Webinar on Migration to Public Cloud Azure and Visma Connect

Flex Applications held a webinar to inform and answer questions about the migration of their systems to Public Cloud Azure and the integration with Visma Connect. Jenny Gülich from Customer Success and Oskar, Head of Development, led the session, covering technical details, user management, and future features. The goal was to create confidence and provide clear information ahead of the move.

---

1. 🔄 Migration Status and Scope

- Flex Applications has been using Public Cloud themselves since April, with customers joining from May.
- In early August, approximately 100 customers were migrated, bringing the total to over 130 customers and 17,000 users.
- The migration is going well, and the team feels confident in the process.

2. 🔐 Single Sign-On (SSO) – Instructions and Functionality

- SSO instructions are now published on the Flex Applications website under Customer Center → Azure and Visma Connect.
- Existing SSO solutions like Google, Okta, Ping, and Entra can continue to be used as before.
- It is possible to configure and verify SSO before the migration.
- Users do not need to set a password in Visma Connect if SSO is used.
- You can configure the login so that only SSO is allowed in Flex Applications.

3. 📧 Email Verification and Users Without an Inbox

- Many users have email addresses without an inbox, which creates verification challenges.
- Development is underway to eliminate the need for email verification if the domain is verified (e.g., a work email).
- This feature is expected to be ready by the end of September or early October.
- Administrators can send verification emails to users who have not verified their email, and mass mailing is also possible.
- You can filter the user registry to see who has and has not verified their email.
- Users must have unique email addresses, but email aliases can be used for multiple accounts linked to the same inbox.

4. 🔐 Two-Factor Authentication (2FA)

- 2FA is not mandatory today.
- 2FA is likely to be required in spring 2026 at the earliest, but nothing is fully decided.
- Information and guidance will be sent out well in advance of the implementation.
- Those who already have 2FA via SSO (e.g., Entra) can continue to use it as usual.

5. 🌐 New URLs for Timeclock and API

- Timeclock will have a new URL after the move, for example, timeclock.flexhom.com/default/xxxx.
- The old URL to the web application will lead to a landing page with information and links to the new URLs.
- Flex HRM Mobile automatically redirects to the new URL for existing users. New users need to use mobile.flexhrm.com or a QR code.
- The API will have a new URL, and integrations will need to be pointed to it.
- The old API URL will forward calls to the new one, but a change is recommended as soon as possible.
- Timeclock users who do not need access to the application do not need to verify their email. If an employee is only using Timeclock to clock in and out, they can do so with their employee number or key card.

6. 🔒 Firewalls and IP Addresses

- Flex Applications will have a new IP address in Azure.
- The IP address is documented on the information page under "Breaking Changes" and "FAQ."
- Customers with a strict firewall may need to open it for the new IP address.

7. 🔜 BankID Login

- Planned for launch in 2026; a more exact date has not been set.
- Information and instructions will be sent out as the date approaches.

8. 📊 Reporting and Payroll Preparation

- The functionality for reports, payroll files, and payroll preparation is not affected by the move.
- All data is migrated, including time reports and expense reports that are in progress or have been attested.
- Users can continue to report time as usual after the move.

9. 🛠️ Integrations and Corporate Credit Card Links

- Corporate credit card links should work as usual after the migration.
- It is recommended to check the functionality after the move.
- Integrations with other systems need to update the API URL.

10. 📄 Information Page and Documentation

- All information, instructions, and FAQs are collected on a dedicated information page on the Flex Applications website.
- Documentation can be downloaded as a PDF and Word file for internal distribution.
- The webinar was recorded and will be available for review.

Conclusion:

The migration to Public Clock Azure is progressing as planned, covering over 130 customers and 17,000 users. Flex Applications has developed clear instructions and documentation for SSO, verification, new URLs, and integrations to facilitate the transition. Users can continue their work with time reporting and payroll preparation as usual, and administrators have tools to manage verification and communication. Future features such as BankID and the requirement for two-factor authentication are planned and will be communicated well in advance. The information page is continuously updated with questions and answers.

Focus on the Most Important Point:

Single Sign-On (SSO) and Verification

- SSO is a central part of the migration, and many questions have focused on how it will work after the move.
- Flex Applications has now published a detailed SSO guide on its website that describes the step-by-step process for configuring SSO in Azure and Visma Connect.
- Existing SSO providers such as Google, Okta, Ping, and Entra can continue to be used without change.
- It is possible to configure and test SSO before the migration to ensure that login works smoothly afterward.

- Users with SSO do not need to set a password in Visma Connect, and it is possible to control the login process so that only SSO login is allowed in Flex Applications.
- For SSO configuration, it is recommended to create a new application in Entra and generate a new certificate according to the guide.
- A major challenge is the verification of email for users without an inbox, but development is underway to eliminate the need for email verification if the domain is verified. This is expected to be ready by the end of September or early October.
- Administrators can send verification emails to users who have not verified their email, and there is functionality for mass mailings and filtering in the user registry.
- Unique email addresses are required per user, but email aliases can be used to manage multiple accounts linked to the same inbox.

This SSO and verification solution is crucial for ensuring a smooth and secure login after the migration and for minimizing disruptions and support issues.