



# HP ArcSight ESM

Software Version: 6.9.0c

## Cases Editor UI Customization Tech Note

August 7, 2015

## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

## Support

#### Contact Information

<b>Phone</b>	A list of phone numbers is available on the HP ArcSight Technical Support Page: <a href="https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.hp.com">https://softwaresupport.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.hp.com">https://protect724.hp.com</a>

# Contents

Customizing the Case Editor User Interface .....	4
Introduction .....	4
Best Practices .....	4
Case Customization Workflow .....	5
Changing the Case Editor UI Structure .....	5
Switching from Extended to Simple View of the Case Editor .....	7
Simple view .....	8
Changing Tab and Header Labels .....	10
Changing Field Labels .....	11
Adding and Removing Tabs .....	13
Customizing Field Labels .....	18
Setting Fields as Mandatory .....	19
Mapping Case Details To Audit Events .....	20
Send Documentation Feedback .....	22

# Customizing the Case Editor User Interface

Introduction .....	4
Best Practices .....	4
Case Customization Workflow .....	5
Changing the Case Editor UI Structure .....	5
Mapping Case Details To Audit Events .....	20

## Introduction

This technical note for HP ArcSight Professional Services describes how to customize the Cases user interface on the ArcSight Console and ArcSight Command Center to meet customers' requirements.

All illustrated examples in this tech note are from ArcSight Console.

## Best Practices

Customizing the Cases UI involves modifying files in the Manager, then copying the modified files in ArcSight Console installation as appropriate. For ArcSight Command Center, keep the modified copies in the same Manager location.

Before starting the customization process, stop the user interfaces, then stop ArcSight Manager. After restoring the modified files to the appropriate directories, restart the Manager, then start the UIs.

To ensure continuous ArcSight services, copy the required customized files to the final location in the following sequence:

1. Copy the customized files to the Manager installation.
2. Copy the customized files to the ArcSight Console installation.

Before deploying your customizations, always perform and validate them in a test environment first before deploying to the production environment.

If you are changing the UI structure, you are modifying the original `caseui.xml` file. Always make a backup of the original before making changes. Provide a mechanism of backing up each revision of the file as you continue to modify the structure.

When customizing labels, determine the localization requirements. Then modify the locale-specific properties file according to the instructions. The default language in properties files is English. Even if you are customizing in English, you must create and then modify the English locale version of the

properties file.

Always back up original and customized files to preserve your changes through upgrades. The original files on the Manager include:

```
/opt/arcsight/manager/config/caseUI.xml  
/opt/arcsight/manager/i18n/common/label_strings.properties  
/opt/arcsight/manager/i18n/common/resource_strings.properties  
/opt/arcsight/manager/config/audit/case.default.properties
```

When following instructions to edit property files, do not edit the left-side values.

## Case Customization Workflow

Follow this general sequence to implement the Cases Editor UI customizations for the customer:

1. Based on customer requirements, modify the property files by following the instructions in this document. Each set of instructions includes details about the file you will modify.
2. Back up the modified files by following the instructions in this document. These backups are important for migrating the customizations after software upgrades.
3. Test the customizations. The test environment should consist of a single ArcSight Console installation and one ArcSight Manager. The Manager installation includes the ArcSightCommand Center.

The rest of this document refers to any or all of these interfaces as “UI.”

4. Plan your deployment schedule when it is least disruptive to the UI users. For changes to take effect, ESM services must be stopped and restarted.
5. Deploy to production.

## Changing the Case Editor UI Structure

The file, `arcsight\Manager\config\caseui.xml`, controls the case editor’s structure on the UI. Changes to this file simultaneously affect all UIs where cases are exposed.

The following example shows a portion of the `caseui.xml` file. The blocks of statements called out in the figure pertain to the **Initial** tab:

### caseui.xml file

```
<editor enforceLocking="true" colorTreeBy="consequenceSeverity"
width="480" height="480">
  <tab name="cases.tab.initial" type="container">
    <tab name="cases.tab.attributes" type="base" showExport="true">
      <component name="attributesTable" type="table">

        <parameter name="cases.header.case" type="header"/>
        <parameter name="name" type="resourceName"/>
        <parameter name="displayId" type="int" readOnly="true"/>

        <parameter name="cases.header.ticket" type="header"/>
        <parameter name="ticketType" type="stringList"/>
        <parameter name="stage" type="stringList"/>
        <parameter name="frequency" type="stringList"/>
        <parameter name="operationalImpact" type="stringList"/>
        <parameter name="securityClassification" type="stringList"/>
        <parameter name="consequenceSeverity" type="stringList"/>
        <parameter name="reportingLevel" type="int"
readOnly="true"/>

        <parameter name="cases.header.incidentInformation"
type="header"/>
        <parameter name="detectionTime" type="string">
```

The diagram includes several red annotations on the XML code: a circle labeled '1' around the 'initial' attribute of the first tab; a circle labeled '2' around the 'initial' attribute of the first tab; a circle labeled '3' around the 'displayId' parameter; a circle labeled '4' around the 'reportingLevel' parameter; and a circle around the 'ticket' parameter in the 'cases.header' section.

The following example shows the Case Editor UI based on the structural definition in `caseui.xml`:

### Case Editor on ArcSight Console

Event Inspector Case Editor

Initial Follow Up Final Events Attachments Notes

Attributes Description Security Classification

Case

- Name
- Display ID
- Ticket
- Ticket Type
- Stage
- Frequency
- Operational Impact
- Security Classification
- Consequence Severity
- Reporting Level

Incident Information

- Detection Time
- Estimated Start Time
- Estimated Restore Time

Common

- External ID
- Alias (Display Name)
- Description
- Version ID
- Deprecated

Assign

- Owner
- Notification Groups

Through the `caseui.xml` file, you can:

- Switch from the Case Editor's default extended view to the simple view. See ["Switching from Extended to Simple View of the Case Editor" below](#).
- Add or remove tabs. Tabs can contain editor content, or tabs can contain subtabs for better content organization. See ["Adding and Removing Tabs" on page 13](#).
- See ["Setting Fields as Mandatory" on page 19](#).

## Switching from Extended to Simple View of the Case Editor

The UIs support two versions of the case editor:

- Extended, or default, view
- Simple view

## Extended View

The extended view, which is the default view, exposes all case attributes as in "[Case Editor on ArcSight Console](#)" on the previous page. Customers may regard this view as complex and too much for their needs.

## Simple view

The simple view below exposes less attributes and is also easy to implement.

### Simple View of the Case Editor

The screenshot shows the 'Case Editor' window with the 'Attributes' tab selected. The interface is divided into three main sections: 'Case', 'Common', and 'Assign'. Each section contains a table of attributes.

Case	
* Name	
Display ID	0
Stage	Queued
Consequence Severity	0-None

Common	
External ID	
Alias (Display Name)	
Description	
Version ID	
Deprecated	<input type="checkbox"/>

Assign	
Owner	
Notification Groups	

**Caution:** For safekeeping, back up the original `caseui.xml` file before modifying it. You will be modifying `caseui.xml` directly.

### To switch from extended to simple view:

1. On the Manager, back up the original `arcsight\Manager\config\caseui.xml` by renaming it, as an example.



2. Open caseui.xml with your preferred editor.

The top section of the file contains the definitions for the extended view.

3. Comment out the extended view definitions:

```
<!--
* Copyright 2003 ArcSight, Inc. All Rights Reserved.
*
* This software is the proprietary information of ArcSight, Inc.
* Use is subject to license terms.
*
* $Workfile: caseui.xml $
-->
<!--
<editor enforceLocking="true" colorTreeBy="consequenceSeverity" width="480"
height="480">
  <tab name="cases.tab.initial" type="container">
    <tab name="cases.tab.attributes" type="base" showExport="true">
      <component name="attributesTable" type="table">

        <parameter name="cases.header.case" type="header"/>
        <parameter name="name" type="resourceName"/>
        <parameter name="displayId" type="int" readOnly="true"/>

      .
      .
      .

    <tab name="cases.tab.other" type="base">
      <component name="otherTable" type="table" weight="4">
        <parameter name="history" type="stringList"/>
        <parameter name="noOccurrences" type="int"/>
        <parameter name="lastOccurrenceTime" type="date"/>
        <parameter name="resistance" type="stringList"/>
        <parameter name="consequenceSeverity" type="string" readOnly="true"/>
        <parameter name="sensitivity" type="string" readOnly="true"/>
      </component>
      <component name="recordedData" type="textarea" nbRows="4"/>
      <component name="inspectionResults" type="textarea" nbRows="4"/>
      <component name="conclusions" type="textarea" nbRows="4"/>
    </tab>
  </tab>
</editor>
-->
```

**Insert the beginning comment tag here**

**Insert the ending comment tag here**

4. Scroll down to the lower portion of the XML file that contains the definitions for simple view.  
Remove the comments, as shown:

```
<!-- Use the following for the a simple view upon the Cases Schema -->
<!--editor enforceLocking="false" colorTreeBy="stage" width="350"
height="480">
  <tab name="cases.tab.attributes" type="base" showExport="true">
    <component name="attributesTable" type="table">
      <parameter name="cases.header.case" type="header"/>
      <parameter name="name" type="resourceName"/>
      <parameter name="displayId" type="int" readOnly="true"/>
      <parameter name="stage" type="stringList"/>
      <parameter name="consequenceSeverity" type="stringList"/>
      <parameter name="common" type="commonResourceAttrs"/>
    </component>
  </tab>
</editor -->
```

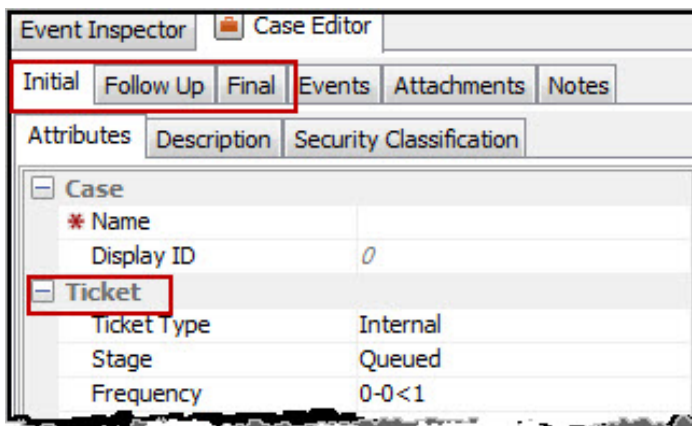
Remove these comment tags

5. If any of the UIs are running, stop them; then stop Manager.
6. To see your changes, start Manager, then start the affected UIs as appropriate.

## Changing Tab and Header Labels

"Changing Tab and Header Labels" above shows an area on the Case Editor that will be used as examples in this procedure.

**Tab and Header Labels Defined in label\_strings.properties**



In this procedure, you will modify a copy of label\_strings.properties to map the labels for your tabs and headers.

**Caution:** Do not modify label\_strings.properties directly. The steps instruct you to make a copy of it first. By default, the strings are in English. Rename the copy using the format label\_strings\_<locale>.properties. To change the labels in English, you would rename the file label\_strings\_en.properties.

## To change tab and header labels:

1. On the Manager, copy the file, `opt\arcsight\manager\i18n\common\label_strings.properties` and rename it as `label_strings_<locale>.properties`.
2. In `label_strings_<locale>.properties`, locate the statements prefixed by `cases.tab.xxx` or `cases.header.xxx`. Based on the example in ["Tab and Header Labels Defined in label\\_strings.properties" on the previous page](#), look for these lines:

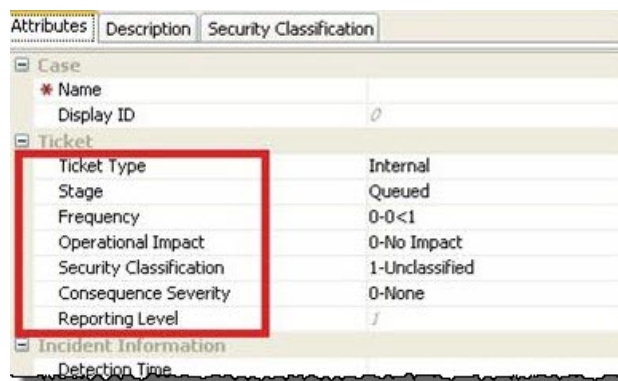
```
cases.tab.initial=Initial
cases.tab.followup=Follow Up
cases.tab.final=Final
.
.
cases.header.ticket=Ticket
```

3. Change the right-side values with your labels as required.
4. Back up the localized file for safekeeping.
5. If the ArcSight Console services are running, stop them as appropriate; and then stop Manager.
6. Copy the modified `label_strings_<locale>.properties` as required:
  - For Console, copy the file in `arcsight\console\i18n\common\`
  - For Command Center, keep the localized copy in the same Manager location.
7. Start Manager to deploy your changes, then start the UIs to see the changes.

## Changing Field Labels

The screenshot below shows an area on the Case Editor that are used as examples in this procedure.

### Field Labels Defined in `resource_strings.properties`



In this procedure, you will modify a copy of `resource_strings.properties` to set the label values for the fields defined in `caseui.xml`.

**Caution:** Do not modify `resource_strings.properties` directly. The steps instruct you to make a copy of it first. By default, the strings are in English. Rename the copy using the format `resource_strings_<locale>.properties`. Even if you are customizing in English, create a localized English version and call it `resource_strings_en.properties`.

### To change field labels:

1. On the Manager, copy the file, `opt\arcsight\manager\i18n\common\resource_strings.properties` and rename it as **`resource_strings_<locale>.properties`**.
2. In `resource_strings_<locale>.properties`, locate the statements prefixed by `extendedcase.attribute.xxx`. The statements for the example, "[Field Labels Defined in resource\\_strings.properties](#)" on the previous page, are

```
extendedcase.attribute.tickettype.label=Ticket Type
extendedcase.attribute.tickettype.shortlabel=Ticket Type
extendedcase.attribute.stage.label=Stage
extendedcase.attribute.stage.shortlabel=Stage
extendedcase.attribute.frequency.label=Frequency
extendedcase.attribute.frequency.shortlabel=Frequency
extendedcase.attribute.operationalimpact.label=Operational Impact
extendedcase.attribute.operationalimpact.shortlabel=Operational Impact
extendedcase.attribute.securityclassification.label=Security Classification
extendedcase.attribute.securityclassification.shortlabel=Security Classification
extendedcase.attribute.consequenceseverity.label=Consequence Severity
extendedcase.attribute.consequenceseverity.shortlabel=Consequence Severity
extendedcase.attribute.reportinglevel.label=Reporting Level
extendedcase.attribute.reportinglevel.shortlabel=Reporting Level
```

Notice that there are two attributes for each label change: `label` and `shortlabel`.

3. Modify the field label by changing the value after the equal sign (=). For consistency, modify both the `label` and `shortlabel` versions of the particular label property. The `shortlabel` attribute is useful if you want to provide a shortened version of the original label. For example, if `label` is **Ticket Type**, you can have **Tkt** for `shortlabel`. If the column width is eventually reduced, the shortened version can be displayed instead.
4. Back up the file for safekeeping.
5. If the UIs are running, stop them as appropriate, then stop Manager.
6. Copy the modified `resource_strings_<locale>.properties` into these directories as required:

- For Console, copy the file in `arcsight\console\i18n\common\`
  - For Command Center, keep the localized copy in the same Manager location.
7. Start Manager to deploy your changes, then start the UIs to see the changes.

## Adding and Removing Tabs

This sample procedure illustrates how to add and remove tabs on the Case Editor. The procedure adds the following tabs:

- EE Analysis
- IR Analysis
- Legacy Cases

Next, the procedure removes the following tabs and their associated UI elements shown in the screenshot below:

- Follow Up
- Final

First define the tab structure for new tabs in `caseui.xml`, then define labels in the localized version of `label_strings.properties`. The example uses the default English locale. Next, comment out the tabs to be removed from the UI.

### Follow Up and Final Tabs for removal:

The left screenshot shows the 'Follow Up' tab with the following sections: 'Actions Taken', 'Planned Actions', 'Recommended Actions', and 'Followup Contact'. The right screenshot shows the 'Final' tab with the following sections: 'Incident Information', 'Vulnerability', 'Other', 'Attack Mechanism', 'Attack Agent', 'Misc', '(Name) (Description)', 'Attack Target', 'Attack Service', 'Attack Impact', and 'Final Report Action'.

Note on the above example that the Final tab is a container tab. It has many associated components and fields that are to be removed along with the container itself.

### To remove tabs:

1. On the the Manager, back up the original arcsight\Manager\config\caseui.xml. In caseui.xml, comment out the definitions for the tabs to be removed:

#### To remove the Follow Up tab:

```
<!-- Insert the start comment tag
<tab name="cases.tab.followup" type="base">
  <tab name="cases.tab.attackMechanism" type="base">
    <component name="actionsTaken" type="textarea" />
    <component name="plannedActions" type="textarea" />
    <component name="recommendedActions" type="textarea" />
    <component name="followupContact" type="textarea" />
  </tab>
-->
Insert the ending comment tag-->
```

### To remove the Final tab:

```
<!--Insert the start comment tag
<tab name="cases.tab.final" type="container">
  <tab name="cases.tab.attackMechanism" type="base">
    <component name="attackMechanismTable" type="table" weight="5">
      <parameter name="attackMechanism" type="string" readOnly="true"/>
      <parameter name="attackProtocol" type="string"/>
      <parameter name="attackOs" type="string"/>
      <parameter name="attackProgram" type="string"/>
      <parameter name="attackTime" type="date"/>
    </component>
    <component name="attackTarget" type="textarea" />
    <component name="attackService" type="textarea" />
    <component name="attackImpact" type="textarea" />
    <component name="finalReportAction" type="textarea" />
  </tab>
  <tab name="cases.tab.attackAgent" type="base" >
    <component name="attackAgentTable" type="table">
      <parameter name="attackAgent" type="string" readOnly="true"/>
      <parameter name="attackLocationId" type="string"/>
    </component>
    <component name="attackNode" type="textarea" weight="2"/>
    <component name="attackAddress" type="textarea" weight="2"/>

  </tab>
  <tab name="cases.tab.incidentInformation" type="base">
    <component name="incidentInformationTable" type="table">
      <parameter name="incidentSource1" type="string" readOnly="true"/>
      <parameter name="incidentSource2" type="string" readOnly="true"/>
    </component>
    <component name="incidentSourceAddress" type="textarea" weight="7"/>
  </tab>
  <tab name="cases.tab.vulnerability" type="base">
    <component name="vulnerabilityTable" type="table">
      <parameter name="vulnerability" type="string" readOnly="true"/>
      <parameter name="vulnerabilityType1" type="stringList"/>
      <parameter name="vulnerabilityType2" type="stringList"/>
    </component>
    <component name="vulnerabilityEvidence" type="textarea" nbRows="4"/>
    <component name="vulnerabilitySource" type="textarea" nbRows="4"/>
    <component name="vulnerabilityData" type="textarea" nbRows="4"/>
  </tab>
  <tab name="cases.tab.other" type="base">
    <component name="otherTable" type="table" weight="4">
      <parameter name="history" type="stringList"/>
      <parameter name="noOccurrences" type="int"/>
      <parameter name="lastOccurrenceTime" type="date"/>
      <parameter name="resistance" type="stringList"/>
    </component>
  </tab>
-->
```

```
<parameter name="consequenceSeverity" type="string" readOnly="true"/>
<parameter name="sensitivity" type="string" readOnly="true"/>
</component>
<component name="recordedData" type="textarea" nbRows="4"/>
<component name="inspectionResults" type="textarea" nbRows="4"/>
<component name="conclusions" type="textarea" nbRows="4"/>

</tab>
</tab>
Insert the ending comment tag-->
```

You are ready to add tabs to replace those you removed.

### To add tabs:

1. Add the definitions for the tabs based on the following examples.

#### To add the EE Analysis tab:

```
<tab name="cases.tab.ee" type="container">
  <tab name="cases.tab.eecaseinfo" type="base">
    <component name="vulnerabilitySource" type="textarea" nbRows="4"/>
    <component name="plannedActions" type="textarea"/>
    <component name="recommendedActions" type="textarea"/>
    <component name="actionsTaken" type="textarea"/>
  </tab>
</tab>
```

#### To add the IR Analysis tab:

```
<tab name="cases.tab.ir" type="container">
  <tab name="cases.tab.ircaseinfo" type="base">
    <component name="attackImpact" type="textarea"/>
    <component name="recommendedActions" type="textarea"/>
    <component name="conclusions" type="textarea" nbRows="4"/>
  </tab>
</tab>
```



### To add the Legacy Cases tab:

```
<tab name="cases.tab.legacy35" type="container">
  <tab name="cases.tab.description35" type="base">
    <component name="attackTarget" type="textarea"/>
    <component name="affectedElements" type="textarea"/>
    <component name="estimatedImpact" type="textarea"/>
    <component name="affectedSites" type="textarea"/>
  </tab>
</tab>
```

2. Copy the file, `opt\arcsight\manager\i18n\common\label_strings.properties` and rename it as **label\_strings\_<locale>.properties**. By default, the labels are in English. If you are localizing the labels in English, you would rename the file `label_strings_en.properties`.
3. To this copy, add the following lines under `#Cases` to provide header and tab labels for the new tabs.

```
#Cases
.
.
cases.tab.ee=EE Analysis
cases.tab.ir=IR Analysis
cases.tab.legacy35=Legacy Cases
.
.
```

4. Copy `opt\arcsight\manager\i18n\common\resource_strings.properties` and save it as **resource\_strings\_<locale>.properties**. By default, the labels are in English. If you are localizing the labels in English, you would rename the file `resource_strings_en.properties`.
5. To this copy, add the following statements to provide field labels under `# Labels for cases`.

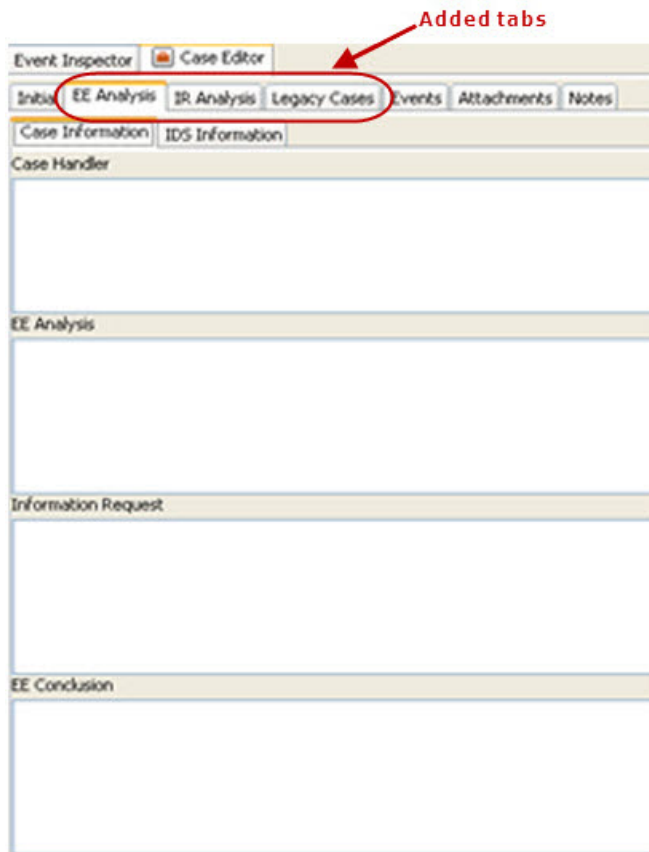
```
# Labels for cases.
extendedcase.attribute.plannedactions.label=EE Analysis
extendedcase.attribute.plannedactions.shortlabel=EE Analysis
extendedcase.attribute.recommendedactions.label=Information Request
extendedcase.attribute.recommendedactions.shortlabel=Information Request
```

6. Stop the UIs, then stop Manager.
7. Copy the customized `caseui.xml` to the `/config` folder of the Manager.
8. Copy the customized `label_strings_<locale>.properties` and `resource_strings_<locale>.properties` files into the ArcSight Console's `arcsight\console\i18n\common` directory.

For Command Center, keep the localized copy in the same Manager location.

9. Start Manager to deploy your changes, then start the UIs to see the changes. The example, ["Added Tabs on the Case Editor UI" on the next page](#), shows the results of the customization:

## Added Tabs on the Case Editor UI



## Customizing Field Labels

Use the localized `label_strings_<locale>.properties` or `resource_strings_<locale>.properties` file to rearrange, rename, re-use available fields across tabs, or change labels of drop-down options. Any changes to field labels will not require changes to `caseui.xml` since you are not changing the structure.

### To customize field labels:

An example of a field label defined in `label_strings.properties` is

```
remove.all=Remove All
```

If you want the label to say `Remove Everything` instead of `Remove All`:

1. Create a localized version of `label_strings.properties` using the filename format, `label_strings_<locale>.properties`.

2. Modify the `remove.all` property in the localized version of the property file with your localized text.

### To customize and rearrange the order of drop-down list items:

An example of a drop-down list is a case's Stage property on the Attributes tab. The definition in the `resource_strings.properties` file states:

```
extendedcase.stages=Queued,Initial,Follow-Up,Final,Closed
```

Change the list sequence of the `extendedcase.stages` property in the localized version of the file, for example, on the `resource_strings_<locale>.properties` file, like this alphabetized sequence:

```
extendedcase.stages=Closed,Final,Follow-Up,Queued
```

## Setting Fields as Mandatory

**Caution: Back up the original `caseui.xml` file before modifying it.**

Unlike with the other properties file, you will be modifying `caseui.xml` directly. You should back up the original `caseui.xml` file for safekeeping.

When customizing any settings, do not edit the left-side values in any properties files.

On the Cases Edit/View panel, only the Name field is mandatory by default. If you have business requirements for making additional fields of string and text area types as mandatory, follow these instructions.

You cannot set the following fields as mandatory: read-only fields such as the Resource ID which is automatically set by the system, headers, tables, container, and base types.

You can set the following fields as mandatory: string, stringlist, text area, and date types. Refer to ["Changing the Case Editor UI Structure" on page 5](#) to understand how the `caseui.xml` elements are mapped to the Case Editor UI.

1. In a copy of `caseui.xml`, locate the field you want to mark as mandatory.

Following are statements for the Ticket table fields on a case's Attributes tab, as an example:

```
<parameter name="operationalImpact" type="stringlist" />
<parameter name="consequenceSeverity" type="stringlist" />
```

1. Insert the setting, **mandatory = "true"** as shown:

```
<parameter name="operationalImpact" type="stringlist" mandatory="true"/>
<parameter name="consequenceSeverity" type="stringlist" mandatory="true"/>
```

**Note:** If your mandatory field happens to have the additional setting:

```
readonly="true"
```

then the field will require a value.

1. Make sure there are no locked cases before closing the UIs.
2. If any of the UIs are running, stop them; then stop Manager.
3. Copy the customized `caseui.xml` to the `config` folder of the Manager.
4. Start Manager to deploy your changes, then start the UIs to see the changes.

On the ArcSight Console and Command Center, the fields you set as mandatory are denoted by a red asterisk. Note that after making this customization, if the user opens cases created in an older version of ESM, the old case's editor cannot be closed unless the user enters values in the required fields.

**Note:** Rules that create or update cases will not check for mandatory fields and will still execute successfully. You can manually configure the rule action to set the mandatory fields with values if you want. Refer to the *ArcSight Console User's Guide's* section, "Rule Authoring," for details.

## Mapping Case Details To Audit Events

This topic describes information about customizing the mapping information from case details into audit events.

Through mapping, you can configure case-related audit events to include values picked up from case details. Once mapped, changes to those case details will trigger the audit events, and in turn you can use ArcSight analytics (rules, filters, and so on) to further track and manage those cases.

The file for mapping case details to audit events is shipped with the ArcSight Manager component. The default case details properties are in

```
\arcsight\Manager\config\audit\case.default.properties
```

To customize any case detail mapping, you will enter your customizations in

```
\arcsight\Manager\config\audit\case.properties
```

**Caution:** When editing properties files, keep the following in mind:

- For any changes to property settings, do not edit `case.default.properties` directly. Instead, edit its corresponding override file without default in the filename, `case.properties` instead.
- Refer to the ESM Administrator's Guide's chapter on Managing and Changing Properties File Settings for more details on how and where to edit settings.

The `case.properties` file contains the following information:

```
# The default case audit event configuration. This file maps
# audit event attributes to values from the corresponding cases.
# The format for the values in the properties file is in the velocity
# template language.
#
# For an explanation of velocity see
# http://jakarta.apache.org/velocity/user-guide.html
#
# Overrides for these properties must be placed into case.properties.

# Example:
#deviceCustomString3=$history
#deviceCustomString3Label=Case History
#oldFileName=Action: "$caseAction" Status: "$stage"

flexNumber1=$math.divide( $math.subtract( $modificationTime, $createTime ), 60000 )
flexNumber1Label= Time To Resolution (Min.)
fileId=$displayId
deviceCustomString1=$ticketType
deviceCustomString1Label= Ticket Type
flexString2=$stage
flexString2Label= Stage
deviceCustomString3=$operationalImpact
deviceCustomString3Label= Operational Impact
deviceCustomString4=$securityClassification
deviceCustomString4Label= Security Classification
deviceCustomString5=$consequenceSeverity
deviceCustomString5Label= Consequence Severity
deviceCustomString6=$associatedImpact
deviceCustomString6Label= Associated Impact
flexString1=$owner
flexString1Label= Owner
fileCreateTime=$createTime
fileModificationTime=$modificationTime
```

To change property settings, edit the corresponding `case.properties` file by changing the right-hand value of the properties. Make a backup copy of this file for safekeeping. After a software update, you will copy the updated `case.properties` file to the same directory so that your customizations are retained.

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Cases Editor UI Customization Tech Note (ESM 6.9.0c)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [arc-doc@hp.com](mailto:arc-doc@hp.com).

We appreciate your feedback!