

Стандарти и насоки в техническото писане

Николай Кънчев
Валентин Атанасов

ФМИ, Софтуерна документация
2020/2021

Съдържание

Преговор

Why Tech-Write in English?

What Writing?

What is Technical Writing All About?

Structuring

Simplicity

Precision

Verb Choice

Clarity

Formatting

Преговор

От предишната лекция вие научихте:

Писането на документация като част от софтуерния процес.

Какъв процес следва документацията?

Анализ

Дизайн

Разработка

Редакция

Публикация

Поддръжка

Why Tech-Write in English?



The language of the WWW

Informally worldwide standard language

The language of the business

Tech English is a simplified, standardized version of the language

What Writing?

Type	Example	Purpose	Style
<p>Creative</p>  <p>Let me not to the marriage of true minds Admit impediments. Love is not love Which alters when it alteration finds, Or bends with the remover to remove: O no; it is an ever-fixed mark, ...</p> <p>W. Shakespeare</p>	<p>Novel Short story Newspaper Blog</p>	<p>Excite Entertain Inform Express opinion Motivate Share emotions</p>	<p>Long and complex sentences Synonyms Ambiguity Humor Satire</p>
<p>Technical</p>  <p>Eclipse Dirigible is an open source project that provides Integrated Development Environment as a Service (IDEaaS), as well as integrated runtime execution engines. The applications created with Eclipse Dirigible comply with the Dynamic Applications concept and structure.</p> <p>Dirigible Online Help</p>	<p>Software help Technical blog Specification</p>	<p>Inform Instruct Support decision making Enable implementation Enable operations</p>	<p>Short sentences Terminology Active voice Clarity Correctness Consistency Impartiality</p>

Remember: The purpose of our writing determines our style.

What is Technical Writing All About?

Tech writing is about:

Good structuring

Simplified language

Precision

Verb choice and active voice

Clarity and conciseness

Formatting

Technical writing is NOT about:

Writing like Shakespeare



<http://arcticcirclecartoons.com/comics/february-9-2016/>

Structure

Structure your content into logical (and visual) chunks

Headings

Paragraphs

Sections

Tables

Bulleted lists

Numbered lists

Configuring Authentication for Your Application

This is an optional procedure that you can perform to configure the options for the authentication methods you defined for your application. You have an application with authentication defined in its `web.xml` or source code. See [Enabling Authentication](#). For each authentication method, you can select a custom combination of options. You may need to select more than one option if you want to enable more than one way for users to authenticate for this application. If you select more than one option, SAP HANA Cloud Platform will delegate authentication to the relevant login modules consecutively in a stack. When a login module succeeds to authenticate the user, authentication ends with success. If no login module succeeds, authentication fails.

Trusted SAML 2.0 identity provider - Authentication is implemented over the Security Assertion Markup Language (SAML) 2.0 protocol, and delegated to SAP ID service or custom identity provider (IdP). The credentials users need to present depend on the IdP settings.

User name and password - HTTP BASIC authentication with user name and password. The user name and password are validated either by SAP ID service (default) or by an on-premise SAP NetWeaver AS Java. See [Using an SAP System as an On-Premise User Store](#).

Client certificate - Users authenticate with a client certificate installed in an on-premise SAP NetWeaver Application Server for Java system. See [Enabling Client Certificate Authentication](#).

Application-to-Application SSO - Used for AppToAppSSO destinations. See [Application-to-Application SSO Authentication](#).

Note: When you select Trusted SAML 2.0 identity provider, Application-to-Application SSO becomes enabled automatically.

OAuth 2.0 token - Authentication is implemented over the OAuth 2.0 protocol. Users need to present an OAuth access token as credential. See [Protecting Applications with OAuth 2.0](#).

In your Web browser, open the Cockpit. See [Cockpit](#).

Enter the **Java Applications** section.

Click the application you want to configure.

Enter the **Authentication Configuration** section.

To configure the default settings, choose **Custom**, and then choose **Edit**.

WALL OF TEXT

Configuring Authentication for Your Application

This is an optional procedure that you can perform to configure the options for the authentication methods you defined for your application.

Prerequisites

- You have an application with authentication defined in its `web.xml` or source code. See [Enabling Authentication](#).

Context

The following table describes the available authentication options. For each authentication method, you can select a custom combination of options. You may need to select more than one option if you want to enable more than one way for users to authenticate for this application.

If you select more than one option, SAP HANA Cloud Platform will delegate authentication to the relevant login modules consecutively in a stack. When a login module succeeds to authenticate the user, authentication ends with success. If no login module succeeds, authentication fails.

Table 1: Authentication Options

Authentication Options	Description
Trusted SAML 2.0 identity provider	Authentication is implemented over the Security Assertion Markup Language (SAML) 2.0 protocol, and delegated to SAP ID service or custom identity provider (IdP). The credentials users need to present depend on the IdP settings. See ID Federation with the Corporate Identity Provider .
User name and password	HTTP BASIC authentication with user name and password. The user name and password are validated either by SAP ID service (default) or by an on-premise SAP NetWeaver AS Java. See Using an SAP System as an On-Premise User Store .
Client certificate	Users authenticate with a client certificate installed in an on-premise SAP NetWeaver Application Server for Java system. See Enabling Client Certificate Authentication .
Application-to-Application SSO	Used for AppToAppSSO destinations. See Application-to-Application SSO Authentication .
	Note When you select Trusted SAML 2.0 identity provider , Application-to-Application SSO becomes enabled automatically.
OAuth 2.0 token	Authentication is implemented over the OAuth 2.0 protocol. Users need to present an OAuth access token as credential. See Protecting Applications with OAuth 2.0 .

Procedure

- In your Web browser, log on to the cockpit, and select an account. See [Cockpit](#).
Make sure that you have selected the relevant global account to be able to select the right account.
- Enter the **Java Applications > Java Applications** section.
- Click the application you want to configure.
- Enter the **Authentication Configuration** section.
- To configure the default settings, choose **Custom**, and then choose **Edit**.
You can configure existing authentication methods or create new ones. If you need to restore the default state of all default methods, choose the **Restore** button for the entire panel. If you need to restore the default state of a particular method, choose the **Restore** button for that method (not available for custom methods you defined).
- Save the changes to the authentication configuration.
- Restart the application so the changes can take effect.

Example

You have a Web application that users access using a Web browser. You want users to log in using a SAML identity provider. Hence, you define the FORM authentication method in the `web.xml` of the application. However, later you decide to provide mobile access to your application using the OAuth protocol (SAML is not optimized for mobile access). You do this by adding the **OAuth 2.0 token** option for the FORM method for your application. In this way, desktop users will continue to log in using a SAML identity provider, and mobile users will use an OAuth 2.0 access token.

Related Information

[Enabling Authentication](#)
[Specifying Authentication Mechanisms \(general information\)](#)

Headings

Table

Ordered Steps

Example



Simplicity

- Use simple language and grammar.
 - ✓ Go to *File* -> *New* and enter your new file name.
 - × Provided that your desire is to create a new file, we would strongly recommend that you open the New option from the File menu, and enter the first file name that comes to your mind. Actually, you have no other options.
- Use short sentences (example: see above).
- Use positive formulations where possible.

Note: There can be exceptions when you have to use the negative formulation.

 - ✓ Always encrypt passwords before sending.
 - × Avoid sending unencrypted passwords.
 - ✓ Do not send passwords in plain text.
- Do not use long series of nouns that modify one another or a long series of prepositional phrases. Instead, split them up into smaller, more manageable units.
 - ✓ Check the port signals from the adapter card of the device.
 - × Check the device adapter card port signals.
- Use American English.

Precision

Write true information

Use correct and consistent terminology

- Avoid using “synonyms” (always use the same term)

- Introduce the abbreviations you use

- Use existing terminology

- Create new terms if not available

- Avoid professional jargon

Use correct navigation paths

Use correct product or component names

Avoid ambiguity, vagueness

Verb Choice

- Use precise verbs.
 - ✓ Change / Save / Delete / Import / Create / ...
 - × Maintain / do the thing / kindly do the needful / ...
- Can or May?
 - Can = possible for the user or the system.
 - May or might = possible state or outcome.

Verb Choice

MUST = an absolute requirement

MUST NOT = “shall not” – absolute prohibition

SHOULD = “recommended” – there may exist valid reasons in some circumstances to ignore a particular item

SHOULD NOT = “not recommended”

MAY = “optional” – you can choose whether to implement this action or not

Clarity

- Use active voice.
 - Passive voice conveys no information about who is doing what to whom or to what
 - ✓ You create users in the Admin UI.
 - ✓ The system generates random user IDs.
 - × Users are assigned random IDs when created.
- Address the user directly with “you” (if appropriate)
- Define clearly who does what (the user, the application, the system administrator)
- Use imperative in steps and instructions
 - ✓ Create a new project file (*File -> New -> Project*).
 - × The administrator must create a new project file.
- Provide useful context
 - Describe sequence of activities (what is 1st, 2nd, 3rd, ...)
 - Add prerequisites and results of activities (including possible errors)

Formatting is Important

Proper formatting enables visual screening of your documentation

Use proper spaces between paragraphs, sections, headings, lists, tables, and so on

Emphasize keywords

Use special font or formatting for:

- Menu paths

- Code samples

- UI elements

Additional Tips

Avoid humor – culture specific

Avoid gender references

Avoid professional jargon

Use spell checker

Use Google search whenever in doubt

Благодарим Ви за вниманието!

Стандарти и насоки в техническото писане

Николай Кънчев
Валентин Атанасов

ФМИ, Софтуерна документация
2020/2021

Exercise 1

Write a short how-to guide

1. On your local device, open a browser and use this URL: <https://www.techsmith.com/tutorial-camtasia.html>. Scroll to *All Tutorials* and select one and watch it.
2. Analyze the video tutorial (5 min):
 - Who are the target users? What is their level of competence?
 - What is the aim of this tutorial?
3. Imagine this video is the input sent to you by the responsible developers. Create a short guide based on this tutorial following the writing guidelines in the lecture and handout (30 min).
(You may use the Word app to create your document)
4. At home, send the document you've created to our e-mail address: fmi.docu2020@gmail.com