**DIGITALISERINGSSTYRELSEN – eDelivery**

**User Manual for new Access POints**

.

.

.

.

.

.

.

.

.

.

.

.

.

.

.

.

|  |  |
| --- | --- |
| **Version:** | 1.0 |
| **Status:** | Final |
| **Author:** | Netcompany |



**Dokumenthistorik**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Status | Comments |
| 1 | 20-12-2019 | Netcompany | Final | Output from eDelivery pilot project |

**References**

|  |  |  |  |
| --- | --- | --- | --- |
| References | Title | Author | Version |
|  |  |  |  |

Contents

[1 Glossary: 3](#_Toc27729794)

[2 Introduction 4](#_Toc27729795)

[2.1 The eDelivery system 5](#_Toc27729796)

[3 Updating ServiceGroup metadata in the SMP 6](#_Toc27729797)

[3.1 No SMP access solution. 6](#_Toc27729798)

[3.2 Service group admin access 6](#_Toc27729799)

[3.2.1 Creating a new service metadata entry 7](#_Toc27729800)

[4 Domibus admin console 8](#_Toc27729801)

[4.1 User types 8](#_Toc27729802)

[4.2 The Domibus Interface 9](#_Toc27729803)

[4.3 Basic operations 9](#_Toc27729804)

[4.3.1 Updating the truststore 9](#_Toc27729805)

[4.3.2 Upload and edit PMode 9](#_Toc27729806)

[4.3.3 Download a received message 9](#_Toc27729807)

[4.3.4 Test connectivity between two access points. 10](#_Toc27729808)

[5 Sending data using a backend system 11](#_Toc27729809)

# Glossary:

|  |  |
| --- | --- |
| Term | Description |
| Access Point (AP) | The Access Point (AP) serve as the primary participants in the CEF eDelivery network. These AP-participants use the network to transfer documents between each other and learn about other participants using the SMP and its provided metadata. The AP of CEF eDelivery implements the AS4 message exchange protocol according to the CEF eDelivery AS4 profile. This ensures standardized, interoperable, secure and reliable data exchange. |
| AS4 | AS4 (Applicability Statement 4) is an open standard messaging protocol based on web services to securely exchange messages between participants. The AS4 profile of CEF eDelivery is the AS4 Usage Profile/ implementation guidelines initially defined by e-SENS based on the AS4 specification of OASIS, itself a profile of OASIS ebXML Messaging Services Version 3.0, which in turn is based on various Web Services specifications of OASIS. The eDelivery AS4 profile is now maintained by CEF. |
| Capability Lookup | Capability Lookup is a technical service to accommodate a dynamic and flexible interoperability community. A capability lookup can provide metadata about the communication partner’s interoperability capabilities on all levels defined in the European Interoperability Framework (Legal, Organizational, Process, Semantic and Technical interoperability levels). The metadata can be used to dynamically set interoperability parameters between the Sending and Receiving Parties. |
| CEF eDelivery | CEF eDelivery is a building block helping public administrations businesses and citizens to exchange electronic data and documents with each other in an interoperable, secure, reliable and trusted way. |
| Domain Name System (DNS) | The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. |
| Domibus | Domibus is the open source project of the AP maintained by the European Commission. |
| Dynamic Discovery | To send messages using the CEF eDelivery messaging infrastructure, the AP of the sending party needs to obtain the communication information of the receiving party, e.g. lookup address and its communication capabilities. Such information can be obtained via a Static or a Dynamic discovery process.  The static discovery process uses a static list of the receiving parties stored on the sending AP and their configuration which is programmatically selected and added to the message. Dynamic discovery allows the sending AP to query an external service storing up-to-date information about every receiving party in the network. The dynamic discovery in CEF eDelivery is implemented with three components, namely the SMP, the SML and the DNS. The benefits of the dynamic model are more automation, higher scalability and more flexibility – however the dynamic model also have a higher lookup overhead compared to the static model. |
| Keystore | A .jks file containing **public/private key certificates** for encrypting network traffic between participants. In other words, the keystore contains the private certificate that is used locally by the SMP/AP. |
| Participant | Every individual instance of a component of the eDelivery network – for instance the SMP, SML and various AP’s. |
| Service Metadata | Information necessary for invoking a service using CEF eDelivery components. It is a combination of information on the end entity recipient (such as its identifier, certificate, supported business documents and processes in which it accepts those documents) and its associated endpoints (such as the transport protocol and its address). |
| Service Metadata Locator (SML) | Service Metadata Locator (SML) is a component of CEF eDelivery that is responsible for Dynamic Service Location: in order to send a message, the AP of a sending party needs to discover where the information about a receiving party is stored. The SML serves this purpose and guides the AP of the sending party towards this location, which is called the SMP.  In other words, the SML is used to retrieve/add/update/delete information about the receiving parties and SMPs location on a Domain Name System (DNS). The SML is a centralized component and is essential for Dynamic Discovery. |
| Service Metadata Publisher (SMP) | Service Metadata Publisher (SMP) is a component of CEF eDelivery that is responsible for Capability Lookup: once the AP of the sending party discovered the address of the receiving party's SMP (Service Metadata Publisher), it is able to retrieve the required information to interoperate with the receiving party (i.e. metadata). SMP are registers of the message exchange capabilities and location of parties (i.e. metadata). SMP's are usually used in a distributed way and are essential for Dynamic Discovery. |
| Truststore | A .jks file containing **authentication certificates** for determining whether participants are trustworthy. In other words, the truststore contains all the certificates that are used publicly by the SMP/AP. |
| Domain | A Domain on an SMP can be seen as a subgroup. A SMP can have only one domain or several domains. Each domain is individually registered to the SML. |

# Introduction

The goal of this user guide is to describe the use of the different interfaces associated with the eDelivery solution, relevant to a local AP administrator. The guide will describe and explain the steps required for a functioning Access Point (AP) capable of sending and receiving messages. This includes the use of the Domibus admin console, and briefly the Service metadata publisher (SMP) User interface and how and where and AP admin would have access. This document will also cover the basics of updating the access point on the SMP. This guide expects that the Domibus is already installed and that functioning certificates and PMode’s have been obtained.

The main steps in setting up a functioning AP by getting and using a template provided by Digitaliseringsstyrelsen is:

1. Receive this document along with preproduced code from Digitaliseringsstyrelsen.
2. Set up the local Domibus according to received Installation guide.
3. Contact Digitaliseringsstyrelsen to get a ServiceGroup created according to your needs.
4. Upload the Provided PMode and adapt it to your local settings.
5. Integrate to AP from custom backend system

In this manual it is assumed that the documentation and installation of a local Domibus AP has been completed.

* Section 3 covers the contact and setup of a ServiceGroup on the SMP
* Section 4 covers the setup, and use of the Domibus interface required for a functioning connection to an external AP
* Section 5 briefly introduces the web service plugin and points the reader in the correct direction for interfacing a custom backend system to the AP.

## The eDelivery system

EDelivery is a system connecting several access points sending messages using the AS4 protocol. The eDelivery network consists of a large number of Access Points (AP) each AP is registered to an SMP. The SMP then registers its connected AP’s to a centrally controlled Service metadata Locator (SML) that updates the DNS network so that each individual AP’s name points to its SMP. Any AP can now by only knowing the name of another AP find its SMP and query it for additional info such as IP, metadata and message protocols. This method allows for an easily scalable and secure messaging platform. Depending on desired security the network can be more or less open, however with the AS4 protocol any message is encrypted, and both the sender AP and receiver AP is verified. After two Access points have discovered each other the process is as follows:

1. Submit: sends message
2. Send: processing step 1
   1. Validation and compression of the user message.
   2. Signing of the compressed message;
   3. Encryption of the signed compressed message.
3. Send: processing step 2
   1. Receives and decrypts the encrypted message
   2. Verifies the sender’s signature
   3. Decompresses the decrypted message
   4. Validates the original user message
   5. Sends the acknowledgement to the sender Access Point
   6. Archives the user message
4. Deliver: receives message

# Updating ServiceGroup metadata in the SMP

Depending on the desired solution two different approaches can be taken.

1. Let the SMP admin handle all registration
2. Let the SMP admin handle initial setup but do maintenance locally.

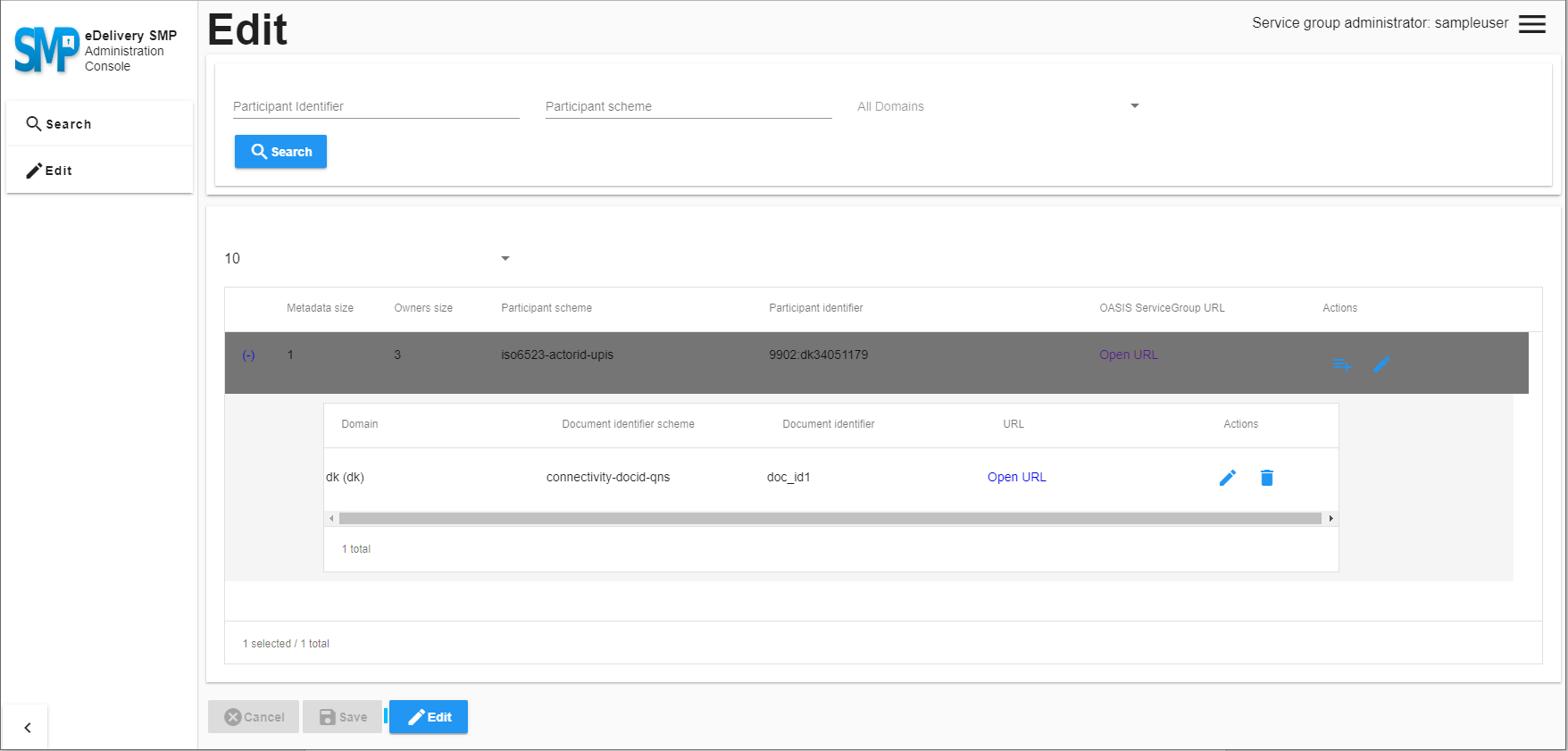
The first approach is desired if the characteristics of the AP is expected to remain static for a long duration, however if the metadata needs to be updated often then the second approach is more appropriate.

## No SMP access solution.

If the SMP administrator is in charge of handling the AP’s metadata, then the admin should be contacted using the provided information. The information required can vary depending on the SMP solution, however the most important is a list of unique document identifiers, E.g. “journal\_type3”. and a matching endpoint, E.g. <http://212.98.96.26:8080/domibus/services/msh> The endpoint needs to match the Domibus instance responsible for the document identifier.

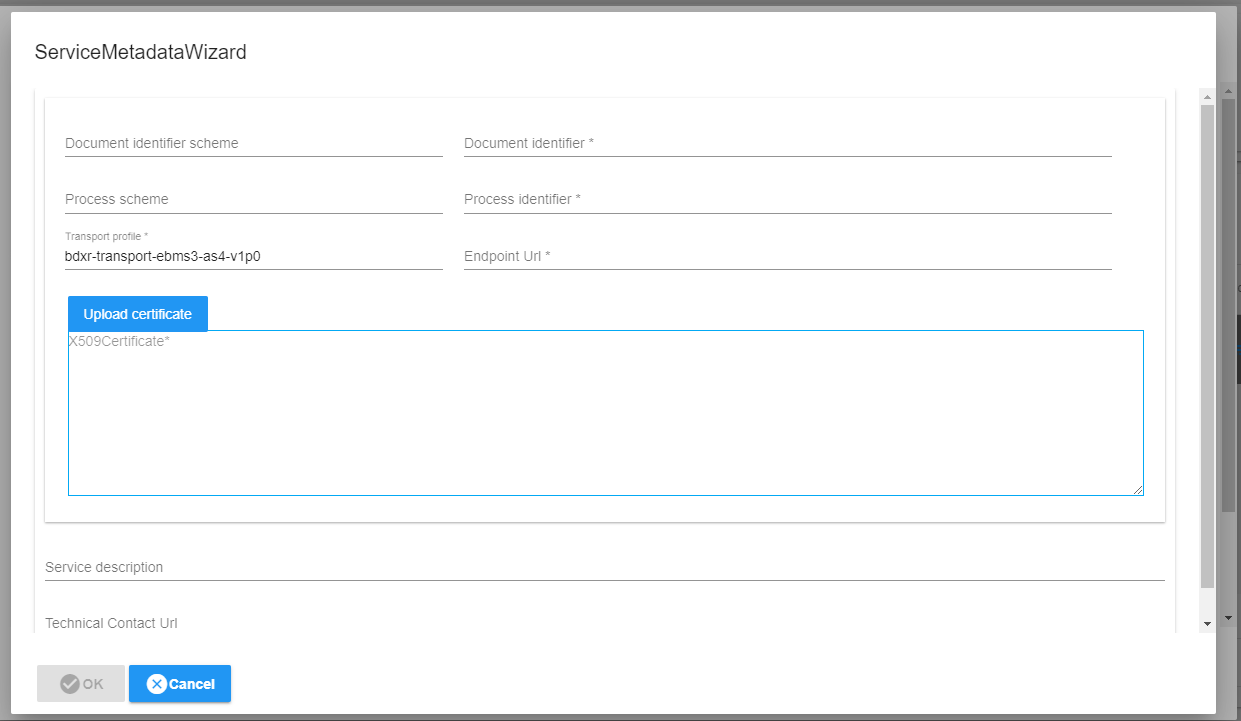
## Service group admin access

Depending on what level of access has been granted and how often changes to the metadata is required a user can be made in the SMP so the owner of the AP can login and directly add service Metadata. In this example a sampleuser has been created and given access to the service group 9902:dk34051179. Now the AP owner can update and manage its own metadata using the SMP admin console.



### Creating a new service metadata entry

Pressing the “Add service metadata” button opens a menu where an identifier scheme and identifier can be input along with a metadata XML. This can either be put in directly or the metadata wizard can be used. From here the relevant information can be pasted, after pressing ok, validate the metadata entry and click ok again before saving.

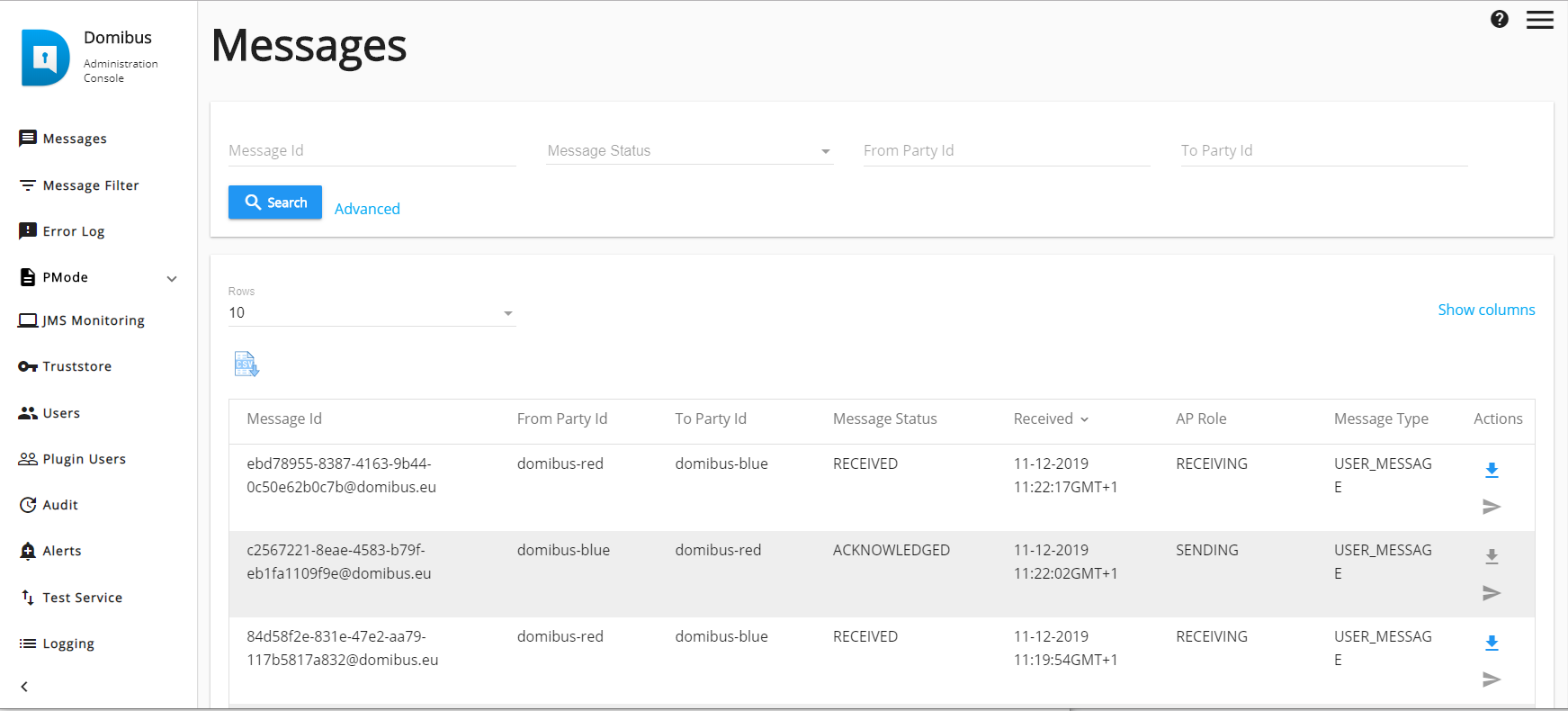


# Domibus admin console

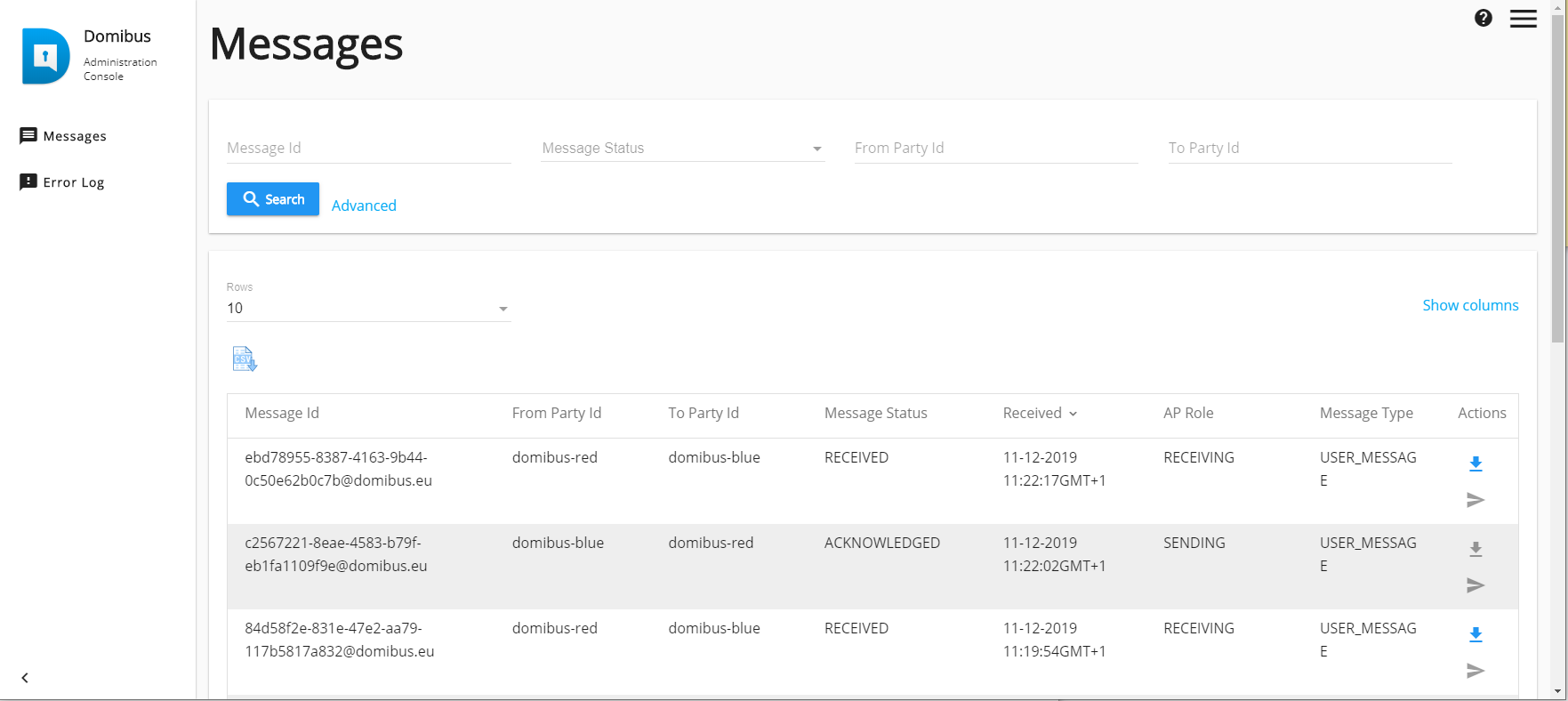
When connecting to your locally hosted Access Point you will be greeted with a login screen. From here you can either login as an admin or as a user. In this guide the user level access will not be discussed in depth as it is simply an admin but with considerably less rights.

## User types

The Domibus has as mentioned two levels of access, admin and user.

The admin user has access to all settings and can update the various settings in the console. 

The user only has access to the messages and the error log, the user can download received messages but not alter or see any settings. This level of access is suitable for someone overseeing the AP but without the technical knowhow or seniority to actually configure it.



## The Domibus Interface

A quick overview of the options in the Domibus Administration console and their purpose. The interface is generally quite straightforward and if the installation guide has been followed there should be nothing missing that won’t be addressed later.

|  |  |
| --- | --- |
| **Tab** | **Description** |
| Messages | List of incoming and outgoing messages, options, and log of earlier messages. |
| Message filter | On this page, the administrator can apply defined filters and access them individually. Useful if the access point is used by many backend systems. |
| Error log | Continuous list of error messages |
| PMode | Options for uploading or reviewing the current PMode file |
| JMS monitoring | Used to monitor and manage the contents of the JMS queues. |
| Truststore | Manage the AP side truststore |
| Users | User management, create new users or admins |
| Plugin Users | Manage the plugin users. |
| Audit | overview of changes made in PMode, Message Filter and Users pages |
| Alerts | General alerts related to Domibus. |
| Test Service | Basic test of communication between two access points. |
| Logging | Admin and Super admin users can change the Logging levels at runtime for the Domibus application. |

## Basic operations

These are the operations needed to set up a working AP. This includes updating the truststore and uploading and editing the current PMode.

### Updating the truststore

Depending on whether static or dynamic discovery is desired the truststore of the individual AP’s needs to be configured differently. In the case of dynamic discovery, the truststore should include the private key for the AP and the public key for the SMP. And in the case of static discovery it should include its own private key and the public key for all connected AP’s.

### Upload and edit PMode

To upload a new PMode go to the PMode tab, click the current tab and scroll to the bottom, click upload and browse to the location of the PMode .xlm. Alternatively click the archive tab and click restore next to one of the archived PMode files.

Editing the PMode can be done right in the Domibus interface if a new action e.g. set document type Journal-3 as an accepted input.

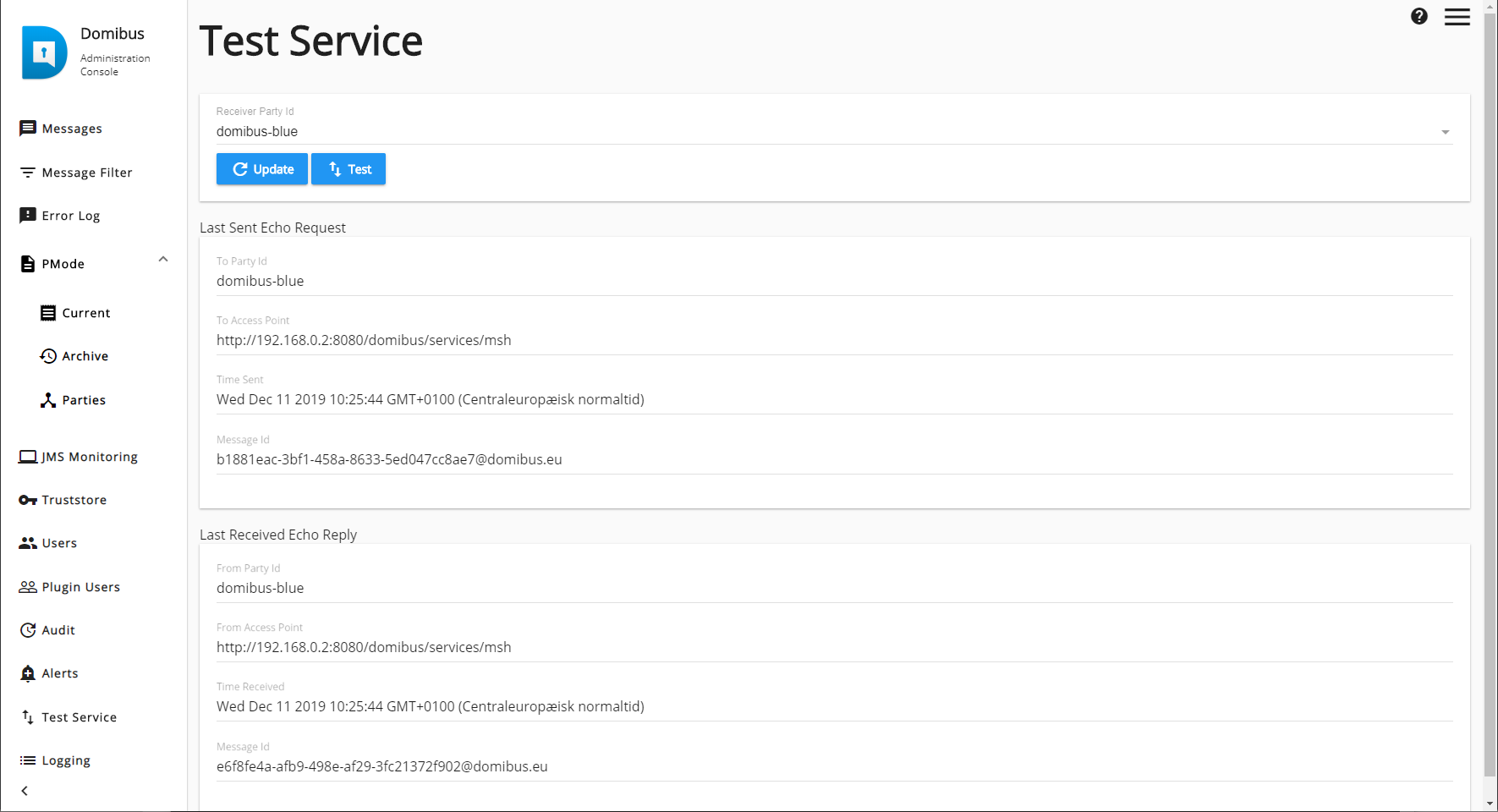
### Download a received message

Generally, the messages received by the access point will be handled by another backend system, however it is possible to manually download the received messages under the message tab.

### Test connectivity between two access points.

To test the connectivity between two access points, go through the test services tab and pick the desired receiver party Id from the drop-down list. The Party Id list is taken from the PMode.

To test the connection, press test, and then update. The Echo should be back near instantly if the other AP is already known. For the Test Service to work it needs to be configured in both the testing AP and the receiving AP.



# Sending data using a backend system

The interface used in the provided setup is a Web Service plugin and the steps required to interface with it is described in “Interface Control Document of the default WS plugin” pdf found at <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus>. Alternatively, a testing guide is also found at the same location describing the installation and test using the open source software SoapUI.