Link to article: https://discover.claromentis.com/knowledgebase/articles/946

User Management FAQ

Introduction

Below is a list of questions which are frequently asked by Claromentis sales team and prospects looking for an Intranet solution. The article covers frequently asked questions about SSO, user provisioning and users directory syncronisation.

Related articles

- Integrating with existing Identity Providers (SSO) and User Directories
- Single Sign On (SSO), User Provisioning, and User Directory Synchronisation
- Important information (for new customers and supplier reviews)
- Claromentis People API reference

FAQ

User management capabilities

- Q: **What exactly is available in the core product to satisfy user provisioning and SSO with no additional cost?**

  A: LDAP Integration with NTLM configuration

- Q: **What are the obvious use cases in user provisioning and SSO that the Claromentis Intranet cannot currently solve?**

  A: Here are the typical scenarios where we have limitations

  a. Systems over 1000 users which only use Azure or Okta user directory: user provisioning - no; SSO - yes

  b. Multiple Microsoft AD domains: user provisioning - yes; SSO - no

  c. Multiple Azure or Okta user directories: user provisioning - no; SSO - no

- Q: **What is an accurate description of a complex setup that Claromentis product cannot support, such as a multi-tenancy environment? How can Claromentis team determine if the customer's Active Directory (or other solution) is too complex for the Intranet system?**

  A: Here are the typical scenarios where we have limitations

  a. When using Azure for SSO, we can only configure SSO with a single tenancy

  b. When using more than one AD domain for user provisioning, we are unlikely to support SSO. To support this setup, we would require that the customer configures an Identity Provider that has trust between the domains

  c. When using a .local AD domain (internal facing domain), it is not possible to use LDAP integration for SaaS.

- Q: **What common technology stacks used by our customers would mean we can provision users but we can't provision groups?**

  A: Typically, if we can provision users during their logon process but cannot sync their details on a scheduled basis then we are unlikely to sync / map their group membership from an external directory. Looking at the matrix below, you will see that Google/Twitter/FB and OneLogin,

Centrify, Duo, ADFS with NO Microsoft AD cannot support group mapping / sync.

- Q: **What common technology stacks used by our customers would mean we can provision users but for which we can't create org charts?**

  A: In order to support org chart creation, an external directory must provide Claromentis with the user's manager username as part of the sync. If this information is available, then the org chart creation is available.

- Q: **What products and configurations does Claromentis recommend to customers for SSO to work, taking into account the different user directory technologies, such as Active Directory, Okta, etc.?**

  A: See the User access and management matrix below

- Q: **What do we offer Google users that have no other solution in place?**

  A: Social connect - see https://discover.claromentis.com/knowledgebase/articles/309

'User directory sync' module, available from Marketplace

- Q: **When should we recommend 'User directory sync' marketplace module**

  A: We recommend using the 'User sirectory sync' module when

  a. When a small to medium customer uses Azure AD or Okta as their identity provider and does not want to expose / does not have Microsoft AD;

  b. When customer has a third party directory capable of scheduling a CSV file export

- Q: **Why does the 'User directory sync' module have CSV as an option - how does that differ from the existing core product functionality which imports users from a CSV?**

  A: We added two features which can be used to automate user sync from a csv file:

  a. Remote CSV file. Imagine you have an HR system which can auto-generate a CSV file containing user information. That file can be updated on a regular basis and stored on a file server accessible to you as the system admin and to the HR system. If you allow web access to that file to Claromentis' User directory sync, you can then automate your Intranet's user profile updates.

  b. Intranet DMS. Alternatively, you can store the user directory information CSV file on your Intranet DMS and schedule automatic user sync by pulling the data from that file regularly. The benefit of this feature comes from the fact that you can perform version control on the CSV file in DMS, allowing you to roll back a sync if you spot undesired effects of your latest sync. This is also useful if changes to your users are less frequent, but you still want a scheduled sync.

Groups management

- Q: **What happens if Groups are automatically provisioned from an external user directory, such as AD, but then a customer manually adds a user to a local group in Intranet?**

  A: AD users will be removed from that local group. Therefore we recommend using Roles for managing users locally during onboarding of the new system. Roles membership is not affected by user synchronisation from an external directory

  When User directory sync or LDAP integration are configured to map groups from the external directory, then the user's group membership will be updated according to how it is set up in that directory.

  For example, 'user a' is a member of 'AD-Intranet' group, which is a group set in an AD directory. 'User a' has also been added to 'Local-Intranet' group, which is created and managed manually on Intranet. Here are possible scenarios:

  a. If Group mapping is enabled, then 'user a' will no longer be a member of 'Local-Intranet' group after the next user sync.

  b. If Group mapping is then disabled, then 'user a' will stay in 'AD-Intranet' group and 'Local-Intranet' group after the next sync. It is important to note that group mapping from external directory will no longer take place in this scenario

---

User email addresses

- Q: **Must a user have an email address to have an Intranet account? What are the implications if they do not?**

  A: Currently yes, but we are considering making it optional in the future. If a user is not configured with their own email address, they cannot receive email notifications, but they can still have in-system notifications. Please check Email in ClaMailMessage article for more details

- Q: **Can a user be configured with personal emails not connected to the Intranet domain?**

  A: Yes, as long as we have a valid email address.

User access and management matrix

Customer stack			Claromentis solution			
Tech Used by client	SaaS / OnPrem	No of users	Suggested setup	SSO	User provisioning at logon	Directory sync + Group mapping + Org chart
Microsoft AD	OnPrem	any	LDAP Integration + NTLM config	yes	no	yes
Microsoft AD	SaaS	any	LDAP Integration + Login Handler	yes	yes	yes
Azure AD	any	<1000	User directory sync + Login Handler	yes	yes	yes
Azure AD + Microsoft AD	any	>1000	LDAP Integration + Login Handler	yes	yes	yes
OKTA	any	<1000	User directory sync + Login Handler	yes	yes	yes
OKTA + Microsoft AD	any	>1000	LDAP Integration + Login Handler	yes	yes	yes
OneLogin, Centrify, Duo, ADFS + Microsoft AD	any	any	LDAP Integration + Login Handler	yes*	yes	yes
OneLogin, Centrify, Duo, ADFS; NO Microsoft AD	any	any	Login Handler	yes*	yes	no
Microsoft AD + 3rd party directory with CSV export	any	any	LDAP Integration + Login Handler + User directory sync	yes	yes	yes
OneLogin, Centrify, Duo, ADFS + 3rd party directory with CSV export	any	any	User directory sync + Login Handler	yes*	yes	yes
Google, Facebook, Twitter	any	any	Social connect	yes**	no	no
Any identity provider + capability to update users via API	any	any	Login Handler + People API	yes	yes	yes

* OneLogin, Cenrify and Duo supported up to Claromentis version 8.13 on SaaS

**using “login with Google/FB/Twitter” button

Last modified on 6 December 2023 by Hannah Door

Created on 18 August 2023 by Stas Dreiling

Tags: customer, intranet, marketplace, sales, login, SSO, user