Saas Self-Services

User Guide

Hopex Aquila

Bizzdesign

INTRODUCTION TO HAS CONSOLE

Overview

The Hopex Application Server (HAS) console is a web-based administration interface used to manage the technical configurations and modules of a Hopex instance. It supports both On-Premises and SaaS deployment models.

☛ *For an architectural overview, refer to the HOPEX Application Server (HAS) Architecture Overview.*

Prerequisites

Deployment Model	Requirements
On-Premises	Hopex Application Server must be installed. See HOPEX Application Server (HAS) Installation Guide.
SaaS	A Delegated Administrator must be provisioned by Bizzdesign Cloud Services (MCS) to access the HAS console.

Scope

Feature	Purpose	Required Role	Deployment
Create Users	Create users with various roles. See Creating a User Account as an Administrator.	Administrator / Custom	On-Premises
Create a Delegated Administrator	Grant selected users access to the HAS console in SaaS environments. See Creating a Delegated Administrator.	Delegated Administrator	SaaS
Create an API key in the HAS console	Create API keys that are not associated with a Hopex session. See Creating an API Key.	Administrator / Custom	On-Premises

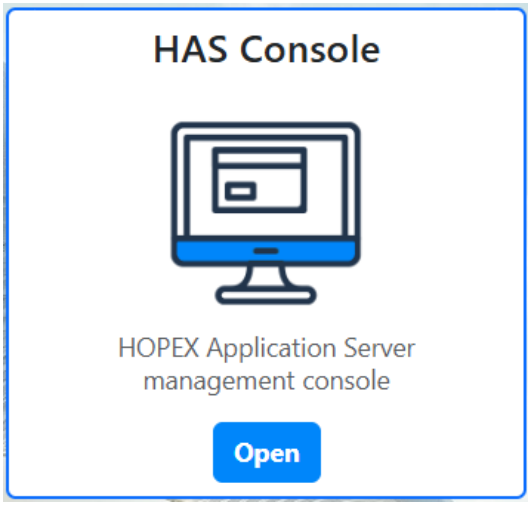
Feature	Purpose	Required Role	Deployment
Authentication configuration	Configure Hopex, Windows, SAML2 or OpenID Connect authentication. See HOPEX Unified Authentication Service.	Administrator / Custom	On-Premises
Single Sign-On (SSO)	Configure SSO using SAML2 or OpenID Connect. See Configuring Single Sign-On (SSO) as a Delegated Administrator.	Delegated Administrator	SaaS
SMTP server	Configure the SMTP server for email transmission. See Configuring the SMTP Server.	All Roles	All Deployments
Module Import	Import additional modules. See Importing a Module into HOPEX.	All Roles	All Deployments
Move to Production & Down Alignment	Ensure consistency and reliability across environments. See Move to Production & Down Alignment.	Delegated Administrator	SaaS

SaaS / On-Prem Common Features

Accessing the HAS Console

To access the Hopex Application Server (HAS) console:

1. Navigate to your instance portal.
2. On the **HAS Console** tile, click **Open**.



3. Log in using your credentials:
   - Enter your **Login** and **Password**.
   - If Single Sign-On (SSO) is enabled, click **Single Sign-On** instead.
4. Click **Sign in**.

Configuring the SMTP Server

SMTP (Simple Mail Transfer Protocol) server configuration enables email sending.

If your server is hosted by Bizzdesign as part of the SaaS offering, the SMTP server configuration is managed by Bizzdesign Cloud Services (MCS).

SMTP Parameter	Description
Default address of author via SMTP (FROM)	When an automated email (like a password setup email) needs to be sent, and the system cannot find a specific sender email address (such as the administrator's email), it uses this default email address instead.
Default address of sender via SMTP (SENDER)	Used for security/authentication purposes. Emails are sent as SENDER@domain.com on behalf of [User@domain.com]. Ensures deliverability and compliance with corporate policies. Can be used in Hopex Workflow notifications, see *Managing E-mails and Notifications*
SMTP Server	The domain that handles outgoing emails. Must match the domain used in the FROM and SENDER addresses.
SMTP Port and security	By default: 25 For secure communication use either: • (SSL): **SMTP port**: 465 and select **Activate SMTP SSL Support** • (TLS): **SMTP port**: 587 and select **Activate SMTP TLS Support**
Activate SMTP Authentication Support (Optional)	Select if your SMTP server requires credentials and enter corresponding username and password
Activate SMTP Proxy (Optional)	Select if a proxy is required and provide the proxy address and port

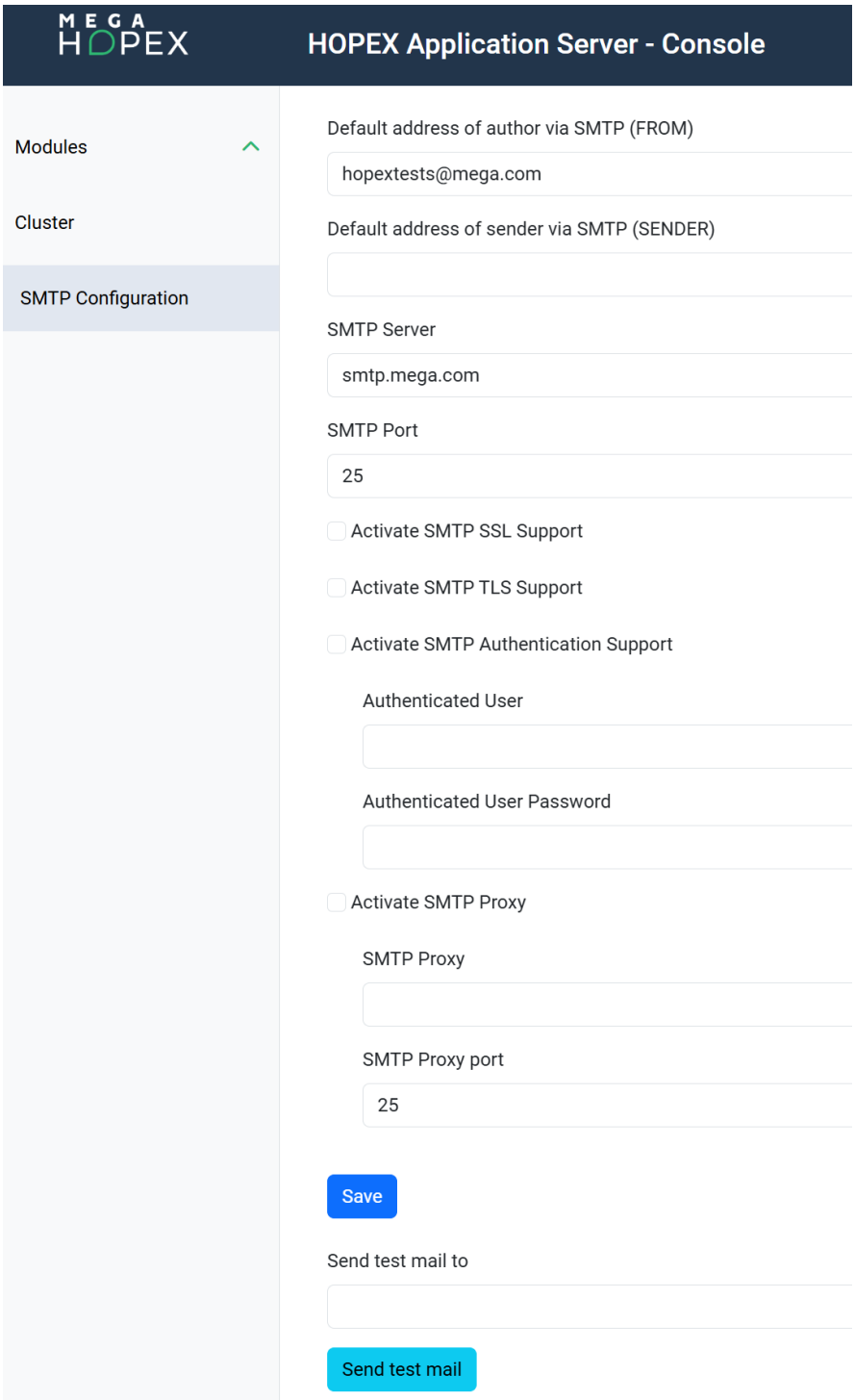
To configure the SMTP server:

1. Access the HAS Console.

   ☛ *See Accessing the HAS Console.*

2. In the navigation menus, select **SMTP Configuration**.
3. Enter the SMTP parameters.
4. Click **Save** to apply the configuration.

5. (Optional) Check the configuration, see Testing the SMTP Settings.



Testing the SMTP Settings

To test the SMTP Settings:

1. Access the HAS Console.

   ☛ *See Accessing the HAS Console.*

2. In the navigation menus, select **SMTP Configuration**.
3. In the **Send test mail to** field enter a test email address.
4. Click **Send test mail**.

Importing a Module into Hopex

Certain Hopex Solutions require additional modules to be imported before use.

To import a module:

❱ See Importing a Module into HOPEX.

SaaS Specific Features

Creating a Delegated Administrator

The initial Delegated Administrator must be assigned by MEGA Cloud Services (MCS). Once this role has been assigned, you can create additional Delegated Administrators as needed.

To create a Delegated Administrator:

1. Access the HAS Console.

   ☛ *See Accessing the HAS Console.*

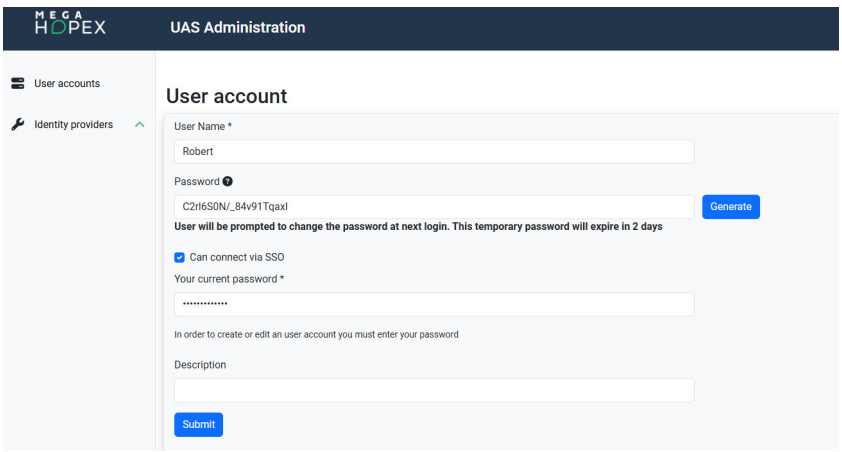
2. In the navigation menus, select **Modules > Authentication > User accounts.**
3. Click **Create**.
4. Enter the user details:
   - **User Name**: enter the new user's name
   - **Password**: enter a temporary password or click **Generate**.

     The password expires in two days and must be shared with the user for first-time login.

   - (Optional) Select **Can connect via SSO** to allow login via Single Sign-On.

     ☛ *See Configuring Single Sign-On (SSO) as a Delegated Administrator.*

   - **Your current password**: enter your own current password to confirm changes.
   - (Optional) Add a **Description**.
5. Click **Submit** to confirm.



Configuring Single Sign-On (SSO) as a Delegated Administrator

Single Sign-On (SSO) simplifies access to Hopex by integrating with your organization's identity provider (IdP), such as Google Workspace or Azure AD, using SAML2 or OpenID Connect protocols.

Users can access multiple applications (including Hopex) without needing to re-authenticate.

To configure Single Sign-On (SSO):

1. Access the HAS Console.
   ☛ *See Accessing the HAS Console.*
2. In the navigation menus, select **Modules > Authentication > Identity providers.**
3. Choose the appropriate protocol (**SAML2** or **OpenID Connect**) based on your identity provider.
4. Click **create**.
5. Enter the required parameters for the selected protocol (see corresponding tables below).
   ☛ *For examples, see Configuration examples.*
6. Click **Save**.
   The HAS instance and all related nodes are restarted. All users are disconnected.

SAML2 parameters

Tab	Parameter	Description
General	Display Name	Name of the button displayed on the login page for the SAML2 Identity Provider.
	Entity Identifier (Entity Id)	Identity of the Service Provider used when sending requests to the Identity Provider and in metadata.
	Metadata location	Location of the Identity Provider metadata (URL, absolute path, or relative path, e.g., ~/App_Data/IdpMetadata.xml). By default, the Entity Id is interpreted as the metadata location.
	Groups Authorized	Allows filtering of Hopex-related groups. Without filtering, you may encounter HTTP 400 errors due to large cookies generated from retrieved claims.
	ClaimForRoles	Name of the claim used for the role.
	ClaimForSub	Name of the claim used for the sub.
	ModulePath	Application root relative path for the Saml2 Assertion Consumer EndPoint (default: AuthServices). Each configured SAML2 must have a distinct value.

Tab	Parameter	Description
Certificate and Signature	Certificate friendly name	Certificate used by the Service Provider for signing or decryption.
	Want assertion signed	Select if you want assertions to be signed.
	Want AuthnRequests signed	Select if you want AuthRequests sent to the Identity Provider to be signed.
	Authenticate Request Signing Behavior	Defines AuthRequest signing behavior: • IfIdpWantAuthnRequestsSigned (default): sign only if required by the IdP • always: always sign AuthRequests (AuthnRequestsSigned set to true in metadata) • never: never sign AuthRequests
	Certificate use	Defines certificate usage: • Both (default) • Signing • Encryption
Organization	Name / Email / Url	Information (name, email, URL) describing the organization responsible for the entity.
Contact	Email	Collection of contacts for the SAML2 entity.

OpenID Connect parameters

Parameter	Description
Display Name	Name of the button displayed on the login page for the OpenID Connect provider. Also used in the calculation of the RedirectURL (specific to OpenID Connect), which is displayed on the login page.
Authority server URL	Defines the location of the OpenID server.
Proxy URL	If a proxy is configured on the same server as UAS, this URL defines the outgoing address for the protocol to reach its endpoints (e.g., DiscoveryEndPoint, TokenEndPoint).
Client Identifier	Identifier of your application.
Secret client	Authentication method for the client: • Client Secret (less secure) • Certificate defined by a Thumbprint and an Audience (TokenEndPoint URL of your IdentityServer) to read the Access Token via the certificate.
Scopes	Required scopes for the OpenID server: • openid (mandatory, provides JWT claims) • Additional scopes (e.g., email, profile) for extra claims.
ClaimForRoles	Name of the claim used for the role.

Parameter	Description
ClaimForSub	Name of the claim used for the sub.
MetadataAddress server URL	DiscoveryEndPoint URL providing metadata of the OpenID Connect provider (token endpoints, scopes, etc.). Typically: [AuthorityServerURL]/.well-known/openid-configuration. Usually not required if Authority Server URL is set.
Groups Authorized	Allows filtering of Hopex-related groups. Without filtering, you may encounter HTTP 400 errors due to large cookies generated from retrieved claims.

Resolving Duplicate User Issues in SSO Migration

Common scenarios

Duplicate user records are commonly observed in the following scenarios:

- Migration from an on-premises solution (e.g. Windows authentication) to a SaaS solution
- Transition from username/password authentication to SSO

Issue

During a migration to Single Sign-On (SSO), the login identifier often changes. This can result in the creation of two separate user records (Person System) in the system for the same physical person—one using the legacy login and one using the new SSO login.

As a result, users may experience issues such as unexpected password expiration prompts or loss of access rights due to mismatched identities.

Solution

To prevent duplication and preserve existing identity attributes (IdAbs) and access assignments, update the original login identifiers to match the SSO format.

To update login identifiers:

1. Access the login characteristics.

   ☛ *See Viewing the Characteristics of a Login.*

2. Update the **Name** of the login according to the SSO format.

Move to Production & Down Alignment

Presentation

Purpose

Using a ***Move to Production*** approach ensures that the exact same module, already tested in Development and Staging environments, is deployed to

Production. This guarantees consistency and reduces the risk of environment-specific bugs.

Using a ***Down Alignment*** approach ensures that lower environments reflect the state of Production.

- A manual Down Align (Production to Development) can be triggered on demand when developers need to mirror Production to debug, reproduce issues, or validate changes.
- An automatic Down Align (Production to Staging) is systematically performed before any Staging deployment. It ensures Staging is always a clean, up-to-date Production replica, enhancing confidence in pre-prod testing.

Prerequisites

These features are available only if all the following conditions are met:

- Self-Services are configured in the **Hopex Cloud Portal** by Mega Cloud Services (MCS).
- Your organization uses the **Enterprise SaaS offer** (not available with the Essential offer).
- You are logged in as a Delegated Administrator.

Move to Production

Procedure Overview

Action	Environment	Remarks
Schedule a Move to Staging	Development	
Validate a Move to Staging	Staging	
Move to Staging Process	(Automated)	May take several hours Includes an automatic Down Align from Production to Staging
Test Staging	Staging	Recommended: Test your Staging environment before scheduling the Move to Production.
Schedule a Move to Production	Staging	
Validate a Move to Production	Production	
Move to Production Process	(Automated)	May take several hours

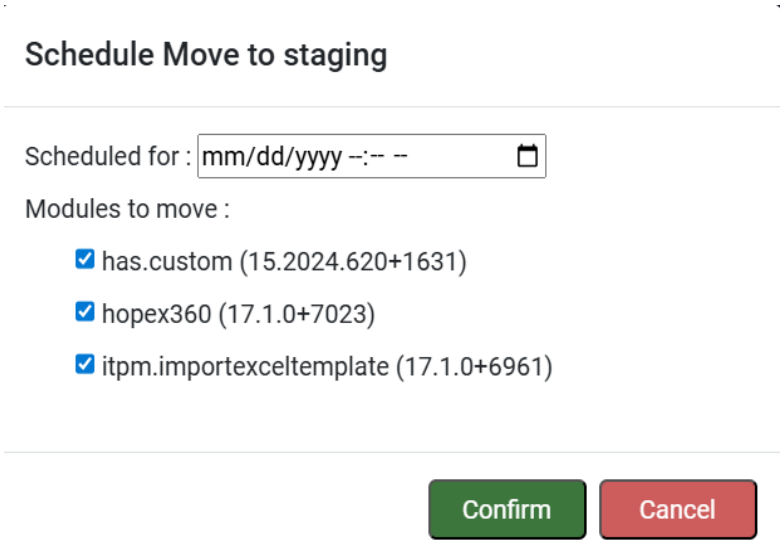
Schedule a Move to Staging

From the Development environment, you can schedule a Move to Staging, which will be executed only after validation in the Staging environment.

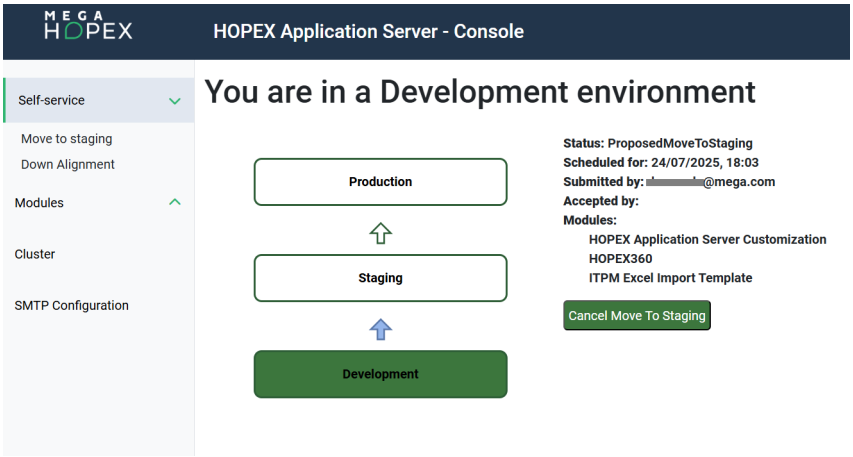
To schedule a Move to Staging:

1. Access the HAS console of your Development environment.
2. In the navigation bar, select **Self-service > Move to Staging.**

3. Click **Schedule Move to Staging**.



4. Select
   - the adequate date and time
   - the module(s) you want to deploy
5. Click **Confirm**.
   The Move to Staging is scheduled and requires validation in the Staging environment.



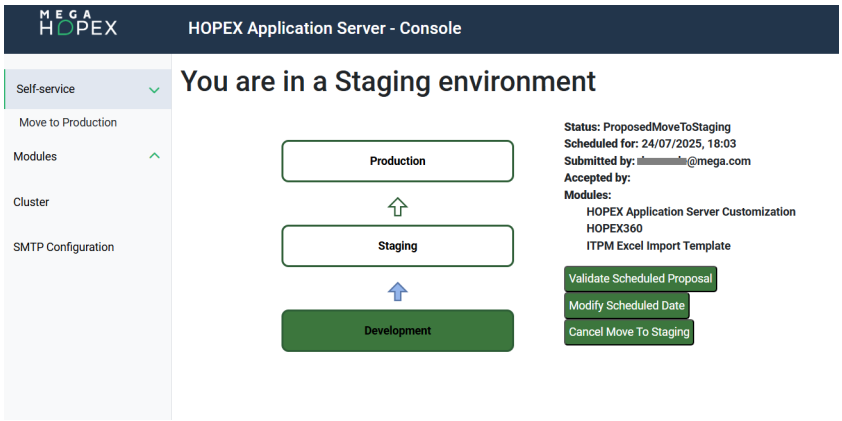
Validate a Move to Staging

From the Staging environment, you can validate the scheduled Move to Staging. If needed, you also have the option to modify or cancel the proposal.

To validate a Move to Staging:

1. Access the HAS console of your Staging environment.

2. In the navigation bar, select **Self-service > Move to Production**.
3. Click **Validate Scheduled Proposal**.
   The Move to Staging process can take several hours to complete. As the first step, an automatic Down Align is performed to synchronize the Staging environment with the current state of Production.



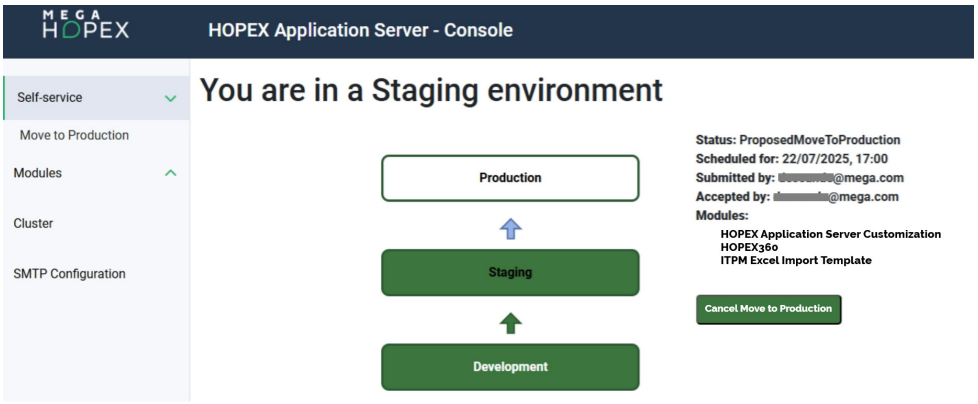
Schedule a Move to Production

From the Staging environment, you can schedule a Move to Production, which will be executed only after validation in the Production environment.

> **After a Move to Staging, make sure to test the Staging environment before scheduling a Move to Production.**

To schedule a Move to Production:

1. Access the HAS console of your Staging environment.
2. In the navigation bar, select **Self-service > Move to Production.**
3. Click **Validate & Schedule Move to Production**.
   A Schedule Move to staging window appears.
4. Select the adequate date and time.
5. Click **Validate & Schedule**.
   The Move to Production is scheduled and requires validation in the Production environment.

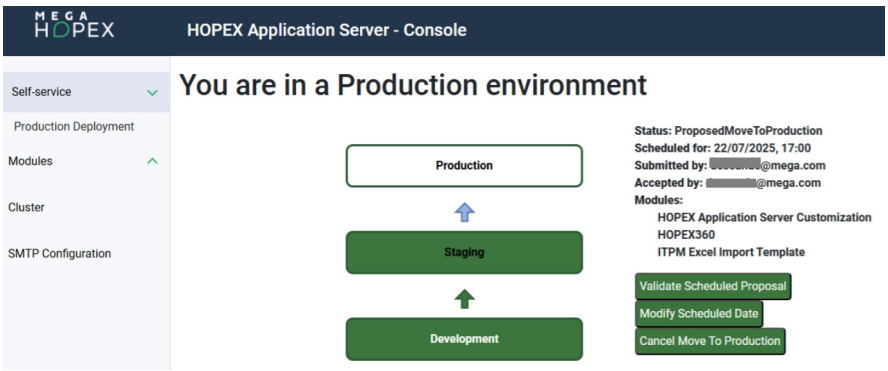


Validate a Move to Production

From the Production environment, you can validate the scheduled Move to Production. If needed, you also have the option to modify or cancel the proposal.

To validate a Move to Production:

1. Access the HAS console of your Production environment.
2. In the navigation bar, select **Self-service > Production Deployment**.
3. Click **Validate Scheduled Proposal**.
   The Move to Production process can take several hours to complete.



Down Alignment

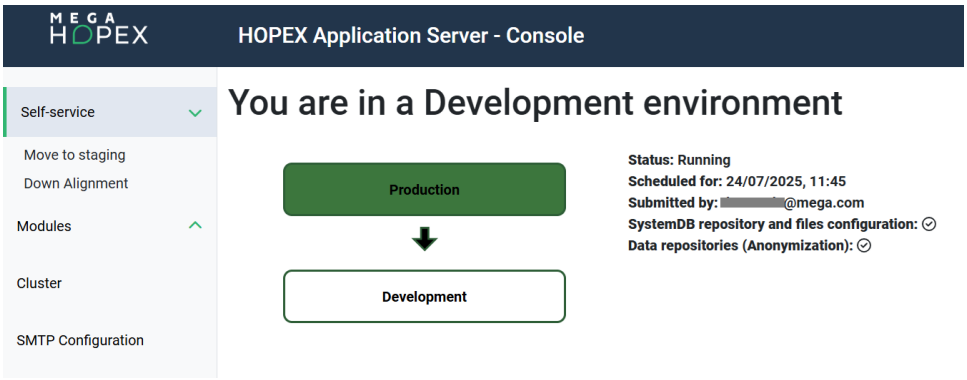
Schedule a Down Alignment

You can schedule a Down Alignment in order to synchronize the Development environment with the current state of Production.

To schedule a Down Alignment:

1. Access the HAS console of your Development environment.
2. In the navigation bar, select **Self-service > Down Alignment**.
3. Click **Schedule Down Align**.
   A Down Align window appears.
4. Select the adequate date and time
5. Select what to synchronize from Production to Development:
   - SystemDB repository and files configuration: this refers to the configurations of the modules.
   - Data repositories (data from your repositories is anonymized)

6. Click **Confirm**.



On-Premises Specific Features

Creating a User Account as an Administrator

To create a user account as an Administrator:

1. Access the HAS console:

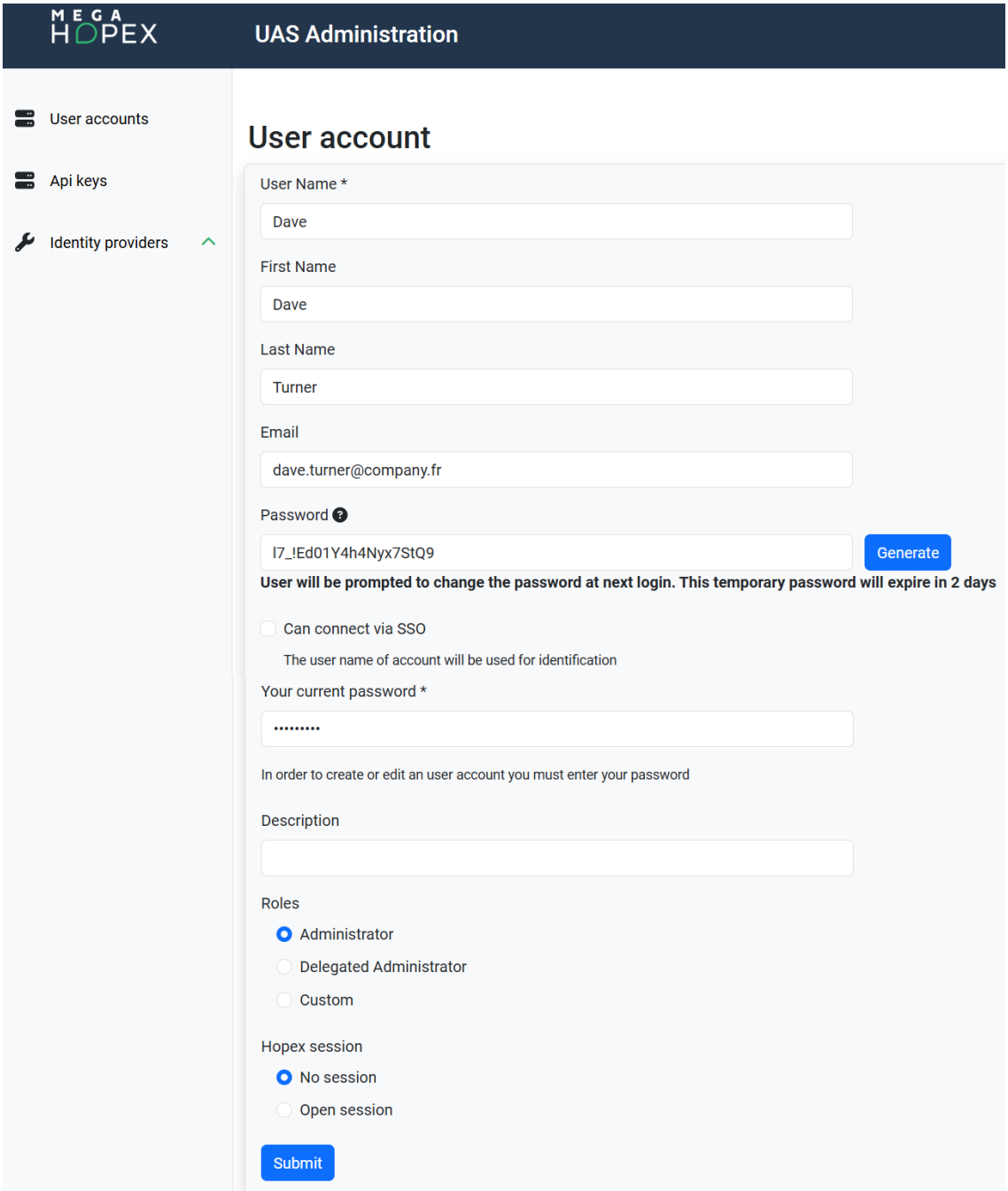
   ☛ *See Accessing the HAS Console.*

2. In the navigation menus, select **Modules > Authentication > User accounts**.
3. Click **Create**.
4. Fill in the following fields:
   - **User Name**
   - **Password**: enter a temporary password or click **Generate**.

     ☛ *The password expires in two days and must be shared with the user for first-time login.*

   - **Your current password**: enter your own password.
   - (Optional) Add a description.
5. **Role** (choose based on required access level):
   - **Administrator**: Full administrative access.
   - **Custom**: Limited permissions in the HAS Console and/or Hopex Supervisor.
   - **Delegated Administrator**: Minimal access, typically used in SaaS contexts.
6. Choose a Hopex session:
   - No session: no access to Hopex repositories.
   - Open session: grants access to Hopex repositories.

7. Click **Submit**.



Configuring Authentication as an Administrator

As an Administrator, you can configure the following:

- Hopex Native Authentication
- Windows Authentication
- SAML2 Provider
- OpenID Connect Provider

> ☛ *For step-by-step guidance, refer to the HOPEX Unified Authentication Service.*

Creating an API Key

API keys not associated with a Hopex session must be created directly in the **HAS Console**.

> ☛ *API keys associated with a Hopex session must be created via HOPEX Administration, see Managing API Keys.*

To create an API key in the **HAS console**:

1. Access the HAS console:
   > ☛ *See Accessing the HAS Console.*
2. In the navigation menus, select **Modules** > **Authentication > Api keys.**
3. Click **Create**.
4. Enter a key **Name**.
5. Configure the Roles:
   - **Administrator:** Grants full access to perform all operations in the HAS Console with administrative rights.
   - **Custom:** Grants limited permissions for certain operations in the HAS Console and/or Hopex Supervisor.
6. Click **Submit**.
7. Copy and save the key immediately.
   > ☛ *The key will not be retrievable later.*