Two-Factor Authentication Guide

User Manual for New and Existing Users

Last Updated: December 2019
Copyright


This publication contains information that is confidential and proprietary to Secureworks and is subject to your confidentiality obligations set forth in your contract with Secureworks or affiliates thereof. This publication and related hardware and software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Copying and/or reverse engineering of any Secureworks hardware, software, documentation, or training materials is strictly prohibited.

This publication and related Secureworks software remain the exclusive property of Secureworks. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronic or mechanical, photocopying, recording, or otherwise without the prior written permission from Secureworks.

Due to continued service development, the information in this publication and related software may change without notice. Please report any errors to Secureworks in writing. Secureworks does not warrant that this publication or related hardware or software is error-free. Please refer to your contract with Secureworks for any provided warranty information.

Secureworks and iSensor are registered trademarks of Secureworks. All other trademarks are the property of the respective owners.
# Table of Contents

**Introduction** ............................................................................................................................ 4  
  How Two-factor Authentication Works ................................................................. 4  
  In This Document You Will Learn ................................................................. 4  
  Contact Us ................................................................. 4  

**Password & Duo** ..................................................................................................................... 5  
  Getting Started ................................................................................................................... 5  
  Configuring Password & Duo for New Users ........................................................... 6  
    Creating Your Portal Password .............................................................. 6  
    Installing and Registering Duo Mobile ......................................................... 6  
    Generating your Certificate to Receive Encrypted Emails ..................................... 6  
  Changing to Password & Duo for Existing Users .................................................. 7  
  Getting Started with Your Duo Registration ......................................................... 8  
  Choosing Your Device for Duo Mobile ............................................................ 8  
  Registering a Mobile Phone ................................................................. 9  
    Smartphone Devices ......................................................................................... 9  
    Other Types of Mobile Phones ......................................................................... 9  
  Registering a Tablet .............................................................................................. 10  
  Registering a Landline ........................................................................................ 10  
  Logging in to the Secureworks Client Portal ....................................................... 11  
    Using the Remember Me Feature .............................................................. 11  
  Managing Your Password & Duo Authentication ................................................ 12  
    Using DUO on a New Device with a New Number ............................................ 12  

**Password & Certificate** ...................................................................................................... 13  
  Getting Started .............................................................................................................. 13  
  Configuring Password & Certificate for New Users ............................................. 14  
    Creating Your Portal Password .............................................................. 14  
    Generating Your Certificate ............................................................................ 14  
    Importing Your Certificate ............................................................................... 14  
  Changing to Password & Certificate for Existing Users ....................................... 16  
  Logging in to the Secureworks Client Portal ....................................................... 17  
  Managing Your Password & Certificate Authentication ...................................... 17  

**Appendix A: Email Encryption Instructions** ......................................................................... 18  
  How do I install my digital certificate into Outlook 2016 to decrypt email? ............ 18  
  How do I install my digital certificate on my iOS device to decrypt email? ............ 18  

**Appendix B: Disabling Certificate Prompt** .......................................................................... 20
Introduction

This document contains information on how to register and configure your two-factor authentication using either Password & Duo or Password & Certificate. Two-factor authentication uses a second factor (mobile device or certificate), which prevents anyone, except you, from logging in, even if your password is compromised.

Password & Duo is the default and recommended authentication option, while Password & Certificate is available as an alternative.

How Two-factor Authentication Works

Once you register your account, you will launch the Secureworks Client Portal and authenticate in one of the following manners:

› If your account is provisioned with the recommended, default Password & Duo, you will log in with your Portal password and then verify your identity with Duo Mobile using one of your registered devices.

› If your account is provisioned with the alternative Password & Certificate, you will verify your identity by selecting your security certificate that is imported into your web browser and then complete your authentication with your Portal password.

In This Document You Will Learn

Password & Duo:

› How to set up Password & Duo authentication for new users
› How to change your Portal authentication to Password & Duo for current users
› How to log in to the Client Portal with Password & Duo authentication
› How to manage your Password & Duo authentication, including reactivating Duo Mobile on a current or new device

Password & Certificate:

› How to set up Password & Certificate authentication for new users
› How to change your Portal authentication to Password & Certificate for current users
› How to log in to the Client Portal with Password & Certificate authentication
› How to manage your Password & Certificate authentication, including downloading a copy of your current certificate or generating a new one

Contact Us

For questions about how to get started, contact the Secureworks Security Operations Center and use option 2 for assistance.

› Inside the US: 1-877-838-7960
› United Kingdom: 0808 234 2477
› Australia: 1800 760 854
› All Other Locations: +1 404-235-1044
Password & Duo

You can download the Duo Mobile application on your mobile device or tablet to use to authenticate to the Secureworks Client Portal. The application will be notified when you attempt to log in to the Portal and will send your device a push notification to confirm your identity. Alternatively, a passcode can be obtained in the mobile application and entered to confirm your identity.

**NOTE:** This option can be used when your mobile device does not have internet access.

If you do not have a smartphone or tablet, you can authenticate using your landline phone or mobile phone via phone call. Duo Mobile will call your landline or mobile phone and prompt you to confirm your login.

The following device types are supported by Duo Mobile:

<table>
<thead>
<tr>
<th>Device</th>
<th>Duo Push</th>
<th>Passcode</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android phone</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows phone 7</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Android tablet</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>iPad tablet</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cell phone</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Land line</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Options in **bold** are recommended

Getting Started

**New Secureworks Portal Users**

**Note:** Password & Duo is the default authentication method for new users.

Go to:

[Configuring Password & Duo for New Users](#)

**Existing Secureworks Portal Users**

**Note:** If you are using a legacy authentication method, it is recommended to change your method to Password & Duo.

Go to:

[Changing to Password & Duo for Existing Users](#)
Configuring Password & Duo for New Users

This section contains information on how to register and configure Password & Duo authentication for new users.

Creating Your Portal Password

After your Portal account is created, you will receive an email from the Secureworks Security Operations Center (SOC) (service@secureworks.com). The email is titled “Secureworks Portal Registration.” Locate the email in your inbox to get started.

1. Click on the link in the email and follow the prompts to create your Portal password: https://portal.secureworks.com/idm/resetpassword.
2. The Reset Password page displays. Type your email address associated with your Portal account and click RESET PASSWORD. An email is sent to your account.
3. Open the Password Reset Request email and click the link in the email to create your password.
   
   **NOTE:** The password reset link included in this email is good for one click only. If you receive a “Password reset failed” error, it is possible that a security system such as Mimecast or Safe Links has detonated the link. To avoid this, repeat Step 1 to request a new password reset email. Once you receive this, copy and paste the password reset link into your browser rather than clicking it.
4. Enter and retype your new Portal password, and then click RESET PASSWORD.

Installing and Registering Duo Mobile

Now it is time to set up your second authentication factor using Duo Mobile and your mobile phone, tablet or landline phone.

2. The Duo Start Setup screen displays. Scroll down, click START SETUP, and follow the directions on the screen. If you have questions about setting up your devices to support Duo authentication, see the Getting Started with Your Duo Registration section in this document for more information.

Generating your Certificate to Receive Encrypted Emails

After completing the preceding steps and logging in to the Portal for the first time, you will be prompted to generate your Security Certificate to receive encrypted emails. Alternatively, use this link to generate your Certificate.

1. On the Generate Certificate page, choose to Create Password Manually and then verify your new password, or Generate Strong Random Password. Click GENERATE CERTIFICATE when complete.
   
   **IMPORTANT:** This is your new CERTIFICATE password—not your Portal password—used only when importing your certificate into your email client. Be sure to copy and keep your Certificate password in a secure location for use when importing your certificate.
2. Please see “Email Encryption Instructions” for instructions on how to import your certificate into your email application. The certificate is only used for receiving encrypted emails when you use Password & Duo authentication.
Changing to Password & Duo for Existing Users

It is recommended to change your authentication method to Password & Duo if you are not currently using this method. Setting up your new authentication for the Secureworks Client Portal will only take a few minutes.

**NOTE:** Although you may be changing your authentication from certificate-based to Password & Duo, you still need your certificate to receive encrypted email.

To manually change your authentication method, follow these steps:

1. Log in to the Secureworks Client Portal using your current authentication.
2. From the top toolbar, select **Account > Account Management**.
3. Authenticate to the Secureworks Identity Manager and click **AUTHENTICATION OPTIONS**.
4. Select **PASSWORD AND DUO** and click **SAVE**.
5. Close out of your browser completely to end your session. It is also recommended to clear your browser cache and SSL state.
   
   **NOTE:** If you are prompted to select a Certificate when launching the Portal, click **CANCEL** and you will be redirected to the Secureworks Client Portal Login and Password screen (see Disabling Certificate Pop-up to disable this behavior).
7. Type your email address in the Email field and click **CONTINUE**.
8. Type your Portal password in the Password field and click **LOGIN**.
   
   **NOTE:** If you don’t remember your password or have not yet created one, click **FORGET PASSWORD?** to reset your password or use this link: https://portal.secureworks.com/idm/resetpassword.
9. After you have successfully authenticated with your password, the **Duo Start Setup** screen displays and you can begin registration.
10. Scroll down, click **START SETUP**, and follow the directions on the screen. If you have questions about setting up your devices to support Duo authentication, see the Getting Started with Your Duo Registration section in this document for more information.
Getting Started with Your Duo Registration

This section assumes you have authenticated with your Portal password and are ready to begin registering your second authentication factor with Duo Mobile. If you are not at the Duo Start Setup screen, follow the steps in the Configuring Password & Duo Authentication for New Users, or the Changing to Password & Duo for Existing Users section.

Choosing Your Device for Duo Mobile

After clicking START SETUP from the Duo Start Setup screen, choose the type of device you want to register with Duo Mobile, and click CONTINUE. You will be able to add more than one device after your initial setup. Please continue to the appropriate section based on your selection for further instructions.

Device Options include:

- Mobile Phone - Registering a Mobile Phone
- Tablet (Apple or Android) - Registering a Tablet
- Landline - Registering a Landline
Registering a Mobile Phone

When you select Mobile Phone, the Enter your Phone Number screen displays.

1. Select your country from the drop-down list and type your mobile number in the box below.

2. A green check mark displays if the mobile number format is correct. Check the box indicating that you verified the number is correct, and click CONTINUE.

3. The Choose Platform screen displays. Choose your device type, and click CONTINUE. If you are registering a smartphone (iPhone, Android, or Windows Phone) proceed to the Smartphone Devices section. If you are registering a non-smartphone device, proceed to the Other Types of Mobile Phones section.

**NOTE:** We recommend that you add a second device, either Mobile or Landline, to your Duo Mobile account after your initial registration. This will allow a second authentication option if you lose your primary mobile device. For details on managing Duo Mobile devices, please see the Managing Your Password & Duo Authentication section.

Smartphone Devices

When you select your smartphone device type (iPhone, Android, or Windows Phone), the Install Duo Mobile screen displays.

1. Follow the platform-specific instructions on the screen to install Duo Mobile on your device. After installing the app, return to the enrollment window and click I HAVE DUO MOBILE.

2. The Activate Duo Mobile screen displays. Activating the app links it to your account so you can use it for authentication. Activate Duo Mobile by scanning the barcode with the app’s built-in barcode scanner. Follow the platform-specific instructions for your device.

   **NOTE:** If you can’t scan the barcode, click the link to HAVE AN ACTIVATION LINK EMAILED TO YOU INSTEAD. Open the email and click the activation link.

3. Click CONTINUE, which is clickable after you scan the barcode successfully or click the activation link from the email.

4. Your device is successfully enrolled. Choose whether you would like to be asked to choose an authentication method each time you log in, or whether you would like to automatically receive a Duo Push or phone call. Click SAVE to save your choice.

5. Click CONTINUE TO LOGIN and you are ready to log in to the Portal using your Duo + Password authentication. See Logging in to the Secureworks Client Portal for more information.

Other Types of Mobile Phones

When you select Other (and cell phones) as your device type, you have successfully enrolled your mobile device capable of authenticating via phone call.

1. Choose whether you would like to be asked to choose an authentication method each time you log in, or whether you would like to automatically receive a phone call. Click SAVE to save your choice.

2. Click CONTINUE TO LOGIN and you are ready to log in to the Portal using your Duo + Password authentication. See Logging in to the Secureworks Client Portal for more information.
Registering a Tablet
When you select Tablet for your device, the **Choose Platform** screen displays.

1. Choose your device's operating system and click **CONTINUE**.

2. The **Install Duo Mobile** screen displays. Follow the platform-specific instructions on the screen to install Duo Mobile on your device. After installing the app, return to the enrollment window and click **I HAVE DUO MOBILE**.

3. The **Activate Duo Mobile** screen displays. Activating the app links it to your account so you can use it for authentication. Activate Duo Mobile by scanning the barcode with the app's built-in barcode scanner. Follow the platform-specific instructions for your device.

   **NOTE:** If you can’t scan the barcode, click the link to **HAVE AN ACTIVATION LINK EMAILED TO YOU INSTEAD**. Open the email and click the activation link.

4. Click **CONTINUE** from the **Activate Duo Mobile** screen, which is clickable after you scan the barcode successfully or click the activation link from the email.

5. Your device is successfully enrolled. Choose whether you would like to be asked to choose an authentication method each time you log in, or whether you would like to automatically receive a Duo Push. Click **SAVE** to save your choice.

6. Click **CONTINUE TO LOGIN** and you are ready to log in to the Portal using your Duo + Password authentication. See [Logging in to the Secureworks Client Portal](#) for more information.

Registering a Landline
When you select Landline Device, the **Enter Your Phone Number** screen displays.

1. Select your country from the drop-down list and type your phone number in the box below.

2. A green check mark displays if the format is correct. Check the box indicating that you verified the number is correct, and click **CONTINUE**.

3. Your landline phone is successfully enrolled. Choose whether you would like to be asked to choose an authentication method each time you log in, or whether you would like to automatically receive a phone call. Click **SAVE** to save your choice.

4. Click **CONTINUE TO LOGIN** and you are ready to log in to the Portal using your Duo + Password authentication. See [Logging in to the Secureworks Client Portal](#) for more information.
Logging in to the Secureworks Client Portal

To log in to the Secureworks Client Portal using Password & Duo authentication, navigate to the Secureworks Client Portal (https://portal.secureworks.com/portal) and follow these steps:

1. Enter the email address associated with your Portal account and click CONTINUE.

2. The password prompt displays. Enter your Portal password that you created when you received the Portal Registration email or when you reset your password. Click LOGIN.

3. The Duo Authentication screen displays. You can authenticate to the Portal using one of the following methods, depending on the device you enrolled:
   - **Duo Push** – Duo Mobile will push a challenge to your smartphone or tablet. Tap APPROVE on your device to authenticate. This requires your device to have data service or be on a Wi-Fi network. To use this option, select SEND ME A PUSH from the Duo Authentication screen and tap APPROVE from the notification or in the Duo Mobile app on your device.
     
     **NOTE:** If you are not notified of the notification on your device, you may need to open the Duo Mobile app to view the pending request and approve.
   - **Phone Call** – Duo Mobile will call your phone. Answer the call and press the 5 key to authenticate. To use this option, select CALL ME from the Duo Authentication screen and press 5 to log in after answering the call.
   - **Passcode** – Generate a passcode in the Duo Mobile app on your device to use to log in. To use this option, select ENTER A PASSCODE from the Duo Authentication screen and enter the six-digit passcode you create in the Duo Mobile app on your mobile device or tablet. Click LOG IN to authenticate to the Client Portal.

   **TIP:** Before you log in, click the REMEMBER ME checkbox to avoid having to perform Duo authentication again for one week. See the following section for more details

Using the Remember Me Feature

The Remember Me feature allows you to bypass Duo authentication for one week. After enabling, simply enter your email address and password to authenticate until the duration has passed, at which time Duo will prompt you to confirm your identity again. Using this feature saves you the time of having to confirm your identity with Duo, getting you into the portal more quickly and easily.

To use this feature, remember these tips:

〉 Enable this feature by clicking the REMEMBER ME FOR 7 DAYS checkbox from the Duo Authentication prompt before selecting your Duo authentication method.

〉 If you chose to automatically receive a Duo Push or phone call during setup, you must click CANCEL to select the REMEMBER ME feature, as the option is hidden by the Duo status message if a Duo Push or phone call is in progress.

★★★★★ Have Feedback?
Managing Your Password & Duo Authentication

After you have successfully registered your device, you can enroll another device and manage already registered devices from the Duo Authentication screens.

**Tip:** If you have replaced your phone but have the same phone number, you can still access the Settings by having Duo Mobile call your number to authenticate and then reactivate Duo Mobile on your new device (see below).

1. After entering your email address and Portal Password, select the SETTINGS option on the Duo Authentication screen. Select ADD A NEW DEVICE to begin the process of adding another device with which to authenticate, or select MY SETTINGS & DEVICES to manage your already registered devices.

2. Both options require that you first verify your identity by authenticating with one of your already registered devices. Select your authentication device and method to proceed.

3. If adding a new device, follow the steps in the preceding Choosing your Device for Duo Mobile section. To manage current devices and settings, proceed to the next step.

4. Select the action you would like to take from the following options:
   - **Default Device and Log In** – Choose which device you would like to be your default authentication device from the dropdown list, and whether you would like Duo Mobile to automatically send a Duo Push or Phone Call when logging in to the Portal.
     
     **Note:** If you only have one registered device, it will automatically be default with no option to change.
   - **Change Device Name** – Select the gear icon next to your device and click CHANGE DEVICE NAME to change the name of the device (i.e. Work Phone, Home Phone).
   - **Reactivate Duo Mobile** – Select the gear icon next to your device and click REACTIVATE DUO MOBILE to reactivate Duo Mobile. See Choosing your Device for Duo Mobile.
   - **Deleting Device** – Select the gear icon next to your device and click DELETE DEVICE to remove the device from the list.
     
     **Note:** If you only have one registered device, you cannot delete. Add a new device first, and the option will be available.

5. Click SAVE when you are finished managing your devices.

To manage your Portal password or certificate used to view encrypted email, navigate to the Identity Manager by selecting ACCOUNT MANAGEMENT from the Account menu in the Portal, or directly with this link: https://portal.secureworks.com/idm.

1. **Manage your Certificate** – In the Secureworks Identity Manager, click DOWNLOAD CERTIFICATE to view a list of your current certificates and their expiration dates. Select the certificate you wish to download a copy of and then click DOWNLOAD.
2. **Manage your Password** – In the Secureworks Identity Manager, click CHANGE PASSWORD to change your Portal password.

If you need to generate a new certificate, click the NEED TO GENERATE A CERTIFICATE? link prior to entering your Portal password on the login page, and follow the steps here.

If you need to reset your Portal password, click the FORGOT PASSWORD? link on the login page, and follow the steps here.

**Using DUO on a New Device with a New Number**

If you have replaced your phone and have a new number and did not add the new device prior to losing access to your previous number, please contact the SOC to reset your DUO account.
Password & Certificate

With this alternative authentication option, you will need to generate a security certificate and import it into any web browser you wish to use to access your Secureworks services as a first authentication factor. After confirming your certificate in your browser, you will be prompted to enter your Portal password as your second factor.

**NOTE:** You will not be able to access your Secureworks services unless your certificate is imported into the browser you are using. You can import the same certificate into multiple browsers and machines if needed using the same password you create when generating the certificate.

Getting Started

**New Secureworks Portal Users**

**Note:** Password & Duo is default for new users, but your User Admin may have chosen the alternative Password & Certificate authentication method for your account.

Go to:

[Configuring Password & Certificate for New Users](#)

**Existing Secureworks Portal Users**

**Note:** If you wish to change your authentication method from a legacy method or from Password & Duo, you can use the alternative Password & Certificate method.

Go to:

[Changing to Password & Certificate for Existing Users](#)
Configuring Password & Certificate for New Users

This section contains information on how to configure Password & Certificate authentication for new users.

Creating Your Portal Password

After your Portal account is created, you will receive an email from the Secureworks Security Operations Center (SOC) (service@secureworks.com). The email is titled “Secureworks Portal Registration.” Locate the email in your inbox to get started.

1. Click on the link in the email and follow the prompts to create your Portal password: https://portal.secureworks.com/idm/resetpassword.
2. The Reset Password page displays. Type your email address associated with your Portal account and click RESET PASSWORD. An email is sent to your account.
3. Open the Password Reset Request email and click the link in the email to create your password.
4. Enter and retype your new Portal password then click RESET PASSWORD.

Generating Your Certificate

After completing the preceding steps to set your Portal password, follow these steps to generate your Security Certificate.

1. Click the NEED TO GENERATE A CERTIFICATE? link from the Client Portal login screen, or use the following link to generate your new Certificate: https://portal.secureworks.com/idm/generatecert.
2. Type your email address associated with your Portal account and click GENERATE CERTIFICATE. An email is sent to your account.
3. Open the Certificate Request email and click the link in the email to generate your Certificate.
4. On the Generate Certificate page, choose to Create Password Manually and then verify your new password, or Generate Strong Random Password. Click GENERATE CERTIFICATE when complete.

IMPORTANT: This is your new CERTIFICATE password—not your Portal password—used only when importing your certificate into your email client. Be sure to copy and keep your Certificate password in a secure location for use when importing your certificate.

Importing Your Certificate

After completing the preceding steps to generate your Certificate, follow these steps to import your Certificate into your browser. Once your certificate is imported, see Logging in to the Secureworks Client Portal for more information.

NOTE: Import steps differ by browser, browser version, and operating system. Use these steps as general guidelines for common Windows browsers and refer to your browser or system documentation. If you need assistance, contact the SOC and they will be glad to help.

› Internet Explorer (Version 11):

1. Select INTERNET OPTIONS from the menu, and from the CONTENT tab, click CERTIFICATES.
2. Ensure you are viewing the PERSONAL tab and click IMPORT.
3. Follow the prompts of the Certificate Import Wizard to navigate to the location of your saved certificate. NOTE: You may need to alter the File Type to Personal Information Exchange or All Files.
4. When prompted for the Password for the private key, enter the password you created when generating your certificate, NOT your Portal password.

› Chrome (Version 70):

1. Select SETTINGS from the menu.
2. Scroll down to click ADVANCED and choose MANAGE CERTIFICATES from the Privacy and Security section.
3. Chrome uses the Windows Certificate Store. Follow steps 2 through 4 in the preceding IE instructions.

Firefox (Version 60):

1. Select OPTIONS from the menu and choose the PRIVACY & SECURITY section.
2. Click VIEW CERTIFICATES from the Security section.
3. From the YOUR CERTIFICATES tab, click IMPORT.
4. Navigate to the location of your saved certificate. When prompted for the password used to encrypt this certificate, enter the password you created when generating your certificate, NOT your Portal password.
Changing to Password & Certificate for Existing Users

The Password & Duo method is our default and recommended authentication method, but if you have need for an alternative, you can change to Password & Certificate manually.

To manually change your authentication method, follow these steps:

1. Log in to the Secureworks Client Portal using your current authentication.
2. From the top toolbar, select Account > Account Management.
3. Authenticate to the Secureworks Identity Manager and click AUTHENTICATION OPTIONS.
4. Select PASSWORD AND CERTIFICATE and click SAVE.
5. Close out of your browser completely to end your session. It is also recommended to clear your browser cache and SSL state.
7. Select your certificate from the popup to authenticate. If you need to generate a new certificate, follow the instructions here to create a new one and import it into your browser.
8. After confirming your certificate, enter your Portal password in the Password field and click LOGIN.

**NOTE:** If you don’t remember your password or have not yet created one, click FORGET PASSWORD? to reset your password or use this link: https://portal.secureworks.com/idm/resetpassword.
Logging in to the Secureworks Client Portal

To log in to the Secureworks Client Portal using Password & Certificate authentication, navigate to the Secureworks Client Portal (https://portal.secureworks.com/portal) and follow these steps:

1. Select your Portal certificate from the popup when prompted.
2. The password prompt displays. Enter your Portal password that you created when you received the Portal Registration email or when you reset your password. Click LOGIN.
3. The Client Portal displays.

Managing Your Password & Certificate Authentication

Use the following options to manage your authentication after successfully creating your Portal password, generating your certificate, and importing it into your browser. From the Client Portal, select ACCOUNT MANAGEMENT from the Account menu, or authenticate to the Identity Manager directly with your Portal credentials by navigating to: https://portal.secureworks.com/idm.

- Manage your Certificate – In the Secureworks Identity Manager, click DOWNLOAD CERTIFICATE to view a list of your current certificates and their expiration dates. Select the certificate you wish to download a copy of and then click DOWNLOAD.
- Manage your Password – In the Secureworks Identity Manager, click CHANGE PASSWORD to change your Portal password.

If you need to generate a new certificate, click the NEED TO GENERATE A CERTIFICATE? link prior to entering your Portal password on the login page, and follow the steps here.

If you need to reset your Portal password, click the FORGOT PASSWORD? link on the login page, and follow the steps here.
Appendix A: Email Encryption Instructions

How do I install my digital certificate into Outlook 2016 to decrypt email?

If you have a Digital Certificate, you can use it to digitally sign and encrypt emails. When you are using Microsoft Outlook as your email client, you will need to first configure Outlook to use your certificate. **NOTE:** The certificate installation process differs slightly for previous versions of Outlook.

Before you begin, you must have your Digital Certificate download to your computer. If you are a new Portal user, you should have received instructions on how to download your certificate in the Secureworks Portal Registration Email. See the [Generating Your Certificate](#) section for more details.

1. Once you have your Digital Certificate downloaded to your computer, open Outlook.
2. Click the **FILE** tab in the top navigation menu, and click **OPTIONS** from the left navigation menu.
3. The **Outlook Options** window displays. Select **TRUST CENTER** in the left navigation menu.
4. The information in the main window changes. Click **TRUST CENTER SETTINGS…**
5. The **Trust Center** window displays. Click **EMAIL SECURITY** from the left navigation menu.
6. The information in the main window changes. In the **Digital IDs (Certificates)** section, click **IMPORT/EXPORT…**
7. The **IMPORT/EXPORT DIGITAL ID** window displays. With the **IMPORT EXISTING DIGITAL ID FROM A FILE** radio selected, click **BROWSE** next to the Import File field and browse to the folder in which your Digital Certificate is saved to select your Certificate.
8. In the Password field, input the password you created when generating the Certificate, and click **OK**.
9. In the **Encrypted e-mail** section of the **Trust Center** window, next to Default Setting, click **SETTINGS…**
10. The **Change Security Settings** window displays.
11. Click the **CHOOSE...** button next to Signing Certificate.
12. Select your Secure Email Certificate from the select Certificate dialog box. Outlook should automatically choose the same secure email certificate as your signing certificate for the encryption certificate. If you can’t locate the certificate, click the **CHOOSE...** button in the Encryption Certificate and select your secure email certificate from the select certificate dialog box.
13. Confirm the **SEND THESE CERTIFICATES WITH SIGNED MESSAGES** box is checked.
14. Click **OK** to return to the Options dialog box.
15. Click **OK** to return to Outlook.

**NOTE:** Only Outlook is supported for certificate decryption. We do not guarantee compatibility with any other platforms.

How do I install my digital certificate on my iOS device to decrypt email?

After you receive or download your certificate to your iOS device, open the digital certificate by tapping the file. This will start the process to install the certificate as a new profile on your iOS device. If a certificate is sent in an email, it will appear as an attachment. Safari can be used to download certificates from a web page.

1. The Install Profile screen displays. Tap **INSTALL**. Tap details to see more information about the certificate.
2. You will then be prompted with a warning message, “Installing this profile will change settings on your iOS device.” Tap **INSTALL NOW**.
3. If your iOS device has a PIN or Passcode, you will need to enter it to verify the device belongs to you. If you don’t have a PIN or Passcode set up, the next screen will require you to add your certificate password. This is the password you set up when you downloaded your certificate.

4. The certificate will continue to install and you will be presented with the certificate information when it is finished installing. Tap DONE.

**NOTE:** At the time of writing, no third-party mobile apps (including Outlook for mobile) support certificate decryption. The stock iOS mail application is the only mobile app confirmed to be compatible. We strongly recommend the use of the Secureworks Mobile App over attempting to import a certificate on a mobile device.
Appendix B: Disabling Certificate Prompt

If you are an existing user that switched to Duo + Password authentication but previously authenticated to the Portal using a certificate, you may want to disable the certificate prompt every time you launch the Portal.

From a Windows machine, follow these steps:

1. Press the **Windows Key + R**, type `certmgr.msc` and hit **Enter**.
2. From the Certificates window, navigate to the **PERSONAL > CERTIFICATES** folder.
3. Right-click your Secureworks certificate from the list and select **PROPERTIES**.
4. In the **General** tab, select **ENABLE ONLY THE FOLLOWING PURPOSES** and uncheck **CLIENT AUTHENTICATION**.
5. Click **OK** to save your new settings.