

OpenText™ SOAR Integrations

Email and notification configuration guide

Version : 26.2

PDF Generated on : April 10, 2026

Table of Contents

1. Email and notification configuration guide	1
1.1. Overview of the SOAR notification system	2
1.2. Set up notifications in SOAR	5
1.3. Configure notification channels	9
1.3.1. User decision notifications	10
1.3.2. Workflow approval (analyst decision) notifications	16
1.3.3. Case notification	19
1.3.4. Workflow notification	23
1.3.5. Action and rollback approval notification	27
1.3.6. Action and rollback notification	32
1.3.7. Enrichment notifications	35
1.3.8. Use automation bits	37
1.4. SMTP mail server capabilities	42
1.5. Template parameter reference	50
1.6. Troubleshoot common notification issues	55

1. Email and notification configuration guide

This guide provides a comprehensive reference for configuring and managing the OpenText SOAR Email & Notification System. It covers the end-to-end notification workflow, from enabling notifications and creating templates to configuring individual notification channels and troubleshooting common issues. Practical examples and sample templates are included throughout to support immediate implementation

Intended audience

This document is intended for SOAR administrators and security analysts responsible for managing and configuring notifications within the SOAR platform. Familiarity with SOAR playbook concepts and basic HTML is helpful but not required.

1.1. Overview of the SOAR notification system

SOAR provides a built-in notification system that keeps analysts, administrators, and stakeholders informed about security incidents, playbook progress, and actions taken on integrated systems. Notifications are delivered through email and are driven by configurable templates that support dynamic parameters.

The notification system serves two primary purposes:

- **Operational awareness** — Informing analysts and case owners about changes to cases, playbook progress, enrichment results, and actions executed on external systems.
- **Approval workflows** — Requesting confirmation from system administrators or integration owners before SOAR executes actions (such as blocking an IP on a firewall) or rolling back previously executed actions.

Notification types

SOAR supports the following notification types:

Notification Type	Purpose
User Decision	Asks end users true/false questions to gather input during playbook execution.
Workflow Approval (Analyst Decision)	Asks analysts for their decision via email at playbook analyst decision elements.
Case Notification	Notifies assignees and watchers when a case attribute changes (status, severity, labels, etc.).
Workflow Notification	Informs analysts or analyst groups about playbook progress and case details.
Action & Rollback Approval	Requests confirmation from integration owners / system admins before executing or rolling back an action.
Action & Rollback Notification	Notifies designated contacts about actions taken on an integration.
Enrichment Notification	Notifies analysts about enrichment execution results.

Each notification type has its own default template and supports a specific set of dynamic parameters that are automatically populated at runtime.

Notification workflow

The following is the typical notification workflow in SOAR:

1. A trigger event occurs (case change, playbook step, action execution, etc.).
2. SOAR resolves the appropriate notification template.
3. Dynamic parameters in the template are replaced with runtime values.
4. SOAR sends the notification through the configured SMTP server.

For approval-type notifications, SOAR monitors the recipient's reply to determine the next step in the workflow.

1.2. Set up notifications in SOAR

This section covers the prerequisites and initial configuration steps required before notifications can be sent.

Prerequisites

Before configuring notifications, ensure the following:

- **SMTP server:** An SMTP Mail Server must be configured under **Respond > Configuration > Integrations**. This is required for all email-based notifications, including those sent from automation bits using the `atar.notify()` method.
- **User permissions:** The user configuring templates must have access to the **Respond > Configuration > Customization Library** menu.
- **SOAR configuration parameters:** To manage notifications, configure the following parameters under **Respond > Configuration > Parameters**:

Parameter	Description	Type
ApprovalEMailEnabled	Enables action and rollback approval emails.	Boolean. Default: False
ApprovalEMailFrom	From address used to send user decision notifications, action and rollback approval emails.	String. e.g., john.doe@example.com
CaseNotificationURL	SOAR URL added in notifications.	String. e.g., https://OpenText SIEM/soar/? tenant=default
IncomingMailIntegration	Integration ID of SMTP server for incoming mail. SMTP integration should be configured with IMAP.	Integer.
NotificationEMailFrom	From address used to send notification emails.	String. e.g., john.doe@example.com
OutgoingMailIntegration	Integration ID of email server for outgoing mail. Required for sending notification emails.	Integer.

Manage templates

Notification templates are managed under the **Configuration > Customization Library menu**. SOAR ships with a set of default templates, one for each notification type:

Default Template Name	Notification Type
User Decision Notification Email Template	User Decision
Workflow Approval E-mail Template	Workflow Approval
Case Notification Template	Case Notification
Workflow Notification E-mail Template	Workflow Notification
Action Approval E-mail Template	Action Approval
Rollback Approval E-mail Template	Rollback Approval
Action Notification E-mail Template	Action & Rollback Notification
Enrichment Notification E-mail Template	Enrichment Notification

You can modify the default templates or create custom templates and reference them in your playbooks.

Create a template

To create a notification template:

1. Navigate to **Configuration > Customization Library**.

2. Click **Create New Customization**.
3. Fill in the **Name** and **Description** fields.
4. Select the template **Type** as **HTML template**.
5. Write your template content using the supported parameters for the notification type.
6. Click **Save**.

**Note**

You can create as many custom templates as needed and assign them to different playbook elements. This is particularly useful when different playbooks require different notification formats or levels of detail.

1.3. Configure notification channels

This section covers each notification type in detail, including its purpose, available parameters, and a sample HTML template ready for use.

- [User decision notifications](#)
- [Workflow approval \(analyst decision\) notifications](#)
- [Case notification](#)
- [Workflow notification](#)
- [Action and rollback approval notification](#)
- [Action and rollback notification](#)
- [Enrichment notifications](#)
- [Use automation bits](#)

1.3.1. User decision notifications

User decisions are True/False type of checkpoints used to request end users or organizational users for input about certain situations — for example, asking whether they are aware of a failed log in attempts on their account.

When a user decision notification is sent, the recipient replies with a keyword to indicate their answer. SOAR reads the reply using the "IncomingMailIntegration" configured and follows the corresponding branch in the playbook:

- **Approve keyword** → SOAR follows the "True" leg of the User Decision element.
- **Deny keyword** → SOAR follows the "False" leg of the User Decision element.

Both keywords are configured in the playbook.

User Decisions use the following default template file under **Configuration > Customization Library menu**:

- User Decision Notification Email Template

You can create as many templates as you need and use them in playbooks.

Parameters

Parameter / Group	Description	Type
<code>\$rule.name\$</code>	Playbook name.	String
<code>\$approveKeyword\$</code>	Keyword the user replies with to follow the "True" leg. Set in playbook.	String
<code>\$denyKeyword\$</code>	Keyword the user replies with to follow the "False" leg. Set in playbook.	String
Case Parameters	See Template Parameter Reference section for the full list.	—

Sample HTML template

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<meta charset="UTF-8">
```

```
<title>Your approval required!</title>
```

```
</head>
```

```
<body>
```

```
Hello,<br>
```

```
<br>
```

```
Multiple login attempts have been detected for your account and we need your confirmation about it. <br>
```

```
Are you aware of this activity? <br>
```

```
<br>
```

```
<b>Remote System:</b> $source$ <br>
```

```
<b>User Account:</b> $user$ <br>
```

```
<br>
```

```
Your case details:<br>
```

```
<b>ID:</b> $case.serial$<br>
```

```
<b>Date:</b> $case.creationTime$ <br>
```

```
<b>SOC Team Member:</b> $case.assignee.name$: $case.assignee.email$
```

```
<br>
```

```
<br>
```

```
Please simply send a reply with $approveKeyword$ or $denyKeyword$<br><br>
```

```
Kind Regards,<br>
```

```
SOC Team.<br>
```

```
</body>
```

```
</html>
```

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<meta charset="UTF-8">
```

```
<title>Your approval required!</title>
```

```
</head>
```

```
<body>
```

```
Hello,<br>
```

```
<br>
```

```
Multiple login attempts have been detected for your account and we need your confirmation about it. <br>
```

```
Are you aware of this activity? <br>
```

```
<br>
```

```
<b>Remote System:</b> $source$ <br>
```

```
<b>User Account:</b> $user$ <br>
```

```
<br>
```

```
Your case details:<br>
```

```
<b>ID:</b> $case.serial$<br>
```

```
<b>Date:</b> $case.creationTime$ <br>
```

```
<b>SOC Team Member:</b> $case.assignee.name$: $case.assignee.email$
```

```
<br>
```

```
<br>
```

```
Please simply send a reply with $approveKeyword$ or $denyKeyword$<br><br>
```

```
Kind Regards,<br>
```

```
SOC Team.<br>
```

```
</body>
```

```
</html>
```

1.3.2. Workflow approval (analyst decision) notifications

Workflow approvals are used to ask analysts for their decision via email at playbook analyst decision elements. This is commonly used when a playbook reaches a point that requires human judgment before proceeding.

Unlike user decisions (which are true/false), workflow approvals present the analyst with case context and a link to the SOAR interface to review and proceed.

Workflow approval notifications use the following template file under **Configuration > Customization Library** menu:

- Workflow Approval E-mail Template

Parameters

Parameter / Group	Description	Type
\$rule.name\$	Playbook name.	String
\$description\$	Description added to the playbook analyst decision element.	String
Case Parameters	See Template Parameter Reference section for the full list.	—

Sample HTML template

```

<!DOCTYPE html>
<html>
<head>
<style>
table {
  font-family: arial, sans-serif;
  border-collapse: collapse;
  width: 100%;
}
td, th {
  border: 1px solid #dddddd;
  text-align: left;
  padding: 8px;
}
tr:nth-child(even) {
  background-color: #dddddd;
}
</style>
<meta charset="UTF-8">
<title>OpenText SIEM SOAR Playbook Decision for Case Id: $case.serial$</title>
</head>
<body>
Hello,<br>
<br>
A case is waiting for your decision. Please review and proceed the playbook.<br>
<br>
<b>Decision Details:</b> $description$
<br><br>
Case Details:<br>
<table>
  <tr><td>Case</td><td><a href="https://OpenText SIEM/ soar/?
tenant=default#/cases/$case.serial$" >
  $case.serial$ - $case.subject$</a></td></tr>
  <tr><td>Description</td><td>$case.description$</td></tr>
  <tr><td>Assignee</td><td>$case.assignee.name$</td></tr>
  <tr><td>Severity</td><td>$case.ticketSeverity.name$</td></tr>
  <tr><td>Status</td><td>$case.ticketStatus.name$</td></tr>
  <tr><td>Labels</td><td>$case.labels :{LABEL | "$LABEL.name$" }$</td></tr>

```

```
</table>  
<br><br>  
Kind Regards,<br>  
SOC Team.  
</body>  
</html>
```

1.3.3. Case notification

Case notifications automatically inform the case assignee and watchers when a change occurs on a case. SOAR monitors and reports changes to the following attributes:

- Assignee and watcher(s)
- Severity
- Status
- Labels
- Description
- Subject / Title
- Comments

Parameters

Parameter / Group	Description	Type
<code>\$events\$</code>	Change event details (e.g., "15-03-2026 05:02:41 - Status changed to In Progress by john.doe").	String
Case Parameters	See Template Parameter Reference section for the full list.	—

Sample HTML template

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<style>
```

```
table {
```

```
font-family: arial, sans-serif;
```

```
border-collapse: collapse;
```

```
width: 100%;
```

```
}
```

```
td, th {
```

```
border: 1px solid #dddddd;
```

```
text-align: left;
```

```
padding: 8px;
```

```
}
```

```
tr:nth-child(even) {
```

```
background-color: #dddddd;
```

```
}
```

```
</style>
```

```
<meta charset="UTF-8">
```

<title>OpenText SIEM SOAR Case Notification for Case Id: \$case.serial\$</title>

</head>

<body>

Hello,

We want to inform you that there is a change in OpenText SIEM SOAR Case: \$case.serial\$

which is either assigned to you, or you are watching.

Change: \$events\$

Case Details:

<table>

<tr><td>Case</td><td>

\$case.serial\$ - \$case.subject\$</td></tr>

<tr><td>Description</td><td>\$case.description\$</td></tr>

<tr><td>Assignee</td><td>\$case.assignee.name\$</td></tr>

<tr><td>Severity</td><td>\$case.ticketSeverity.name\$</td></tr>

<tr><td>Status</td><td>\$case.ticketStatus.name\$</td></tr>

<tr><td>Labels</td><td>\$case.labels :{LABEL | "\$LABEL.name\$" }\$</td></tr>

</table>

```
<br><br>
```

```
Kind Regards,<br>
```

```
SOC Team.
```

```
</body>
```

```
</html>
```

1.3.4. Workflow notification

Workflow notifications are triggered within playbooks to inform analysts or analyst groups about playbook progress and case details. These are informational — they do not require a reply.

SOAR ships with the following default template file under **Configuration > Customization Library menu**:

- Workflow Notification E-mail Template

However, you can create custom templates and assign them to individual notification elements in your playbooks.

Parameters

Parameter / Group	Description	Type
<code>\$rule.name\$</code>	Playbook name.	String
<code>\$startTime\$</code>	Playbook execution start time (e.g., "2026-03-12 11:12:55").	Date
Alert Parameters	See Template Parameter Reference section for the full list.	—
Case Parameters	See Template Parameter Reference section for the full list.	—

Case scope variable

In addition to the standard parameters, workflow notifications support the following scope variables:

Variable	Description
\$offenders\$	Offender scope items associated with the case.
\$impacts\$	Impact scope items associated with the case.
\$related\$	Related scope items associated with the case.

Sample HTML template

```

<!DOCTYPE html>
<html>
<head>
<style>
table {
  font-family: arial, sans-serif;
  border-collapse: collapse;
  width: 100%;
}
td, th {
  border: 1px solid #dddddd;
  text-align: left;
  padding: 8px;
}
tr:nth-child(even) {
  background-color: #dddddd;
}
</style>
<meta charset="UTF-8">
</head>
<body>
Hello,<br>
<br>
We want to notify you that we're executing playbook "$rule.name$" on Case:
<a href="https://OpenText SIEM/ soar/?
tenant=default#/cases/$case.serial$">$case.serial$ -
$case.subject$</a><br>
Playbook execution started at $startTime$<br>
<br>
<b>Case Details:</b><br>
<table>
  <tr><td>Case</td><td><a href="https://OpenText SIEM/ soar/?
tenant=default#/cases/$case.serial$">
  $case.serial$ - $case.subject$</a></td></tr>
  <tr><td>Description</td><td>$case.description$</td></tr>
  <tr><td>Assignee</td><td>$case.assignee.name$</td></tr>
  <tr><td>Severity</td><td>$case.ticketSeverity.name$</td></tr>
  <tr><td>Status</td><td>$case.ticketStatus.name$</td></tr>

```

```

<tr><td>Labels</td><td>${case.labels :{LABEL | "${LABEL.name$"} }$</td></tr>
<tr><td>Creation Time</td><td>${case.creationTime$</td></tr>
<tr><td>Modification Time</td><td>${case.modificationTime$</td></tr>
</table>
<br><br>
<b>Case Scope:</b><br>
<table>
  <tr><td>Offenders</td><td>${offenders$</td></tr>
  <tr><td>Impacts</td><td>${impacts$</td></tr>
  <tr><td>Related</td><td>${related$</td></tr>
</table>
<br><br>
<b>Alert Details:</b><br>
<table>
  <tr><td>Alert Source</td><td>${alert.AlertSource.name$</td></tr>
  <tr><td>Alert Id (OpenText SIEM SOAR)</td><td>${alert.id$</td></tr>
  <tr><td>Alert Id (Remote)</td><td>${alert.externalAlertId$</td></tr>
  <tr><td>Alert Date</td><td>${alert.date$</td></tr>
  <tr><td>Alert Params</td><td>${alert$</td></tr>
</table>
<br><br>
Kind Regards,<br>
SOC Team.
</body>
</html>

```

1.3.5. Action and rollback approval notification

Action and rollback approvals request confirmation from system administrators or integration owners before SOAR executes or rolls back an action on an external system. This is a critical safeguard — for example, asking firewall administrators to confirm before blocking an IP address.

The approval workflow operates as follows:

1. SOAR sends the approval request email to the person designated in the Approval From field of the integration configuration.
2. The recipient reviews the request and replies with APPROVE or DENY.
3. SOAR retrieves the approval status through the IncomingMailIntegration.
4. If approved, SOAR proceeds with the action. If denied, SOAR discards the action.

SOAR provides separate default templates for action approvals and rollback approvals:

- Action Approval E-mail Template
- Rollback Approval E-mail Template

Parameters

Parameter / Group	Description	Type
<code>\$rule.name\$</code>	Playbook name.	String
Action Parameters	See Template Parameter Reference section for the full list.	—
Case Parameters	See Template Parameter Reference section for the full list.	—

Sample HTML template

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<style>
```

```
table {
```

```
font-family: arial, sans-serif;
```

```
border-collapse: collapse;
```

```
width: 100%;
```

```
}
```

```
td, th {
```

```
border: 1px solid #dddddd;
```

```
text-align: left;
```

```
padding: 8px;
```

```
}
```

```
tr:nth-child(even) {
```

```
background-color: #dddddd;
```

```
}
```

```
</style>
```

```
<meta charset="UTF-8">
```

<title>Your approval is required!</title>

</head>

<body>

Hello,

We need your approval for the following action:

<table>

<tr>

<th>Device / System Name</th>

<th>Address / URL</th>

<th>Action</th>

<th>Parameters</th>

</tr>

\$actions :{ACTION |

<tr>

<td>\$ACTION.device.name\$</td>

<td>\$ACTION.device.address\$</td>

<td>\$ACTION.request.capability.capability\$</td>

<td>\$ACTION.params\$</td>

</tr>

```
}$
```

```
</table>
```

```
<br><br>
```

```
For your reference:<br>
```

```
<b>Case ID:</b> $case.serial$<br><br>
```

```
Please simply reply with APPROVE or DENY.<br>
```

```
<br>
```

```
Kind Regards,<br>
```

```
SOC Team.
```

```
</body>
```

```
</html>
```

1.3.6. Action and rollback notification

Action notifications inform the person designated as Notifier in the integration configuration about actions that SOAR has executed on the integration. These are informational and do not require a reply.

Action notifications use the following template file under **Configuration > Customization Library Menu**:

- Action Notification Email Template

Notification frequency

The frequency of action notifications is controlled by the **ActionNotificationPeriod** parameter under **Configuration > Parameters**. The default value is 600 seconds (5 minutes). SOAR batches action notifications within this period into a single email.

Parameters

Parameter / Group	Description	Type
<code>\$rule.name\$</code>	Playbook name.	String
Action Parameters	See Template Parameter Reference section for the full list.	—
Case Parameters	See Template Parameter Reference section for the full list.	—

Sample HTML template

```

<!DOCTYPE html>
<html>
<head>
<style>
table {
  font-family: arial, sans-serif;
  border-collapse: collapse;
  width: 100%;
}
td, th {
  border: 1px solid #dddddd;
  text-align: left;
  padding: 8px;
}
tr:nth-child(even) {
  background-color: #dddddd;
}
</style>
<meta charset="UTF-8">
<title>Action Notification</title>
</head>
<body>
Hello,<br>
<br>
Here is the summary of actions taken by OpenText SIEM SOAR:<br>
<table>
  <tr>
    <th>Date</th>
    <th>Device / System Name</th>
    <th>Address / URL</th>
    <th>Action</th>
    <th>Parameters</th>
    <th>Status</th>
  </tr>
  $actions :{ACTION |
  <tr>
    <td>$ACTION.executionDate$</td>
    <td>$ACTION.device.name$</td>

```

```

<td>${ACTION.device.address}$</td>
<td>${ACTION.request.capability.capability}$</td>
<td>${ACTION.params}$</td>
<td>${ACTION.status.visibleName}$</td>
</tr>
}$
</table>
<br><br>
Kind Regards,<br>
SOC Team.
</body>
</html>

```

1.3.7. Enrichment notifications

Enrichment notifications inform analysts and the person designated as Notifier in the integration configuration about enrichment execution results.

Enrichment notifications use the following template file under **Configuration > Customization Library Menu**:

- Enrichment Notification E-mail Template

Parameters

Parameter / Group	Description	Type
<code>\$message\$</code>	Notification message (e.g., "Started successfully on case #5737").	String
<code>\$capabilityVisibleName\$</code>	Enrichment capability executed (e.g., "IP Query").	String
Case Parameters	See Template Parameter Reference section for the full list.	—

Sample HTML template

```

<html>
<head>
<title></title>
</head>
<body>
Hello,<br><br>
$capabilityVisibleName$ - $message$
<br>
<b>[Case Details]</b>
<br>
<b>Case:</b>
<a href="https://OpenText SIEM/soar/?
tenant=default#/cases/$case.serial$" >$case.serial$ -
$case.subject$</a><br>
<b>Severity:</b> $case.ticketSeverity.name$<br>
<br>
Kind Regards,<br>
OpenText SIEM SOAR<br>
</body>
</html>

```

1.3.8. Use automation bits

In addition to template-based notifications, SOAR supports sending email notifications programmatically from automation bits using the `atar.notify()` method. This method uses the SMTP server configured under **Respond > Configuration > Parameters > OutgoingMailIntegration**.

Method signature

```
atar.notify("EMAIL", [email_to], [email_cc], email_subject, email_body)
```

```
atar.notify("EMAIL", [email_to], [email_cc], email_subject,  
email_body_template_name, attributes)
```

Parameter	Description	Type
"EMAIL"	Notification channel identifier.	String
email_to, email_cc	List of recipient email addresses.	List[String]
email_subject	Email subject line.	String
email_body	Email body content (supports HTML).	String
email_body_template_name	Email body content template name.	String
attributes	Variables used in Email templates.	HashMap()

Sample automation bits

The following automation bit retrieves case details and sends a formatted notification email:

```

# Automation bit code sample to email incident details to a recipient.
# In order this automation bit to work, please add an input parameter "Recipient
(String Type)"
# while creating the automation bit.
# atar.notify method uses the SMTP server defined in
Respond>Configuration>Parameters>OutgoingMailIntegration

case = atar.getCase()
case_serial = str(case.getSerial())
case_subject = case.getSubject()
case_severity = case.getTicketSeverity().name

if case.getAssignee() is not None:
    case_assignee = case.getAssignee().getName()
else:
    case_assignee = "Unassigned"

case_status = case.getTicketStatus().getName()
case_description = case.getDescription()
rulename = atar.getAlert().getAlertSourceRuleNames()[0].getRuleName()

# Initialize an empty variable for case_comment_content
case_comment_content = ""
case_comments = case.getComments()
for comment in case_comments:
    comment_created_by = comment.getCreatedByUser()
    if comment_created_by is None:
        comment_created_by = "SOAR Automation"

    case_comment_content = case_comment_content + "User: " +
comment_created_by + " - Comment: " + comment.getContent() + "<br>"

# Get Paramters provided:
email_to = atar.param('Recipient')

# Construct email
email_subject = "New Comment on SOAR Case #" + case_serial + " - " +
case_subject

```

```

email_body = "<html><head>" \
    "<style> table { font-family: arial, sans-serif; border-collapse: collapse; width: 100%; } td, th { border: 1px solid #dddddd; text-align: left; padding: 8px; } tr:nth-child(even) { background-color: #dddddd; } </style>" \
    " <meta charset=\"UTF-8\"></head>" \
    "<body>" \
    "Hello, <br><br> " \
    "We want to inform you that a new comment has been added to the SOAR case #" + case_serial + ".<br><br>" \
    "Case Details:<br>" \
    "<table> " \
    "<tr><td><b>Case</b></td><td><a href=\"https://OpenText SIEM/soar/?tenant=default#/cases/" + case_serial + "\"> " + case_serial + " - " + case_subject + "</a></td></tr>" \
    "<tr><td><b>Description</b></td><td>" + case_description + "</td></tr> " \
    "<tr><td><b>Rule Name</b></td><td>" + rulename + "</td></tr> " \
    "<tr><td><b>Assignee</b></td><td>" + case_assignee + "</td></tr> " \
    "<tr><td><b>Severity</b></td><td>" + case_severity + "</td></tr> " \
    "<tr><td><b>Status</b></td><td>" + case_status + "</td></tr> " \
    "<tr><td><b>Comments</b></td><td>" + case_comment_content + "</td></tr> " \
    "</table>" \
    "<br><br>Kind Regards, <br>SOC Team!<br></body></html>"

# Send Email
atar.notify("EMAIL", [email_to],email_subject, email_body)

```

The following automation bit sends a formatted email using a template:

```

# Automation bit code sample to email using template.
# atar.notify method uses the SMTP server defined in
Respond>Configuration>Parameters> OutgoingMailIntegration

email_to = "aozturk@opentext.com"
email_cc = "oahmet@gmail.com"

attributes = HashMap()
attributes.put("subjectVar", "12345")
attributes.put("bodyVar1", "This is the first variable to be used in body")
attributes.put("bodyVar2", "This is the second variable to be used in body")

#Configure the following email body template under Configuration>Customization
Library.
# You can use varilables in your template and set these varilables in the
automation bit
# using HashMap() function as shown:

#<html>
# <body>
#   First Body Variable = $bodyVar1$ <br>
#   Second Body Variable = $bodyVar2$ <br>
# </body>
#</html>

body_template_name = "Automation Bit – Email Body Template"
email_subject = "New notification $subjectVar$"

#Send Email
atar.notify("EMAIL", [email_to], [email_cc], email_subject, body_template_name,
attributes)

```



Note

When building HTML email bodies in automation bits, ensure that string concatenation handles **None** values gracefully to avoid runtime errors. Always check for **None** before concatenating case attributes

1.4. SMTP mail server capabilities

In addition to template-based automatic notifications, OpenText SOAR SMTP Mail Server integration provides three built-in email action capabilities. These capabilities can be used as workflow steps in playbooks to send emails. Each capability serves a different use case, ranging from simple free-text emails to advanced template-based notifications with attachments and scope-aware recipients. The following subsections describe each capability, its parameters, and practical configuration guidance.

Send Email

The Send Email capability provides an option to send a basic email notification from within a playbook. All fields — recipient, sender, subject, and body — accept free text input, making this the simplest and most flexible email option. Use this capability when you need to send a one-off notification with custom content that does not require templates, scope-based addressing, or attachments.

Typical use cases include:

- Notifying an external stakeholder about an incident.
- Sending a quick status update to a distribution list.
- Delivering a custom message that does not follow a standard template format.

Parameters

Parameter	Input Type	Description
Email to	Free text	The recipient email address. Enter one or more email addresses separated by commas.
Email from	Free text	The sender email address displayed in the "From" field of the outgoing message.
Email subject	Free text	The subject line of the email. Provide a clear, descriptive subject for easy identification.
Email body	Free text	The body content of the email. Supports plain text. Include all relevant details directly in this field.

Configuration guidance

To configure the Send Email step in a playbook:

1. Open the **Playbook Editor** and drag a **Send Email** element onto the workflow canvas.
2. In the element configuration panel, populate the parameters:
 - Email to — Enter the recipient address (e.g., soc-team@example.com). For multiple recipients, separate addresses with commas.
 - Email from — Enter the sender address (e.g., soar-noreply@example.com).
 - Email subject — Provide a descriptive subject (e.g., Incident Alert: Unauthorized Access Detected).
 - Email body — Write the message content directly.

3. Save the playbook element and connect it to the appropriate workflow step.



Note

Because this capability uses free text for all fields, it does not support dynamic template parameters (such as `$case.serial$`). If you need dynamic content, use the Send Advanced Email or Send Email to Scope Items capability instead.

Send Email to Scope Items

The **Send Email to Scope Items** capability is specifically designed to send notifications to email addresses that exist within the case scope. Unlike the other email capabilities, the recipient list is automatically derived from the case scope. SOAR identifies all scope items with the EMAIL_ADDRESS category and sends the notification to those addresses.

This capability is particularly useful in scenarios where the affected parties are already identified as scope items in the case, and you want to notify all of them in a single playbook step without manually specifying each address.

Typical use cases include:

- Notifying all affected users (identified as IMPACT scope items) about a security incident.
- Sending a follow-up communication to all email addresses associated with a phishing case.
- Delivering a standardized notification to scope-derived recipients using a consistent template.

Parameters


Parameter	Input Type	Description
Email to	Case scope	Recipients are automatically derived from the case scope. SOAR sends the email to all scope items with the EMAIL_ADDRESS category.
Email from	Free text	The sender email address displayed in the "From" field.
Email subject	Free text	The subject line of the email. Enter a clear, descriptive subject directly.
Email template	Template based	The email body is generated from a template defined in Configuration > Customization Library. Supports all dynamic parameters available for the notification context.

Configuration guidance

To configure the Send Email to Scope Items step in a playbook:

1. Open the **Playbook Editor** and drag a **Send Email to Scope Items** element onto the workflow canvas.
2. In the element configuration panel, populate the parameters:

3.
 - Email to — This field is pre-configured to pull from the case scope. SOAR automatically identifies all scope items with the EMAIL_ADDRESS category and uses them as recipients.
 - Important: Ensure that the relevant email addresses have been added to the case scope before this step executes. Email addresses can be added via alerts, enrichment steps, or manually by an analyst.
 - Email from — Enter the sender address (e.g., soar-noreply@example.com).
 - Email subject — Enter a descriptive subject line (e.g., Security Notification: Action Required for Your Account). Email template — Select the body template from the Customization Library. The template supports dynamic parameters that are resolved at runtime (see [Template Parameter Reference](#)).
4. Save the playbook element and connect it to the appropriate workflow step.



Note

To control which scope email addresses receive the notification, use a preceding playbook step to filter scope items by role (e.g., IMPACT only) before the notification step. This prevents unintended recipients (such as OFFENDER email addresses) from receiving the notification.

Send Advanced Email

The **Send Advanced Email** capability extends the basic email functionality with support for dynamic recipients, template-based subjects and bodies, and file attachments from the case scope. This is a feature-rich email capability in SOAR and is designed for structured, repeatable notifications that leverage case context.

Key advantages over the basic Send Email capability:

- **Dynamic recipients** — The "Email to" field supports email addresses pulled from the case scope (e.g., scope items with the EMAIL_ADDRESS category), manually entered addresses, and analyst names resolved to their registered email addresses. These sources can be combined.
- **Template-based content** — Both the subject line and the email body are driven by templates from the Customization Library, ensuring consistent formatting and dynamic parameter resolution.
- **Attachments** — Files associated with the case scope (e.g., evidence files, reports) can be attached to the outgoing email.

Typical use cases include:

- Sending a detailed case summary to the assigned analyst and affected users.
- Notifying multiple parties (scope-derived and manually specified) with a standardized template.

Parameters

Parameter	Input Type	Description
<p>Email to</p>	<p>Scope / Free text / Analyst name</p>	<p>One or more recipients. Supports: (1) email addresses from the case scope (EMAIL_ADDRESS category), (2) manually entered addresses, (3) analyst names that SOAR resolves to their registered email. Any combination of these sources is supported.</p>
<p>Email from</p>	<p>Free text</p>	<p>The sender email address displayed in the "From" field.</p>
<p>Email subject</p>	<p>Template based</p>	<p>The email subject is generated from a template defined in Configuration > Customization Library . Dynamic parameters are resolved at runtime.</p>
<p>Email template</p>	<p>Template based</p>	<p>The email body is generated from a template defined in Configuration > Customization Library . Supports all dynamic parameters available for the notification context.</p>

<p>Attachments</p>	<p>Case scope file</p>	<p>Files added from the case scope are attached to the email. Select the relevant scope file items when configuring the playbook element.</p>
---------------------------	------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------

Configuration guidance

To configure the **Send Advanced Email** step in a playbook:

1. Open the **Playbook Editor** and drag a **Send Advanced Email** element onto the workflow canvas.
2. In the element configuration panel, populate the parameters:
 - Email to — Use one or more of the following approaches:
 - Scope-based: Select email addresses from the case scope. SOAR lists available scope items with the EMAIL_ADDRESS category.
 - Manual entry: Type an email address directly (e.g., manager@example.com).
 - Analyst name: Enter an analyst's name (e.g., John Doe). SOAR resolves this to the analyst's registered email address.
 - You can combine all three methods in a single configuration.
 - Email from — Enter the sender address (e.g., soar-noreply@example.com).
 - Email subject — Select a subject template from the Customization Library.
 - Email template — Select the body template from the Customization Library. This template drives the full email content and supports all applicable dynamic parameters (see [Template Parameter Reference](#)).
 - Attachments — Select one or more files from the case scope to attach to the email. These are typically evidence files, logs, or reports that have been added to the case as scope items with the FILEDATA category.
3. Save the playbook element and connect it to the appropriate workflow step.

1.5. Template parameter reference

Alert parameters

Alert parameters are available in Workflow Notification templates.

Parameter	Description	Type	Example
<code>\$alert\$</code>	Full alert object processed by the playbook.	Alert Object	<code>Alert{id=833133, alertSource=AlertSource{name='ArcSight ESM'}, externalAlertId='290779375', params='details : [redacted] ', date=2026-03-11 23:06:10.649}</code>
<code>\$alert.id\$</code>	Reference Id of the alert on SOAR.	String	<code>"833133"</code>
<code>\$alert.date\$</code>	Date of the alert.	Date	<code>"2026-03-11 23:06:10.649"</code>
<code>\$alert.AlertSource.name\$</code>	Alert source name.	String	<code>"ArcSight ESM"</code>
<code>\$alert.alertSeverity\$</code>	Severity of the alert as set by the alert source (for example, priority on ESM)	String	<code>"7"</code>
<code>\$alert.externalAlertId\$</code>	Id of the alert as set by the alert source (e.g., ESM event Id).	String	<code>"290779375"</code>

Action parameters

Action parameters are available in Action Approval, Rollback Approval, and Action Notification templates. The `$actions$` parameter is a list, and you iterate over it using the `StringTemplate` syntax.

Parameter	Description	Type	Example
<code>\$actions\$</code>	Action execution details.	List	—
<code>\$actions : {ACTION \$ACTION.device.name}\$</code>	Name of the integration on SOAR.	String	"Check Point Firewall – Sydney"
<code>\$actions : {ACTION \$ACTION.device.address}\$</code>	Address of the target system.	String	"10.0.24.3"
<code>\$actions : {ACTION \$ACTION.request.capability}\$</code>	Full action type with integration.	String	"CHECKPOINTAPI//BLOCK_IP"
<code>\$actions : {ACTION \$ACTION.request.capability.capability}\$</code>	Action type.	String	"BLOCK_IP"
<code>\$actions : {ACTION \$ACTION.params}\$</code>	Action parameters / values.	String	"IP : 192.168.200.140"

<p>\$actions : {ACTION \$ACTION.executionDate}\$</p>	<p>Date the action was executed.</p>	<p>Date</p>	<p>—</p>
<p>\$actions : {ACTION \$ACTION.status.visibleName}\$</p>	<p>Execution status of the action.</p>	<p>String</p>	<p>—</p>

1.6. Troubleshoot common notification issues

The following table covers the most frequently encountered notification issues and their resolutions.

Symptom	Possible Cause	Resolution
No notifications are sent.	SMTP server is not configured or unreachable.	Verify the SMTP configuration under Respond > Configuration > Parameters > OutgoingMailIntegration . Test connectivity from the SOAR server to the SMTP host.
Case notifications are not sent.	CaseNotificationEnabled is set to False .	Set CaseNotificationEnabled to True under Configuration > Parameters .
Case notification emails contain broken links.	CaseNotificationURL is not set or incorrect.	Set CaseNotificationURL to your SOAR instance URL (e.g., https://OpenText SIEM/soar) under Configuration > Parameters .
Template parameters appear as literal text (e.g., \$case.serial\$).	Parameter name is misspelled or the parameter is not supported for the notification type.	Verify the parameter name against the reference tables in this guide. Ensure the parameter is supported for the specific notification type being used.

<p>Approval emails are sent but replies are not processed.</p>	<p>Reply email is not reaching SOAR, or the reply does not contain the exact keyword.</p>	<p>Verify that the SOAR mail integration can receive incoming mail. Check for IMAP/IMAPS configuration. Ensure the user replies with the exact keyword (e.g., APPROVE , DENY , or the custom keywords set in the playbook).</p>
<p>Action notifications are delayed.</p>	<p>ActionNotificationPeriod is set to a high value.</p>	<p>Reduce the ActionNotificationPeriod value under Configuration > Parameters . The default is 600 seconds.</p>
<p>atar.notify() fails in automation bit.</p>	<p>SMTP configuration is missing or incorrect.</p>	<p>Verify OutgoingMailIntegration settings. Check the automation bit execution logs in the case timeline and the soar-web-app pod logs for stack traces.</p>
<p>Labels or comments are empty in the notification.</p>	<p>The case has no labels or comments at the time of notification.</p>	<p>These parameters resolve to empty strings when no data exists. Consider adding conditional text or verifying case data before sending notifications.</p>



© Copyright 2026 Open Text

For more info, visit <https://docs.microfocus.com>
