End-user experience - v2.5 - SecureAuth IdP RADIUS server

Introduction

This guide illustrates the different types of end-user login experiences using a virtual private network (VPN) to access remote resources through RADIUS on a desktop, web, and mobile two-factor authentication.

NOTE: The images in this document provide examples of some user interfaces; the appearances of user interfaces will differ depending on the RADIUS client model or the VPN client application.

CONTENTS OF THIS DOCUMENT:

Prerequisites

If end-users will use YubiKey devices to obtain a one-time HOTP or TOTP passcode, ensure that the YubiKey devices are supported. See the "YubiKey" section of the SecureAuth Compatibility Guide.

Single screen login workflows

The authentication workflow requires the entry of your username followed by at least one other code entry, such as a password or passcode, before the login button is enabled.

Password Only

1. Enter your username.

2. Enter your password.

One-Time Passcode (TOTP/HOTP) Only

1. Enter your username.

2. In the password field, enter the TOTP.

One-Time Passcode (TOTP/HOTP) / Password

1. Enter your username.

2. In the password field, enter the TOTP, then a "/" (forward slash), followed by the password. For example: 563719/Password!

PIN + TOTP

1. Enter your username.

2. In the password field, enter the PIN followed by the TOTP. For example: 3236198337 – in which 3236 is the PIN and 198337 is the TOTP.

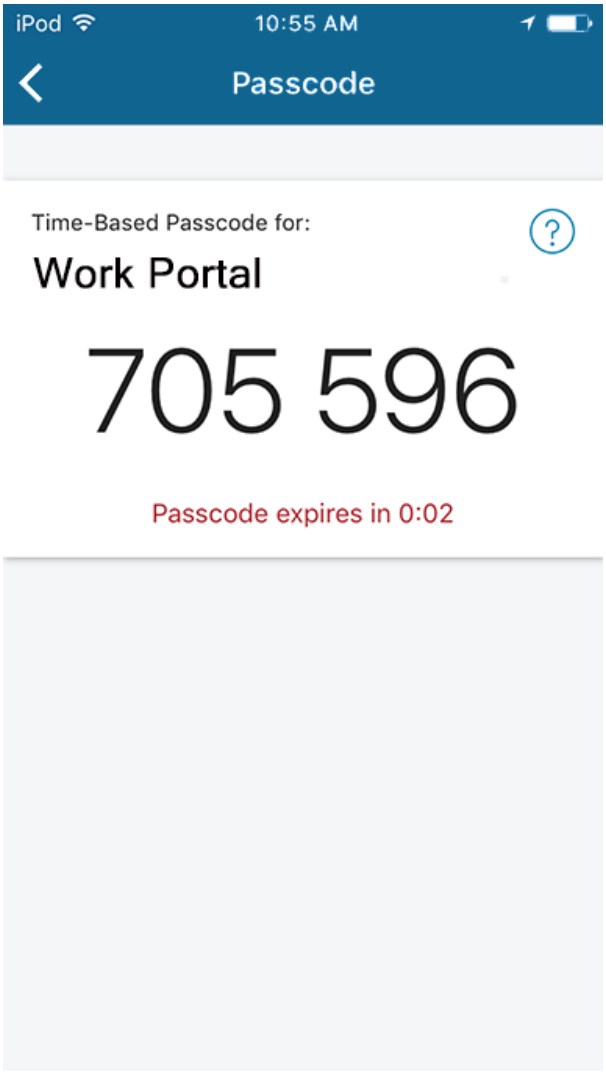
Multi-screen login workflows

Password | One-Time Passcode (TOTP/HOTP)

1. On the initial VPN login screen, enter your username.

2. Enter your password.

3. Get the one-time passcode from the SecureAuth Authenticate App or other SecureAuth TOTP application.



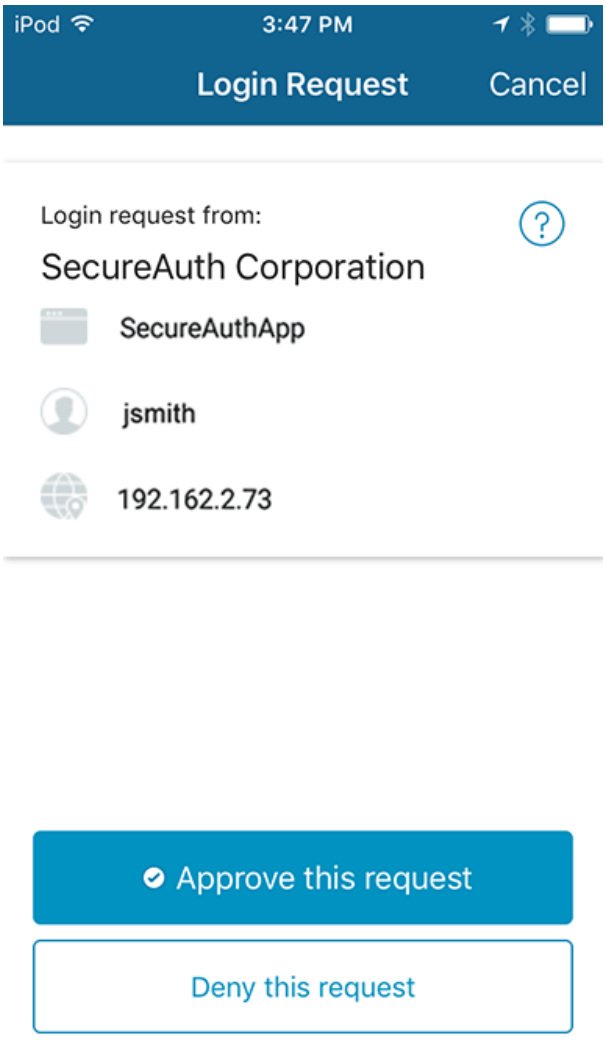
4. On the second VPN login screen, enter your passcode.

Password & Mobile Login Request (Approve / Deny)

1. On the initial VPN login screen, enter your username.

2. Enter your password. The VPN waits for RADIUS to respond.

3. On the mobile app Login Request screen, tap **Approve** or **Deny** request.



Password | One-Time Passcode (TOTP/HOTP) or Second Factor

1. On the initial VPN login screen, enter your username.

2. Enter your password.

3. The response screen prompts you for one of two options:

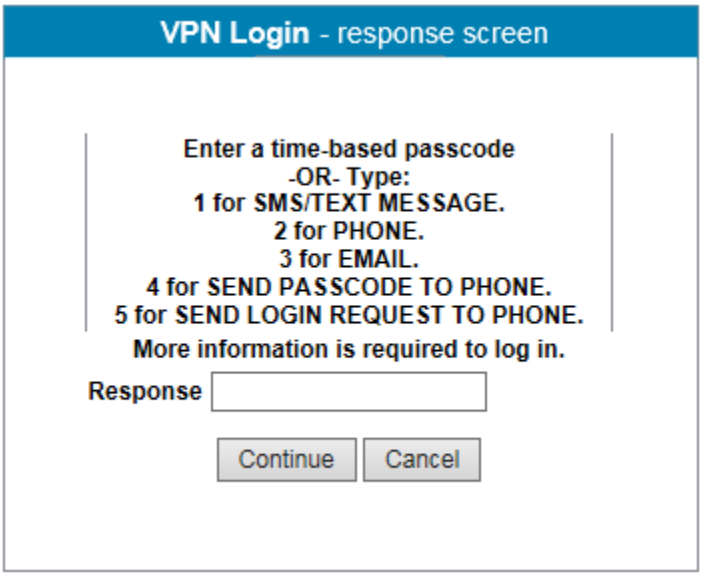
   - Enter an HOTP one-time passcode (from a YubiKey) or a TOTP one-time passcode (from SecureAuth Authenticate, SecureAuth Passcode, or Yubico Authenticator with a YubiKey).

   - Enter the number corresponding to an available Second Factor authentication method:
     - SMS / Text Message Phone
     - Email
     - Send Passcode to Phone (Push Notification)
     - Send Login Request to Phone (Push-to-Accept)
     - PIN

   NOTE: The list of available Second Factor authentication methods is dynamic, since it is based on configured Multi-Factor Authentication options.

4. Make the appropriate entry on the response screen, based on the selected workflow (option "a" or "b" in step 3).

   NOTE: If the **Send Passcode to Phone (Push Notification)** workflow or **PIN** workflow is initially selected, and then another Second Factor authentication option is preferred, entering **0** (zero) in the response field presents the screen with available Second Factor authentication options so another option can be selected.


VPN Login - response screen
Enter a time-based passcode
-OR- Type:
1 for SMS/TEXT MESSAGE.
2 for PHONE.
3 for EMAIL.
4 for SEND PASSCODE TO PHONE.
5 for SEND LOGIN REQUEST TO PHONE.
More information is required to log in.
Response
Continue
Cancel

If selecting option "a" (One-Time Passcode-TOTP/HOTP)...

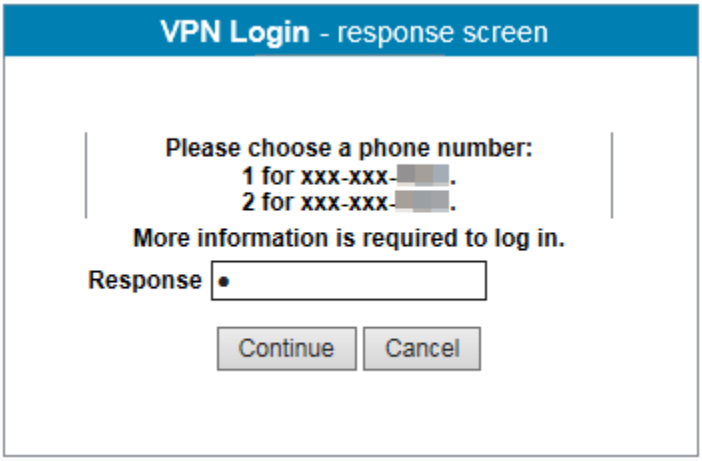
5a. Get the one-time passcode from the SecureAuth Authenticate App (or other SecureAuth TOTP application, such as SecureAuth Passcode), HOTP from YubiKey, or TOTP from a Yubico Authenticator app by using a YubiKey.

6a. Enter the passcode.

If selecting option "b" (Second Factor)...

5b. Enter the number corresponding to an available Second Factor authentication method.

If more than one phone number is set up in your account, select the number corresponding to the phone number to use in the Second Factor authentication workflow session.



The VPN waits for RADIUS to respond.

When the Login Request screen appears on the mobile app, tap Approve or Deny on the screen.

One-Time Passcode (TOTP/HOTP) | Password

1. On the initial VPN login screen, enter your username.

2. Get the one-time passcode from the SecureAuth Authenticate App (or other SecureAuth TOTP application, such as SecureAuth Passcode), HOTP from YubiKey, or TOTP from a Yubico Authenticator app by using a YubiKey.

3. Enter your password on the second VPN login screen.

Username | Second Factor

1. On the initial VPN login screen, enter your username.

2. A password entry is not required.

3. On the response screen, enter the number corresponding to an available Second Factor authentication method:

    1 = SMS / Text Message
    2 = Phone
    3 = Email
    4 = Send Passcode to Phone (Push Notification)
    5 = Send Login Request to Phone (Push-to-Accept)
    6 = PIN

    NOTE: The list of available Second Factor authentication methods is dynamic, since it is based on configured Second Factor authentication options.

4. Proceed with the Second Authentication Factor workflow.

    NOTE: If the **Send Passcode to Phone (Push Notification)** workflow or **PIN** workflow is initially selected, and then another Second Factor authentication option is preferred, entering **0** (zero) in the response field presents the screen with available Second Factor authentication methods so another option can be selected.

    See Password | One-Time Passcode (TOTP/HOTP) or Second Factor for sample screen shots showing the results of selections made at step 4.

Username | Second Factor | Password

1. On the VPN login screen, enter your username.

2. A password entry is not required at this step.

3. On the response screen, enter the number corresponding to an available Multi-Factor Authentication method:

    1 = SMS / Text Message
    2 = Phone
    3 = Email
    4 = Send Passcode to Phone (Push Notification)
    5 = Send Login Request to Phone (Push-to-Accept)
    6 = PIN

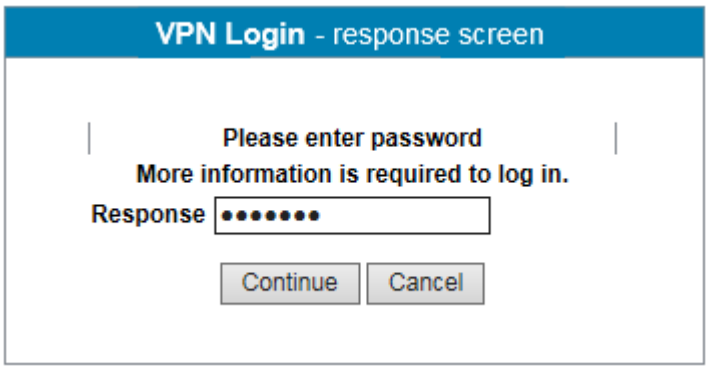
    NOTE: The list of available Second Factor authentication methods is dynamic, since it is based on configured Second Factor authentication options.

4. Proceed with the Second Authentication Factor workflow.

    NOTE: If the **Send Passcode to Phone (Push Notification)** workflow or **PIN** workflow is initially selected, and then another Second Factor authentication option is preferred, entering **0** (zero) in the response field presents the screen with available Second Factor authentication methods so another option can be selected.

    See Password | One-Time Passcode (TOTP/HOTP) or Second Factor for sample screen shots showing the results of selections made at step 4.

5. On the response screen, enter your password.



Password & One-Time Passcode (TOTP/HOTP)

1. On the initial VPN login screen, enter your username.

2. Enter your password.

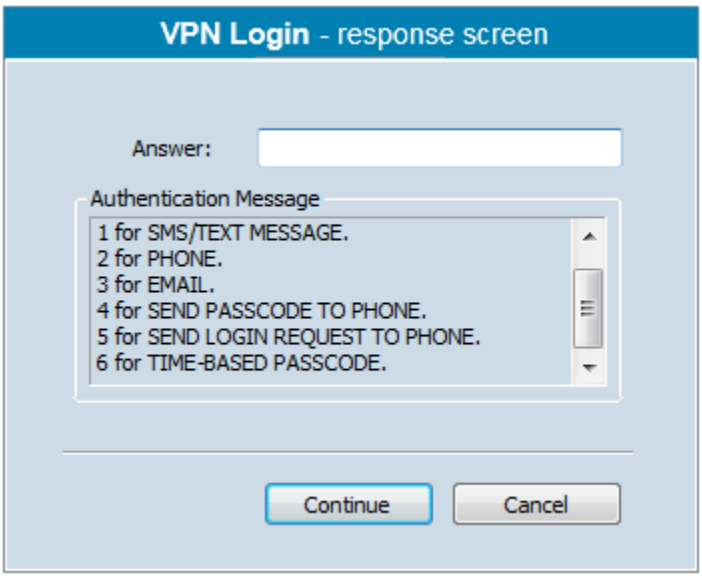
3. Get the one-time passcode from the SecureAuth Authenticate App (or other SecureAuth TOTP application, such as SecureAuth Passcode), HOTP from YubiKey, or TOTP from a Yubico Authenticator app by using a YubiKey.

4. Enter your passcode.

Multiple devices registered for Second Factor authentication

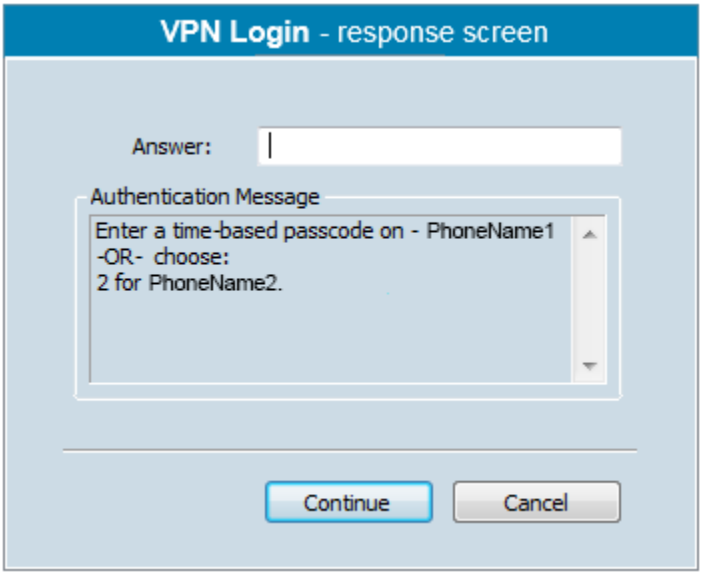
If you have more than one registered mobile device, each with more than one phone number or email address registered, a prompt appears for you to select which mobile device, phone number, or email address to use in the Second Factor authentication workflow session.

1. Select the Second Factor authentication option – for example, "4".



2. Click **Continue**.

3. Since option 4 was selected in this example, a prompt appears for you to select which phone number to use for receiving a passcode.



Related documentation

SecureAuth IdP RADIUS server v2.5 integration guide

Installation guide - v2.5 - SecureAuth IdP RADIUS server

Configuration guide - v2.5 - SecureAuth IdP RADIUS server

SecureAuth Compatibility Guide

Prior version

SecureAuth IdP RADIUS server v2.4 integration guide

Installation guide - v2.4 - SecureAuth IdP RADIUS server

Configuration guide - v2.4 - SecureAuth IdP RADIUS server

End-user experience - v2.4 - SecureAuth IdP RADIUS server