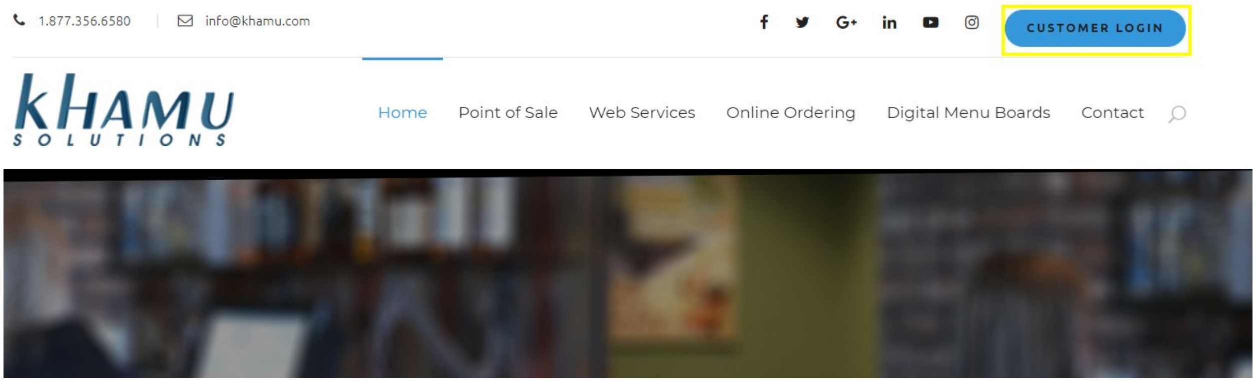
Connecting to Sapphire Remotely

This document reviews how to access your customer account, or K2 Dashboard, from Khamu.com. Once you've signed into your Dashboard, you are able to use the Sapphire Remote Access Portal to view your Sapphire Point of Sale from anywhere with the internet!

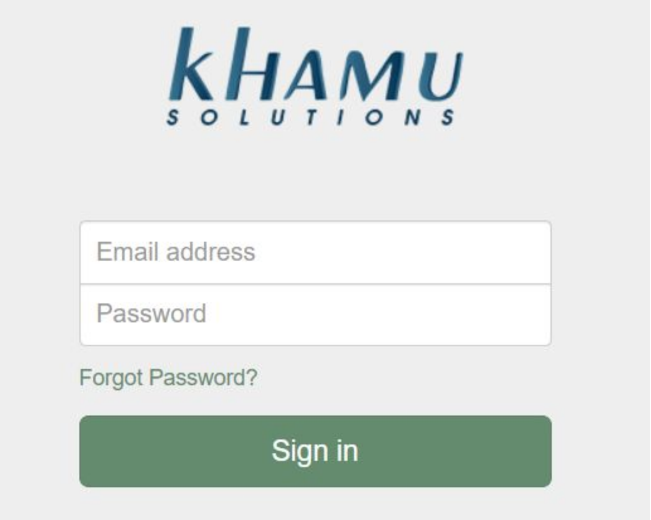
This document assumes that you have a K2 account created already. If you are needing an account set up, reach out to the Khamu Support at (877) 356-6580 or (208) 345-2250 to have one created.

Note: Business owners must give authorization to Khamu before adding additional remote access users

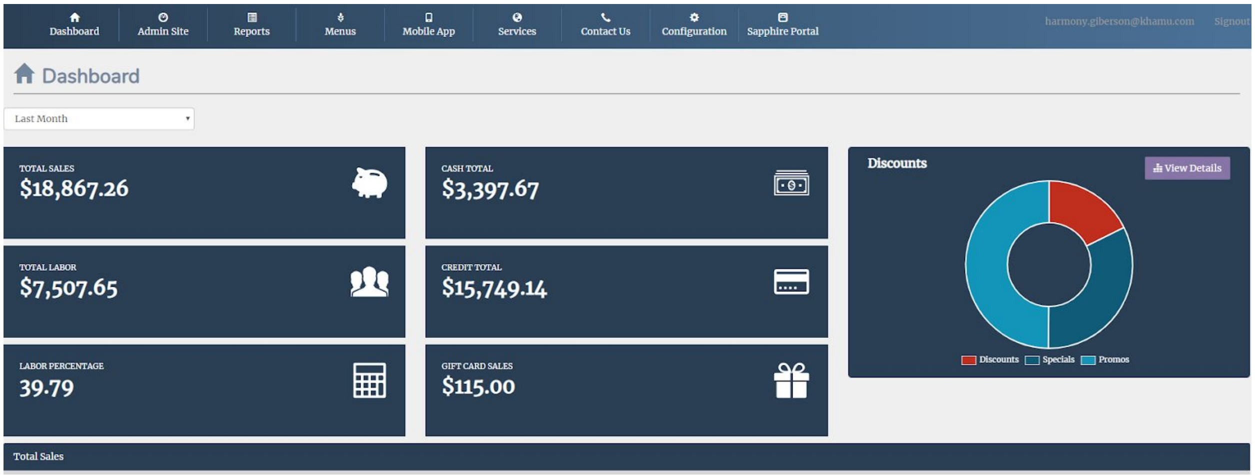
1. Use your internet browser to navigate to our website www.khamu.com. *Our support technicians recommend using Google Chrome, but it isn't a requirement.*
2. Once on our website, select **Customer Login**



3. Enter in your email and password to access the site.



4. Once you've signed in you will see your **K2 Dashboard** visible, this provides a snapshot of your business and is helpful for reporting while on the go.



Dashboard

Last Month

TOTAL SALES $18,867.26

CASH TOTAL $3,397.67

TOTAL LABOR $7,507.65

CREDIT TOTAL $15,749.14

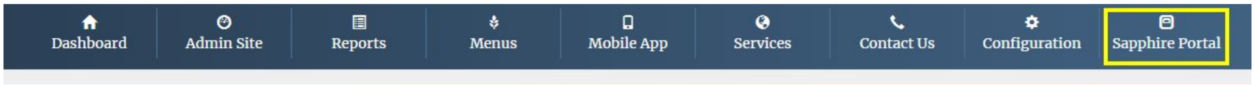
LABOR PERCENTAGE 39.79

GIFT CARD SALES $115.00

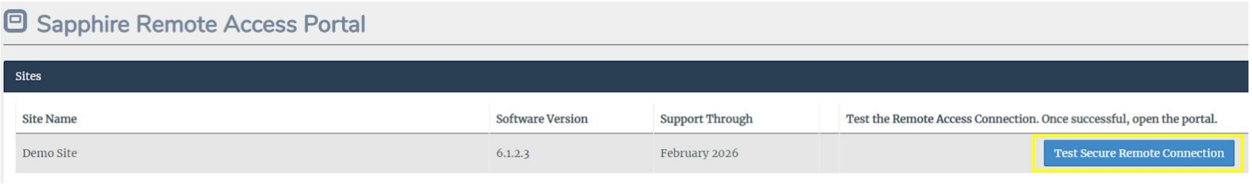
Discounts

Total Sales

5. To access the Remote Access Portal, navigate to the **Sapphire Portal** tab



6. All of your businesses should be displaying here, *if you are missing a location contact Khamu*
7. Select **Test Remote Connection** of the site you would like to view

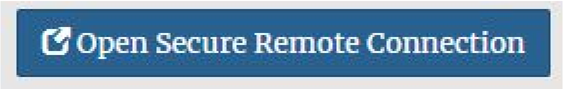


Sapphire Remote Access Portal

Sites

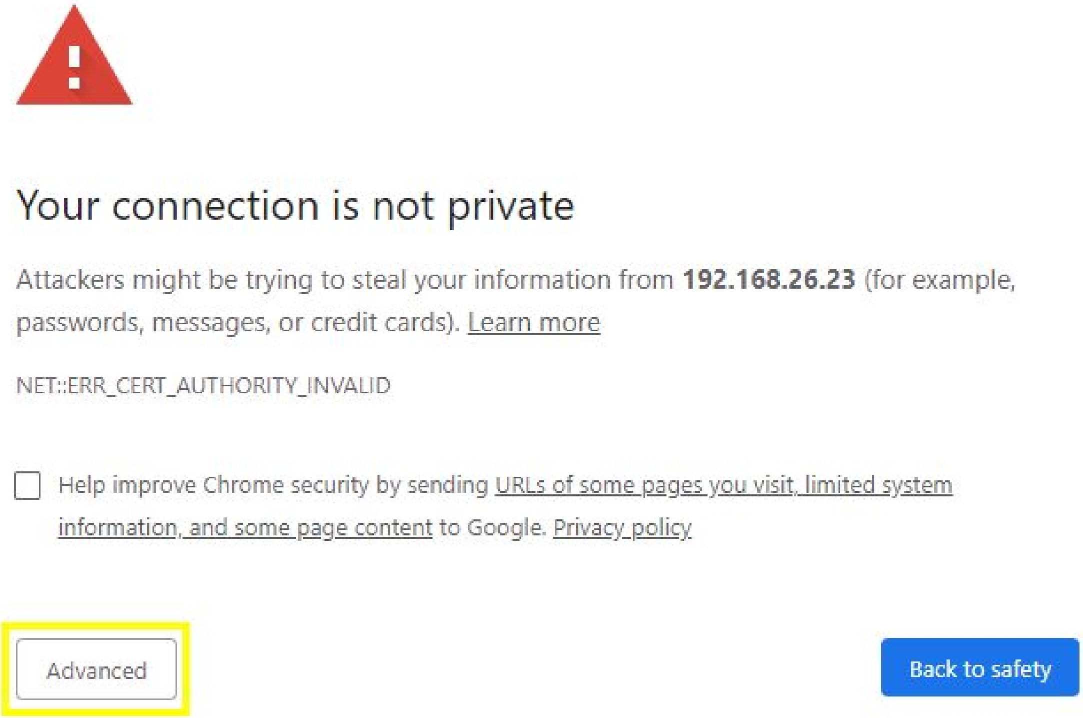
Site Name	Software Version	Support Through	Test the Remote Access Connection. Once successful, open the portal.
Demo Site	6.1.2.3	February 2026	Test Secure Remote Connection

8. Once the connection has been successfully tested, **Open Secure Remote Connection.** *If the Remote Access Portal is not able to open, contact Khamu Support for next steps*



9. You may be brought to a security warning screen, this is normal. Proceed through this. **Note: This varies from browser to browser. Here are the steps for the Chrome browser. See addendum at the end of this document for additional browser steps.*

10. Select Advanced to view more options



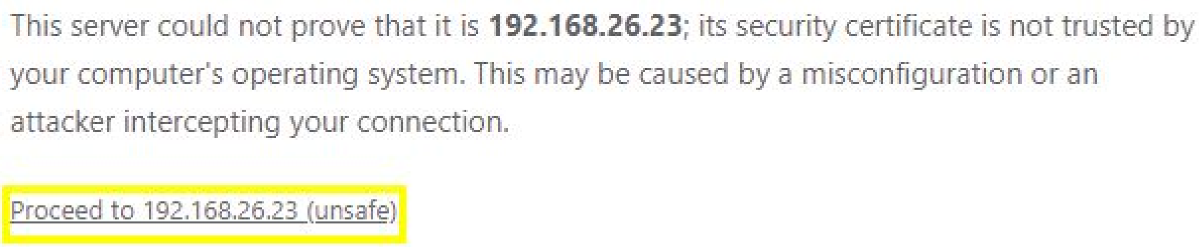
Your connection is not private

Attackers might be trying to steal your information from **192.168.26.23** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

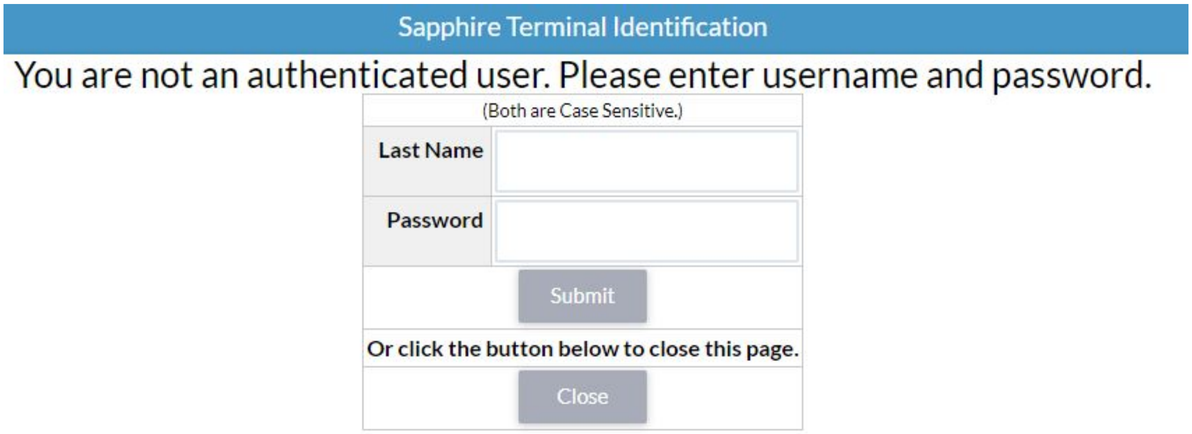
11. Select Proceed to continue to the next screen



This server could not prove that it is **192.168.26.23**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.26.23 (unsafe)

12. If this is the first time you have signed in, you may be brought to a “Sapphire Terminal Identification Screen.”



Sapphire Terminal Identification

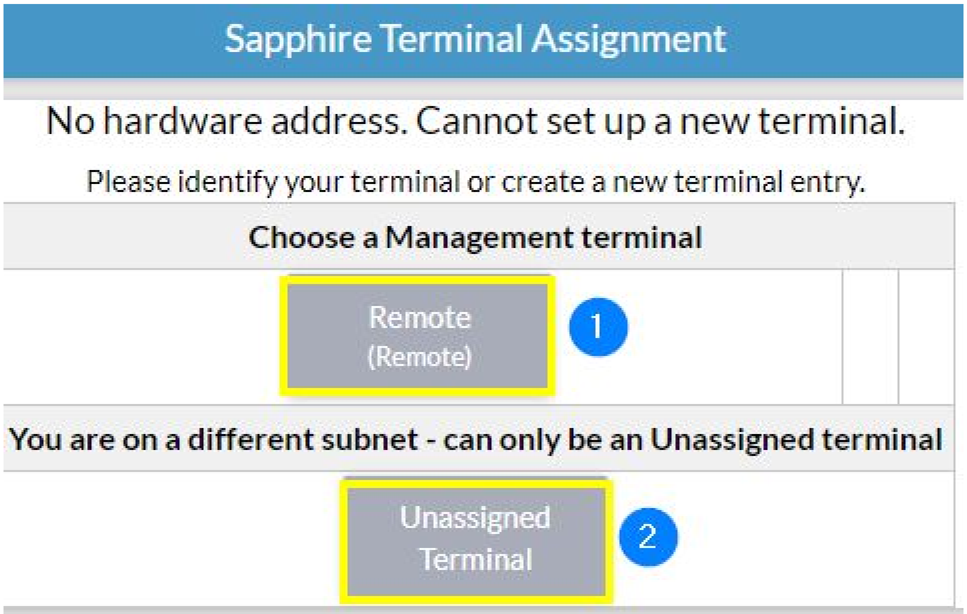
You are not an authenticated user. Please enter username and password.

(Both are Case Sensitive.)

Last Name	
Password	

Or click the button below to close this page.

13. Enter in your Last name and your manage system password. Your last name will need to be capitalized. **Note: If you don't have your last name added in Sapphire, use your first name*
14. Now select your terminal assignment, in most cases you are able to choose "Remote" if not, select "Unassigned Terminal"



Sapphire Terminal Assignment

No hardware address. Cannot set up a new terminal.

Please identify your terminal or create a new terminal entry.

Choose a Management terminal

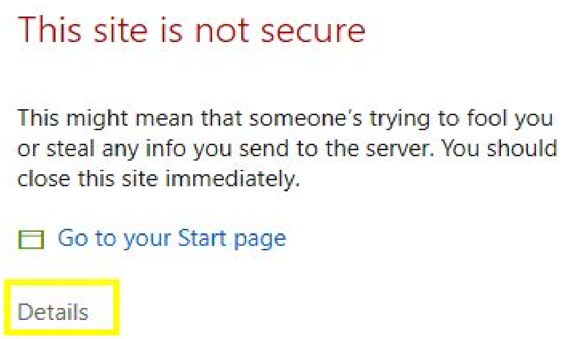
You are on a different subnet - can only be an Unassigned terminal

15. Enjoy using Sapphire in real time!

Additional Browser Security Screens

Microsoft Edge Browser:

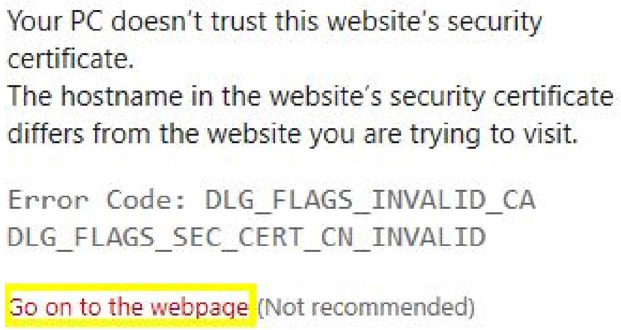
1. Select **Details**



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

2. Select **Go on to the webpage**

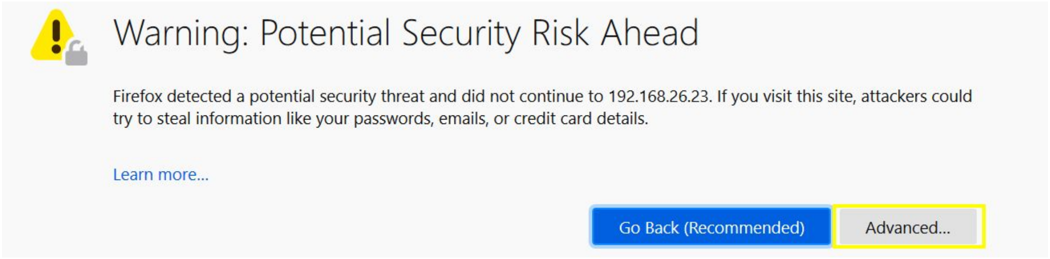


Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

Firefox:

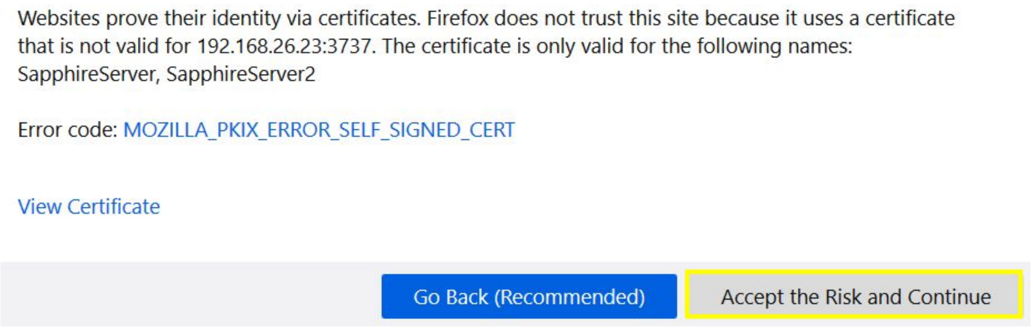
1. Select Advanced



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.26.23. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

2. Select Accept Risk and Continue



Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.26.23:3737. The certificate is only valid for the following names: SapphireServer, SapphireServer2

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT