crownpeak

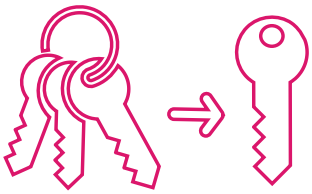
FEDERATED AUTHENTICATION

Enhancing system security and usability

Why choose between efficiency and security when you can have both?

Federated authentication provides a “win-win” scenario for marketing and IT by:

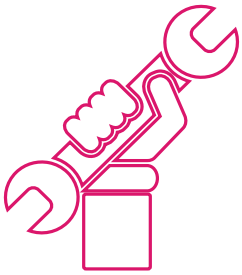
Simplifying the login experience for your end-users



Eliminate the need for more logins and passwords to access Crownpeak and hosting environments.

Use a transparent login that is automatically initiated from corporate credentials.

Remove roadblocks in front of your team and partners so they can get more done.



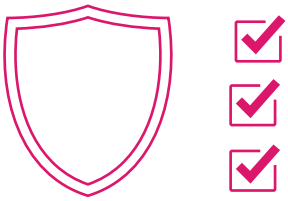
Empowering your information security administrators

Retain complete control over passwords, accounts, and reuse limits.

Cut down on the sheer number of 3rd-party application accounts to be managed (so there’s no more need for chaotic login spreadsheets!).

Centralize access controls.

Strengthening corporate security on your terms



Enable your IT team to easily define its own authentication policy as it sees fit.

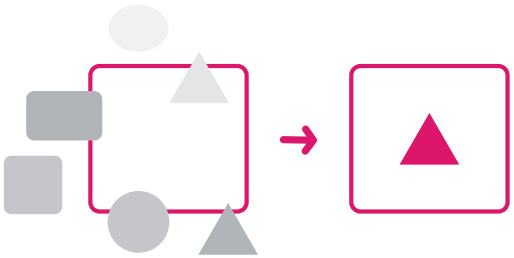
Use your own existing security infrastructure (LDAP, biometrics, multifactor, etc.).

Terminate users’ Crownpeak access immediately by simply removing users from your corporate network.

Why Federated Authentication?

It's like your car's keyless entry and ignition, but for your Web Experience Management platform.

Your business uses a wide variety of web applications every day to get things done. On top of that, there is an equally wide variety of login credentials rules for all of those applications. Managing access for many different users can be dizzying, especially in the enterprise. Not to mention, the more loose ends there are with unregulated passwords, the more vulnerable your organization's data security becomes. So why not opt for one, manageable, secure login for everything if possible?



Federated Authentication provides a convenient solution to these challenges. To best support our customers' needs for both convenience and security, Crownpeak supports Federated Authentication.

With Federated Authentication added to Crownpeak, your security team will have the extensive control they desire to ensure the following:

- Your corporation will have the power to flexibly leverage its network logins to best work with Crownpeak.
- Your users will more efficiently engage with your hub for marketing activities.
- You will rest assured that the Crownpeak WEM platform is as safe as your corporate network.

Is Federated Authentication right for you?

- ☐ Does your organization already use Federated Identity Management (also known as "Single Sign-On" or SSO)?
- ☐ Does your Federated Identity Management Provider support Security Assertion Markup Language 2.0 (SAML 2.0)?
- ☐ Does your IT team offer a vendor integration handbook or guide?

Crownpeak Federated Authentication is an ideal solution for:

- Global enterprises looking to streamline end-user access across a large operational base
- Organizations that need to define their own approach to corporate security and regulatory compliance
- Any Crownpeak customer that already has Federated Identity Management in place

FAQ'S

What is the difference between Authentication and Authorization?

Authentication: "Are you who you say you are?"

Authorization: "What is this person allowed to do?"

How do Authentication and Authorization work with Crownpeak?

Authentication is managed either internally within Crownpeak, externally via a federated identity management relationship with the customer's identity provider, or a hybrid blend of both.

Authorization is always managed within Crownpeak using the platform's Role-Based Access Control (RBAC).

Does Crownpeak support Service Provider (SP) Initiated SSO or Identity Provider (IdP) Initiated SSO?

Crownpeak supports both SP-initiated and IdP-initiated SSO.

Which Federated Identity Management Platforms does Crownpeak support?

We support:

- Microsoft ADFS®
- Ping Identity®
- CA SiteMinder®
- IBM Tivoli™
- Shibboleth™
- OpenAM™
- RM5 IdM™
- and any other SAML 2.0 compatible platform

crownpeak