

Suite Notaro SaaS – Accesso con verifica in due passaggi

Sommario

1. Premessa	2
2. Azioni propedeutiche al Login.....	2
2.1 Installazione Google Authenticator.....	2
2.2 Registrazione del dispositivo.....	3
3. Login con autenticazione a due fattori	7
4. Informazioni aggiuntive.....	9

1. Premessa

In materia di sicurezza informatica è richiesto che l'accesso alla scrivania di Suite Notaro SaaS avvenga tramite meccanismi di "strong authentication" per garantire la salvaguardia dei dati critici contenuti a livello applicativo. Tutti gli utenti dovranno autenticarsi in <https://suite.wki.it/> con doppia password: la prima è quella già in possesso dall'utente, la seconda sarà generata da un'autenticator app installata su Smartphone. Il presente manuale spiega come ottenere la seconda password ed eseguire il login.

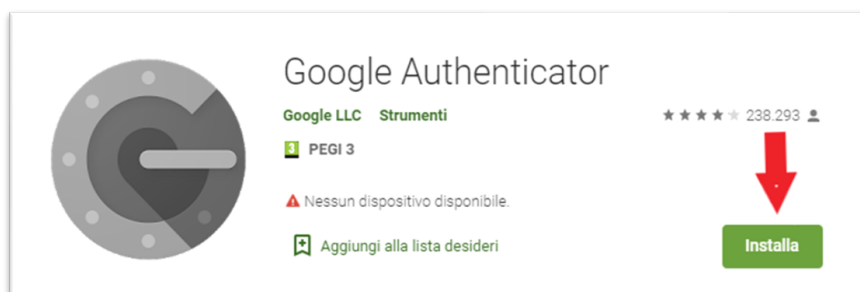
2. Azioni propedeutiche al Login

2.1 Installazione Google Authenticator

Il primo accesso mediante verifica in due passaggi, richiede l'installazione sul proprio smartphone dell'app **Google Authenticator**. Quest'app serve a generare il secondo codice di accesso.

Se si dispone già dell'app Google Authenticator, saltare il presente paragrafo e andare al paragrafo successivo 2.2.

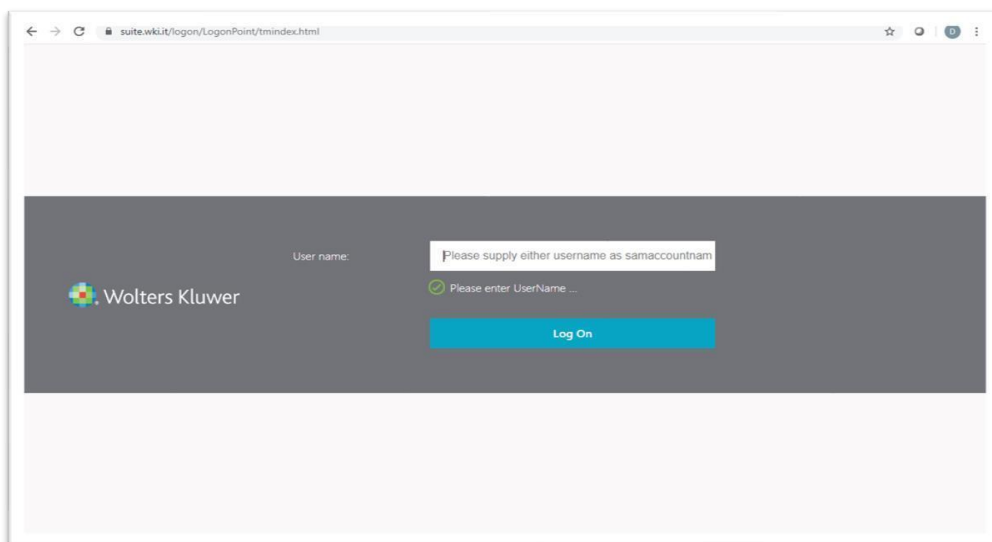
Per l'installazione dell'app sul proprio smartphone aprire lo store di riferimento, cercare "Google Authenticator" e cliccare su Installa.



Al termine dell'installazione l'app sarà disponibile sul proprio smartphone.

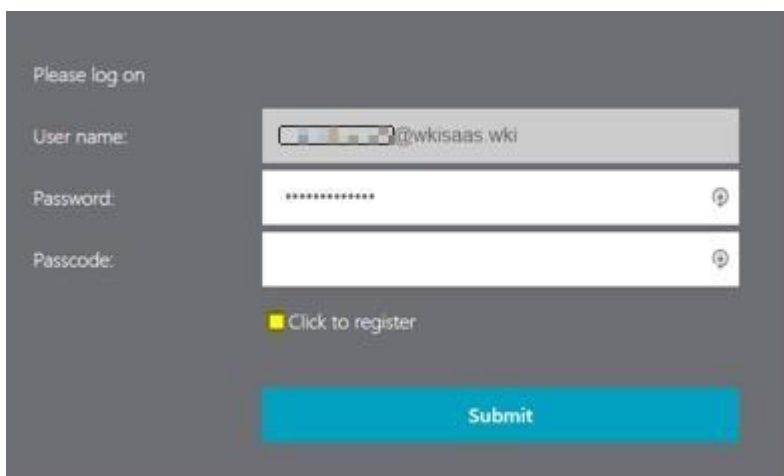
2.2 Registrazione del dispositivo

Lo smartphone da cui generare il codice di accesso va registrato. **Questa operazione va fatta solo una volta sul dispositivo smartphone dove è installata l' App Google Authenticator.** Accedere alla pagina di log on per Suite Notaro SaaS: <https://suite.wki.it/> Inserire la propria username (es. *abc.user01*) e cliccare su “Log on”:



Si rendono disponibili due campi ossia “Password” e “Passcode”.

Inserire nel campo “Password” la password che si inserisce abitualmente per effettuare l’accesso. Apporre il flag su “Click to register”:



Si attiva un nuovo campo chiamato “DeviceName”. Inserire qui una denominazione a propria scelta per identificare lo smartphone in cui è stata installata l’app **Google Authenticator** (esempio sotto: SmartphoneSamsung) e cliccare su “Submit”:

Please log on

User name:

Password:

Passcode:

DeviceName:

Click to register.

NB: Il flag va messo solo per registrare il proprio dispositivo. Una volta registrato il proprio dispositivo, il flag non sarà più apposto.

In caso di registrazione di un secondo dispositivo associato al medesimo account SaaS, scegliere un "DeviceName" diverso.

Dopo aver cliccato su "Submit" si apre la pagina che mostra un QR- Code da scansionare con l'App **Google Authenticator**:



Aprire l'app installata sullo smartphone che si sta registrando, tap sul pulsante "Avvia configurazione":



selezionare “Leggi codice a barre”:



e poi posizionare la fotocamera dello smartphone davanti al codice:

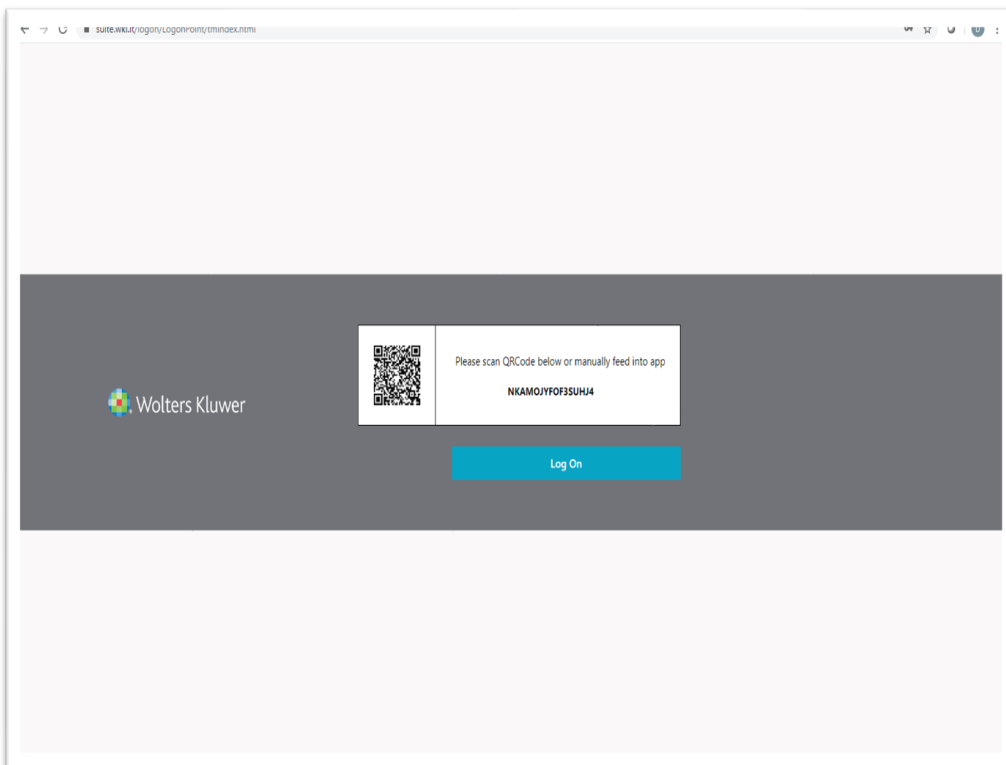


Al termine della scansione del QR- Code, l' App visualizza un codice di 6 cifre associato alla propria user name valido per 30 secondi (ogni 30 secondi ne genera uno nuovo):

Suite Notaro SaaS - Accesso con verifica in due passaggi



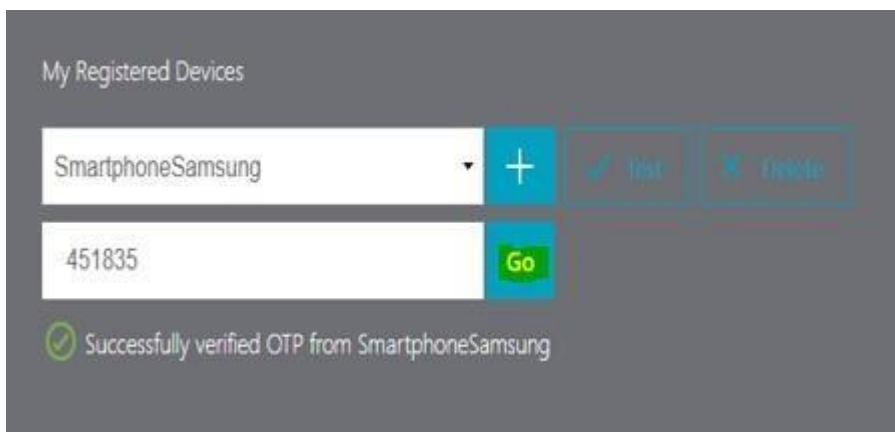
Per ultimare l'associazione, tornare sul PC e cliccare su "Log On":



Il sistema di autenticazione propone un test sulla corretta associazione del dispositivo. Dall'elenco a tendina selezionare il proprio "DeviceName" (es. SmartphoneSamsung), cliccare su "Test":



Inserire il codice presente a video dell'App su Smartphone "Google Authenticator" e confermare con "Go".



Il sistema riporta in verde il messaggio dell'avvenuta associazione. Eseguire il log off dalla pagina andando in alto a destra – menù a tendina – log off.



In caso di errore, inserire un nuovo codice generato dall' app su Smartphone e verificare di aver selezionato il DeviceName.

3. Login con autenticazione a due fattori

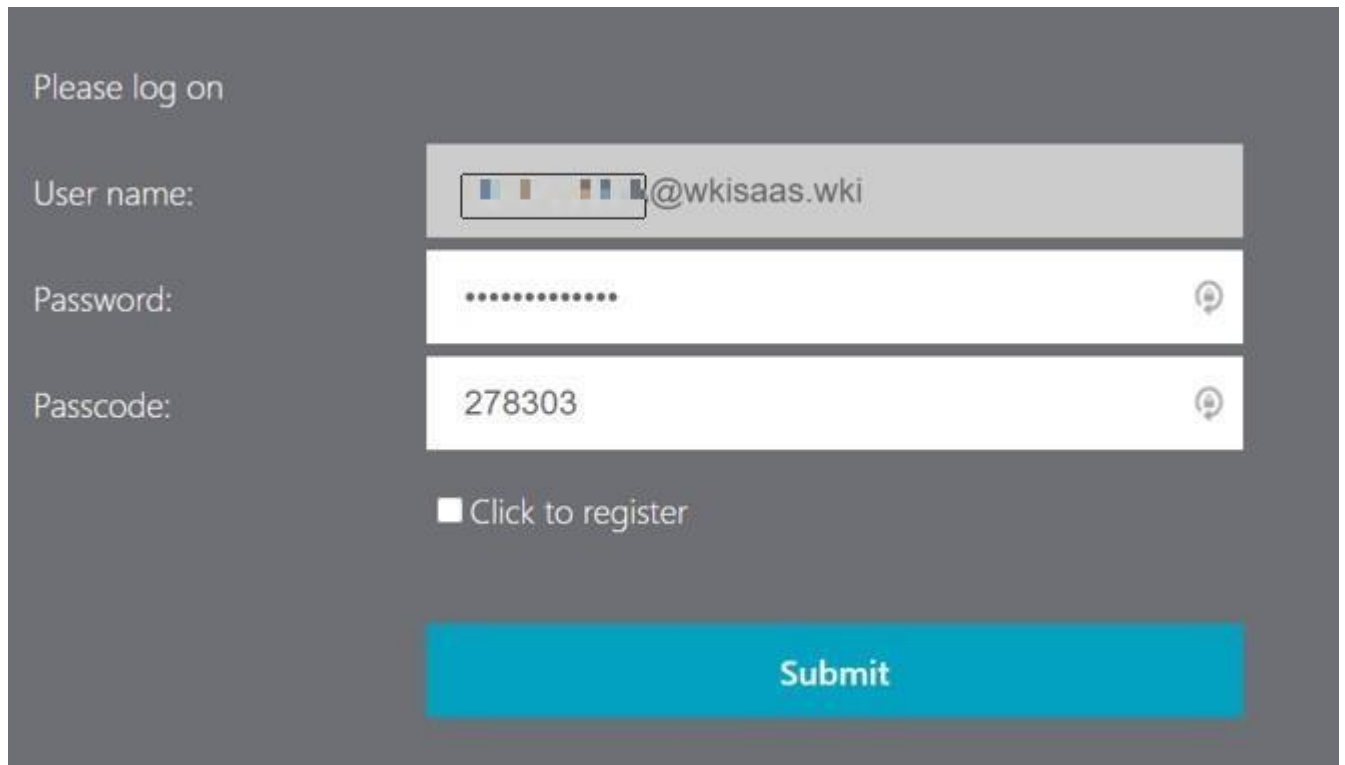
Dopo aver installato l'app ed eseguito la registrazione del proprio smartphone, è possibile procedere con l'autenticazione al sistema Suite Notaro SaaS.

Accedere alla pagina di log on per Suite Notaro SaaS: <https://suite.wki.it/> e inserire la propria user name e password.

Suite Notaro SaaS - Accesso con verifica in due passaggi

Nel campo "Passcode" inserire il codice generato dalla App **Google Authenticator**. Dunque, aprire l' App su Smartphone, visualizzare il codice di 6 cifre e tornare sul PC per inserirlo nell'apposito campo chiamato "Passcode".

Cliccare su "Submit" (senza selezionare la voce "click to register"):



Please log on

User name:

Password:

Passcode:

Click to register

Submit

A questo punto appare la possibilità di aprire la Scrivania e le applicazioni così come accade senza autenticazione a due fattori.

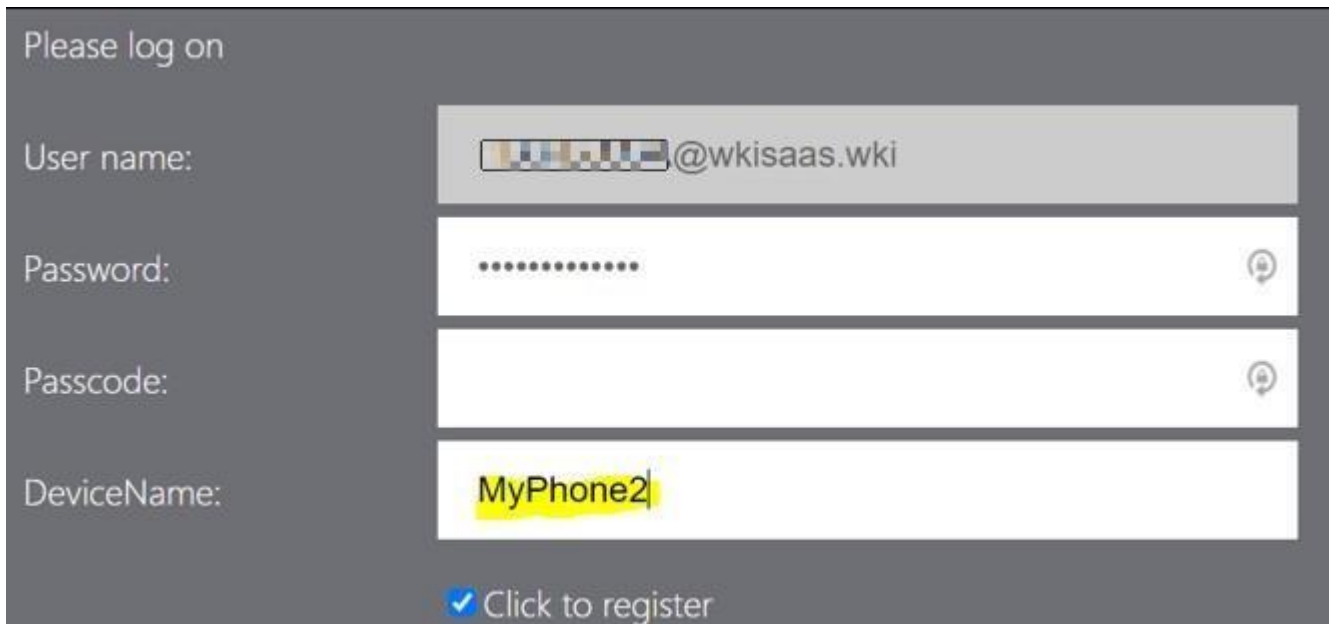
4. Informazioni aggiuntive

1) Mancata accettazione/conferma del token

In caso di mancata accettazione da parte dell'utente, il token sarà rigenerato dopo 30 secondi.

2) Indisponibilità del dispositivo

In caso di indisponibilità del dispositivo (es. telefono guasto, scarico, dimenticato...) è consentita la registrazione di un ulteriore device di backup da associare alla stessa utenza, chiaramente con un "Device Name" diverso:



The screenshot shows a login interface with the following elements:

- Title: "Please log on"
- User name: A text input field containing a blurred image and "@wkisaas.wki".
- Password: A text input field with masked characters (dots) and a visibility toggle icon.
- Passcode: A text input field with a visibility toggle icon.
- DeviceName: A text input field containing "MyPhone2", which is highlighted in yellow.
- At the bottom: A blue checkmark icon followed by the text "Click to register".

3) Token scaduto

Il token è valido per 30 secondi, al termine dei quali viene generato un nuovo token