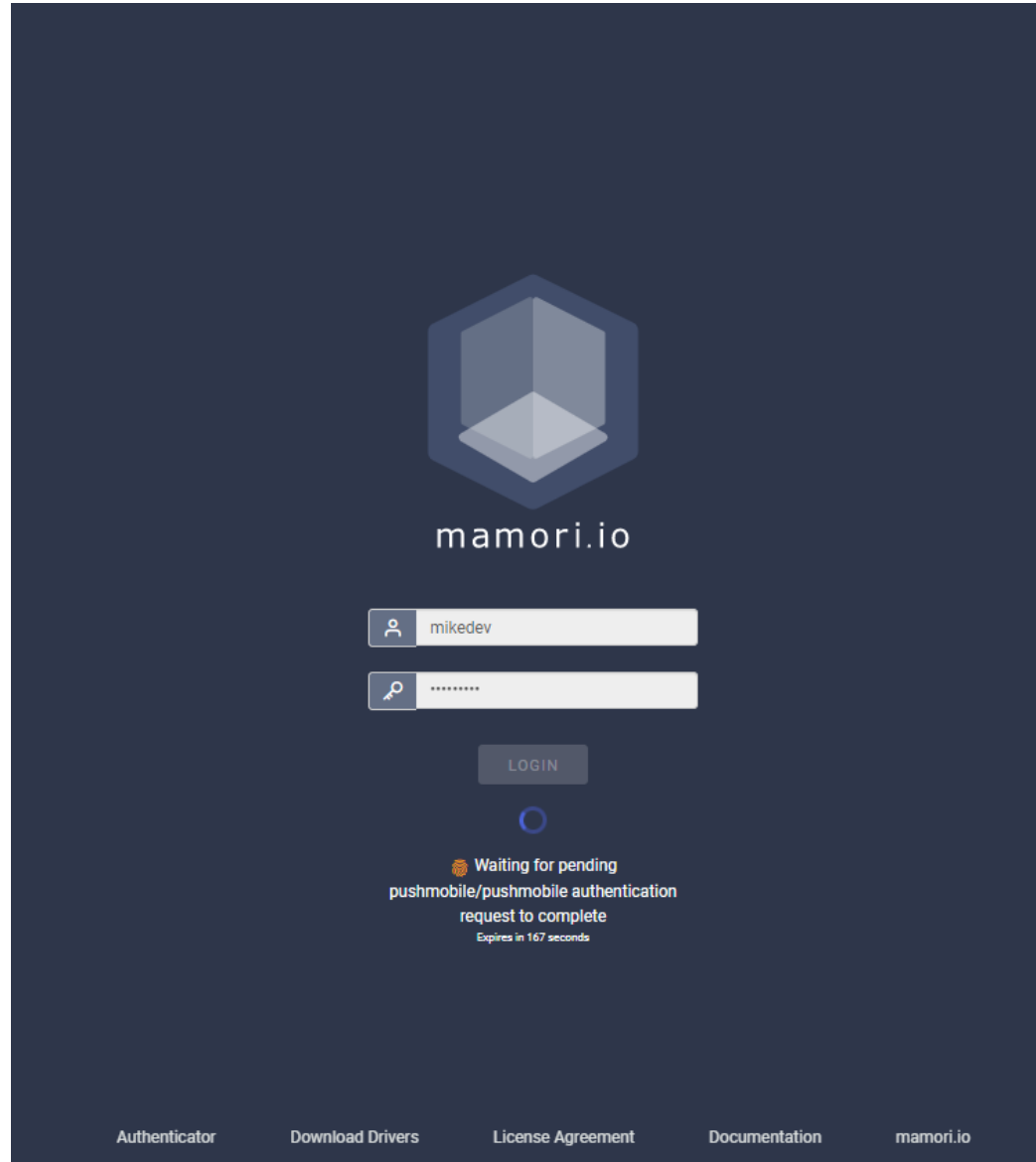
Login to [https:// YOUR MAMORI SERVER /](https://YOUR_MAMORI_SERVER/) again with your credentials and click **Accept** on the mobile app

Remote Access Guide

Portal Login

Step 3/3

1. Login with your AD credentials
2. Scan 2FA QR Code
- 3. Login with AD & 2FA**



The screenshot shows the mamori.io login interface. At the top center is the mamori.io logo, a stylized blue hexagon with a white cube inside. Below the logo is the text "mamori.io". There are two input fields: the first contains the username "mikedev" and the second contains masked characters "*****". Below the input fields is a "LOGIN" button. Underneath the button is a blue circular progress indicator and a message: "Waiting for pending pushmobile/pushmobile authentication request to complete Expires in 167 seconds". At the bottom of the page, there are five links: "Authenticator", "Download Drivers", "License Agreement", "Documentation", and "mamori.io".

You will need to do this for both production and DR servers.

Your 2FA and mobile device registration is complete.

Next steps in the guide are for connecting to

- **Remote Desktop**
- **SSH**
- **HTTP/S**
- **Secret**
- **Database WebSQL Access**

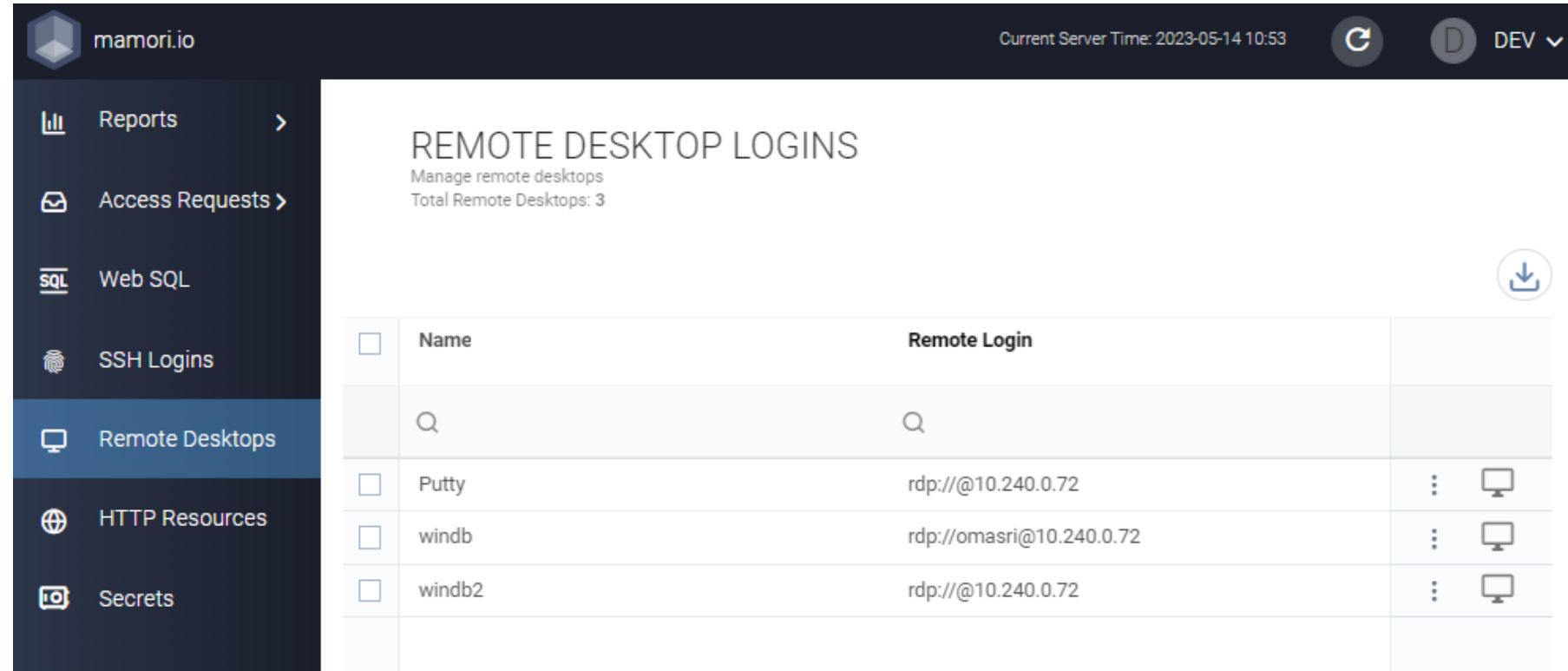
Click on Remote Desktops & Connect

If the connect button is not available, then click on request access.

Remote Access Guide

RDP Access

1. Login to the access portal
2. **Click on Remote Desktops & Connect** (you will be 2FA verified on every new RDP connection)



The screenshot shows the mamori.io dashboard. The top navigation bar includes the mamori.io logo, the current server time (2023-05-14 10:53), a refresh button, and a user profile icon labeled 'DEV'. The left sidebar contains a menu with the following items: Reports, Access Requests, Web SQL, SSH Logins, Remote Desktops (highlighted), HTTP Resources, and Secrets. The main content area is titled 'REMOTE DESKTOP LOGINS' and includes the subtitle 'Manage remote desktops' and 'Total Remote Desktops: 3'. A search bar is present above a table of remote desktops. The table has columns for 'Name' and 'Remote Login'. Each row includes a checkbox, the name, the remote login address, and a menu icon with a monitor symbol.

<input type="checkbox"/>	Name	Remote Login	
	Q	Q	
<input type="checkbox"/>	Putty	rdp://@10.240.0.72	:
<input type="checkbox"/>	windb	rdp://omasri@10.240.0.72	:
<input type="checkbox"/>	windb2	rdp://@10.240.0.72	:



mamori.io

Click on SSH Logins & Connect

If the connect button is not available, then click on request access.

Remote Access Guide

SSH Access

1. Login to the access portal
2. Launch the desired SSH server

<input type="checkbox"/>	Name	Remote Login	Private Key	
	Q	Q	Q	
<input type="checkbox"/>	app1_server	ssh://root@45.124.54.218	cluster_ecdsa	⋮
<input type="checkbox"/>	app1_server_02	ssh://developer@45.124.54.218		⋮
<input type="checkbox"/>	app1_server_03	ssh://45.124.54.218		⋮
<input type="checkbox"/>	elk	ssh://root@10.240.0.93	cluster_ecdsa	⋮
<input type="checkbox"/>	mserver	ssh://root@127.0.0.1	cluster_ecdsa	⋮

Remote Access Guide

Web APP Access

1. Login to the access portal
2. Launch the desired resource

Click on HTTP Resources & Connect

If the connect button is not available, then click on request access.



<input type="checkbox"/>	Name	Remote URL	Excluded from PAC	
	Q	Q	(All) <input type="checkbox"/>	
<input type="checkbox"/>	monitoring	https://demo.mamori.io/monitor	<input checked="" type="checkbox"/>	⋮
<input type="checkbox"/>	elk	http://10.240.0.93:5601/app/home#/	<input type="checkbox"/>	⋮
<input type="checkbox"/>	elkDNS	http://elk.sandbox:5601/app/home#/	<input type="checkbox"/>	⋮

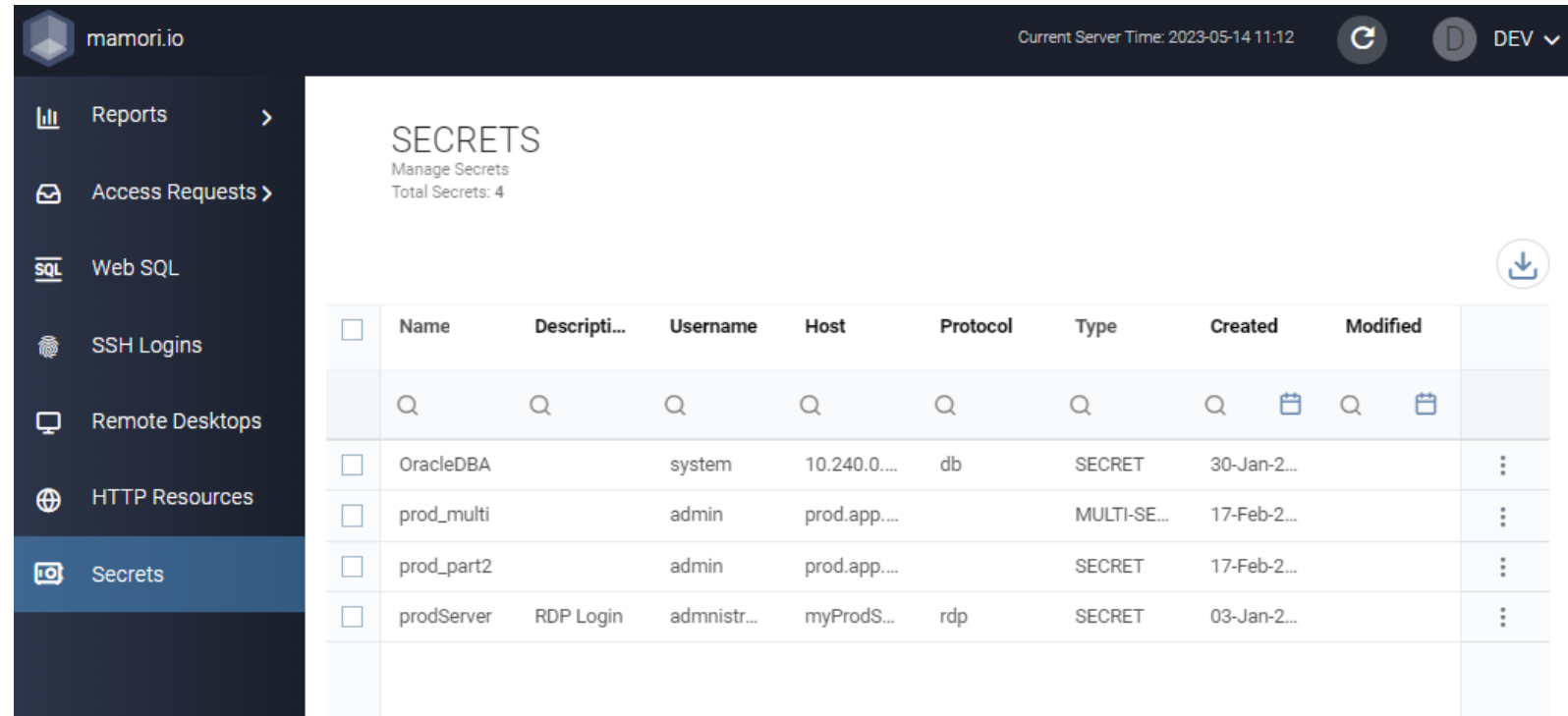
Click on Secrets & Reveal

If the reveal button is not available, then click on request access.

Remote Access Guide

Secret Access

1. Login to the access portal
2. Launch the desired SSH server



mamori.io Current Server Time: 2023-05-14 11:12 DEV

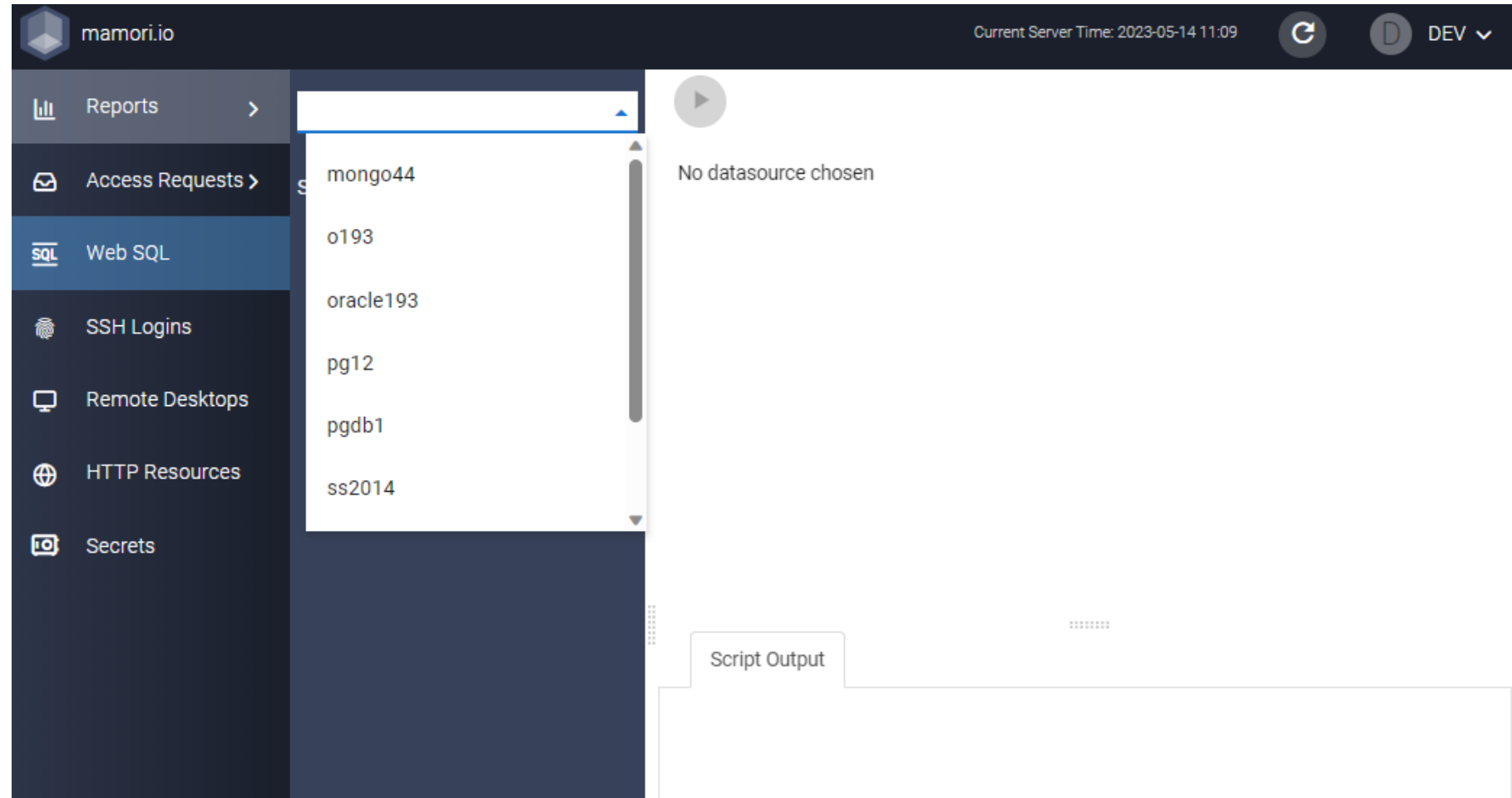
SECRETS

Manage Secrets
Total Secrets: 4

<input type="checkbox"/>	Name	Descripti...	Username	Host	Protocol	Type	Created	Modified	
<input type="checkbox"/>	OracleDBA		system	10.240.0...	db	SECRET	30-Jan-2...		⋮
<input type="checkbox"/>	prod_multi		admin	prod.app...		MULTI-SE...	17-Feb-2...		⋮
<input type="checkbox"/>	prod_part2		admin	prod.app...		SECRET	17-Feb-2...		⋮
<input type="checkbox"/>	prodServer	RDP Login	administr...	myProdS...	rdp	SECRET	03-Jan-2...		⋮

Click on Web SQL & Select Database

1. Login to the access portal
2. **Select the target database**
3. Run queries



The screenshot shows the mamori.io web interface. The top navigation bar includes the mamori.io logo, the current server time (2023-05-14 11:09), a refresh button, and a dropdown menu for the environment (DEV). The left sidebar contains several menu items: Reports, Access Requests, Web SQL (highlighted), SSH Logins, Remote Desktops, HTTP Resources, and Secrets. A dropdown menu is open under the 'Web SQL' item, displaying a list of databases: mongo44, o193, oracle193, pg12, pgdb1, and ss2014. The main content area shows a play button and the text 'No datasource chosen'. At the bottom, there is a 'Script Output' section with a dotted line indicating a scrollable area.

Enter Query and Click Run button

Remote Access Guide

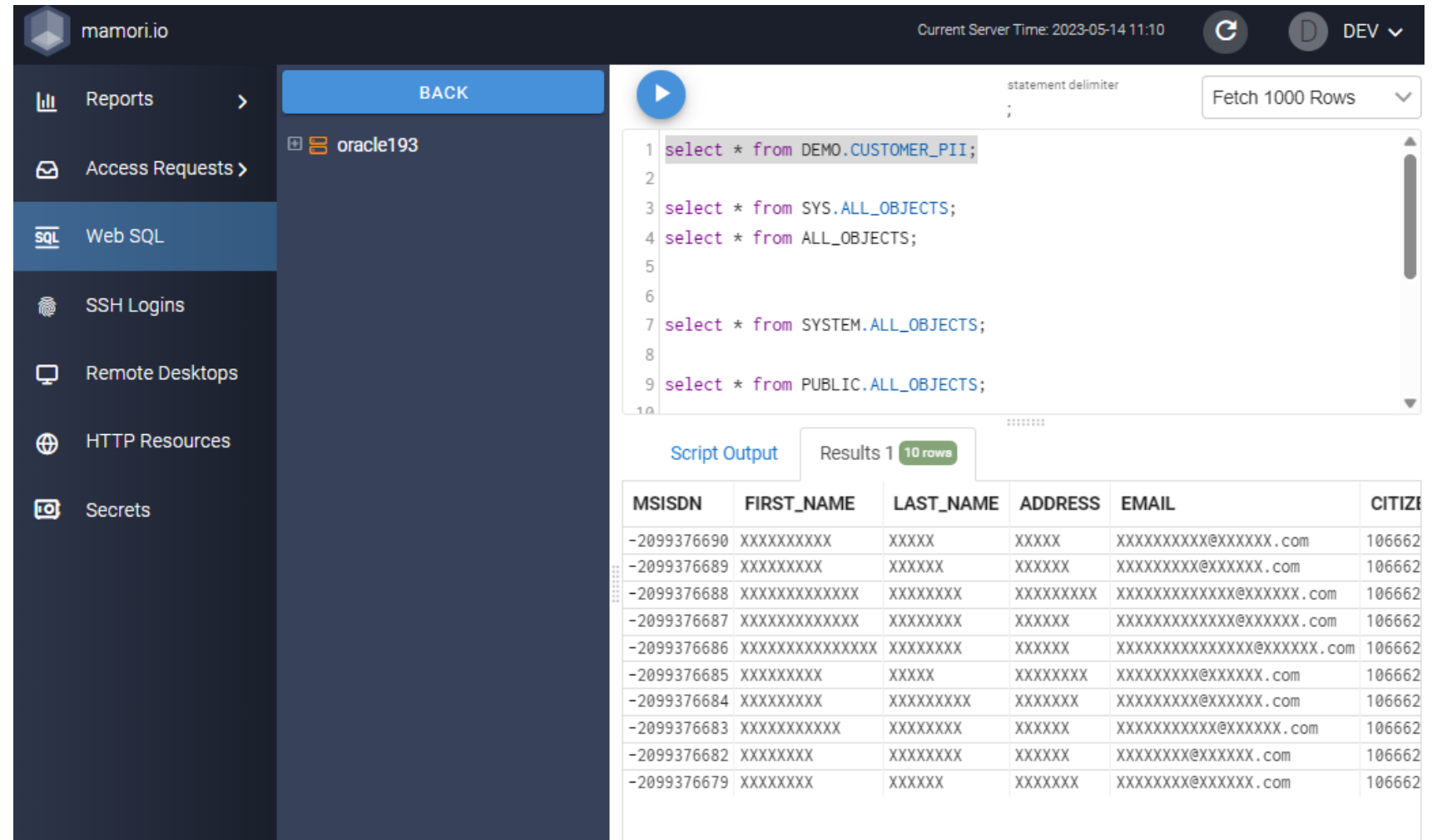
Database Access

Step 3/3

1. Login to the access portal
2. Select the target database
3. **Run queries**

Note:

Masking and encryption policies will apply



The screenshot shows the mamori.io interface for running SQL queries. The left sidebar contains navigation options: Reports, Access Requests, Web SQL (selected), SSH Logins, Remote Desktops, HTTP Resources, and Secrets. The main area shows a query editor with the following SQL code:

```
1 select * from DEMO.CUSTOMER_PII;  
2  
3 select * from SYS.ALL_OBJECTS;  
4 select * from ALL_OBJECTS;  
5  
6  
7 select * from SYSTEM.ALL_OBJECTS;  
8  
9 select * from PUBLIC.ALL_OBJECTS;  
10
```

Below the query editor, there are tabs for "Script Output" and "Results 1 10 rows". The "Results 1 10 rows" tab is active, displaying a table with the following columns: MSISDN, FIRST_NAME, LAST_NAME, ADDRESS, EMAIL, and CITIZENSHIP.

MSISDN	FIRST_NAME	LAST_NAME	ADDRESS	EMAIL	CITIZENSHIP
-2099376690	XXXXXXXXXX	XXXXX	XXXXX	XXXXXXXXXX@XXXXXX.com	106662
-2099376689	XXXXXXXXXX	XXXXX	XXXXX	XXXXXXXXXX@XXXXXX.com	106662
-2099376688	XXXXXXXXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXXXXXXXX@XXXXXX.com	106662
-2099376687	XXXXXXXXXXXXXX	XXXXXXXX	XXXXXX	XXXXXXXXXXXXXX@XXXXXX.com	106662
-2099376686	XXXXXXXXXXXXXXXX	XXXXXXXX	XXXXXX	XXXXXXXXXXXXXXXX@XXXXXX.com	106662
-2099376685	XXXXXXXXXX	XXXXX	XXXXXXXX	XXXXXXXXXX@XXXXXX.com	106662
-2099376684	XXXXXXXXXX	XXXXXXXX	XXXXXX	XXXXXXXXXX@XXXXXX.com	106662
-2099376683	XXXXXXXXXXXX	XXXXXXXX	XXXXXX	XXXXXXXXXXXX@XXXXXX.com	106662
-2099376682	XXXXXXXXXX	XXXXXXXX	XXXXXX	XXXXXXXXXX@XXXXXX.com	106662
-2099376679	XXXXXXXXXX	XXXXXX	XXXXXX	XXXXXXXXXX@XXXXXX.com	106662