IBM Enterprise Content Management System Monitor

Configuration Guide

IBM Enterprise Content Management System Monitor
Version 5.6.0

Configuration Guide

SC27-9240-07

Table of Contents

This document contains information about the configuration of the IBM Enterprise Content Management System Monitor after it is installed. The target audience for this guide are those who install or maintain ESM environments or users with administrative privileges.

Preface

About this document

This document is written as plain text document and provided as html / pdf. The newest ESM related documents can be found in the help section of the console.

Who should read this guide?

The target audience for this guide are those who install or maintain ESM environments.

Every effort has been made to provide you with complete installation instructions. If information becomes available after the creation of the installation media from which you accessed this guide, we will provide an updated version of the guide on the IBM Customer Service and Support web site (https://www.ibm.com/support). As a general rule, you should refer to the IBM web site to obtain the current version of this guide.

This guide provides instructions for installing and/or upgrading IBM Enterprise Content Management System Monitor, and identifies the IBM/FileNet and 3rd Party products that are certified for the current release. Be aware that each release of IBM Enterprise Content Management System Monitor may have multiple Interim Fixes, or Fix Packs available for installation, each with potentially different dependencies and installation requirements. Therefore, before you attempt to install or upgrade IBM Enterprise Content Management System Monitor, review the list of releases and their associated dependencies on the IBM Support web site (https://www.ibm.com/support).

Before you start

Users of the guide should have knowledge about Unix and/or Microsoft Windows® operating system, web servers, database systems and middleware platforms. The configuration of managed systems (clients) requires advanced knowledge of all IBM ECM systems that should be monitored.

You should read the Upgrade Notes section below!

If you lack the requisite skill sets it is strongly recommended to have IBM Lab Services or a certified ValueNet Partner in order to install this product.

TIP

For tips and tricks regarding the configuration and maintenance of IBM Enterprise Content Management System Monitor please check the CENIT Field Guides at IBM ESM Field Guides.

The updated documentation can be downloaded from the IBM download pages.

Feedback on documentation

Send your comments by e-mail to comments@us.ibm.com. Be sure to include the name of the product, the version number of the product, and the name and part number of the book (if applicable). If you are commenting on specific text, include the location of the text (for example, a chapter and section title, a table number, a page number, or a help topic title)

Administration Dashboard

The administration dashboard offers the possibility to adjust Server Settings, review the audit log, manage users and login modules, such as LDAP integration and administrate SMTP and SNMP forwarding.

Server

Once you have selected the server icon on the left, two options are offered. You can either adjust server settings or review the audit log.

Settings

Double-click on the Settings button to open the Server Settings.

Monitoring

Disable Base Monitoring for New Agents

You can enable or disable the automatic deployment of the base monitoring for new agents. The base monitoring contains the setup of the following probes:

- cpu
- memory
- diskspace

Database Cleanup

Database Cleanup Interval

Default is 60 minutes. Specify the interval in minutes that is used to clean up the database.

Database Max Sample Count

Default is 1.5 million. Specify the amount of samples that should be stored in the database.

IMPORTANT If you use H2 as database, do not specify more than 1.5 million.

Database Max Incident Count

Default is 1.5 million. Specify the amount of incidents that should be stored in the database.

IMPORTANT If you use H2 as database, do not specify more than 1.5 million.

Max Reports Per Report Configuration

Default is 100. Specify the amount of reports that should be stored for a report configuration.

Session

Session Timeout Enabled

Check to enable the session timeout. The user is logged out due to inactivity after x minutes. Default is disabled.

Session Timeout Interval

Specify the timeout interval in minutes after that the user is getting logged out due to inactivity. Default is 5.

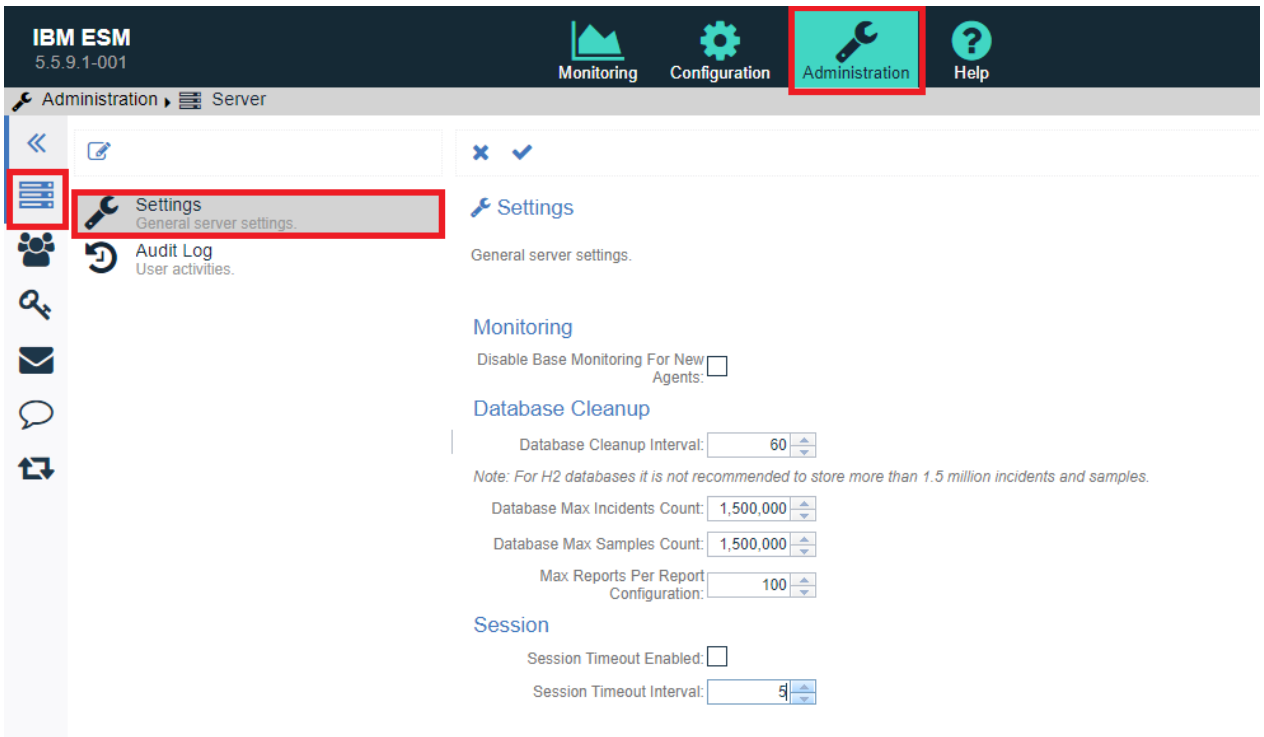


Figure 1. Image of Administration Server Settings

Audit Log

Choose the audit log icon from the sidebar. This will open the audit log on the right side of the sidebar.

You have the possibility to reload the audit log.

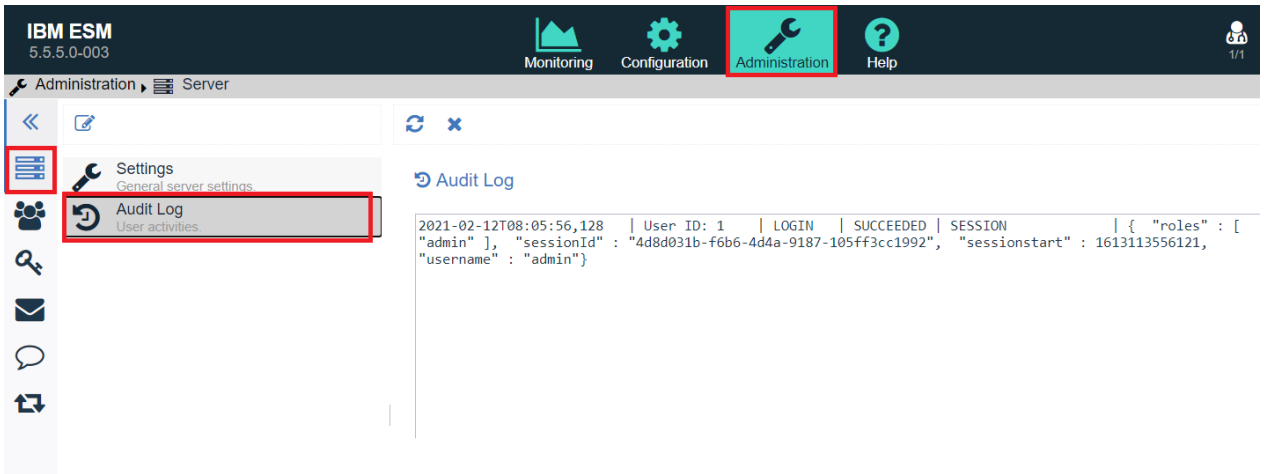


Figure 2. Image of Administration Server Audit Log

User Management

In the administration of ESM users the following data is mandatory for the technical operation of the service: UserID, password. Additional information, including personal information which is subject to the GDPR regulation (e.g. email, full name, phone #) is optional and under the control of the client to provide or not provide.

Starting from ESM version 5.5.11.0-001 onwards the roles have changed. The previous role "user" is removed and completely replaced with the "guest" role.

Description of the roles

admin

- No limitations

operator

- No permission to change existing configurations of any kind
  - This implies also no ad-hoc execution of existing tasks with changed parameters
  - This implies also no ad-hoc execution of existing reports with changed parameters except the period settings below "Ad Hoc Run".

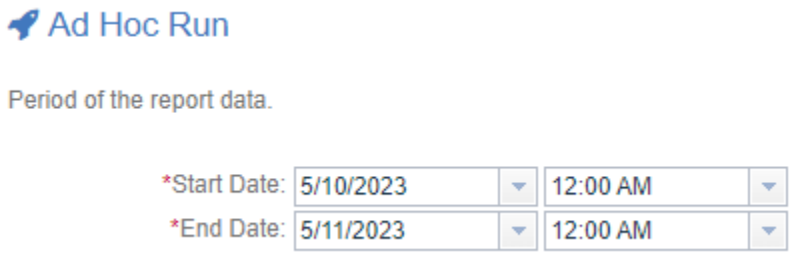


Figure 3. Image of AdHocRun

- No permission to create new configurations of any kind
- Permission to execute existing probes, tasks, and reports.
- Permission to acivate and deactivate existing probes (only in new Operational UI)
- Permission to acivate and deactivate existing tasks.
- Not allowed to create sample filters.
- No access to "Administration", but its own settings (password changes allowed)
- Agents Editor:
  - Permission to restart an agent
  - No permission to update an agent
  - No permission to delete an agent

  guest
- Read-only without all below + all limitations from above.
  - Existing Reports can be used to create pdfs.

Adding an Internal User

Choose the user management icon from the sidebar. This will open a list containing all users. Per default only the admin account exists.

Click on the "Create a new User" icon at the top of the bar. This will open the "User Editor" for internal users at the right site.

Image of User Editor Internal

Complete the settings for the user and save it by clicking at the "Save" icon at the top.

The following parameters can be set:

Account Name (Required)

Specify the name that should be used for the account.

Role (Required)

Select one of the roles from the drop down. Possible roles are

- admin
- guest
- operator
- user

E-mail (Optional)

If specified, the address can be reused within ESM e.g. for sending reports.

Password (Required)

Specify the password that should be used for the account. The password must be at least 10 characters long and must contain at least one uppercase letter, one lowercase letter and one digit.

Confirm Password (Required)

Specify the password that should be used for the account. The given password is compared with the "Password" parameter.

Full Name (Optional)

You can specify the full name of the user here.

Phone Number (Optional)

You can specify the phone number of the user here.

Room (Optional)

You can specify the room number / name of the user here.

Enabled

If checked, the account can be used for login. Otherwise, the account only exists but is not able to log in.

Adding an External User

Choose the user management icon from the sidebar. This will open a list containing all users. Per default only the admin account exists.

Click on the "Create a new external User" icon at the top of the bar. This will open the "User Editor" for external users at the right site.

Image of User Editor External

Complete the settings for the user and save it by clicking at the "Save" icon at the top.

The following parameters can be set:

Account Name (Required)

Specify the name that should be used for the account.

Role (Required)

Select one of the roles from the drop down. Possible roles are

- admin
- guest
- operator
- user

E-mail (Optional)

If specified, the address can be reused within ESM e.g. for sending reports.

Full Name (Optional)

You can specify the full name of the user here.

Phone Number (Optional)

You can specify the phone number of the user here.

Room (Optional)

You can specify the room number / name of the user here.

Enabled

If checked, the account can be used for login. Otherwise, the account only exists but is not able to log in.

User Preferences

Once a user account is created or modified, the lower section shows the user preferences. You can define a threshold severity for notifications.If defined, notifications about incidents with a severity level equal or higher than the specified will pop up as long as the ESM console is opened in a browser. The browser can be lowered to the task bar and the tab can be inactive.

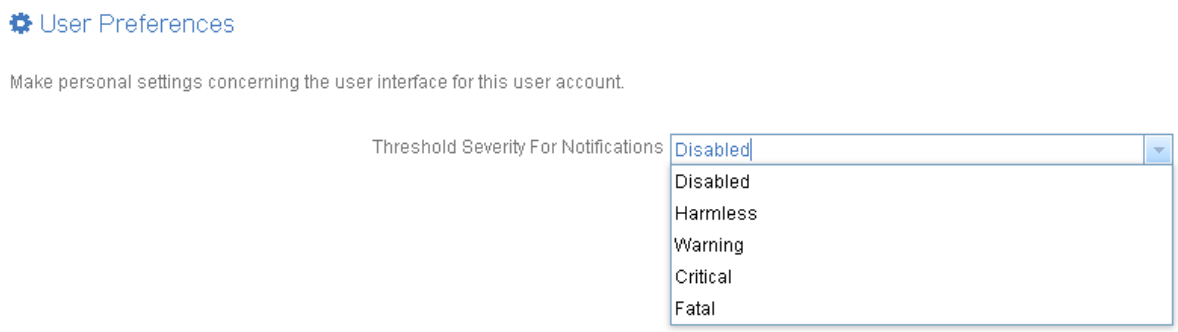


Image of User Preferences Settings

The incident pop up looks like this.

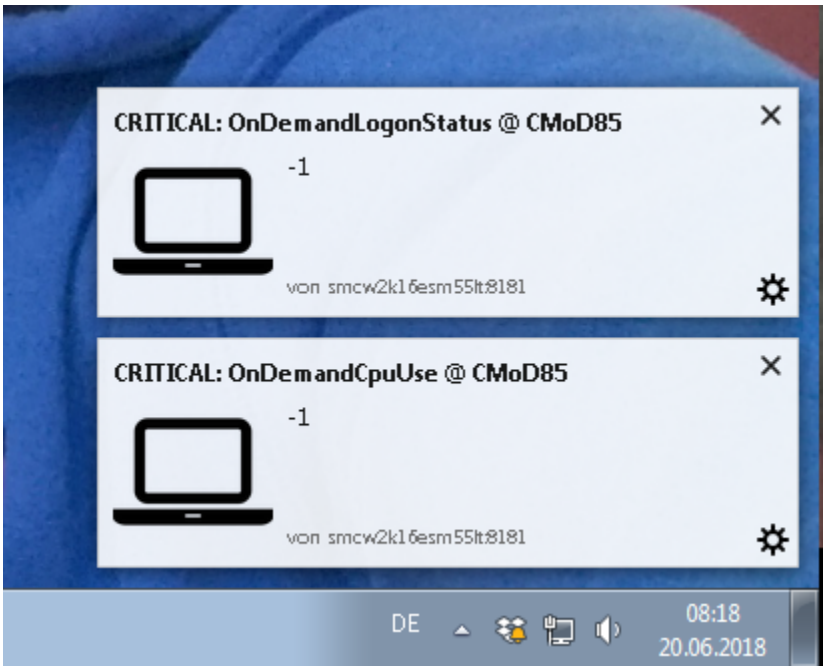


Image of incident pop up

NOTE Not all browsers do support this feature and in some it´s deactivated per default.

Login Module

ESM provides the possibility to log in with an LDAP account. The most common LDAP Types are supported.

Add a new Login Module

Choose the login module icon from the sidebar. This will open a list of already created login modules. Per default no login module is available but multiple can exist.

Click on the "Create a new Login Module" icon at the top of the bar. This will open the "Login Module Editor" at the right site.

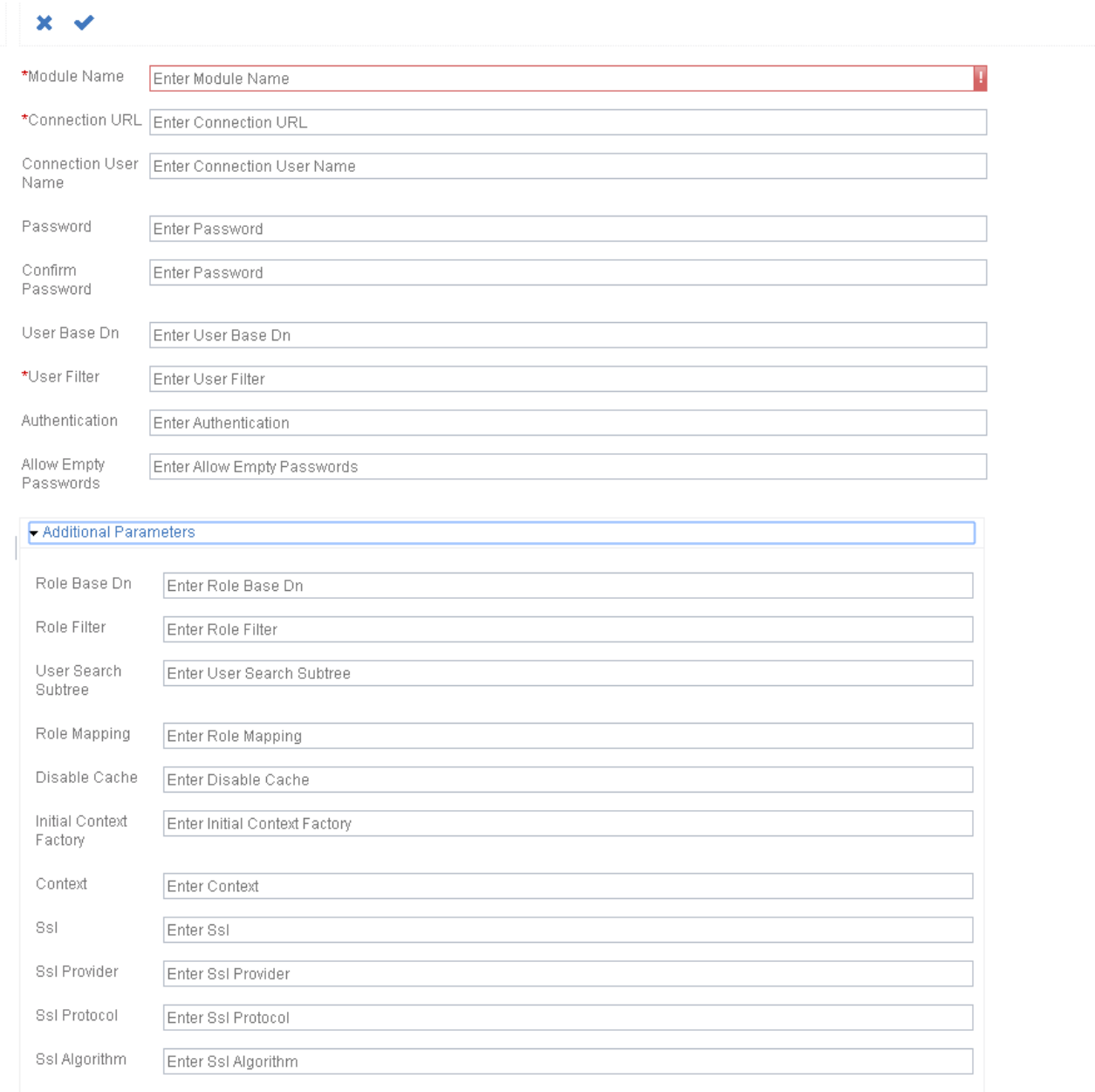


Image of Login Module Editor

Complete the settings for the login module and save it by clicking at the "Save" icon at the top.

Parameters needed for default setup

Table 1. The following parameters can be set:

Parameter	Description
Module Name (Required)	Specify the name that should be used for the module.
Connection URL (Required)	The LDAP connection URL, e.g. ldap://hostname:389
Connection User Name (Required)	Admin username to connect to the LDAP. This parameter is currently required - bind user
Password (Required)	Admin password to connect to the LDAP. Only used if the Connection User Name is specified.
Confirm Password (Required)	Enter Password again
User Base Dn (Optional)	The LDAP base DN used to looking for user, e.g. Ou=Users,DC=MyDomain,DC=com
User Filter (Required)	The LDAP filter used to looking for user, e.g. (uid=%u) where %u will be replaced by the username
Authentication (Optional)	Define the authentication backend used on the LDAP server. The default is simple. Possible values are: none, simple and GSSAPI (with Kerberos only). You can combine these with ldaps (URL) of course.
Allow Empty Passwords (Optional)	Specify whether log in with empty password is allowed true) or not (false).

Parameters for advanced setup

Table 2. The following parameters can be set for advanced configuration:

Parameter	Description
Role Base Dn (Optional)	The LDAP base DN used to looking for roles, e.g. Ou=Role,DC=MyDomain,DC=com
Role Filter (Optional)	The LDAP filter used to looking for user's role, e.g. (member:=uid=%u). By using search filters, you can define search criteria that provide better control to achieve more effective and efficient searches. See documentation of your LDAP service provider for details.
User Search Subtree (Optional)	If "true", the user lookup will be recursive (SUBTREE). If "false", the user lookup will be performed only at the first level (ONELEVEL).
Role Mapping (Optional)	Define a mapping between roles defined in the LDAP directory for the user, and corresponding roles in Karaf. The format is ldapRole1=karafRole1,karafRole2;ldapRole2=karafRole3,karafRole4.

Parameter	Description
Disable Cache (Optional)	Specifies whether to disable the authentication cache. The authentication cache can be enabled for performance reasons. However, you can disable the authentication cache for debug or measurement purposes.
Initial Context Factory (Optional)	Define the initial context factory used to connect to the LDAP server. The default is com.sun.jndi.ldap.LdapCtxFactory
Context (Optional)	
Ssl (Optional)	If "true" or if the protocol on the connection.url is ldaps, an SSL connection will be used
Ssl Provider (Optional)	The provider name to use for SSL
Ssl Protocol (Optional)	The protocol name to use for SSL (e.g. SSL)
Ssl Algorithm (Optional)	The algorithm to use for the KeyManagerFactory and TrustManagerFactory (e.g. PKIX)
Ssl Keyalias (Optional)	The key alias to use for SSL
Ssl Timeout (Optional)	Timeout in milliseconds
User Names Trim (Optional)	
Ldap Ctx Factory (Optional)	
Role Name Attribute (Optional)	The LDAP role attribute containing the role string used by Karaf, e.g. cn
Role Search Subtree (Optional)	If "true", the role lookup will be recursive (SUBTREE). If "false", the role lookup will be performed only at the first level (ONELEVEL).
Ldap Read Timeout (Optional)	Timeout in milliseconds for reading from LDAP. 0 means no timeout is specified.
Ldap Connect Pool (Optional)	
Context Java Naming Referral (Optional)	A JNDI application uses the Context.REFERRAL(in the API reference documentation) ("java.naming.referral") environment property to indicate to the service providers how to handle referrals. The following table shows the values defined for this property. If this property has not been set, then the default is to ignore referrals. Possible Settings are: ignore =Ignore referrals, follow = Automatically follow any referrals, throw = Throw a ReferralException for each referral

Mail Server administration

Choose the Mail Server administration icon from the sidebar. This will open a list of already created SMTP server setups. Per default no setup is available.

Click on the "Create a new Mail Server" icon at the top of the bar. You can distinguish if you want to add an SMTP Server or an Azure Server at this point. The corresponding editor is opened at the right site.

====SMTP Server Editor

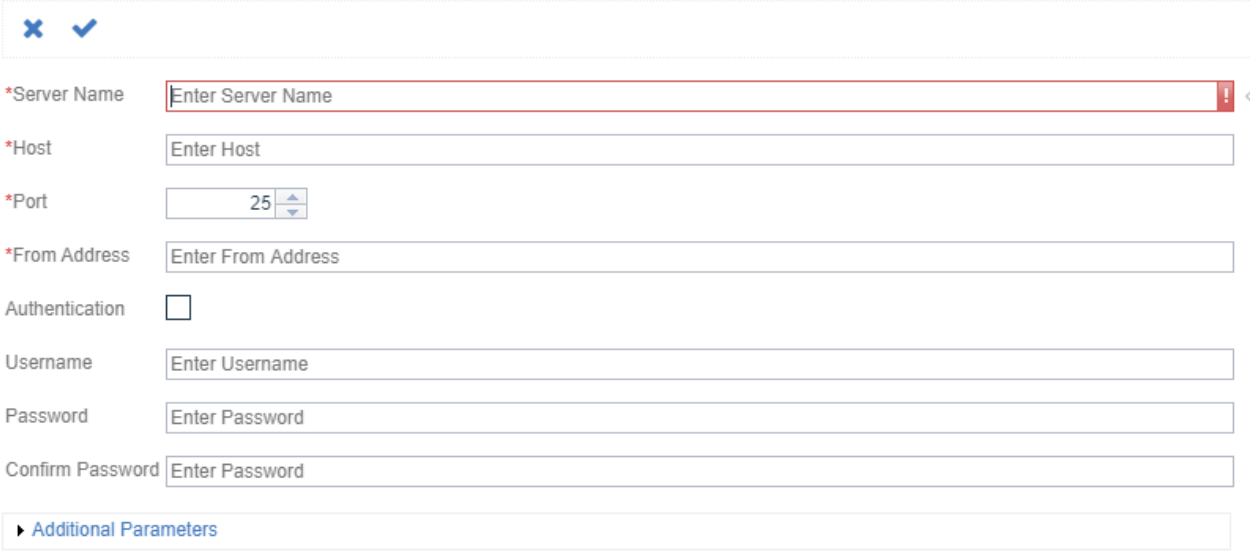


Image of SMTP Server Editor

The following parameters can be set:

SmtpServer

Server Name

Specify the name that should be used for storing the setup.

Host

Specify the hostname which can be used for the connection to the SMTP Server.

Port

Specify the port of the SMTP server here. Most the time this is 25 for SMTP servers.

From Address

Specify the email address of the sender here.

Authentication

Check if authentication is required.

Username

If a certain user for the SMTP connection must be used, specify the user name here.

Password (Optional)

Only need if a certain user must be used, specify the password for the user here.

Confirm Password (Optional)

Only need if a certain user must be used, specify the password for the user here. The given password is compared with the "Password" parameter.

The following additional options (expert mode) are available:

Connection Timeout

Connection timeout in milliseconds. Default: infinite.

Timeout

Description: Socket read timeout value in milliseconds. This timeout is implemented by java.net.Socket. Default: infinite.

Write Timeout

Description: Socket write timeout value in milliseconds. This timeout is implemented by using a java.util.concurrent.ScheduledExecutorService per connection that schedules a thread to close the socket if the timeout expires. Thus, the overhead of using this timeout is one thread per connection. Default: infinite.

Local Host

Email address to use for SMTP MAIL command. This sets the envelope return address. NOTE: mail.smtp.user was previously used for this. Default: Defaults to msg.getFrom() or InternetAddress.getLocalAddress().

Local Address

Local address (host name) to bind to when creating the SMTP socket. Should not normally need to be set, but useful with multi-homed hosts where it’s important to pick a particular local address to bind to. Default: The address picked by the Socket class.

Local Port

Local port number to bind to when creating the SMTP socket. Default: The port number picked by the Socket class.

Sign on with EHLO

If false, do not attempt to sign on with the EHLO command. Normally failure of the EHLO command will fall back to the HELO command; this property exists only for servers that don’t fail EHLO properly or don’t implement EHLO properly. Default: true.

Auth Mechanisms

If set, lists the authentication mechanisms to consider, and the order in which to consider them. Only mechanisms supported by the server and supported by the current implementation will be used. The default is "LOGIN PLAIN DIGEST-MD5 NTLM", which includes all the authentication mechanisms supported by the current implementation except XOAUTH2. Default: LOGIN PLAIN DIGEST-MD5 NTLM.

Auth Login Disable

If true, prevents the use of AUTH LOGIN command. Default: false.

Auth Plain Disable

If true, prevents the use of AUTH PLAIN command. Default: false.

Auth Digest MD5 Disable

If true, prevents the use of AUTH DIGEST-MD5 command. Default: false.

Auth NTLM Disable

If true, prevents the use of AUTH NTLM command. Default: false.

Auth HTML Domain

The NTLM authentication domain. Default: empty.

Auth NTLM Flags

NTLM protocol-specific flags. Search the internet for details. Default: empty.

Auth XOAUTH2 Disable

If true, prevents use of the AUTHENTICATE XOAUTH2 command. Because the OAuth 2.0 protocol requires a special access token instead of a password, this mechanism is disabled by default. Enable it by explicitly setting this property to "false" or by setting the "mail.smtp.auth.mechanisms" property to "XOAUTH2". Default: false.

Submitter

The submitter to use in the AUTH tag in the MAIL FROM command. Typically used by a mail relay to pass along information about the original submitter of the message. See also the setSubmitter method of SMTPMessage. Mail clients typically do not use this. Default: Not set.

DSN Notify

The NOTIFY option to the RCPT command. Either NEVER, or some combination of SUCCESS, FAILURE, and DELAY (separated by commas). Default: Not set.

Allow 8bit MIME

If set to true, and the server supports the 8BITMIME extension, text parts of messages that use the "quoted-printable" or "base64" encodings are converted to use "8bit" encoding if they follow the RFC2045 rules for 8bit text. Default: Not set, so maybe false.

Send Partial

If set to true, and a message has some valid and some invalid addresses, send the message anyway, reporting the partial failure with a SendFailedException. If set to false (the default), the message is not sent to any of the recipients if there is an invalid recipient address. Default: false.

Quit Wait

If set to false, the QUIT command is sent and the connection is immediately closed. If set to true (the default), causes the transport to wait for the response to the QUIT command. Default: true.

SSL Check Server Identity

If set to true, check the server identity as specified by RFC 2595. These additional checks based on the content of the server’s certificate are intended to prevent man-in-the-middle attacks. Default: false.

Enable SSL

Enables SSL regardless of the port used or the protocols specified in SSL Protocols. To enable it, enter "true" here. Default: false.

SSL Protocols

Specifies the SSL protocols that will be enabled for SSL connections. The property value is a whitespace separated list of tokens acceptable to the javax.net.ssl.SSLSocket.setEnabledProtocols method. Defaults: not set.

SSL Cipher Suites

Specifies the SSL cipher suites that will be enabled for SSL connections. The property value is a whitespace separated list of tokens acceptable to the javax.net.ssl.SSLSocket.setEnabledCipherSuites method. Default: not set.

SASL Enable

If set to true, attempt to use the javax.security.sasl package to choose an authentication mechanism for login. Default: false.

SASL Mechanisms

A space or comma separated list of SASL mechanism names to try to use. Default: Not set.

SASL Authorization Id

The authorization ID to use in the SASL authentication. Default: If not set, the authentication ID (user name) is used.

SASL Realm

The realm to use with DIGEST-MD5 authentication. Default: Not set.

SASL Use Canonical Hostname: If set to true, the canonical host name returned by InetAddress.getCanonicalHostName is passed to the SASL mechanism, instead of the host name used to connect. Default: false.

User Set

If set to true, use the RSET command instead of the NOOP command in the isConnected method. In some cases sendmail will respond slowly after many NOOP commands; use of RSET avoids this sendmail issue. Default: false.

NOOP Strict

If set to true (the default), insist on a 250 response code from the NOOP command to indicate success. The NOOP command is used by the isConnected method to determine if the connection is still alive. Some older servers return the wrong response code on success, some servers don't implement the NOOP command at all and so always return a failure code. Set this property to false to handle servers that are broken in this way. Normally, when a server times out a connection, it will send a 421 response code, which the client will see as the response to the next command it issues. Some servers send the wrong failure response code when timing out a connection. Do not set this property to false when dealing with servers that are broken in this way. Default: true.

====Azure Server Editor

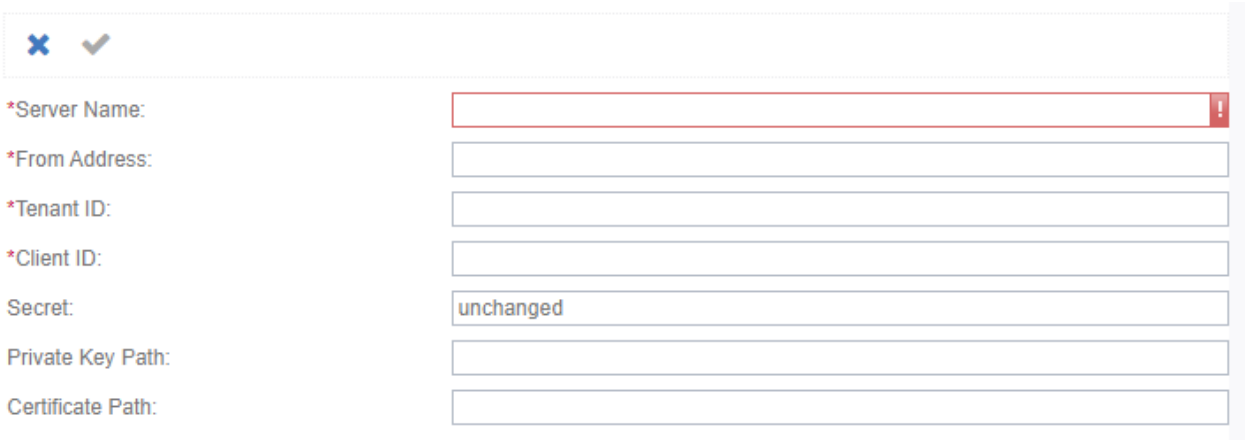


Image of AZURE Server Editor

The following parameters can be set:

AzureServer

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

From Address

Specify the email address of the sender here.

IMPORTANT The `From Address` must be a valid user principal name (identical to the email address) or Object ID (UUID) of an existing user.

Tenant Id

ID of the Azure tenant as shown in the Azure portal. Required.

Client Id

ID of the application as shown in the Azure portal. Required.

Secret

This value is created during application registration in the Azure portal. Required if application is configured to use client secret for authentication.

Private Key Path

FQ file name of private key file. Required if application is configured to use certificate for authentication.

Certificate Path

FQ file name of certificate file. Required if application is configured to use certificate for authentication.

SNMP Server administration

Choose the SNMP Server administration icon from the sidebar. This will open a list of already created SNMP server setups. Per default no setup is available.

Click on the "Create a new Item" icon at the top of the bar. This will open the Subsystem Editor for "SnmpTarget" at the right site.

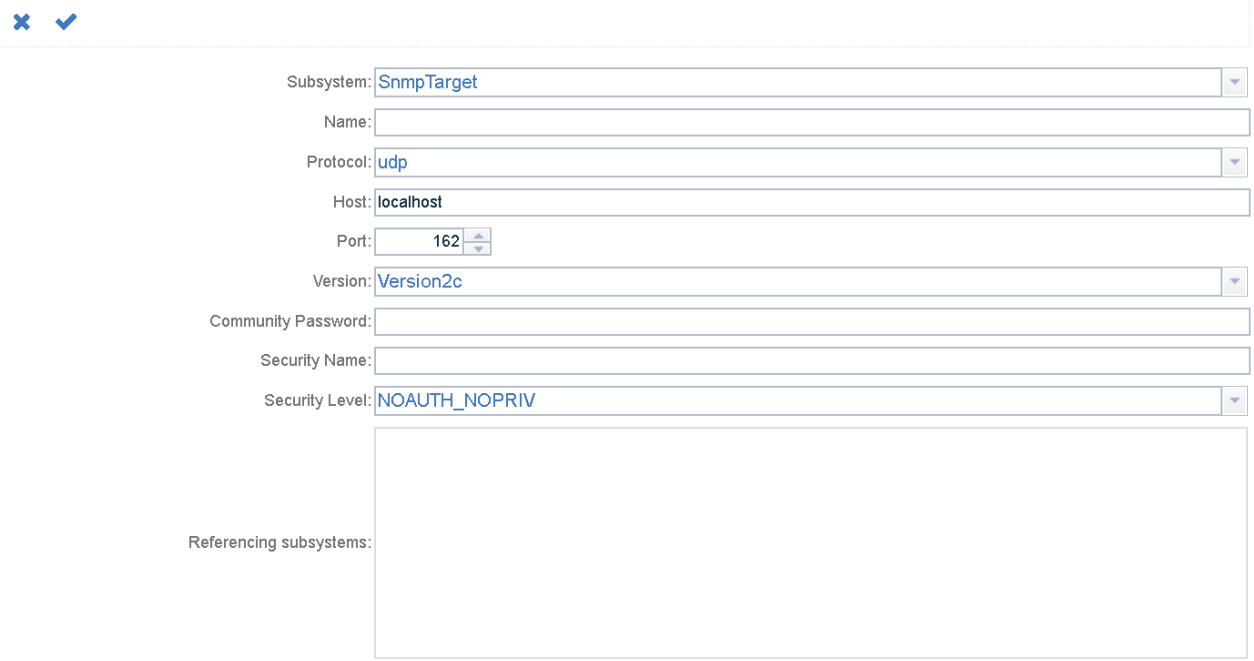


Image of SNMP Editor

The following parameters can be set:

SnmpTarget

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Protocol

Choose between udp and tcp from dropdown. The default is udp.

Host

Specify the SNMP Manager host here. IP address or hostname can be used

Port

Default 162. Specify the listening port of the SNMP manager host here.

Version

Select the SNMP Version from the drop down. Possible values are Version2c and Version3

Community Password

Please ask your SNMP Administrator if a community password is needed. Enter it here in case.

Security Name

Please ask your SNMP Administrator for the Security Name. Enter it here in case.

Security level (only needed for SNMP Version 3)

Ask your SNMP Administrator for the correct setting.

Configuration Import/Export

Using this functionality, administrators can export the full configuration of the ESM server. The configuration will be stored in a UTF-8 encoded JSON file. The file can be imported on the same or any other server.

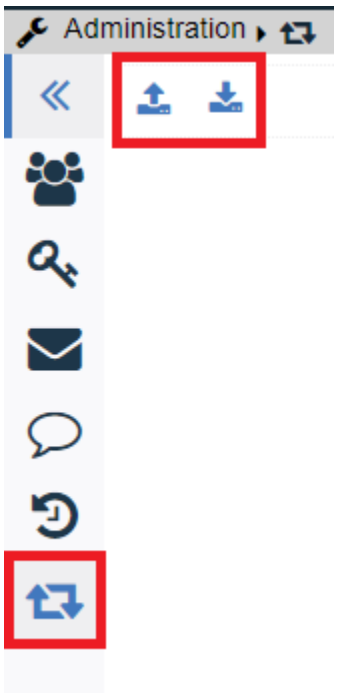


Image of Export and Import View

The following configuration will be exported:

- Agents
- All subsystems and the structure of the subsystems.
- All sample filters.
- All Situation configurations/structures:
  - Probe configurations (status always set to "non-active").
  - Agent connections.
  - Schedules.
  - Evaluations.
  - Escalation and duplicate detection configurations.
  - Automation configurations (aka task triggers and tasks).
- All tags.
- All situation groups.
- All task configurations.

- All custom knowledge base entries.
- All report configurations.
- All user accounts.
  - incl user specific settings. like dashboards, notification etc.
- All external systems defined in "Administration":
  - LDAP
  - SMTP
  - SNMP

Export the configuration:

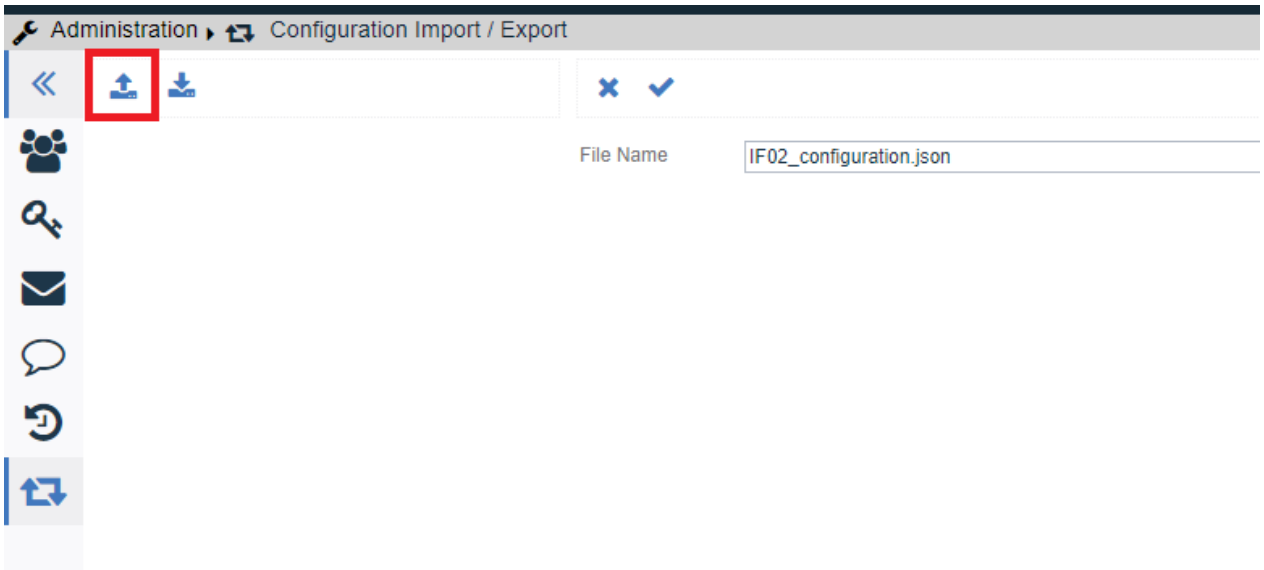


Image of Export

NOTE All data specified above will be exported.

Import the configuration:

NOTE Before the data can be imported, the server must be up and running completely. It can happen that the function can be accessed before this is the case. Usually it is enough to wait 2 to 3 minutes after server start. To verify you can check the status page "http(s)://<your server>[:<port>]/status" of your ESM server. Check if all bundles are satisfied or active.

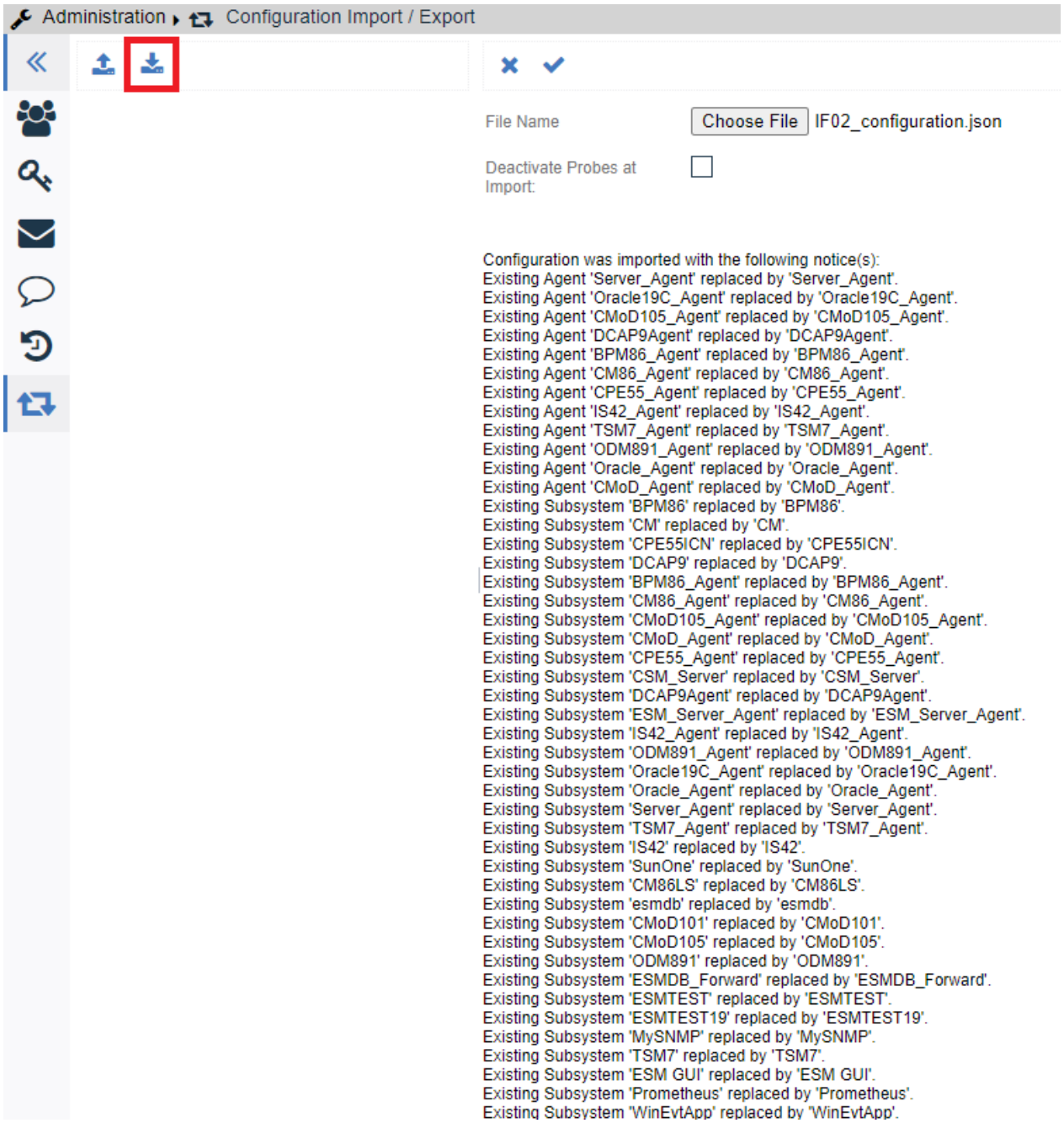


Image of Import

NOTE All data will be imported. You can specify if you want to deactivate all probes during the import.

ConfigurationDashboard

Context help for configuration of Subsystems and Situations

For the configuration of subsystems and situations a context help is shown next to the needed parameters on the right. The information is derived directly from the help information. It looks like this:

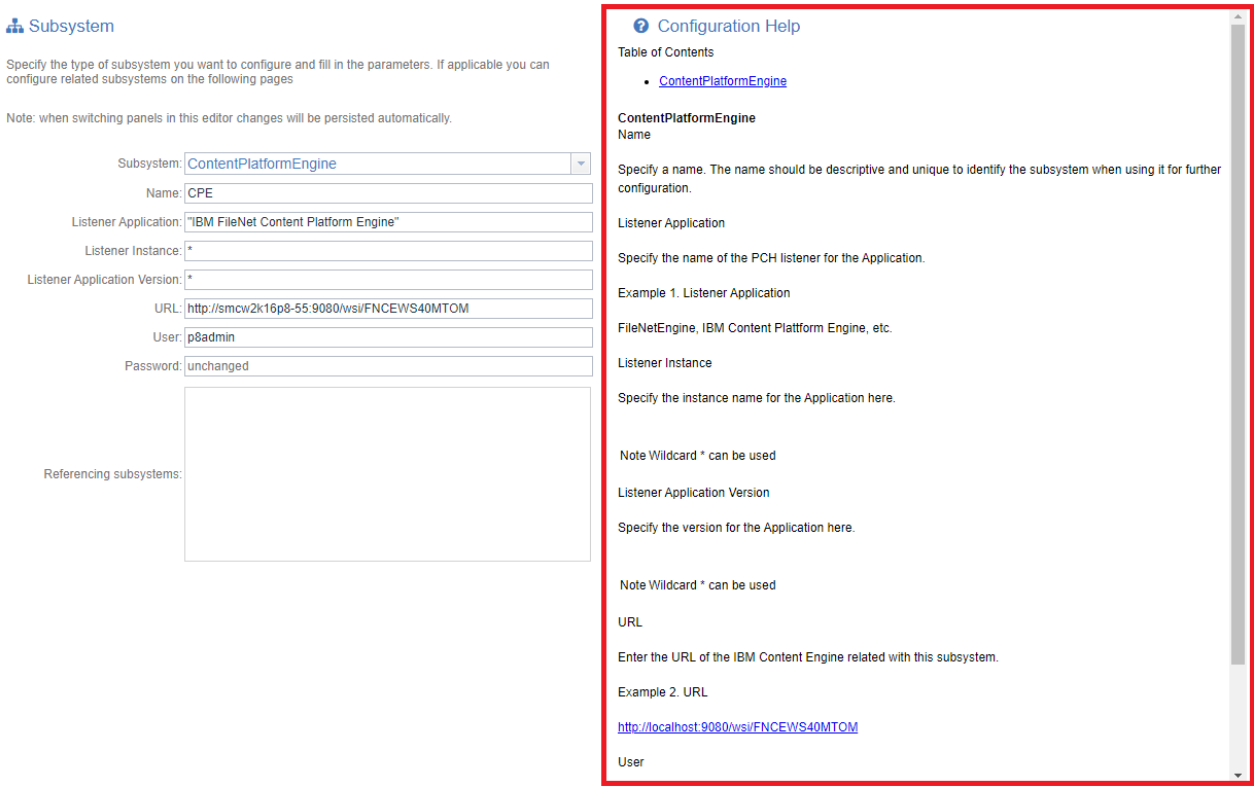


Image of configuration help

Creation of Subsystems

This chapter describes the creation of subsystems. From the main window select "Configuration" and choose the "Subsystems" icon from the sidebar. In the upper part of the sidebar actions, such as "Create a new Subsystem", "Create a new Probe", "Modify the selected Subsystem" and "Remove the selected Subsystem", can be triggered.

Also a subsystem can be duplicated or a deep copy can be triggered.

Duplicate means the selected subsystem is copied and all references of the origin subsystem are also referenced.

Deep copy means, the subsystems as well as the all referenced subsystems are copied. A new subsystem for each is created with name copy. The references are created between the newly created subsystems.

Each subsystem consists of certain parameters. In addition, a referencing subsystem can be selected. This mechanism is used to pack depending subsystems e.g. a database on a certain DB server. Once a subsystem references another subsystem it will be listed as a child subsystem in the sidebar.

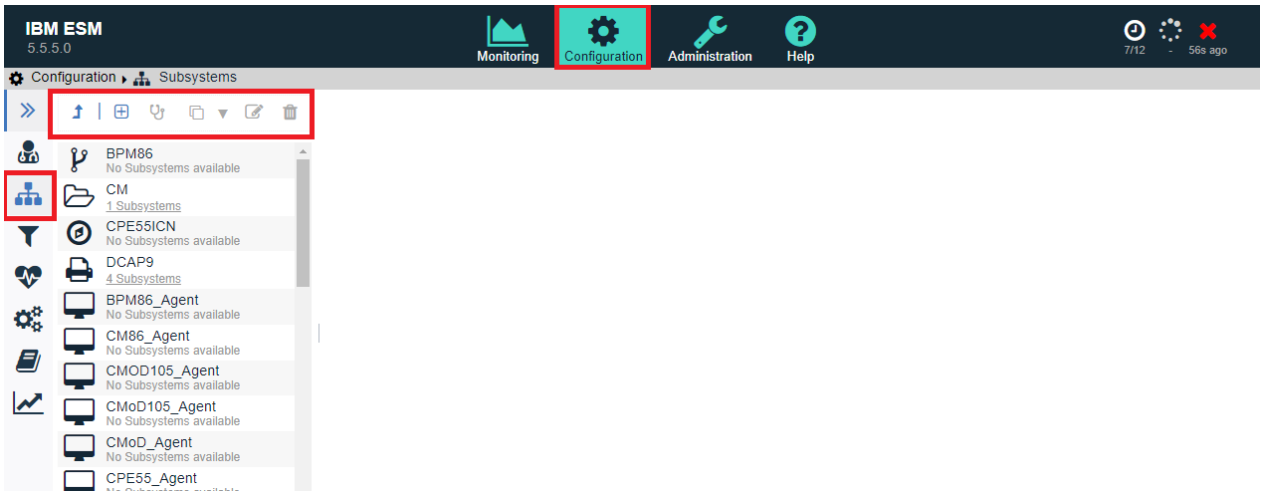


Image of Configuration Subsystem

The following section describes the subsystems and the needed parameters.

AzureServer

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

From Address

Specify the email address of the sender here.

IMPORTANT The `From Address` must be a valid user principal name (identical to the email address) or Object ID (UUID) of an existing user.

Tenant Id

ID of the Azure tenant as shown in the Azure portal. Required.

Client Id

ID of the application as shown in the Azure portal. Required.

Secret

This value is created during application registration in the Azure portal. Required if application is configured to use client secret for authentication.

Private Key Path

FQ file name of private key file. Required if application is configured to use certificate for authentication.

Certificate Path

FQ file name of certificate file. Required if application is configured to use certificate for authentication.

BusinessAutomationWorkflow

For Business Automation Workflow (BAW), no separate subsystem has been implemented so far. To monitor BAW the probes and subsystems of CaseManager (including CPE etc.) and BusinessProcessManager can be used.

BusinessProcessManager

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

NOTE Add a Url subsystem for the parameters address, user and password. For secure connections, a keystore subsystem must be configured there as well.
The user should be a member of administrator group. Otherwise, the delete snapshot tasks will not work.

CaseManager

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Listener Application

Specify the name of the PCH listener for the Application.

Example 1. Listener Application

```
IBM Case Manager
```

Listener Instance

Specify the instance name for the Application here.

NOTE Wildcards like * or ? can be used

Cebi

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

CE Library Path

Required. Enter the path to the IBM Content Engine's libraries.

Example 2. CE Library Path

```
C:\Program Files (x86)\IBM\FileNet\CEClient\
```

Java Path

Specify the path to java without /bin of the configured subsystem product here.

Example 3. JavaPath

```
C:\Program Files (x86)\Java\jre7
```

Installation Path

Specify the path where the product is installed. Required.

Example 4. Installation Path

```
C:\Program Files (x86)\IBM\FileNet\ContentEngine\tools\CEBI\
```

WebSphere Path

Optional. In case of running CEBI Tool on WebSphere Application Server enter its installation path here.

Websphere Options

Optional. In case of running CEBI Tool on WebSphere Application Server enter additional options here.

NOTE On UNIX / Linux, option names or values that contain whitespaces are not supported.

ContentCollector

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

ContentIntegrator

The ContentIntegrator (ICI) subsystem will be referenced in the ContentIntegratorConnector subsystem.

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

ContentIntegratorConnector

The ContentIntegratorConnector subsystem should reference the ContentIntegrator (ICI) subsystem.

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

RMI Host

Enter the hostname that is used in the Content Integrator Bridge script for the RMI connection. Search for the RMI URL in the script.

RMI Port

This is the RMI port for the Content Integrator RMI Bridge Connector to which the monitors shall connect to. The probe can be run in two modes. The port `1250` is used (for mode `Check All`) and `1251` (for mode `Check One`) as default.

ContentNavigator

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

NOTE Add a Url subsystem for the parameters address, user and password. For secure connections, a keystore subsystem must be configured there as well.

The URL must include the ICN context root, e.g. `/navigator`.

Example 5. Address

```
http://localhost:9080/navigator
```

ContentPlatformEngine

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Listener Application

Specify the name of the PCH listener for the Application.

Example 6. Listener Application

```
FileNetEngine, IBM Content Plattform Engine, etc.
```

Listener Instance

Specify the instance name for the Application here.

NOTE Wildcard * can be used

Listener Application Version

Specify the version for the Application here.

NOTE Wildcard * can be used

NOTE Add a Url subsystem for the parameters address, user and password. For secure connections, a keystore subsystem must be configured there as well.

Database

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Name

Specify the name of the database.

Database Username

Specify the name of the user for log in to the database. This user is used for monitoring the database and must have sufficient rights.

Database Password

Specify the password of the user for log in to the database.

Database Schema

Specify the schema that is used within the database.

Database Port

Specify the port which is used for the database connection. This parameter can be reused in the JDBC Connection Template of subsystem Database with $DatabasePort.

JDBC Connection Template

Specify the connection template (JDBC URL) for the database. The template consists of two parts. One for the database type and one for the database itself. $DatbaseHost, can be used to integrate the Hostname setting from an Rdbms subsystem. $DatabasePort and $DatabaseName will be replaced with the settings of Database Name and Database Port of this configuration.

Example 7. JDBC Connection Template of Postgresql

```
jdbc:postgresql://$DatabaseHost:$DatabasePort/$DatabaseName
```

NOTE The database subsystem must reference a RDBMS subsystem.

Datacap

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Listener Application

Specify the name of the PCH listener for the Application.

Example 8. Listener Application

```
Datacap
```

Listener Instance

Specify the instance name for the Application here.

NOTE Wildcards like * or ? can be used

DatacapApplication

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration. ==== Db2

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Name

Specify the name of the database.

Database Username

Specify the name of the user for log in to the database. This user is used for monitoring the database and must have sufficient rights.

Database Password

Specify the password of the user for log in to the database.

Database Schema

Specify the schema that is used within the database.

Database Port

Specify the port which is used for the database connection. This parameter can be reused in the JDBC Connection Template of subsystem DB2 with $DatabasePort.

JDBC Connection Template

Specify the connection template (JDBC URL) for the database. The template consists of two parts. One for the database type and one for the database itself. $DatbaseHost, can be used to integrate the Hostname setting from an Db2Rdbms subsystem. $DatabasePort and $DatabaseName will be replaced with the settings of Database Name and Database Port of this configuration.

Example 9. JDBC Connection Template of DB2

```
jdbc:db2://$DatabaseHost:$DatabasePort/$DatabaseName
```

NOTE The db2 subsystem must get referenced in a DB2RDBMS subsystem.

Db2Rdbms

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Host

Specify the server name where the database is located on. This parameter can be reused in the JDBC Connection Template of subsystem DB2 with $DatabaseHost.

JDBC Driver Class

Specify the JDBC driver class for the database type. The field is predefined with the current value for DB2.

Example 10. JDBC Driver Class

```
com.ibm.db2.jcc.DB2Driver
```

NOTE The db2rdbms subsystem should reference a matching db2 subsystems.

Environment

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

NOTE This subsystem is used for logically structuring (grouping) the monitored environment in ESM.

- Always top level
- Cannot be nested with other environment subsystems
- Only has a name
- No probes available for this subsystem

FilePath

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Path

Specify the path where the files should be searched. Linux/Unix, Windows and UNC Format is possible:

- Linux/Unix: /tmp/test
- Windows: C:\temp\test
- UNC: \\RemoteHost\temp\test

Username

Optional: You can specify a user account to connect to a UNC path if required. The domain might be required e.g. Domain\User.

Password

Optional: If a user is required, please specify the password here.

Host

Normally each connected Agent gets automatically defined in a host subsystem. The settings are defined during the installation of the agent. It is possible to define additional hosts, e.g. for remote monitoring.

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Hostname

Enter the DNS name of the Host. Can be hostname only or full qualified with domain. Depends on how the host can be reached.

Icc4Sap

NOTE Configure one subsystem instance per ICC4SAP instance.

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

InstallationPath

Required. Enter the path where ICC4SAP is installed.

archint.ini Path

Required. Enter the path to the archint.ini of the ICC4SAP instance.

archint.ini Filename

Required. Enter the name of the ini file of the ICC4SAP instance. Default is archint.ini.

Service Suffix

Optional. Service suffix used to identify service and process names if several instances of ICC4SAP are installed.

Host

Required. Specify the hostname of the Collector Server.

Port

Required. Specify the port number of the Collector Server. You can find it as Webport in the corresponding archint.ini file of the ICC4SAP instance.

ImageImport

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Type

Specify the import Type, valid values are:

```
• HPII
• MRII
```

ImageServices

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Domain Name

Specify the name of the ImageServices domain.

Service Display Name

Windows only: Specify the display name of the IS control service. Default name is "IS ControlService".

FN_PATH Location

Specify the path where the software is installed, e.g. /fnsw for UNIX, <drive letter>:\fnsw for Windows.

FN_LOC_PATH Location

Specify the path to /local or \fnsw_loc e.g. /fnsw/local for UNIX, <drive letter>:\fnsw_loc for Windows.

Database Library Path

Optional: For local database servers. Enter the path to your RDBMS installation.

- Oracle: Path to the bin directory where the Oracle tools are installed:
  - Unix: /usr/oracle
  - Windows: <drive letter>:/orant
- MSSQL: Path to the binn directory where the MSSQL tools are installed. The location of this directory depends on the MSSQL Server version:
  - MSSQL Server 2000 or MSDE 2000: <drive letter>:/Program Files/ Microsoft Server/80/Tools
  - MSSQL Server 2005: <drive letter>:/Program Files/Microsoft Server/90/Tools
  - MSSQL Server 2008: <drive letter>:/Program Files/Microsoft Server/100/Tools

The installation script searches the binn directory for the tools sqlcmd.exe, osql.exe or isql.exe.

- DB2: Path to the bin directory where the DB2 tools are installed:
  - Unix: /home/<instancename>/sqllib
  - Windows: <drive letter>:/Program Files/IBM/SQLLIB

The installation script searches the bin directory for the tool db2sql92*

Admin User

This parameter is only needed for Unix / Linux based installations. If the ESM Agent is running with the same account as ImageServices specify __NONE__ here. Otherwise specify the user that is used to run ImageServices. In that case the ESM agent user must be able to su to the ImageServices user.

f_maint Password

Required: Specify the password of the f_maint user.

MKF Permanent DB

Specify the name incl. path of the file for the permanent DB here:

Example 11. Windows

```
D:\fnsw\dev\1\PERMANENT_DB0
```

MKF Security DB

Specify the name incl. path of the file for the security DB here:

Example 12. Windows

```
D:\fnsw\dev\1\SEC_DB0
```

MKF Transient DB

Specify the name incl. path of the file for the transient DB here:

Example 13. Windows

```
D:\fnsw\dev\1\TRANSIENT_DB0
```

Storage Libraries

Optional: Comma separated names of the Storage Libraries.

Centera Tools Path

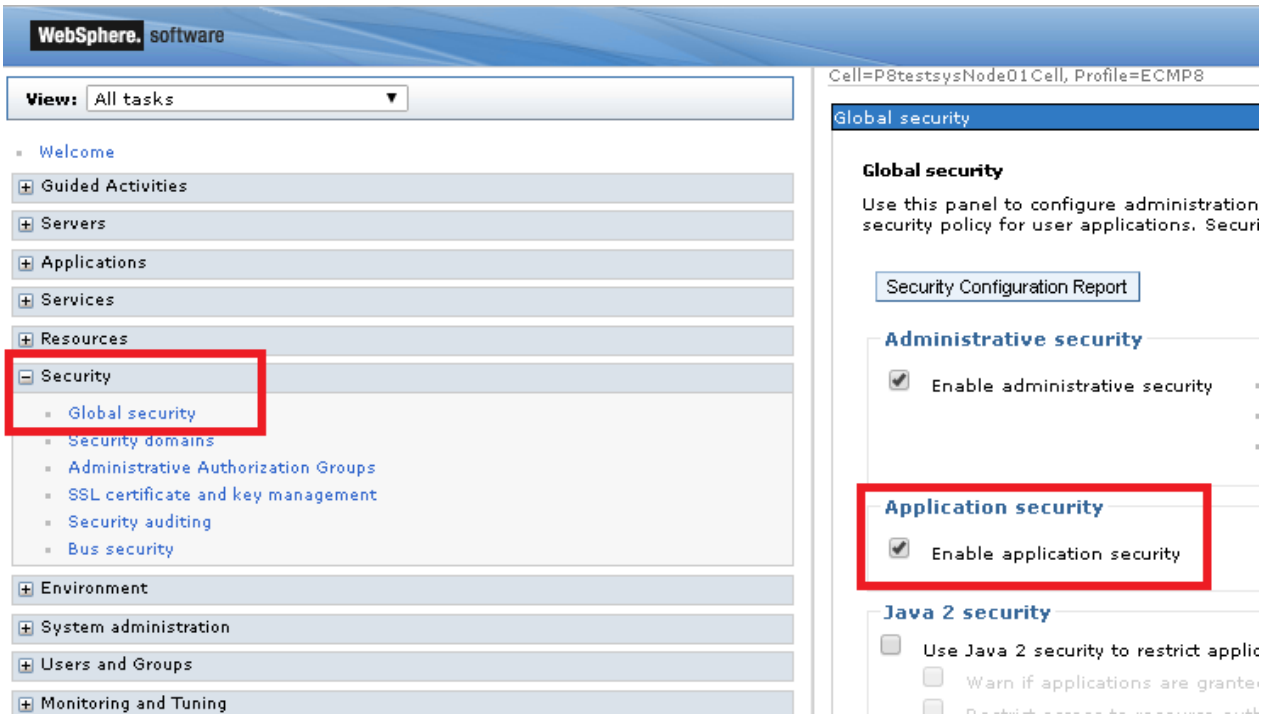
Path to the EMC Centera tools CenteraPing and c-ping.

JMX

Before the JMX subsystem can be used, you need to deploy the ESM MbeanWebApp to the JVM that should be monitored. This can be done on Web Application Server JVMs and standalone JVMs. Please contact your admin to do the deployment. The war file is located on the ESM server in the agent directory.

Deployment in WAS

IMPORTANT To get this working, application security under Security → Global security must be activated. This is because a certain privilege level in WAS is needed for getting specific mbean information.



Start a detailed installation of the war file. The following parts need adjustments:

- Application name: Optional if the application should get a different name than default.
- Cluster and Server: Define to which servers the application should be deployed.
- Virtual host: Specify a host that handles all WC_defaulthost ports needed for the servers where the application should be deployed. You might need to create such a virtual host first.
- Context root: Specify the context root that should be used for reaching out to the application. Typically /mbeanwebapp.
- User and Group mapping: Define a user that should be used to connect to the application. This is typically a service account that should have at least auditor and monitor privileges in WAS.

Finish the setup.

Deployment in Weblogic

Start an installation of the war file. During the setup process select the following:

- Install this deployment as an application
- General: Specify or change the name of the app / context root
- Security: DD only: Use only roles and policies that are defined in the deployment descriptor.
- Source Accessibility: Use the defaults defined by the deployment's targets.
- Plan source accessibility: Use the same accessibility as the application.
- Additional Configuration: Yes take me to the deployment's configuration screen.

→ Finish and save the settings.

- After deploying the app, create a user account "mbeanwebapp" which "currently" must be part of the administrator group.
- As next step, open the configuration of the deployed app. Switch to tab security and select application scope.
- Create a new "Stand-Alone Web Application Scoped Role".
- Name it mbeanwebapp and as Role Condition set: Group has the same Identify Domain as the Administrative Identify Domain: Administrator Or User: mbeanwebapp

You should now be able to access the URL of the app with the account mbeanwebapp at http://<servername>:<Port>/mbeanwebapp?html

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

NOTE

Add a Url subsystem for the parameters address, user and password. For secure connections, a keystore subsystem must be configured there as well.

The address must include the context root specified for the monitored JVM during the deployment of the ESM MbeanWebApplication, usually `/mbeanwebapp`. Make sure to not append a / at the end of the address.

Example 14. Address

```
http://YourWebAppServer:9080/mbeanwebapp
```

Keystore

A Keystore subsystem describes the location(s) of certificates and private key files that will be loaded into the general agent truststore and keystore at runtime. It can point to an existing keystore file, to a directory that contains private key and certificate files or both.

NOTE

Use a relative file or directory name in combination with the sync feature described in the Probes And Situations Guide to deploy a centrally managed truststore or keystore to the agents.

IMPORTANT

As mentioned above, all keystores specified are loaded in a general agent truststore. This happens during the startup of the agent or when the settings in a keystore subsystem is adjusted. If a new certificate is added to the keystore itself this does not happen and therefore the agent must be restarted in that case.

Name

Required. Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Filename

Optional. Specify the location and filename of an existing keystore file. The filename can be relative to the agent installation directory.

Type

Optional. Specify the type of the given keystore file. Possible values are jks and pkcs12.

Password

Optional. The password will be applied to the keystore file (if specified) and all contained private key entries. If an `Input Directory` is specified and contains password-protected private key files, the password will be used for these as well.

Input Directory

Optional. Specify a directory that contains certificates and / or private key file(s) with their corresponding certificate chain(s). The directory can be relative to the agent installation directory.
Certificate files must have one of the following extensions to be recognized: `.cer`, `.crt`, `.der`, `.pem`, `.p7b`
Supported file formats for certificate files are `DER` (binary), `PEM` (Base64-encoded DER) and `PKCS#7` (binary and Base64-encoded)
Private key files must have the extension `.key` to be recognized. The corresponding certificate chain must be located in a file with the same base name as the private key and with a valid certificate file extension (`.cer`, `.crt`, `.der`, `.pem`, `.p7b`) instead of `.key`.
The certificate chain file must contain all certificates in the correct order, starting with the end-entity (leaf) certificate, then the intermediate certificate(s) and finally the root certificate.
Supported file formats for private key files are `DER` (binary) PKCS#1 and PKCS#8, without password only, and `PEM` (Base64-encoded DER) PKCS#1 and PKCS#8, both with and without password

Example 15. Input directory with two private keys with their corresponding certificate chains and an additional certificate

```
/some/path/a_certificate.cer
/some/path/my_private.key
/some/path/my_private.crt
/some/path/some_other_private.key
/some/path/some_other_private.crt
```

LibraryServer

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Text Search Schema

Specify the schema name for the table TTEXTINDEXES. This information is only required for the NetSearchExtenderError probe.

Tls Version

Required. Select the TLS version to use for the connection.

TLS v1.2 and 1.3

The connection will negotiate the TLS version with the server.

TLS v1.2

Enforce TLS v1.2. Connections to a server that supports TLS v1.3 only will fail.

TLS v1.3

Enforce TLS v1.3. Connections to a server that supports TLS v1.2 only will fail.

LDAP

NOTE For secure connections add a keystore to this subsystem. The keystore must contain the root certificate of the LDAP server.

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Path to Configuration Files

Specify the path where the login.conf and krb5.conf is located.

Configuration Name

Specify the name of the configuration that should be used for the connection. The names can be found within the login.conf or krb5.conf file.

Example 16. Example for login.conf properties file for MSADS

```
YourModule
{
    com.sun.security.auth.module.Krb5LoginModule required;
    com.sun.security.auth.module.LdapLoginModule required

userProvider="ldap://<YourDomainServer.your.domain.in.lower.case>:389/OU=<ou>,D
C=<dc1>,DC=<dc2>,DC=<dc3>"
    authIdentity="{USERNAME}@<dc1>.<dc2>.<dc3>"

userFilter="(&(objectClass=user)(userPrincipalName={USERNAME}@<dc1>.<dc2>.<dc3>
))"
    useSSL=false;
};
```

NOTE If the "OU" in your userProvider setting contains a space e.g. "OU=My Users", replace the space with %20. The entry should be "OU=My%20Users" then. Otherwise the probe will return a java exception that says: `Cannot find User's LDAP entry.`

Example 17. Example for krb5.conf properties file for MSADS

```
[libdefaults]
       default_realm = <YOUR.DOMAIN.IN.UPPER.CASE>
       default_tkt_enctypes = rc4-hmac des-cbc-crc des3-cbc-sha1
       default_tgs_enctypes = rc4-hmac des-cbc-crc des3-cbc-sha1
       permitted_enctypes = rc4-hmac des-cbc-crc des3-cbc-sha1
```

```
[realms]
       <YOUR.DOMAIN.IN.UPPER.CASE> = {
          kdc = <YourDomainServer.your.domain.in.lower.case>
          default_domain = <your.domain.in.lower.case>
       }
```

```
[domain_realm]
       .<your.domain.in.lower.case> = <YOUR.DOMAIN.IN.UPPER.CASE>
       <your.domain.in.lower.case> = <YOUR.DOMAIN.IN.UPPER.CASE>
```

Listener

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Listener Host

Specify the server name where the listener is running on.

Listener Port

The default listener port is 32775. Specify the port here.

Interval in Seconds

The default interval is 900 seconds (15 minutes). The interval controls how often the monitored application will send data.

NOTE Setting this interval also affects the interval for the IBM System Dashboard because its value is handled by the monitored application and not by ESM itself.

It is not guaranteed that changing this setting will have an effect as the monitored application may or may not respect the interval.

Logfile

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Logfile Name

Specify the name of the logfile including the absolute path. The entry will always be interpreted as a regular expression (regexp), e.g. a `\` must always be masked by a leading `\`:

Example 18. Example Logfile Name with regex

```
C:\\Agent\\data\\log\\.*sm_[\w]+\.log
```

NOTE It is not recommended to use a broad matching regular expression as this will lead to performance issues.

Mssql

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Name

Specify the name of the database.

Database Username

Specify the name of the user for log in to the database. This user is used for monitoring the database and must have sufficient rights.

Database Password

Specify the password of the user for log in to the database.

Database Schema

Specify the schema that is used within the database.

Database Port

Specify the port which is used for the database connection. This parameter can be reused in the JDBC Connection Template of subsystem Mssql with $DatabasePort.

JDBC Connection Template

Specify the connection template (JDBC URL) for the database. The template consists of two parts. One for the database type and one for the database itself. $DatbaseHost, can be used to integrate the Hostname setting from a MssqlRdbms subsystem. $DatabasePort and $DatabaseName will be replaced with the settings of Database Name and Database Port of this configuration.

Example 19. JDBC Connection Template of MSSQL

```
jdbc:sqlserver://$DatabaseHost:$DatabasePort;databaseName=$DatabaseName
```

NOTE The Mssql subsystem must get referenced in a MssqlRdbms subsystem.

MssqlRdbms

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Host

Specify the server name where the database is located on. This parameter can be reused in the JDBC Connection Template of subsystem Mssql with $DatabaseHost.

JDBC Driver Class

Specify the JDBC driver class for the database type. The field is predefined with the current value for MSSQL.

Example 20. JDBC Driver Class

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

NOTE The MssqlRdbms subsystem should reference a matching Mssql subsystem.

ObjectStore

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Symbolic Name

Specify the symbolic name of the Object Store as configured in ACCE.

CSS Directory

Optional. Enter the main installation directory of the Content Search Services software, if applicable.

NOTE This is not the subdirectory of the CSS server configuration.

TIP Specify the directory that contains the css-servers.xml file.

CSS Server Name

Optional. Enter the real CSS server name. Verify the server name, check the file css-servers.xml.

OnDemand

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Archive Name

Enter the name of the CMOD archive.

Installation Path

Enter the path where the CMOD product is installed at the server.

NOTE This field is only required for CMOD probes that are not API-based and for CMOD tasks.

ODWEK User

This account is used by the probes to logon to OnDemand through ODWEK API.

ODWEK Password

Password of the ODWEK User account.

Database Library Path

UNIX only. Enter the path to the shared libraries for your RDBMS installation. The correct value

depends upon the selected database type. Depending on the OS version (32Bit or 64Bit) you may need to specify the 64 Bit or 32 Bit version of the database libraries here.

NOTE This field is only required for CMOD tasks.

FTS Path

Enter the path to the installation of Full Text Search.

Example 21. FTS Path

```
C:/Program Files/IBM/OnDemand FTS Server/V9.0.
```

Server Name

Enter the server name to use for connections to the OnDemand Web Enablement Kit.

ODWEK Port

Enter the port for the OnDemand Web Enablement Kit, usually 1445.

Ssl Keyring

Optional, only needed if the connection via ODWEK API is established with SSL. The SSL Keyring file can be specified fully qualified for the location on the OnDemand System if the agent is running on the monitored system. Otherwise it must be copied to the ondemand directory of the ESM agent that monitors the OnDemand System remotely. In this case see the "Probes and Situation Guide" chapter "Background information for agents before setting up probes" for more details.

Ssl Keyring Stash

Optional, only needed if the connection via ODWEK API is established with SSL. The SSL Keyting Stash file can be specified fully qualified for the location on the OnDemand System if the agent is running on the monitored system. Otherwise it must be copied to the ondemand directory of the ESM agent that monitors the OnDemand System remotely. In this case see the "Probes and Situation Guide" chapter "Background information for agents before setting up probes" for more details.

OperationalDecisionManager

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Installation Path

Enter the path where the ODM product is installed at the server.

Oracle

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Name

Specify the name of the database.

Database Username

Specify the name of the user for log in to the database. This user is used for monitoring the database and must have sufficient rights.

Database Password

Specify the password of the user for log in to the database.

Database Schema

Specify the schema that is used within the database.

Database Port

Specify the port which is used for the database connection. This parameter can be reused in the JDBC Connection Template of subsystem Oracle with $DatabasePort.

JDBC Connection Template

Specify the connection template (JDBC URL) for the database. The template consists of two parts. One for the database type and one for the database itself. $DatbaseHost, can be used to integrate the Hostname setting from an OracleRdbms subsystem. $DatabasePort and $DatabaseName will be replaced with the settings of Database Name and Database Port of this configuration.

Example 22. JDBC Connection Template of Oracle

```
jdbc:oracle:thin:@//$DatabaseHost:$DatabasePort/$DatabaseName
```

NOTE The Oracle subsystem must get referenced in an OracleRdbms subsystem.

OracleRdbms

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Host

Specify the server name where the database is located on. This parameter can be reused in the JDBC Connection Template of subsystem Oracle with $DatabaseHost.

JDBC Driver Class

Specify the JDBC driver class for the database type. The field is predefined with the current value for Oracle.

Example 23. JDBC Driver Class

```
oracle.jdbc.OracleDriver
```

NOTE The OracleRdbms subsystem should reference a matching Oracle subsystem.

PostgreSql

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Name

Specify the name of the database.

Database Username

Specify the name of the user for log in to the database. This user is used for monitoring the database and must have sufficient rights.

Database Password

Specify the password of the user for log in to the database.

Database Schema

Specify the schema that is used within the database.

Database Port

Specify the port which is used for the database connection. This parameter can be reused in the JDBC Connection Template of subsystem PostgreSql with $DatabasePort.

JDBC Connection Template

Specify the connection template (JDBC URL) for the database. The template consists of two parts. One for the database type and one for the database itself. $DatbaseHost, can be used to integrate the Hostname setting from a MssqlRdbms subsystem. $DatabasePort and $DatabaseName will be replaced with the settings of Database Name and Database Port of this configuration.

Example 24. JDBC Connection Template of PSQL

```
jdbc:postgresql://$DatabaseHost:$DatabasePort/$DatabaseName
```

NOTE The Psql subsystem must get referenced in a PsqlRdbms subsystem.

PostgreSqlRdbms

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Host

Specify the server name where the database is located on. This parameter can be reused in the JDBC Connection Template of subsystem PostgreSql with $DatabaseHost.

JDBC Driver Class

Specify the JDBC driver class for the database type. The field is predefined with the current value for PostgreSql.

Example 25. JDBC Driver Class

```
org.postgresql.Driver
```

NOTE The PsqlRdbms subsystem should reference a matching Psql subsystem.

Rdbms

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Database Host

Specify the server name where the database is located on. This parameter can be reused in the JDBC Connection Template of subsystem Database with $DatabaseHost.

JDBC Driver Class

Specify the JDBC driver class for the database type.

Example 26. JDBC Driver Class of Postgresql

```
org.postgresql.Driver
```

NOTE The Rdbms subsystem should reference a matching Database subsystem.

Resource Manager

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Rmi

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

RMI Host

Specify a server where an II CE RMI Proxy Connector Server product (aka connectors only installation) was installed at.

RMI Port

Enter the RMI port the RMI bridge uses. The default is 1251. Normally this is incremented by one for each separate RMI bridge running at a single server.

RuleExecutionServer

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

NOTE Add a Url subsystem for the parameters address, user and password. For secure connections, a keystore subsystem must be configured there as well.
Typically, the address end with `/res`:

Example 27. Address

```
http://serverName:9080/res
```

The user must have access rights to the REST-API

NOTE A RuleExecutionServer Subsystem must be connected to a referencing Subsystem of Type OperationalDecisionManager.

ServiceManager

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

NOTE Add a Url subsystem for the parameters address, user and password. For secure connections, a keystore subsystem must be configured there as well.

SmtpServer

Server Name

Specify the name that should be used for storing the setup.

Host

Specify the hostname which can be used for the connection to the SMTP Server.

Port

Specify the port of the SMTP server here. Most the time this is 25 for SMTP servers.

From Address

Specify the email address of the sender here.

Authentication

Check if authentication is required.

Username

If a certain user for the SMTP connection must be used, specify the user name here.

Password (Optional)

Only need if a certain user must be used, specify the password for the user here.

Confirm Password (Optional)

Only need if a certain user must be used, specify the password for the user here. The given password is compared with the "Password" parameter.

The following additional options (expert mode) are available:

Connection Timeout

Connection timeout in milliseconds. Default: infinite.

Timeout

Description: Socket read timeout value in milliseconds. This timeout is implemented by java.net.Socket. Default: infinite.

Write Timeout

Description: Socket write timeout value in milliseconds. This timeout is implemented by using a java.util.concurrent.ScheduledExecutorService per connection that schedules a thread to close the socket if the timeout expires. Thus, the overhead of using this timeout is one thread per connection. Default: infinite.

Local Host

Email address to use for SMTP MAIL command. This sets the envelope return address. NOTE: mail.smtp.user was previously used for this. Default: Defaults to msg.getFrom() or InternetAddress.getLocalAddress().

Local Address

Local address (host name) to bind to when creating the SMTP socket. Should not normally need to be set, but useful with multi-homed hosts where it's important to pick a particular local address to bind to. Default: The address picked by the Socket class.

Local Port

Local port number to bind to when creating the SMTP socket. Default: The port number picked by the Socket class.

Sign on with EHLO

If false, do not attempt to sign on with the EHLO command. Normally failure of the EHLO command will fall back to the HELO command; this property exists only for servers that don't fail EHLO properly or don't implement EHLO properly. Default: true.

Auth Mechanisms

If set, lists the authentication mechanisms to consider, and the order in which to consider them. Only mechanisms supported by the server and supported by the current implementation will be used. The default is "LOGIN PLAIN DIGEST-MD5 NTLM", which includes all the authentication mechanisms supported by the current implementation except XOAUTH2. Default: LOGIN PLAIN DIGEST-MD5 NTLM.

Auth Login Disable

If true, prevents the use of AUTH LOGIN command. Default: false.

Auth Plain Disable

If true, prevents the use of AUTH PLAIN command. Default: false.

Auth Digest MD5 Disable

If true, prevents the use of AUTH DIGEST-MD5 command. Default: false.

Auth NTLM Disable

If true, prevents the use of AUTH NTLM command. Default: false.

Auth HTML Domain

The NTLM authentication domain. Default: empty.

Auth NTLM Flags

NTLM protocol-specific flags. Search the internet for details. Default: empty.

Auth XOAUTH2 Disable

If true, prevents use of the AUTHENTICATE XOAUTH2 command. Because the OAuth 2.0 protocol requires a special access token instead of a password, this mechanism is disabled by default. Enable it by explicitly setting this property to "false" or by setting the "mail.smtp.auth.mechanisms" property to "XOAUTH2". Default: false.

Submitter

The submitter to use in the AUTH tag in the MAIL FROM command. Typically used by a mail relay to pass along information about the original submitter of the message. See also the setSubmitter method of SMTPMessage. Mail clients typically do not use this. Default: Not set.

DSN Notify

The NOTIFY option to the RCPT command. Either NEVER, or some combination of SUCCESS, FAILURE, and DELAY (separated by commas). Default: Not set.

Allow 8bit MIME

If set to true, and the server supports the 8BITMIME extension, text parts of messages that use the "quoted-printable" or "base64" encodings are converted to use "8bit" encoding if they follow the RFC2045 rules for 8bit text. Default: Not set, so maybe false.

Send Partial

If set to true, and a message has some valid and some invalid addresses, send the message anyway, reporting the partial failure with a SendFailedException. If set to false (the default), the message is not sent to any of the recipients if there is an invalid recipient address. Default: false.

Quit Wait

If set to false, the QUIT command is sent and the connection is immediately closed. If set to true (the default), causes the transport to wait for the response to the QUIT command. Default: true.

SSL Check Server Identity

If set to true, check the server identity as specified by RFC 2595. These additional checks based on the content of the server’s certificate are intended to prevent man-in-the-middle attacks. Default: false.

Enable SSL

Enables SSL regardless of the port used or the protocols specified in SSL Protocols. To enable it, enter "true" here. Default: false.

SSL Protocols

Specifies the SSL protocols that will be enabled for SSL connections. The property value is a whitespace separated list of tokens acceptable to the javax.net.ssl.SSLSocket.setEnabledProtocols method. Defaults: not set.

SSL Cipher Suites

Specifies the SSL cipher suites that will be enabled for SSL connections. The property value is a whitespace separated list of tokens acceptable to the javax.net.ssl.SSLSocket.setEnabledCipherSuites method. Default: not set.

SASL Enable

If set to true, attempt to use the javax.security.sasl package to choose an authentication mechanism for login. Default: false.

SASL Mechanisms

A space or comma separated list of SASL mechanism names to try to use. Default: Not set.

SASL Authorization Id

The authorization ID to use in the SASL authentication. Default: If not set, the authentication ID (user name) is used.

SASL Realm

The realm to use with DIGEST-MD5 authentication. Default: Not set.

SASL Use Canonical Hostname: If set to true, the canonical host name returned by InetAddress.getCanonicalHostName is passed to the SASL mechanism, instead of the host name used to

connect. Default: false.

User Set

If set to true, use the RSET command instead of the NOOP command in the isConnected method. In some cases sendmail will respond slowly after many NOOP commands; use of RSET avoids this sendmail issue. Default: false.

NOOP Strict

If set to true (the default), insist on a 250 response code from the NOOP command to indicate success. The NOOP command is used by the isConnected method to determine if the connection is still alive. Some older servers return the wrong response code on success, some servers don't implement the NOOP command at all and so always return a failure code. Set this property to false to handle servers that are broken in this way. Normally, when a server times out a connection, it will send a 421 response code, which the client will see as the response to the next command it issues. Some servers send the wrong failure response code when timing out a connection. Do not set this property to false when dealing with servers that are broken in this way. Default: true.

SnmpTarget

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Protocol

Choose between udp and tcp from dropdown. The default is udp.

Host

Specify the SNMP Manager host here. IP address or hostname can be used

Port

Default 162. Specify the listening port of the SNMP manager host here.

Version

Select the SNMP Version from the drop down. Possible values are Version2c and Version3

Community Password

Please ask your SNMP Administrator if a community password is needed. Enter it here in case.

Security Name

Please ask your SNMP Administrator for the Security Name. Enter it here in case.

Security level (only needed for SNMP Version 3)

Ask your SNMP Administrator for the correct setting.

SpectrumProtect

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Alias

Required for UNIX / Linux. Alias as defined in dsm.sys. If no alias is specified, dsmadmc uses the

first server defined in the dsm.sys configuration file. If multiple server nodes are configured for the dsmadmc, the specific alias name has to be set to ensure that the monitor uses the correct server node.

Host

Required for Windows. Specify the server for dsmadmc.

Port

Required for Windows. Specify the port for dsmadmc.

User

Required. Specify the user to use for the connection.
The user specified here must be a user of class analyst. This class can be added for a user with the following command:

```
dsmadmc grant authority <USERNAME> classes=analyst
```

Password

Required. Specify the password to use for the connection.

Installation Path

Required. Specify the path to the dsmadmc binary.

Options

Optional. Specify any required additional options for the dsmadmc tool.

Url

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Address

Specify the address that should be monitored. The address must match the format `<protocol>://<host>:<port>/<path>`. Port and path are optional.
Default ports:

Protocol	Port
http	80
https	443
ldap	389
ldaps	636

NOTE

The Url subsystem can also be used for logstash implementation. In this case the address must be specific.
E.g.: If address: "/logstash" → Logstash can HTTP-POST requests to <agentHostname>:<agentJettyPort>/logstash on the ESM agent.

User

Optional. Specify the name of the user to use to login to the URL if required.

Password

Optional. Specify the password of the user to use to login to the URL if required.

Tls Version

Required. Select the TLS version to use for the connection.

TLS v1.2 and 1.3

The connection will negotiate the TLS version with the server.

TLS v1.2

Enforce TLS v1.2. Connections to a server that supports TLS v1.3 only will fail.

TLS v1.3

Enforce TLS v1.3. Connections to a server that supports TLS v1.2 only will fail.

WindowsEventlog

Create a subsystem for each event log that shall be monitored, e.g. `System` or `Application`. These subsystems only need to be created once, they can then be reused for each agent where eventlog monitoring is deployed.

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Eventlog Name

Specify the eventlog that shall be configured in this subsystem. Default Windows Eventlogs are Application, System, Security, but any other can be used as well. Only one log per subsystem is possible.

WMI

Name

Specify a name. The name should be descriptive and unique to identify the subsystem when using it for further configuration.

Using the Subsystem Configuration Wizard

Once you start configuring any subsystem, the wizard is automatically used. Depending on the choice of your subsystem, the wizard automatically detects which other subsystems are relevant and offers configuration possibilities when the wizard features are used.

Explanation of the items within the Wizard (Entry Page)

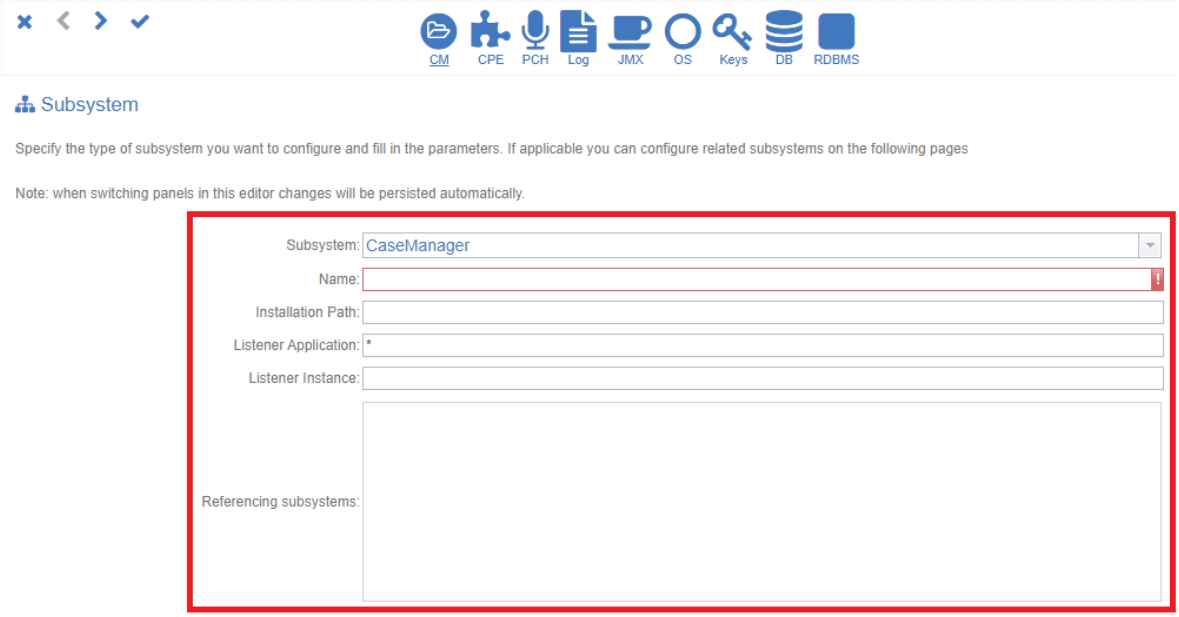


Image of Items for Subsystem Configuration

Use the parameters to configure the subsystem settings. Once finished proceed with the next subsystem.

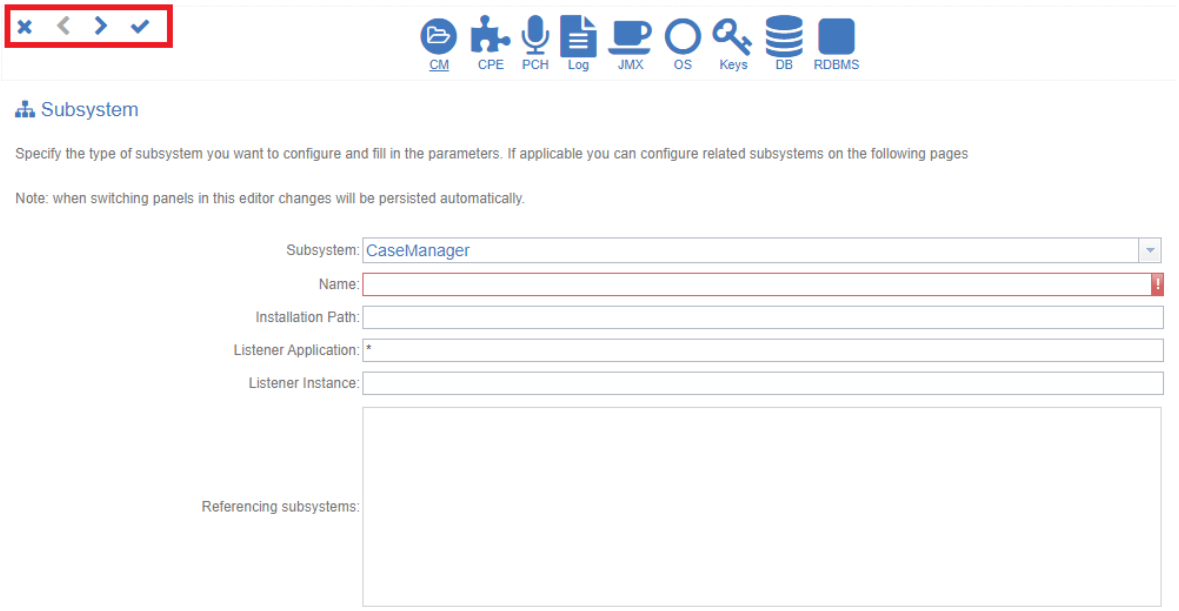


Image of Items in upper left corner

Use these items to browse through the wizard (next/previous subsystem configuration) or save or close the wizard setup.

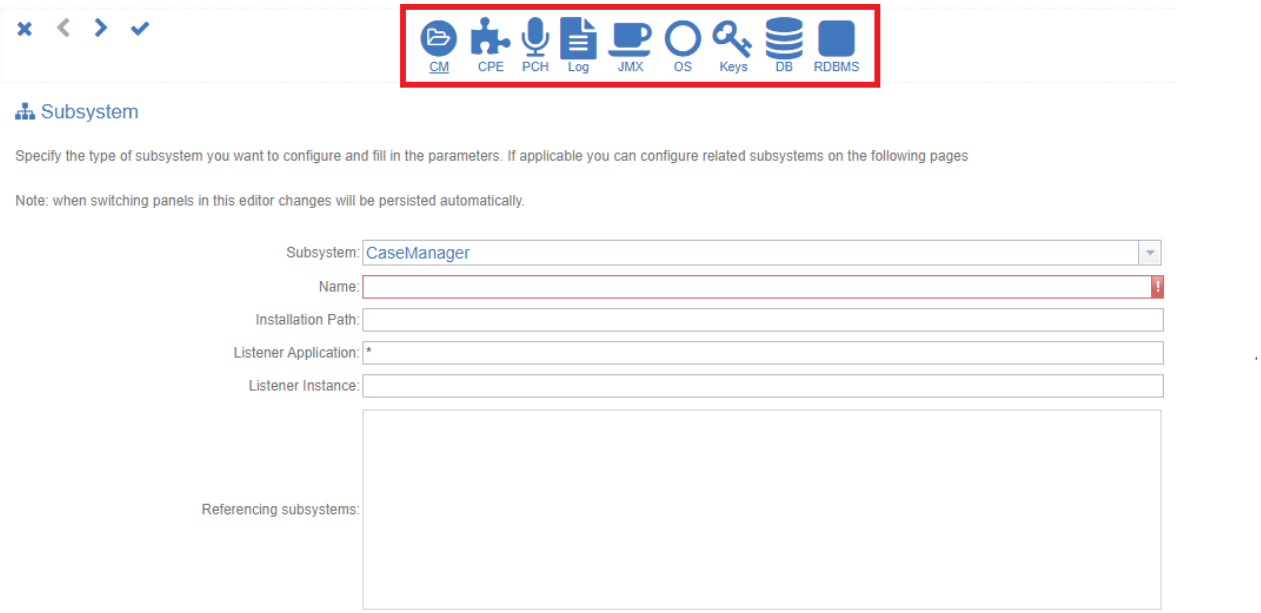


Image of Items in upper middle

These icons show the relevant subsystems for the subsystem that you have selected to configure in the beginning. They can be used to directly switch to the configuration. Mouse over function shows the type as tool tip. The icon for which the current page setup is active is highlighted.

Explanation of the items within the Wizard (Follow Up Page)

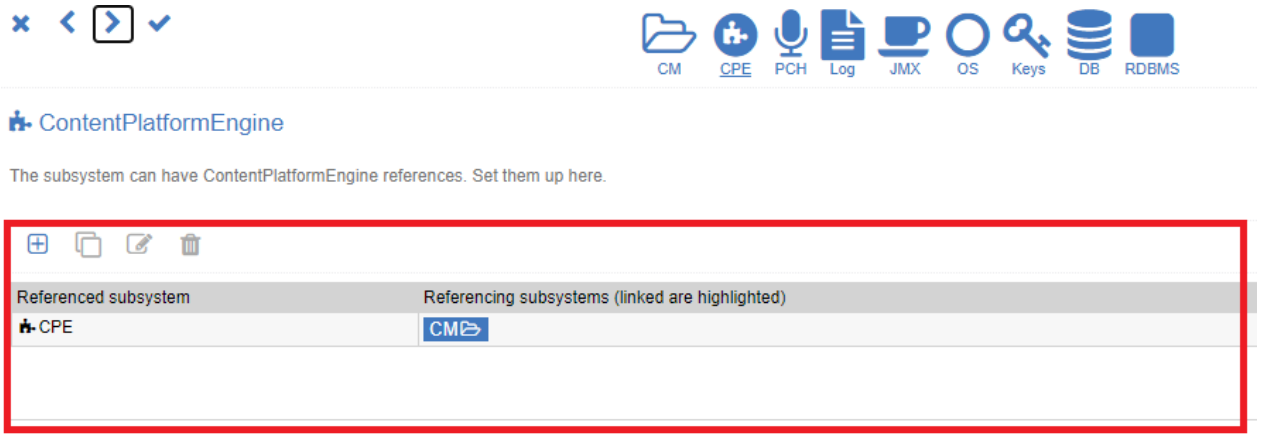


Image of Items to add or select existing subsystem

Any of the follow up pages looks the same. Within the page you can either connect an already existing subsystem or add a new one using the function buttons. You can also copy, edit or delete a subsystem with these buttons.

NOTE Deleting a subsystem only works if it is not referenced in any other subsystem and no probes is using the subsystem settings.

For connecting a subsystem to a parent subsystem, click on the parent in the line of the table where to subsystem is located. The parent should be highlighted afterwards which shows the connection.

If you add a new one, the configuration parameters for the subsystem will open below the currently visible information. Once the setup is saved, the newly created subsystem will become available in the table.

Defining sample filters within the Sample Filter feature

The sample filtering is a mechanism to filter sample depending on certain criteria. If samples match the criteria, they will directly be filtered on the agent.

Per default the editor does not contain any entry.

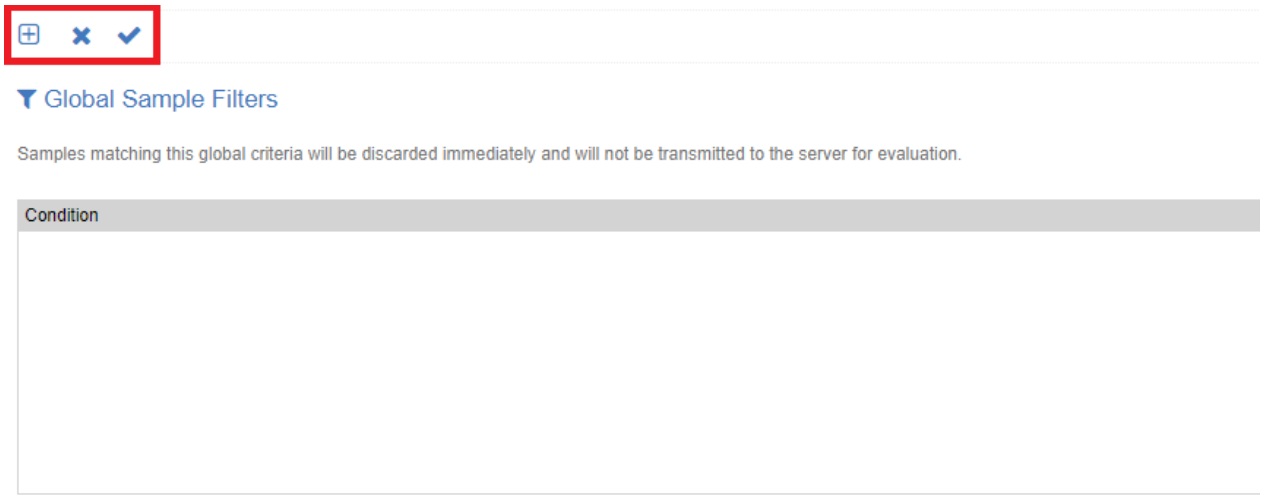


Image of Global Sample Filter Editor

With the tool box buttons entries can be added, changes can be discarded or saved.

The condition entries are equal to the evaluation in the situation. They consist of a sample field, a comparator and the matching part.

You can choose between the following sample fields:

- classification
- error
- message

- probeCfgId
- timestamp
- value

The following comparators are available:

- "! =" = not equals
- "= =" = equals
- "<" = smaller than
- ">" = greater than
- "< =" = equal or smaller than
- "> =" = equal or greater than
- "contains" = containing the followed expression
- "matches" = matching the followed expression

For the matching part enter the needed information manually.

Creation of Reports

This chapter describes the creation of Reports. From the main window select "Configuration" and choose the "Report" icon from the sidebar. In the upper part of the sidebar actions, such as "Create a new Report Configuration" or "Remove the selected Report Configuration" can be triggered.
Each Report configuration can be run ad hoc or scheduled. Created Reports will be shown in the sidebar

Image of Configuration Reporting

Hit the icon for creating a new report. The report editor opens. At the top you have 3 icons for adhoc run, close or save of the report.

Image of Configuration Reporting Action Icons

The editor is divided in 3 sections.

Report Configuration

Report Name

Specify a Reportname. The name should be descriptive and unique to identify the report.

Type

Select the type that should be used for the graph from the drop down. Available types are.

- Incident Count
- Pie Chart

Both Types show a pie chart output. Pie Chart shows the percentage values of the different severity appearances over the specified period. Incident count shows the amount of incidents per severity over the specified period.

NOTE The Incident Count and the Pie Chart reports are using incidents for the creation of report.

- Line Chart
  - Values
  - Values,Min
  - Values,Min,Max
  - Values,Min,Max,Med
  - Values,Min,Trend
  - Values,Min,Max,Trend
  - Values,Min,Max,Med,Trend
  - Values,Trend
  - Min,Max,Med,Trend

Value = Value as given in the Incident Min, Max, Med = Minimum, maximum and median aggregation Trend = Logarithmic, exponential and linear regression trend analysis

Each of the line chart types creates one chart per option. For option Trend 3 charts are created.

- Aggregation

NOTE The line chart reports and the aggregation report are using samples for the creation of report.

This report type can be used to create an aggregation for the given Situation and is very useful in combination with the "raw" listener data situations. It creates a bar chart. This type uses the parameters Aggregation Type and Aggregation Period.

The aggregation period defines the bar, e.g. if hour is used one bar per full hour is created.

The period in the schedule defines how many bars are shown, e.g. if 12 hours is specified there, you will get a report that shows 12 bars.

Reports from this type can be added in the monitoring dashboard as portlet. The portlet is updated in the interval that is given in schedule interval of the report.

Situations

Select the situation(s) that should be used for the graph. Multiselect with CTRL or SHIFT is possible.

Smoothing

Select an option for smoothing of the drop down. Available option are:

- None
- Smooth
- Loess

Aggregation Type

Select the aggregation type from the drop down. Currently, delta is possible here. This parameter can only be used in combination with the report type "Aggregation"

Aggregation Period

Select the aggregation period from the drop down. You can choose between "Auto", "Hours(s)", "Day(s)" and "Week(s)". This defines the period for which the aggregation is created. It is always the full hour, day and week. Auto will automatically define the period, it depends on the period that is given for the schedule of the report.

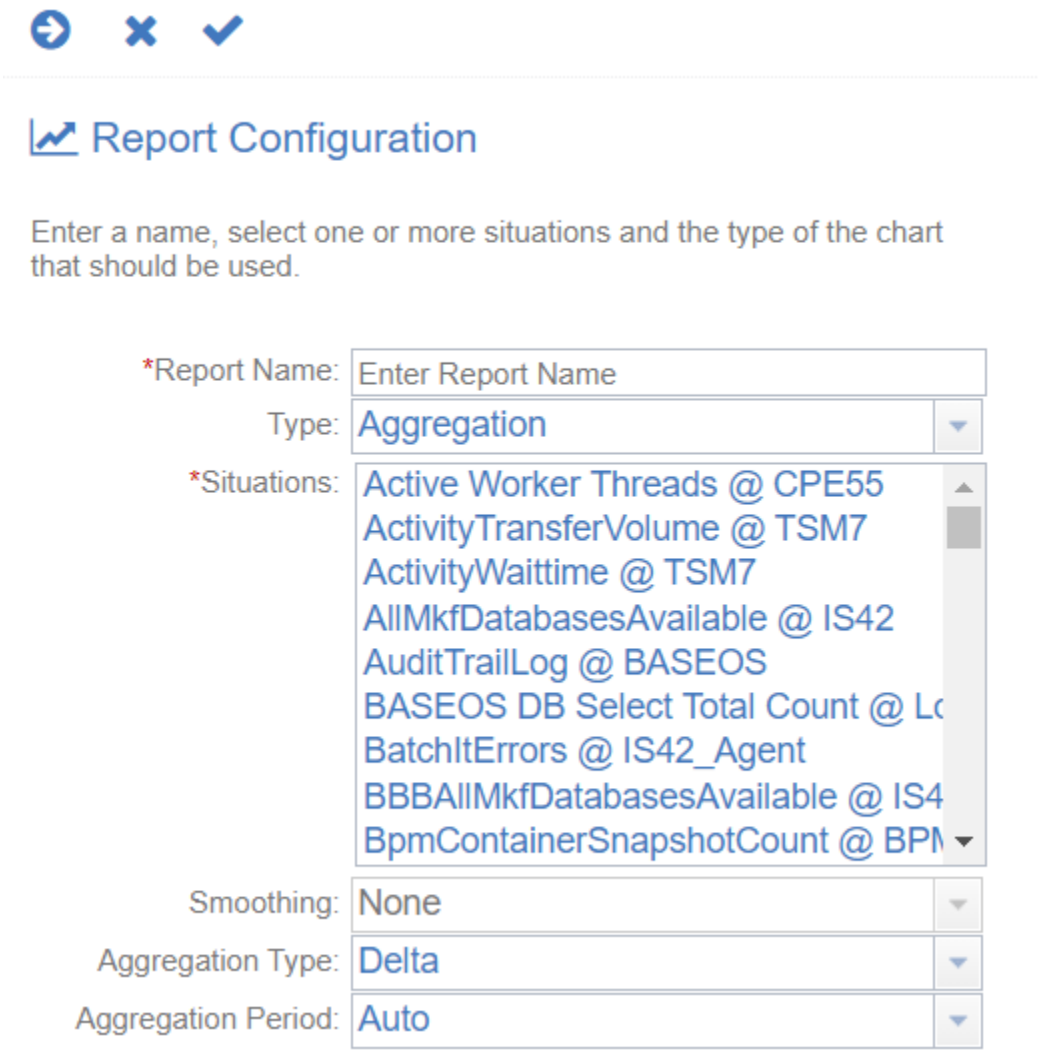


Image of Configuration Reporting Configuration

Ad Hoc Run

In the Ad Hoc Run you can define a start and end date. This defines the timeframe for the reported graph and is only used for the adhoc execution.

Image of Configuration Reporting Ad Hoc Run

NOTE ESM server time is used but browser displays local time.

Schedule

If you want to schedule the report for being created automatically, you need to use this section.

Active

Check if the report should be created automatically. If you want to store the configuration but only execute adhoc reports, uncheck this section.

Start Date

Select the date and time from the drop down. This is the date when the scheduling begins.

NOTE ESM server time is used but browser displays local time.

E-mail Recipients

If you have defined an SMTP setup and you enter a recipient here, the created report will automatically be sent to the recipient.

SMTP Server

Select a listed SMTP server from the drop down. This will be used for sending the mail.

Period

The period defines the timeframe for the reported graph. Once the scheduler starts it's going back the interval and reports over this period. Possible selections are.

- Hours(s)
- Day(s)
- Week(s)
- Month(s)
- Year(s)

Interval

Defines the timeframe for the next run of the report. Possible selections are.

- Second(s)
- Minute(s)
- Hours(s)
- Day(s)
- Week(s)
- Month(s)
- Year(s)

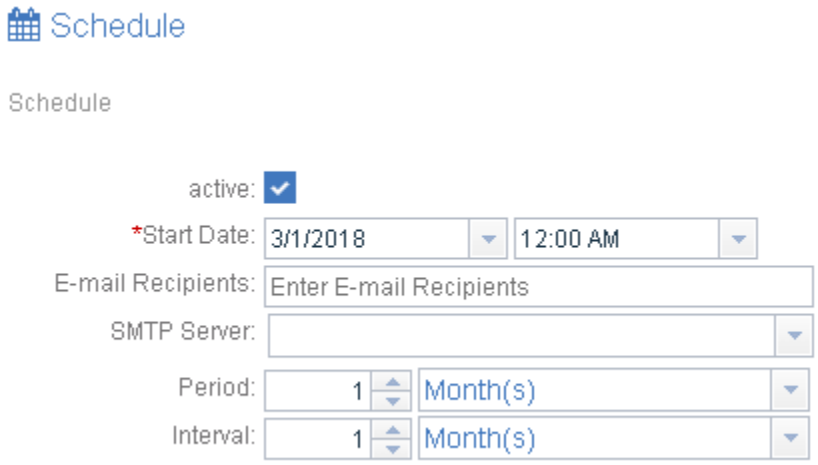


Image of Configuration Reporting Schedule

After you have successfully created a report configuration. The automatically created reports will be shown in the base section of the sidebar once you have selected a report configuration. Double-click on an entry to open the report.

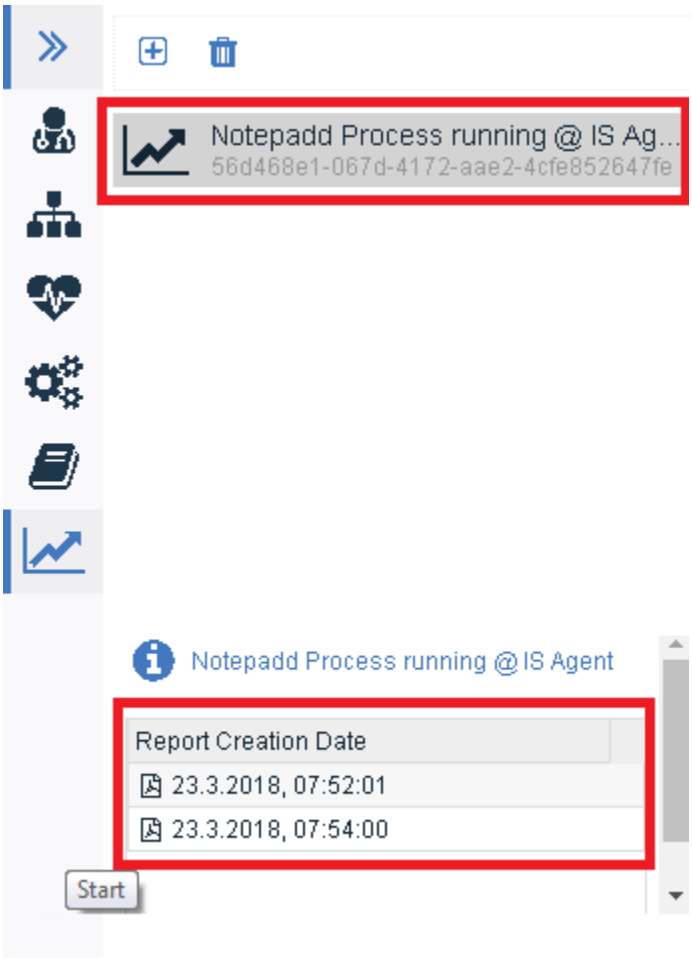


Image of Configuration Reporting Available Reports

Integration with 3rd Party Products

Grafana

ESM offers an out-of-the-box integration with Grafana. A rest api provides the data that is required for Grafana. The URL is as follows:

Example 28. Example URL for Grafana Rest API

```
https://YourESMServer//rest/grafana
```

A how-to for the integration can be found in the field guides via the following URL:

https://www.cenit.com/en_EN/products-solutions/eim/processing-file-and-document-management/software/ibm-ecm-system-monitor/ibm-esm-field-guides.html

Integration via tasks for other 3rd party products

ESM also offers integration via tasks to other 3rd party products.

- Instana
- ServiceNow

Field guides for the integrations are available via the above given URL.

- IBM Cloud Pak for Watson AIOps Please read the chapter in the WebhookExportIncident task that is available in the task guide.

Editor for Maintenance rules

You can find this editor in the Operating Console only. This editor opens when using the Edit button for an existing rule or clicking on the + button in the maintenance sidebar.

A maintenance rule is defined by tag(s) and if a schedule should be used.

The first part defines the tags that are used. Click on the "Add tag …" section and add the tags for which the maintenance should become active. You can select from any tag that is available in the system. All situation that have at least one of the tags that are specified in the config will be set in maintenance mode.

The second part, defines whether you want to use a schedule (define a specific date or repetitive occurrences) or not - de/select the check next to schedule to distinguish. When setting a schedule, you can choose between various schedule types:

On-time event (without any repetition)

Define the start date and time and how long the maintenance should last

Repetitive settings for daily, weekly, monthly, monthly (by week), yearly and yearly (by week)

Daily

Define start time and how long the maintenance should last. The maintenance will be repeated every day.

Weekyly

Define the day of the week, start time and how long the maintenance should last. The maintenance will be repeated every week.

Monthly

Define the day of the month, start time and how long the maintenance should last. The maintenance will be repeated every week.

Monthly (by week)

Define the the week, day of the week, start time and how long the maintenance should last. The maintenance will be repeated every month.

Yearly

Define the month, day of the month, start time and how long the maintenance should last. The maintenance will be repeated every year.

Yearly (by week)

Define the the week, day of the week, month, start time and how long the maintenance should last. The maintenance will be repeated every year.

Advanced

In the advanced option you can set the schedule as a cron information. Also define how long the maintenance should last in here.

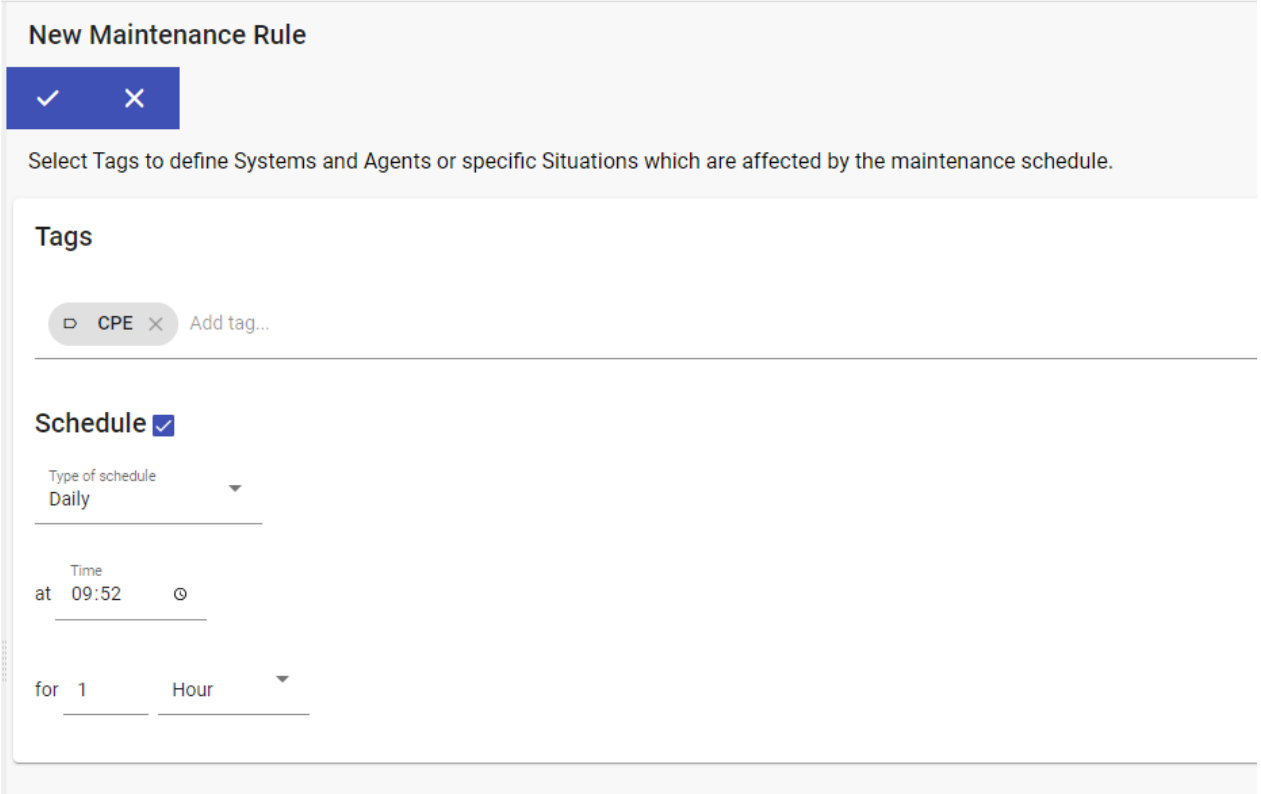


Image of Operational Console Maintenance Editor

After the rule setup is completed you can save it by clicking on the check button above the setup. The name for the rule is set automatically and follows the following template: Tag1[, Tag2, Tag3 …] (readable explanation of the schedule).

The rule specific details view will open automatically after saving in which you can change the state for the rule.

State and meaning of rules

By default (after first setup) a rule is deactivated, meaning the maintenance rule is just stored at the moment and will not be executed.

Once clicking on the slider, it will change it's description to either active or enabled. This depends whether a schedule was defined or not and if the schedule fits the current time. All rules without schedule will be directly active (running) when clicking on the slider. Rules with schedule will usually become enabled and switch to active once the start time is reached.

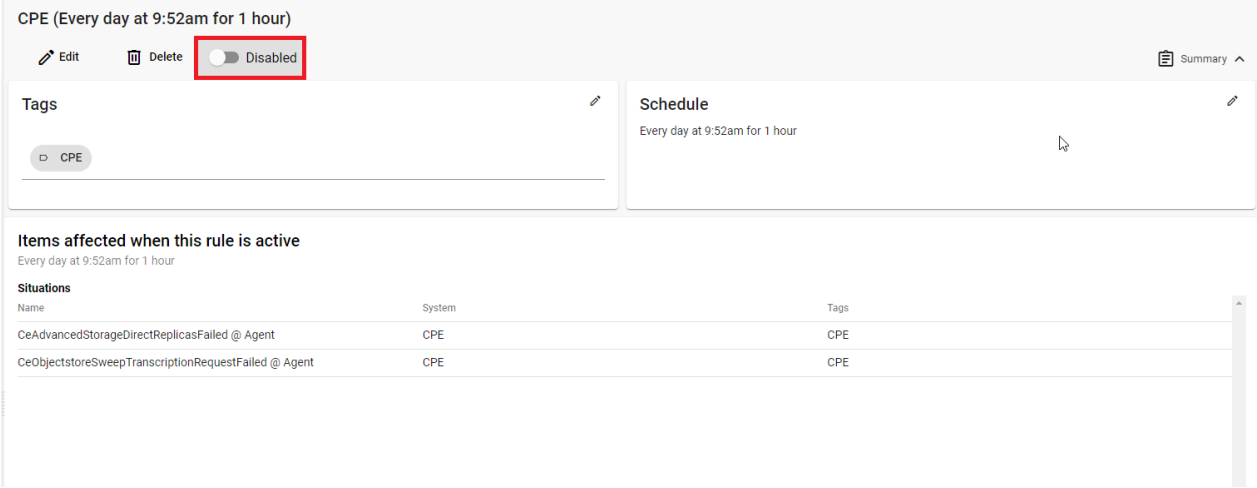


Image of Operational Console Maintenance Rule State

Appendix A: Copyright notice

IBM Enterprise Content Management System Monitor

Appendix B: Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Appendix C: Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others

Product Number: 5724-R91

Printed in USA

SC27-9240-07