

# ***Bravura Security Fabric* Implementation:**

## **Email Notification**

One of the early tasks in a *Hitachi ID Bravura Security Fabric* deployment is to set up an email notification system.

This document contains:

- Requirement
- Solution
- Use case: Sending email when a user is locked out
- Configuration via the wfemail component

## **1 Requirement**

Product administrators need to be notified of events on the *Bravura Security Fabric* server, such as:

- Replication issues
- Auto-discovery issues (listing or loading of the data)
- Disk space issues on the Hitachi ID Suite server
- Long running processes
- Windows Event Log errors

End users need to be notified of actions to take or events that affect them; for example, send users emails when:

- There is an intruder lockout on their account.
- Their passwords are successfully changed.
- There are problems setting passwords, including when there will be automated retry attempts.
- Their password is about to expire.
- They need to enroll.

## 2 Solution

*Hitachi ID Bravura Security Fabric* actively notifies users about events that may require their attention; this is generally done through email. Some *Bravura Security Fabric* features, such as *authorization workflow*, require the ability to notify users and rely heavily on this interaction.

For a production deployment, Hitachi ID Systems recommends that all users have an email address defined in *Bravura Security Fabric*. In most cases, *Bravura Security Fabric* determines email addresses by the value of the EMAIL profile attribute, which can be mapped to an account attribute on a given target system; for example, the EMAIL profile attribute is mapped to the mail attribute in an Active Directory target system by default.

Other options for defining email addresses are detailed in *Determining users' email addresses*.

## 3 Use case: Sending email when a user is locked out

This use case shows you how to configure *Hitachi ID Bravura Security Fabric* to send an email to an administrator when a user is locked out due to too many failed login attempts.

### Requirements

This use case assumes that:

- *Hitachi ID Bravura Security Fabric* and *Hitachi ID Connector Pack* are installed.
- An Active Directory system has been targeted as a source of profiles.
- All users have values defined in the mail attribute on the Active Directory target system.

### Configure email settings

To configure email settings:

1. Log in to *Bravura Security Fabric* as `superuser`.
2. Click **Manage the system** → **Workflow** → **Email configuration**.

**Note:** When you select the **Workflow** tab, *Bravura Security Fabric* directs you to the **Email configuration** menu until the required variables are set.

3. Note the following settings which are set during installation:

**BASE IDSYNCH URL** The URL that will display in all emails to direct users to the *Hitachi ID Bravura Security Fabric* application.

**GLOBAL MAIL PLUGIN** The plugin that sends email to users.

The default setting, `global-mail-plugin`, is overwritten by the `hid_policy_wfemail` component to use the `plugin_wfemail.py` plugin.

**GLOBAL MAIL PLUGIN DIR** The directory path to store messages when they are written to a file.  
The default is `<Program Files path>\Hitachi ID\IDM Suite\Logs\<instance>\mail`.

4. Set the following:

**MAIL SEND METHOD** `SMTP, FILE`

These are the delivery options for notification messages. When the **MAIL SEND METHOD** value includes `FILE`, it writes to a file in the directory specified by **GLOBAL MAIL PLUGIN MAIL DIR**, which by default is `<Program Files path>\Hitachi ID\IDM Suite\Logs\<instance>\mail`. When the value includes `SMTP`, the plugin sends emails.

**MAIL\_SERVER** `<mail server address>` This can be `localhost`.



**RECIPIENT\_EMAIL** The comma-delimited list email addresses of the *Bravura Security Fabric* administrators who should receive notification of events relating to the running of the server; for example `admin@example.corp`.

**SENDER\_EMAIL** The email address that will appear as the sender of emails;  
for example `bravura@example.corp`.

5. Click **Update**.

### Configure the event action

To set up an email action when a user is locked out of *Bravura Security Fabric*:

1. Click **Manage the system** → **Policies** → **Login options**.
2. Select **Configure event**  under the **USER LOGIN LOCKOUT** field.  
A pop-up form appears.
3. Select **Each time this event occurs**  under **send email**.
4. Define the message; for example:

**To** `admin@example.corp`

**From** `bravura@example.corp`

**Subject** `User Lockout`

**Message body** `Due to several failed password attempts  
%USERID% has been locked out. Check for suspicious behavior.`

**Note:** The **Event action strings help** link at the bottom left of the form gives you a guide to variable strings that you can use in the message body.

5. Click **Update**.
6. Close the pop-up form.
7. Click **Update**. The settings will be saved.

## Test the event action

To test the event action:

1. As an end user, in this example `abrahb`, attempt to log into *Hitachi ID Bravura Security Fabric* with the wrong password until you are locked out (3 attempts).
2. Open your email client as the admin user, or go to the `<Program Files path>\Hitachi ID\IDM Suite\→Logs\<instance>\mail\` directory.

You should see that there is a "User lockout" message. Open this message to confirm that it appears as you intended.

**Note:** When the MAIL SEND METHOD includes `FILE` a copy of this email will also be created in the the `<Program Files path>\Hitachi ID\IDM Suite\Logs\<instance>\mail\` directory as a `<date>.eml` file.

3. Open an Administrator Command Prompt and navigate to:  
`<Program Files path>\Hitachi ID\IDM Suite\<instance>\util\`
4. Run the following command to unlock the user:

```
userunlock.exe -user abrahb
```

5. Close the command prompt.

## 4 Configuration via the wfemail component

The component framework provides a way to manage what emails are sent by *Hitachi ID Bravura Security Fabric* to notify and remind users and authorizers of workflow events, including the following:

- Authorizer approvals, denials, and escalations
- Delegation requests
- Batch processing events

The `Functional.hid_policy_wfemail` component controls policy settings for all of the available workflow events in *Bravura Security Fabric*.

This component provides a policy table that allows granular control over the behavior of individual events within *Bravura Security Fabric*. Each event can be configured to send messages to end users via either email or push notification. Each event can also be configured to write sent emails to a file. In addition, the policy table allows any workflow event notification to have its original subject and body overwritten, which permits an administrator to provide their own formatting, structure and logic to *Bravura Security Fabric*.

Installing `Functional.hid_policy_wfemail` will automatically set `GLOBAL_MAIL_PLUGIN` to `wfemail.py`. See the [Bravura Security Fabric Documentation](#) for more information about installing components.

In order to complete email configuration, you must:

## Bravura Security Fabric 12.2.4 Implementation: Email Notification

1. Configure workflow options in **Manage the system** → **Workflow** → **Options** → **Email configuration**, including the email server and sender address.
2. Verify that the HID\_POLICY\_WFEMAIL table in the external data store (**extdb**) is configured for your environment.
3. Configure events to send messages to users via email or push notification.

Manage external data store

Table information hid\_policy\_wfemail

Records to display: 20

Delete	StageNumber	RuleNumber	EventID	Description	PolicyStatus	SendSMTP
<input type="checkbox"/>	1	1	_DEFAULT_POLICY	Default policy rule	Default	True
<input type="checkbox"/>	1	2	_DEFAULT_REPORT	Report policy rule	Default	True
<input type="checkbox"/>	1	3	EVENT_ARCH_CICO_PASSWORD_RANDOMIZED_EMAIL	ARCH CICO Email	Default	False
<input type="checkbox"/>	1	4	EVENT_ARCH_CICO_NOTIFY_USERS_CHECKOUT	ARCH CICO Email	Default	False
<input type="checkbox"/>	1	5	EVENT_ARCH_CICO_NOTIFY_USERS_CHECKOUT_TIMECHANGE	ARCH CICO Email	Default	False
<input type="checkbox"/>	1	6	EVENT_ARCH_CICO_NOTIFY_USERS_CHECKOUT_PENDING	ARCH CICO Email	Default	False
<input type="checkbox"/>	1	7	EVENT_ARCH_CICO_NOTIFY_QUEUED_USERS	ARCH CICO Email	Default	False
<input type="checkbox"/>	1	8	EVENT_ARCH_CICO_NOTIFY_EXPIRED_USER	ARCH CICO Email	Default	False
<input type="checkbox"/>	1	9	EVENT_ARCH_CICO_NOTIFY_REVOKED_USER	ARCH CICO Email	Default	False
<input type="checkbox"/>	1	10	EVENT_ARCH_CICO_NOTIFY_REVOKED_PENDING_USER	ARCH CICO Email	Default	False