Understanding and Managing Business Logic Assessments

Synopsys

2024-04-19

Table of Contents

Chapter 1. Understanding Business Logic Assessments

1.1. Introduction

Business Logic Assessments (BLAs) are manual assessments performed by Threat Research Center engineers for application security vulnerabilities that cannot be tested effectively in an automated fashion. BLAs are intended to complement the automated testing of our WhiteHat service. An annual BLA is included as standard in our PE service. Additional BLA licenses can be purchased separately, for both PE and SE assets.

1.2. Scope

Web applications that utilize Hypertext Transfer Protocol (HTTP) on the application layer, with an underlying Transmission Control Protocol (TCP) transport layer, are eligible for Business Logic Assessments. (The application must also be accessible via a web browser.) BLA coverage extends beyond the base application URL to incorporate any associated host names (URLs) that you provide. Complete functionality coverage for one user access level (role) per application is included with a BLA; any additional user access levels that are provided will only be covered for specific vertical and horizontal authorization tests. The user role with the highest level of access will be used for the full functionality testing, unless you specify otherwise.

Next, see Utilizing Business Logic Assessments to learn how to provide site credentials, schedule a BLA, and review any vulnerabilities that were identified.

Chapter 2. Utilizing Business Logic Assessments

All sites covered under a Premium WhiteHat Dynamic license may receive one annual Business Logic Assessment (BLA). Additional BLAs may be purchased separately. You may also purchase a standalone BLA license for a site that is covered under WhiteHat Dynamic SE (standard dynamic application security testing). If you would like to purchase Business Logic Assessments, please contact Synopsys.

For additional details on any of the following topics, see Site Services Tab.

2.1. Credentialing

In order for a full BLA to be performed, you must provide credentials that will allow the engineers in the Threat Research Center to access your site at the highest level of authorization you want to be tested. To ensure that the site is fully tested, provide credentials with the highest level of authorization available. For more details, see Adding, Editing, or Disabling Business Logic Assessment Credentials.

NOTE

Self-service credentialing is available only for sites covered under a Premium (PE) license. If you want to use a standalone license for a site covered under a Standard (SE) license, contact your Synopsys representative to ensure appropriate credentials are available for the BLA.

2.2. Scheduling your BLA

To ensure that major changes to the site are reviewed promptly, Synopsys recommends scheduling your BLA within the first six months of your contract, or as best suits your business processes.

You can schedule your BLA for any week within your license period for which the TRC Business Logic Analysts are available. We recommend scheduling your BLA early to ensure availability. If there are documents you would like to provide for the reference of the Business Logic Analysts, create a case for our Technical Support department.

If necessary, it is possible to reschedule a BLA that has not yet started in the same interface you used to schedule it. Once your BLA is scheduled, you will see the scheduled BLA in the WhiteHat Dynamic interface when you go to the asset details page for the site in question.

For more details on scheduling your BLA, see Scheduling a Business Logic Assessment.

2.3. Reviewing identified vulnerabilities

Once your BLA has been completed, it is important to review the vulnerabilities that were identified.

To view the completed BLA, go to the asset details page for the site and then select the **Site Services** tab. The completed BLA is listed.

- To see a list of associated vulnerabilities, click **View BLA Verified Vulnerabilities**.
- To generate a report of the vulnerabilities, click **Generate Report**.
- To see details about a given vulnerability, select the specific vulnerability ID.

Site vulnerability details will include the vulnerability class and location as well as the level of risk the vulnerability might pose. From the vulnerability details screen, you can review a summary description of the vulnerability and recommendations for remediating it.

You can also use the "Ask a Question" feature to ask a question directly of the Threat Research Center engineers. This helps ensure you understand the nature of the vulnerability, the risk it poses, and how best to remediate it.

For more information on reviewing the identified BLA-related vulnerabilities, see Reviewing the Completed Business Logic Assessment.

For more information on understanding the Vulnerability Details page, see The Vulnerability Detail Screen: Sites in the WhiteHat Dynamic documentation.

Next, learn more about our proprietary BLA Methodology.

Chapter 3. Methodology

3.1. General Methodology Overview

Our proprietary BLA methodology employs a variety of internal policies and procedures using a combination of browser add-ons, industry standard HTTP proxy tools, and custom tools developed in-house. To provide consistency, a custom-built "Hacklog" tool is used for all BLAs. This tool contains a custom checklist and user-created map of site functionality to ensure testing coverage and provide documentation of all BLA tests performed.

3.2. Production Safety

BLAs are performed with production safety as a top priority. The BLA protocol is designed to avoid any actions that could result in denial of service (DoS) or that could potentially have a negative impact on the application. Special care is taken when testing administrative functionality that could potentially impact other users.

3.3. Business Logic Assessment Services

Business Logic Assessments are included as an annual service in our WhiteHat Dynamic PE services; additional Business Logic Assessments for PE and SE assets can be purchased as add-ons.

Next, learn more about the vulnerability testing that Threat Research Center engineers perform as part of a BLA.

Chapter 4. Testing Overview

Business Logic Assessments search for vulnerabilities based on established industry standards set by WASC and OWASP. The following are the types of tests performed and examples of the vulnerabilities searched for using each test type.

4.1. Injection Testing

Injection testing is used to search for the following vulnerabilities:

- Cross-Site Scripting - Reflective, stored, and DOM
- SQL Injection - both error based and blind
- XML Injection - XML External entities, SOAP, and XPath
- OS Commanding - Standard injections and certain zero day exploits
- Content Spoofing - User controlled error messages, HTML content, Excel export functionality, Flash file FlashVars, Reflected File Download
- URL Redirector Abuse - Standard redirects, login request redirects, logout request redirects, Flash file redirects
- HTTP Response Splitting - CRLF injection into response headers
- LDAP Injection - Login and search functionality
- Improper Input Handling - HTTP parameter pollution, Host Header attacks
- Path Traversal - File upload, file download
- Remote File Inclusion - Server executes remote files

4.2. Inspection Testing

Inspection testing is used to search for the following:

- Fingerprinting - Version information in response headers or body
- Information Leakage - Verbose errors, internal file paths, internal IP addresses, sensitive information in URL
- Autocomplete Attribute - Sensitive inputs including CC and SSN data
- Directory Indexing
- Predictable Resource Location - Common files that are accessible
- Missing Transport Layer Protection - Sensitive content transmitted without SSL/TLS
- ClickJacking

4.3. Authentication and Authorization Testing

Authentication and Authorization tests are used to search for:

- Insufficient Authentication - Insecure Direct Object Reference, weak authentication implementation
- Insufficient Authorization - Access controls, vertical/horizontal privilege escalation

4.4. Session Management Testing

Session Management tests are used to search for:

- Session Prediction - Session token strength and predictability
- Session Fixation - Session token reuse after authentication
- Insufficient Session Expiration - Proper session invalidation
- Unsecured / Non-HTTP-Only Session Cookie - Cookie checks for secure attributes

4.5. Other Logic Testing

In addition to the tests listed above, a BLA also includes assessment of the application’s business logic for vulnerabilities, including:

- Abuse of Functionality - File upload, price modification, contact form abuse
- Brute Force - User enumeration, case insensitive passwords, login automation
- Cross-Site Request Forgery - Sensitive functionality including change password, update profile, creating/deleting content
- Insufficient Password Policy Implementation - Weak passwords
- Insufficient Password Recovery - Password reset workflows including security questions and reset links
- Insufficient Process Validation - Workflow bypasses including registration and checkout
- Application Code Execution - file upload abuse and Server Side Includes
- Insecure Indexing - Search functionality
- Insufficient Anti-automation - Registration, contact forms
- Denial of Service - XML Entity Expansion
- Server Misconfiguration - Web cache deception attack

Next, learn how to manage Business Logic Assessments on the Site Services Tab in the WhiteHat Dynamic interface.

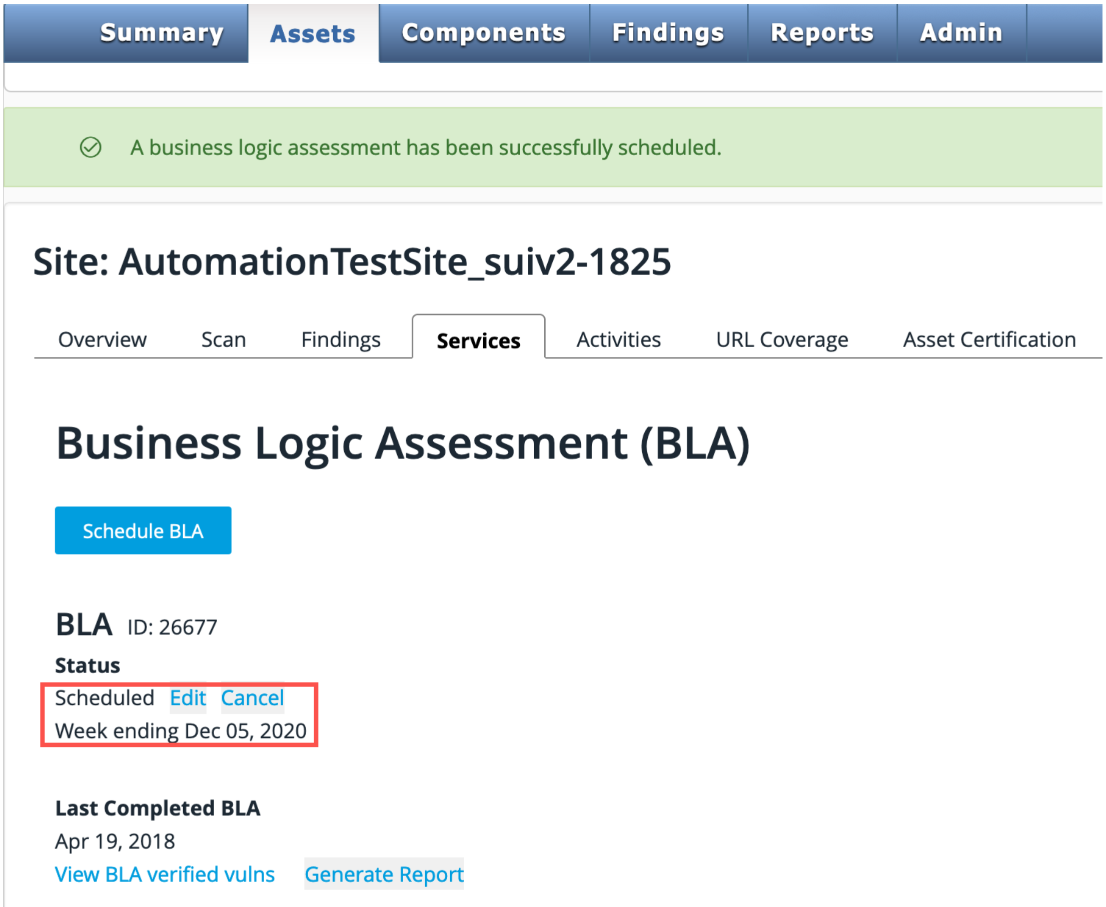
Chapter 5. Site Services Tab

The Site **Services** tab (found on the **Site Details** page for the site in question) allows you to manage your Business Logic Assessments for that site. Within the license period of your Business Logic Assessment (BLA) license, you can:

- Schedule a Business Logic Assessment (BLA) if an unused BLA license is available.
- View the status of a scheduled BLA, if any.
- Edit a future scheduled BLA date, if any.
- Cancel a scheduled BLA.
- View the information on the last completed BLA, if any.
- Add, edit, or delete BLA credentials (for sites covered under PE only).

5.1. BLA Status

You can view the current status of your scheduled BLAs on the Site **Services** tab:



A business logic assessment has been successfully scheduled.

Site: AutomationTestSite_suiv2-1825

Business Logic Assessment (BLA)

BLA ID: 26677

Status

Scheduled

Week ending Dec 05, 2020

Last Completed BLA

Apr 19, 2018

NOTE

You must schedule your BLA during the license period.
If the BLA license period expires without a BLA being scheduled, the business logic

assessment will no longer be available.

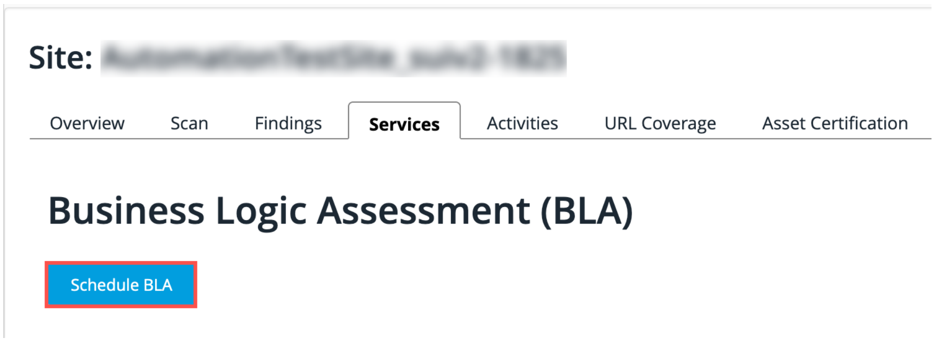
The status of each BLA is displayed:

Status	Description
Scheduled	This BLA has been scheduled for the date shown.
In Progress	This BLA is now in progress.
On Hold	An issue is preventing the BLA from starting; the BLA has been placed on hold pending resolution of that issue. You must resolve the issue before the BLA can be rescheduled and completed as planned. A BLA in **On Hold** status will show an explanation of the issue. To confirm the resolution of an **On Hold** BLA, refer to the associated Salesforce case. This case is referenced in the UI and in the *Business Logic Assessment on hold notice* email that was sent to you.
Reschedule Failed	On rare occasions, it may not be possible to reschedule the BLA automatically. If this happens, either because no date within the license period is available or for any other reason, please contact Synopsys for resolution. Note that if your license period expires before you schedule or reschedule your BLA, that BLA will no longer be available.

5.2. Scheduling a Business Logic Assessment

If you have a license for a Business Logic Assessment (BLA) available, the **Schedule BLA** button is active.

1. Click **Schedule BLA** to begin the scheduling process. To add a license or enquire regarding a license that is not displayed, please contact your Customer Service representative or reach out to Customer Service at support@whitehatsec.com. Note that a BLA can only be scheduled during the associated license period.



Site: [redacted]

Business Logic Assessment (BLA)

NOTE A reminder popup is displayed if you attempt to schedule a BLA but have not yet entered any BLA credentials.

2. You can enter credentials at this point or choose to schedule your BLA without credentials; however, we strongly recommend that you provide credentials to be used in the BLA. If no credentials are provided, the BLA will be performed on only the unauthenticated portions of your site. To ensure the whole of your site undergoes Business Logic Analysis, be sure to provide valid credentials.

For information on entering credentials, see Adding Business Logic Assessment Credentials below.

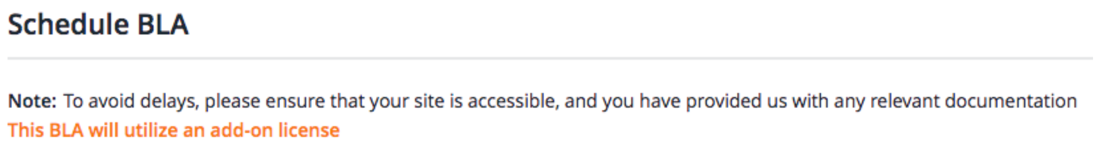
WARNING

Do not edit BLA credentials while a BLA is in progress.
Doing so will result in inconsistencies in your BLA.

The **Schedule BLA Wizard** will walk you through the process of scheduling your BLA.

5.2.1. License Used

The license type that will be used for the BLA you are scheduling will be described at the top of the BLA Scheduling popup. If you have a PE BLA license, that license will be used first; if you will be using an add-on license, that information will be noted here. For example:



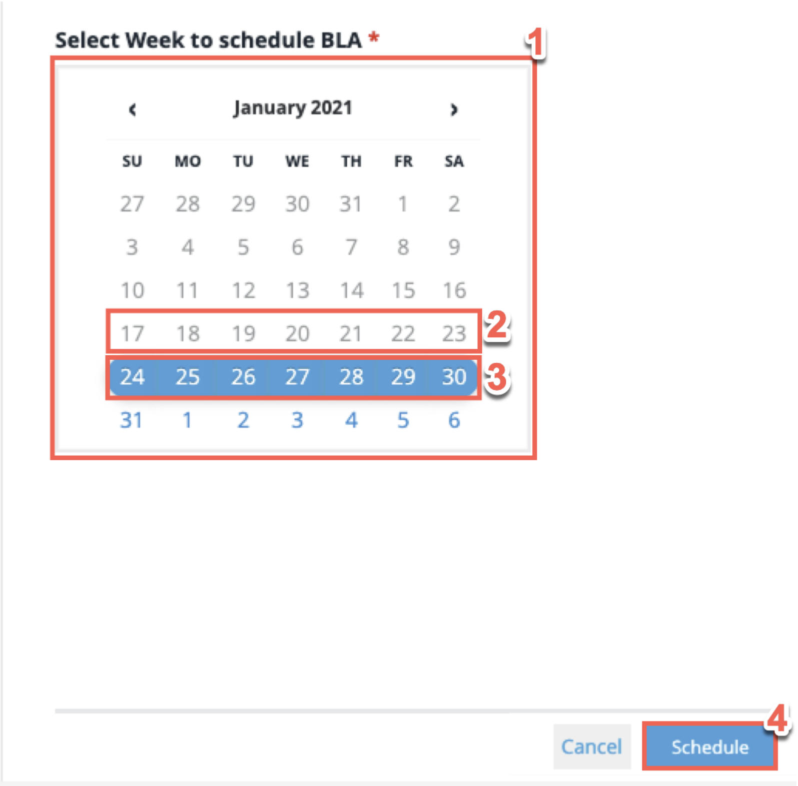
Schedule BLA

Note: To avoid delays, please ensure that your site is accessible, and you have provided us with any relevant documentation

This BLA will utilize an add-on license

5.2.2. Week Scheduled for BLA

1. Use the calendar below the license type to schedule the BLA. Enter < and > to navigate month-by-month and then select the week you would like to schedule. You can only schedule for the current week at the beginning of the week in question, and only if Business Logic Analysts are available.



Select Week to schedule BLA *

January 2021

SU	MO	TU	WE	TH	FR	SA
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

2. Unavailable weeks are shown in gray (See January 17th - 23rd). Weeks outside of your license period will also be shown in gray.
3. Available weeks are shown in blue. The selected week will show a blue highlight as seen for the week of January 24th - 30th above.
4. Select **Schedule** to confirm the dates chosen for your BLA.

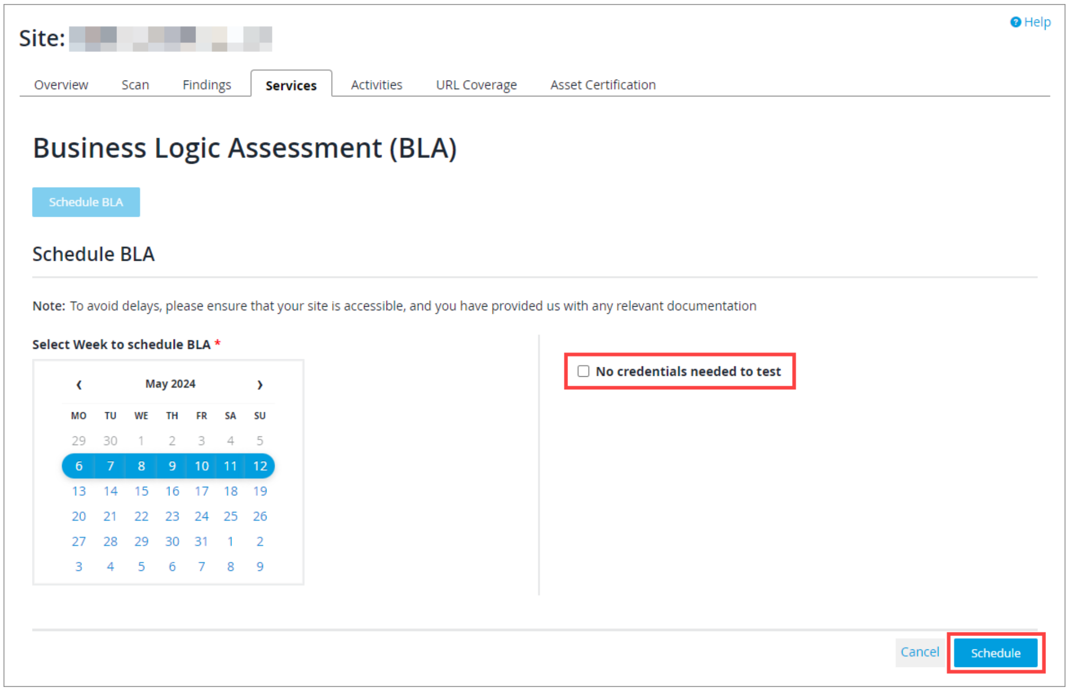
You will receive email confirmation when your BLA has started. If you need to provide additional information, see Providing Information for your BLA.

NOTE

In order to provide an excellent level of service for our customer base, Synopsys' manual testing team can conduct a maximum number of Business Logic Assessments each week. Although Synopsys has one of the largest manual testing teams in the world, this capability is still a finite resource and can be subject to high demand, especially at quarter and year ends. Your Customer Support or Program Manager will work with you to identify urgent needs and help determine a scheduling plan for assessments.

5.2.3. 'No Credentials Needed' Confirmation Checkbox

1. If you decide to have a BLA performed without BLA credentials, select the **No credentials needed to test** checkbox to the right of the calendar. If no BLA credentials are available, this box is checked by default and can only be unchecked if BLA credentials are available.

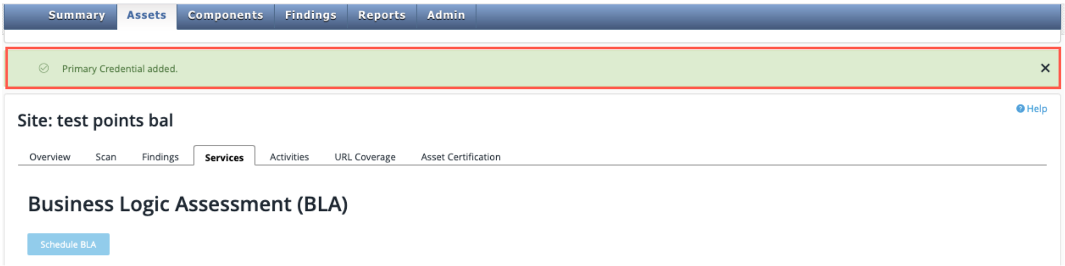


Note: To avoid delays, please ensure that your site is accessible, and you have provided us with any relevant documentation

MO	TU	WE	TH	FR	SA	SU
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

2. When you have selected the week for the BLA to be performed, and ensured that credentials are available or checked the **No credentials needed** checkbox, click **Schedule** to schedule your BLA.

3. Once you have added your primary credentials, you will see a confirmation banner at the top of the page. If you need to make changes, you can edit your credentials on the **Services** page.



Primary Credential added.

Site: test points bal

5.2.4. Providing Information for your BLA

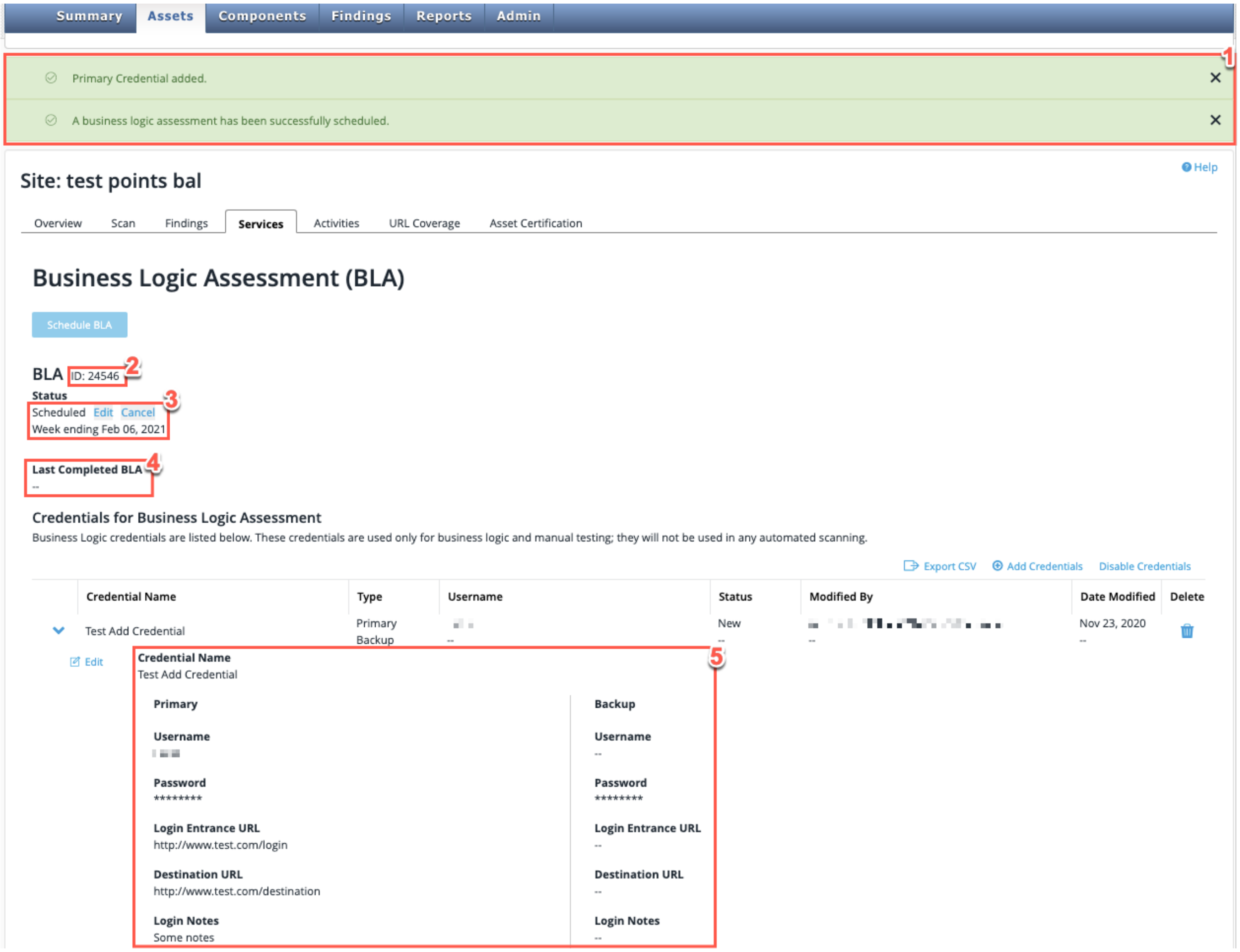
If you want to provide extra information, instructions, or attachments related to your BLA, open a case in the Synopsys Software Integrity Community. You should provide any extra information before the scheduled start date of your BLA.

5.2.5. Canceling a Scheduled BLA

If you need to cancel a Business Logic Assessment, you can do so as long as the assessment is not already in progress. Under the **Assets** tab, select the **Services** sub-tab. Click the **Edit** link next to the scheduled BLA. A confirmation text box displays, asking for a reason for cancellation.

5.3. Reviewing the Completed Business Logic Assessment

Once a Business Logic Assessment has completed, the summary information for that BLA displays on the **Services** tab.



Primary Credential added.

A business logic assessment has been successfully scheduled.

Site: test points bal

Business Logic Assessment (BLA)

BLA ID: 24546

Status

Scheduled Edit Cancel

Week ending Feb 06, 2021

Last Completed BLA

--

Credentials for Business Logic Assessment

Business Logic credentials are listed below. These credentials are used only for business logic and manual testing; they will not be used in any automated scanning.

	Credential Name	Type	Username	Status	Modified By	Date Modified	Delete
	Test Add Credential	Primary Backup	[redacted] --	New --	[redacted] --	Nov 23, 2020 --	

Edit

Credential Name

Test Add Credential

Primary	Backup
Username [redacted]	**Username** --
Password ********	**Password** ********
Login Entrance URL http://www.test.com/login	**Login Entrance URL** --
Destination URL http://www.test.com/destination	**Destination URL** --
Login Notes Some notes	**Login Notes** --

Field No.	Field Name	Description
1	**Confirmation banner**	Once the primary credentials are added and the BLA is scheduled, these confirmation banners will appear on the **Services** page.
2	**ID number**	When a BLA has been successfully scheduled a unique identifying number will be displayed.
3	**Scan Status**	This will display the current status of your BLA and the dates the scan is due to commence.

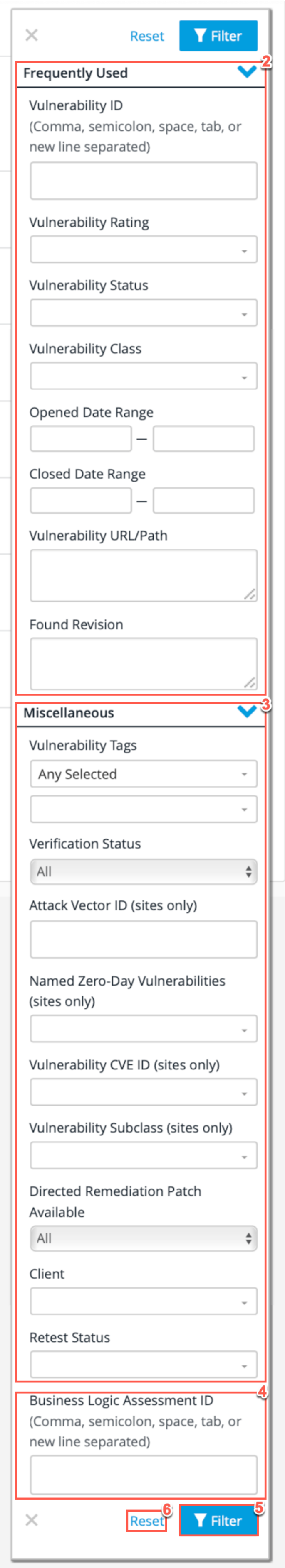
Field No.	Field Name	Description
4	**Last completed BLA**	This will display most recent date of the last completed BLA. This will include the date the BLA was completed and a link allowing you to view the verified vulnerabilities identified in the BLA or to generate a report of those vulnerabilities. In addition, you can view all vulnerabilities associated with a specific BLA or with all BLAs performed for this asset on the Asset Details page or on the Findings page.
5	**Credential Details**	This drop down section for the added credentials displays the details of the primary and backup credentials.

5.3.1. Filtering For Your BLA Findings

When you click **View BLA Verified Vulnerabilities** under **Last Completed BLA**, the **Findings** page displays with a pre-set filter to show you only vulnerabilities that were verified during this specific BLA. You can edit this filter to see vulnerabilities that are associated with additional Business Logic Assessment(s) by ID.

To filter the table:

1. Click the **Filter** button.



Frequently Used

Vulnerability ID
(Comma, semicolon, space, tab, or new line separated)

Vulnerability Rating

Vulnerability Status

Vulnerability Class

Opened Date Range

Closed Date Range

Vulnerability URL/Path

Found Revision

Miscellaneous

Vulnerability Tags: Any Selected

Verification Status: All

Attack Vector ID (sites only)

Named Zero-Day Vulnerabilities (sites only)

Vulnerability CVE ID (sites only)

Vulnerability Subclass (sites only)

Directed Remediation Patch Available: All

Client

Retest Status

Business Logic Assessment ID
(Comma, semicolon, space, tab, or new line separated)

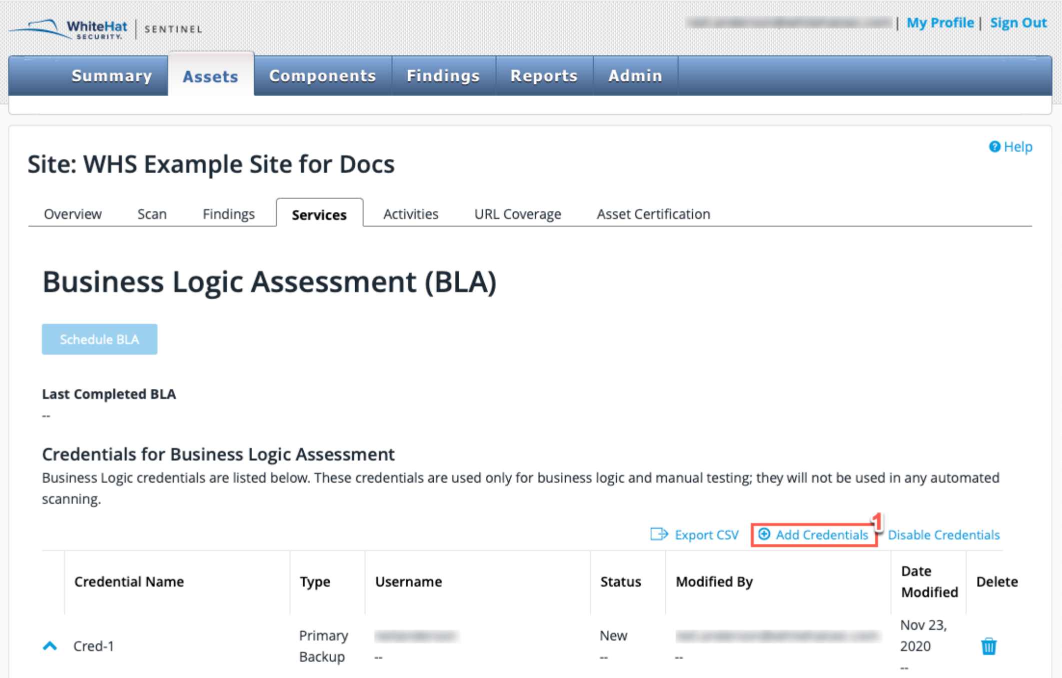
Field No.	Field Name	Description
2	**Frequently Used Filter Options**	These are the most frequently used filters including: • Vulnerability ID • Vulnerability rating • Vulnerability status • Opened date range etc. You can select as many, or as few filters as you require to filter your list of findings.
3	**Miscellaneous**	These are further filter options available to refine your vulnerability findings, including: • Vulnerability Tags • Verification Status • Attack Vector ID • Client • Retest Status etc.
4	**Business Logic Assessment ID**	Enter your BLA ID number here, BLA ID numbers for scheduled BLAs can be seen on the **Services** subtab of the site details page.
5	**Filter**	Select the **Filter** icon to filter all listed vulnerabilities by your filters selected in the previous three steps.
6	**Reset**	Click this to clear all selected filters. **NOTE** Failure to reset the filter means that the filtered results will display the next time that you access the Findings tab. The filter remains in place even after logging out of the WhiteHat Portal and logging back in again. So if you have finished with the filter, use **Reset**.

5.4. Adding, Editing, or Disabling Business Logic Assessment Credentials

5.4.1. Adding Credentials

For sites covered under the WhiteHat Dynamic Premium (PE) service, you can manage your BLA credentials directly in the WhiteHat Portal.

1. Click **Add Credentials** to add site credentials. If you are using a stand-alone BLA license for a site that is covered under the WhiteHat Dynamic Standard (SE) service, please contact Synopsys with your credential information.



Site: WHS Example Site for Docs

Business Logic Assessment (BLA)

Last Completed BLA

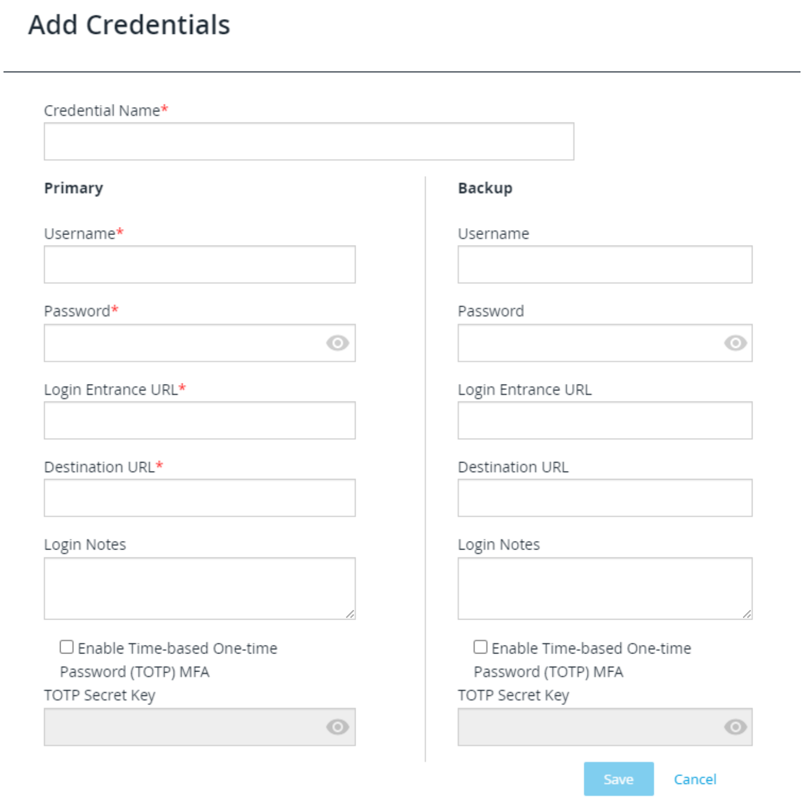
--

Credentials for Business Logic Assessment

Business Logic credentials are listed below. These credentials are used only for business logic and manual testing; they will not be used in any automated scanning.

	Credential Name	Type	Username	Status	Modified By	Date Modified	Delete
^	Cred-1	Primary Backup	[redacted] --	New --	[redacted] --	Nov 23, 2020 --	🗑

2. To create BLA credentials, you must first enter a **Credential Name**. This displays on the **Services** tab.



3. Provide **Primary** login information, which includes:
    - **Username**
    - **Password**
    - **Login Entrance URL**
    - **Destination URL**
4. Add any additional **Login Notes** required for this set of credentials.
5. If the site uses Multi-Factor Authentication (MFA), where users authenticate using a time-based one-time password (TOTP) generated in an authenticator app, perform the following steps:
    a. Select the **Enable Time-based One-time Password (TOTP) MFA** checkbox.
    b. Enter the secret key for your MFA provider account in the **TOTP Secret Key** field.

NOTE	WhiteHat Dynamic supports any TOTP generator - for example, Google Authenticator or Duo Mobile - as long as you provide a secret key. The TOTP provider must uses SHA1 encryption and Base32-encoded secret keys.

6. We strongly recommend including a **Backup** login as well.
7. When you have populated all information fields, click **Save** to save this set of credentials.

NOTE	For information about using SMS-based two-factor authentication for assessments, see SMS-Based Two-Factor Authentication in the WhiteHat Dynamic documentation.

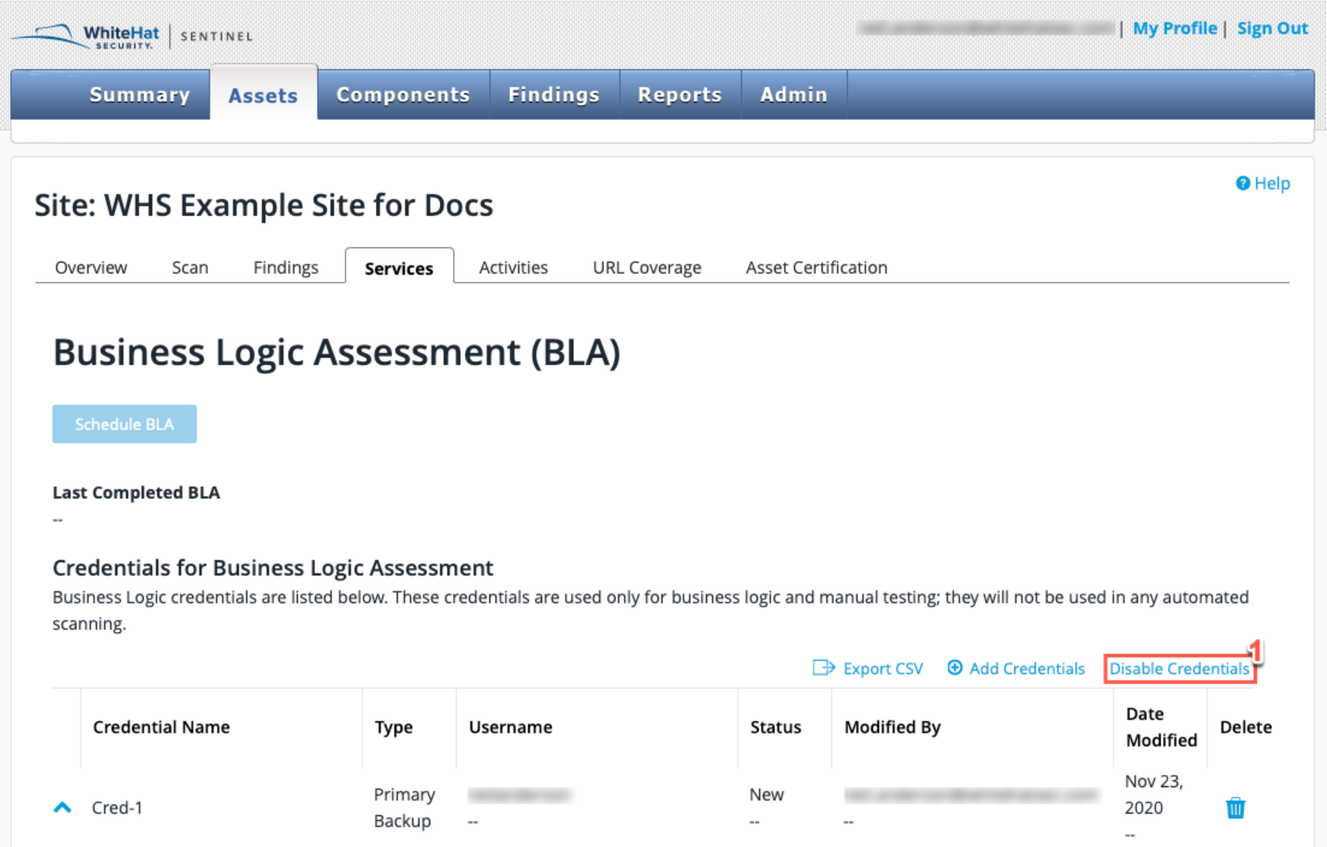
5.4.2. Editing BLA Credentials

To edit BLA credentials, perform the following steps:

1. Click the down arrow next to the credentials you want to edit.
2. Click **Edit** to enable editing.
3. Click **Save** to keep the changes made.

5.4.3. Disabling BLA Credentials

1. Select the set of credentials to disable, and then click **Disable Credentials**.



Site: WHS Example Site for Docs

Business Logic Assessment (BLA)

Last Completed BLA

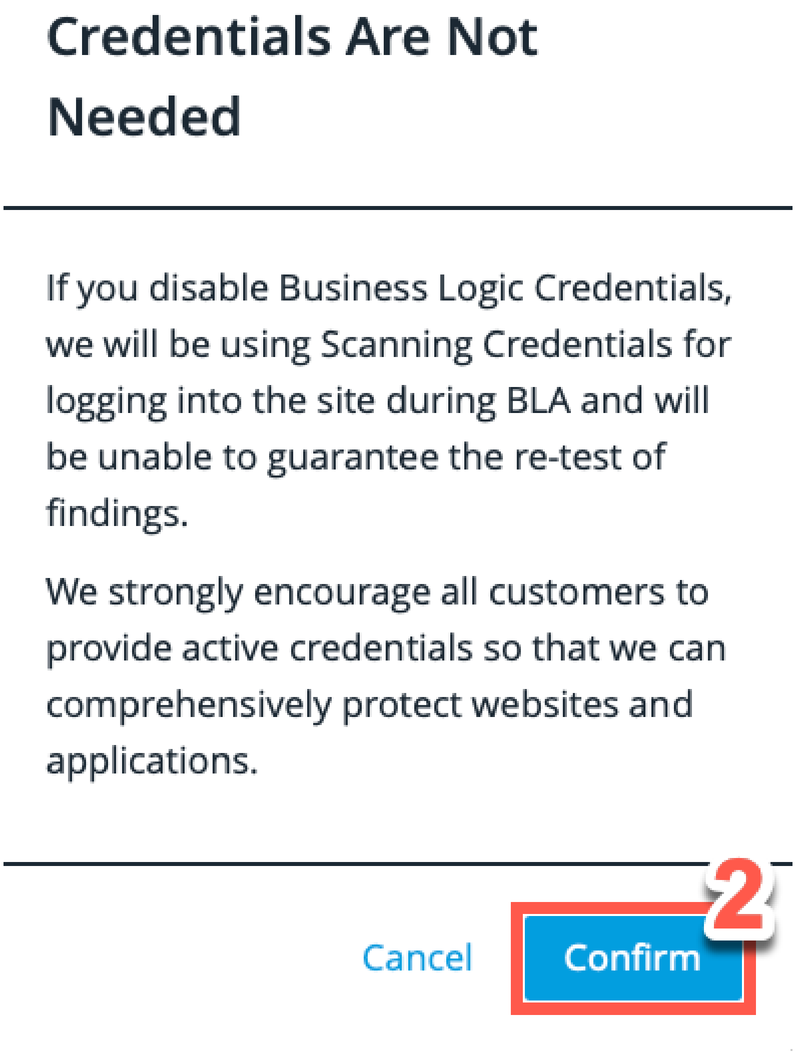
--

Credentials for Business Logic Assessment

Business Logic credentials are listed below. These credentials are used only for business logic and manual testing; they will not be used in any automated scanning.

Credential Name	Type	Username	Status	Modified By	Date Modified	Delete
Cred-1	Primary Backup	[redacted] --	New --	[redacted] --	Nov 23, 2020 --	🗑

2. In the **Credentials Are Not Needed** dialog, select the **Confirm** icon to remove the selected credentials.



Credentials Are Not Needed

If you disable Business Logic Credentials, we will be using Scanning Credentials for logging into the site during BLA and will be unable to guarantee the re-test of findings.

We strongly encourage all customers to provide active credentials so that we can comprehensively protect websites and applications.

Disabled credentials will no longer be used for Business Logic Assessments. Please replace any credentials being disabled to ensure that your BLA can be completed appropriately.

5.4.4. Setting Up Email Notification for BLA Status Changes

If you would like to receive email notifications for particular BLA status changes, you can set that in your Profile.