



Getting Started in the Continuous Dynamic Portal

Black Duck Software, Inc.

2025-05-19

Table of Contents

- 1. Logging On 1
 - 1.1. Welcome to the Continuous Dynamic Portal 1
 - 1.2. The Login Screen..... 1
 - 1.3. Other Actions on the Login Page 2
 - 1.4. Next Steps and Further Reading 3
- 2. Supported Browsers..... 4
- 3. Your Continuous Dynamic Portal Profile 5
 - 3.1. My Profile 7
 - 3.2. Changing Your Password..... 8
 - 3.3. Public Key 9
 - 3.4. API Key..... 9
 - 3.5. Regenerating Your API Key 11

Chapter 1. Logging On

1.1. Welcome to the Continuous Dynamic Portal

When you first take a contract with Black Duck for Continuous Dynamic services, the following is what you can expect:

1. You will receive a welcome email with a link to the Continuous Dynamic Portal.

NOTE

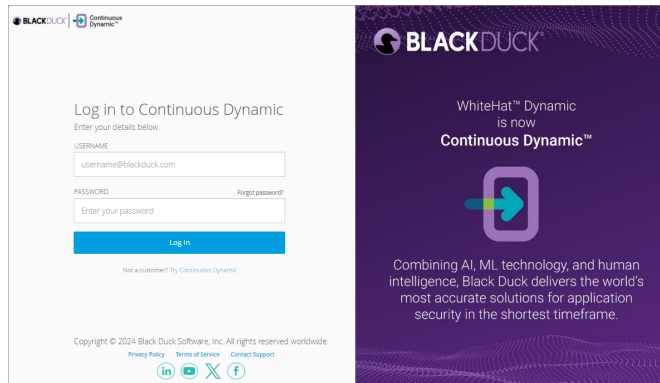
If you do not see your email, check your email Junk/Spam email. If you find it there, do not forget to add the Black Duck email address to your list of **Allowed Senders**. If the email is not there, please contact your Portal administrator, your Black Duck representative, or Black Duck Customer Service.

2. Within 48 hours of receiving your welcome email, click the link to begin the login process.
3. Please type your new password into both fields when prompted to configure your password.
4. You are now ready to login for the first time.

1.2. The Login Screen

Log in to the Portal site, by performing the following steps:

1. Enter your **Username** and **Password** in the provided fields:



The image shows the login interface for Black Duck Continuous Dynamic. It consists of two main panels. The left panel is white and contains the login form. At the top, it says 'Log in to Continuous Dynamic' and 'Enter your details below.' There are two input fields: 'USERNAME' with the example 'username@blackduck.com' and 'PASSWORD' with the prompt 'Enter your password'. A 'Log In' button is at the bottom of the form. Below the button, it says 'Not a customer? Try Continuous Dynamic'. At the very bottom, there is a copyright notice: 'Copyright © 2024 Black Duck Software, Inc. All rights reserved worldwide.' and links for 'Privacy Policy', 'Terms of Service', and 'Contact Support'. The right panel is a purple banner. It features the Black Duck logo at the top. Below it, it says 'WhiteHat™ Dynamic is now Continuous Dynamic™'. There is a large blue arrow icon pointing right. At the bottom, it says 'Combining AI, ML technology, and human intelligence, Black Duck delivers the world's most accurate solutions for application security in the shortest timeframe.'

2. Click **Log In**.
3. Optionally, if you forget your password, click **Forgot Password**.
4. If your instance of the Portal has **multi-factor authentication** (MFA) enabled, as well as username and password credentials, you are required to submit a secondary authentication token into the Portal UI. This single use secondary authentication token will be delivered to you via a text message or phone call to your mobile/cell phone.
 - a. Depending upon your preference, click **Request Code by SMS** or **Request Code by Call**. Once clicked, the following confirmation message displays: **A security code has been sent**.

The screenshot shows a login interface for WhiteHat Security. At the top, it says 'Hello' followed by a greyed-out username field. Below that is another greyed-out field, likely for a password. A message states 'Your account requires additional authentication.' followed by the instruction 'Please request a code to continue:'. There are two blue buttons: 'Request Code by SMS' and 'Request Code by Call'. A red box labeled 'a' highlights these two buttons. Below them is a horizontal line. Then, it says 'Once you have received your 6 digit code, enter it below to proceed to Sentinel:'. There is a text input field for the code, highlighted with a red box labeled 'c'. Below the input field is a blue button labeled 'Submit Code', highlighted with a red box labeled 'd'. At the bottom, it says 'WhiteHat Security © 2002-2021'.

- b. Watch for a text or call to your mobile/cell phone, which will give you a 6-digit code.
- c. Type the provided code into the field provided.
- d. Click **Submit Code**. If the code is not validated, you will not be logged in and you will be asked if you want a new code to be sent again. If the code is validated, you will be successfully logged in.

NOTE

If you do not yet have login credentials, or if you have trouble logging in, please contact your Portal administrator, your Black Duck representative, or Black Duck Customer Support at support@whitehatsec.com.

1.3. Other Actions on the Login Page

Other actions that you can take from the Login page are as follows:

- a. View the [Privacy Policy](#).
- b. View the [Terms of Service](#).
- c. Click [here](#) to email the Support team.
- d. View the most recent version of the **Application Security Statistics Report**, which is published annually by Black Duck.

1.4. Next Steps and Further Reading

TIP

Your next step is to set up [My Profile](#). Also make sure that your current browser is supported here: [The Continuous Dynamic Portal - Supported Browsers](#)

Now you have logged into the Portal, take a look around. Here is some content to get you started:

- [Navigating the Continuous Dynamic Portal](#)
- [The Continuous Dynamic Portal for Managers](#)
- [The Continuous Dynamic Portal for Developers](#)
- [The Continuous Dynamic Portal for Security Teams](#)
- [The Continuous Dynamic Portal for Continuous Dynamic Admins](#)

Chapter 2. Supported Browsers

The Continuous Dynamic Portal provides full, certified support for the **Google Chrome** and **Mozilla Firefox** browsers.



Google Chrome



Mozilla FireFox

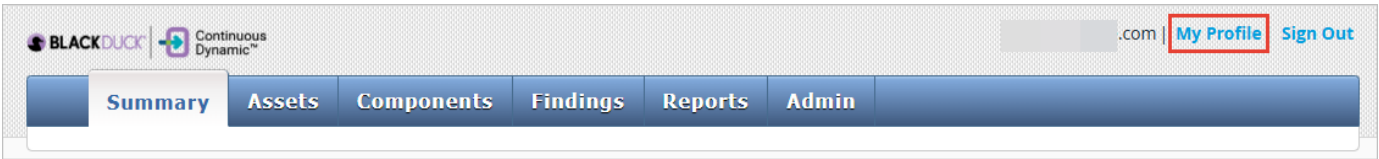
We test our products in the certified browsers and are committed to remediating defects identified during testing or reported by customers. Customers using non-supported browsers may experience incorrect functionality in some features. Black Duck encourages customers to use the supported browser versions, both for Portal functionality and for improved security.

Additional browsers may be supported on a case by case basis, depending on demonstrated business needs. For additional browsers, we will also identify and correct defects where a clear business case can be made for doing so. The same level of support guarantee offered with our Certified Supported browsers, cannot be offered for additional browsers. Some older browsers (e.g. IE11) will not be supported. For these browsers, we will not identify or remediate issues. The following is a summary of policies for certified browsers:

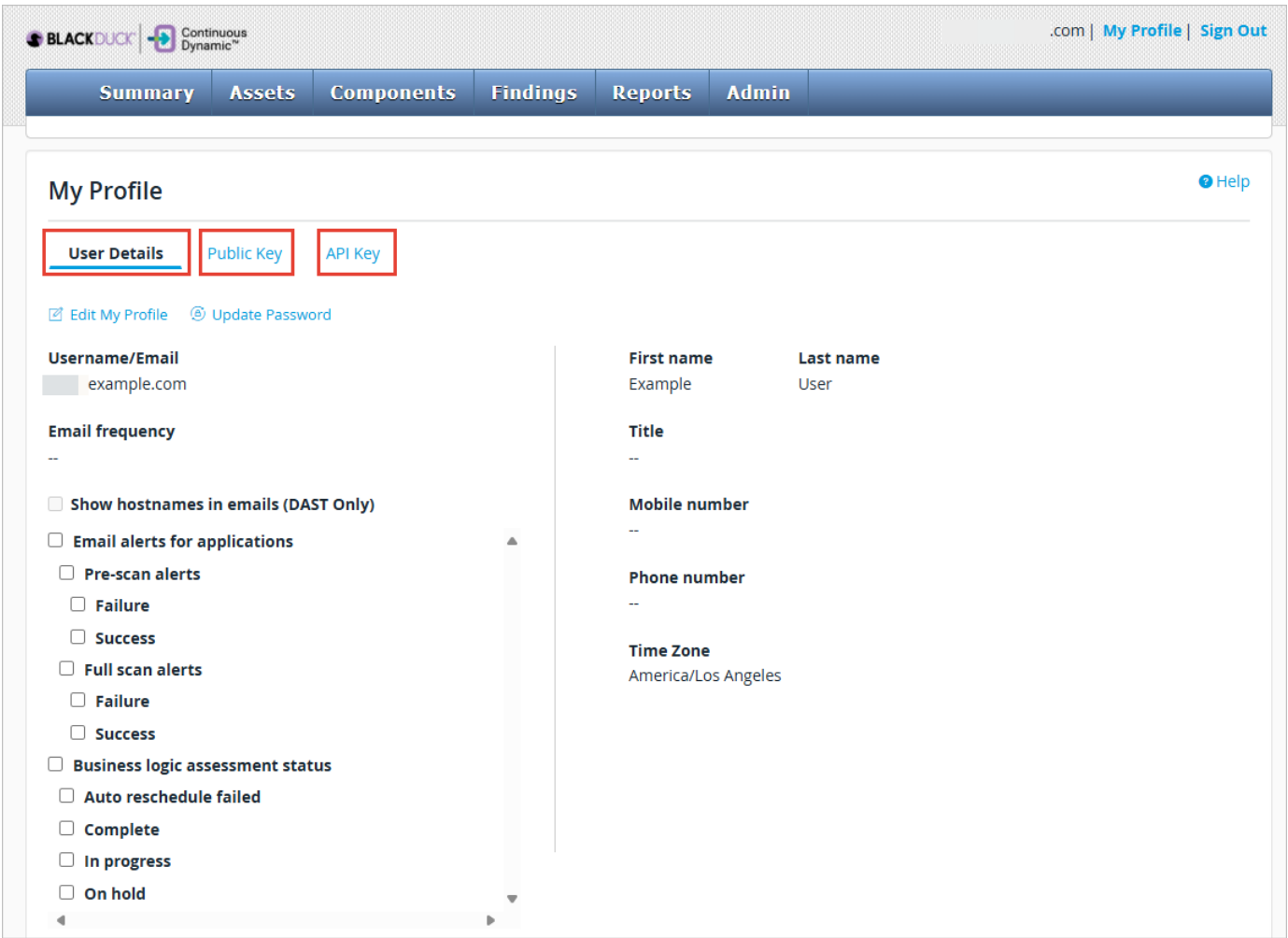
- Certified browsers are fully supported on all supported operating systems.
- Browser releases are evaluated quarterly and browser certifications for the Portal are updated accordingly.
- Discontinued versions of certified browsers will no longer be supported.

Chapter 3. Your Continuous Dynamic Portal Profile

To view your profile, click **My Profile** at the top-right of the Continuous Dynamic Portal interface:



The **My Profile** page is displayed:



Field Name	Description
User Details	Here you can use Edit My Profile to edit information, such as name, title, email, etc. You can also use Update Password .
Public Key	Edit your Public Key encryption information

Field Name	Description
API Key	View, create or regenerate your web API Key information

3.1. My Profile

To edit information in your profile, click **User Details** > **Edit My Profile**.

User DetailsPublic KeyAPI Key

Edit My Profile

Update Password

The **My Profile** editing screen is displayed.

My Profile

Username/Email
colin.hillis@whitehatsec.com

Primary client
Michele Cox Client 1

Email frequency

Show hostnames in emails (DAST Only)

Email alerts for applications

Pre-scan alerts

Failure

Success

Full scan alerts

Failure

Success

Business logic assessment status

Auto reschedule failed

Complete

In progress

On hold

First name*Last name*

Required.Required.

Title

Mobile number

Phone number

Time Zone
America/Los Angeles

Cancel

Save

View or make changes to your profile, as follows:

1. The **First name** and **Last name** fields must be populated.
2. Type your **Title** (e.g. IT Security Manager), **Mobile number**, and **Telephone number**. Then select your appropriate timezone from the **Timezone** drop-down menu.
3. From the **Email frequency** drop-down, select one of the following:
 - **Daily**
 - **Weekly**
 - **Monthly**

NOTE

If you require more granular email frequency, please contact support@whitehatsec.com.

4. Choose your email triggers and select whether or not to see hostnames in DAST-related emails, if that is available to you.

5. Click **Save**.

3.2. Changing Your Password

Password guidelines are determined by your Portal Administrator. Your organization may have adopted single sign-on or multi-factor authentication. If you are using single sign-on, you will not need to enter your Portal password; instead simply log on via your SSO. If you are not using single sign-on and you need to change your password, click **User Details > Update Password**.

User Details

Public Key

API Key

 [Edit My Profile](#)

 [Update Password](#)

The **Update Password** editing window is displayed.

Update Password

Old password*

New password*

Confirm new password*

Cancel

Save

1. Type your **Old password**.
2. Type your **New password** and repeat it in the **Confirm new password** field. Both entries must match to proceed.
3. Click **Save**.

3.2.1. Password Format and Guidance

By default, the Portal will require that your password contain at least six characters, including at least one number and at least one letter. Additionally, password restrictions may be in place, which enforces that your password adopts some or all of the following:

- Uppercase letters
- Lowercase letters

- Numerals
- Special characters
- Excludes all/part of username
- Excludes all/part of email

Always protect your password. If someone else obtains your password, they may gain access to your vulnerability information. Black Duck Support will never ask for your password.

3.3. Public Key

If your server uses Pretty Good Privacy (PGP), you can use your public key to send secure data across potentially insecure networks. You can enter or delete your public key here. If you have questions about PGP, see your network administrator.

1. Click **Public Key** to display the **Public Key** editing page.



The screenshot shows the 'My Profile' page with a 'Help' link in the top right. Below the title, there are three tabs: 'User Details', 'Public Key' (which is selected and highlighted with a red box and a red '1'), and 'API Key'. Below the tabs is a section titled 'Set public key' with a help icon. A large, empty text input field is provided for the public key, outlined with a red box and a red '2'. At the bottom right of the page, there are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted by a red box and a red '3'.

2. Type your key into the free text field.
3. Click **Save**, or **Cancel** to cancel the operation.

3.4. API Key

Each user account may generate a unique 32-character Web API Key, which is used to authenticate your API requests. The Web API key is intended for use inside the applications that are accessing the API. It is not intended for accessing the API through your browser.

3.4.1. If You Have a Portal Password:

To view the API key, or to create a new one:

1. Click **API Key**.

My Profile

[User Details](#) [Public Key](#) **API Key** ¹

Verify password* ⓘ ²

Authenticate ³

2. When prompted for your Portal password, type your password into the text field.
3. Click **Authenticate**

Your key will now be displayed. If you have never requested your API key before, a key will be generated for you.

3.4.2. If You Access the Portal Using Single Sign-On (SSO)

To view the API key, or to create a new one:

1. Click **API Key**.

My Profile

[User Details](#) [Public Key](#) **API Key** ¹

2. Your account requires additional authentication. Choose either **Request Code by SMS** or **Request Code by Call**. Your authentication code will be provided via the option selected.

3. Ensure that the confirmation banner is displayed at the top of the screen, which confirms if the code has been sent.
4. Once the code is received, type it into the **Code** field.
5. Ensure that your key is displayed in the **API key** field. If you have never requested your API key before, a key will be generated for you.

WARNING

Protect your web key. Your key is the equivalent of a user name and password that gives access to all your vulnerability data. Treat it as carefully as any other password. Black Duck *strongly* recommends that you never use your Web API Key in your browser. It is only intended for use when accessing the API programmatically. If you do use it directly in a URL, it is logged to your browser history. Therefore, if you must use your Web API Key in your browser, you are strongly encouraged to clear your browser history/cache automatically every time you log out of the Portal. Otherwise, your key will be visible to anyone who gets physical or electronic access to your browser history.

NOTE

For information about configuring SSO for the Continuous Dynamic Portal, see [about-black-duck-sso.pdf](#).

3.5. Regenerating Your API Key

From time to time, it may be necessary to regenerate your existing API key.

To regenerate your API key, perform the following steps:

1. Enter your password in the text field.

BLACKDUCK Continuous Dynamic™

Summary Assets Components Findings Reports Admin

My Profile [Help](#)

User Details Public Key **API Key**

Verify password* ⓘ

Authenticate

2. Click **Authenticate**.
3. Click **Regenerate API Key**.



4. Click **Confirm**.

Regenerate API Key	
Your existing API key will be deleted and a new API key will be generated, okay to proceed?	
Cancel	Confirm

5. A confirmation banner is displayed at the top of the screen, which confirms the API Key has been regenerated.

My Profile

User Details Public Key **API Key**

Your account requires additional authentication. Please request a code to continue. ⓘ

Request Code by SMS Request Code by Call

Code*

Successfully validated.

API key ⓘ

Regenerate API Key

3. Regenerate your API key:

- First, you must request another authentication code by SMS or phone.**
- Enter your new code in the **Code** field (replacing the previous code) and then click **Submit**.
- Click **Regenerate API Key**.
- In the confirmation dialog, click **Confirm** to proceed.

Regenerate API Key

Your existing API key will be deleted and a new API key will be generated, okay to proceed?

Cancel Confirm

A confirmation banner confirms that the API key was successfully regenerated. The new API key is displayed under **API key**:

[Summary](#)[Assets](#)[Components](#)[Findings](#)[Reports](#)[Admin](#)

✓ API key successfully regenerated!



My Profile

[Help](#)[User Details](#)[Public Key](#)[API Key](#)

Your account requires additional authentication. Please request a code to continue. ①

[Request Code by SMS](#)[Request Code by Call](#)

Code*

Successfully validated.

API key ①[Regenerate API Key](#)