Multi-site Management with Enterprise Security

dotCMS and
SAML Authorization

Introduction

The advent of digital and cloud-based technologies has given us the fourth industrial wave, opening up many growth opportunities.

This new era has enabled brands to strive for operational excellence by automating back-office and front-office processes, and also helped brands to create new business opportunities so they can develop new products and services, generating new streams of revenue as a result.

Recent research by Gartner shows that a majority of enterprises are executing some form of digital ambition, whether that may be optimizing business process, transformation, or both. But oddly enough,

17% of CEOs have declared that they have very little or no digital ambition, with one significant reason being security.[1]

dotCMS wants to change that.

dotCMS **is driven to become the most user-friendly and trusted decoupled headless CMS provider on the market.** The CMS platform can deliver content to a multitude of devices and channels, including :

- Websites
- Intranets
- Extranets
- B2C/B2B Portals
- Mobile apps
- Smart Speakers (Amazon Echo & Google)
- Next-Generation IoT Devices.

As part of dotCMS's vision, they've recently announced the availability of the SAML Authentication Module, that has been developed in conjunction with Ethode.

Key
Takeaways

dotCMS delivers a content foundation-as-a-service that allows enterprises to develop, orchestrate, deploy, & scale their platform to deliver a connected, trusted and continuous digital experience. It is a cloud-ready, decoupled & open framework solution that is aiming for the highest level of NoCode usability in the industry.

Our latest release, dotCMS 5.0, provides a seamless user experience, thanks to its new and improved drag-and-drop capabilities and intuitive authoring experience interface that enables users to develop websites and push content in minutes.

The multi-site capabilities of dotCMS is a widely-used feature, and the introduction of the SAML plugin will further provide a more secure and streamlined user experience.

The SAML module

will enable dotCMS administrators to use a single IdP to manage all their user accounts & control access to multiple sites on the same installation. The plugin will enable enterprises to avoid disruptions as they conduct their daily business processes by efficiently harmonizing security across the entire digital platform.

01. How dotCMS users benefit from the SAML plugin

dotCMS users will benefit from having one set of **credentials to access multiple sites** that are running on dotCMS at the same time.

02. How the new SAML plugin integrate with other service providers

As a best of breed solution, dotCMS, equipped with the new SAML plugin, can integrate the SAML capabilities with **third-party services that share the same Identity provider**, minimizing the need to have separate logins even further.

03. Why dotCMS chose SAML

The SAML plugin provides dotCMS with a secure, **SSO (single sign-on) protocol** that is widely trusted and used by the most security-conscious enterprises.
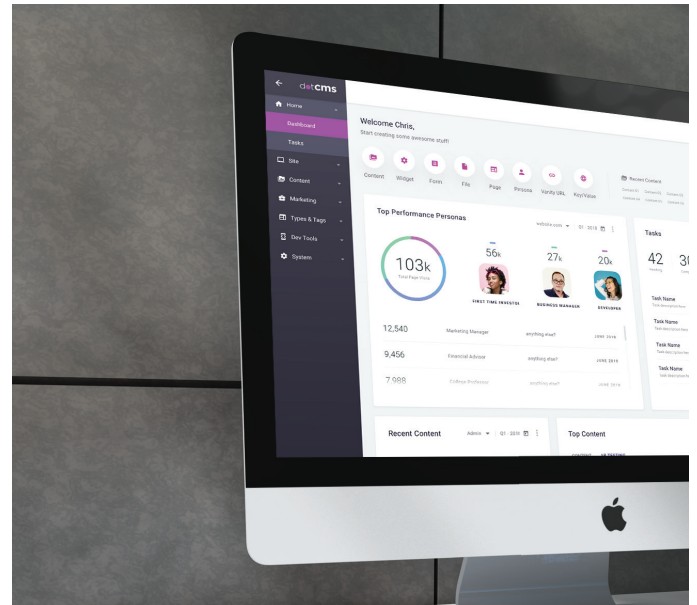
04. How SAML streamlines user account management

The SAML plugin, once installed, provides dotCMS users with a centralized user account management and authentication interface. dotCMS administrators can easily **create profiles, user groups and assign individuals with certain rights and access to tools,** within a few quick clicks.

05. What versions of dotCMS is the new SAML module compatible with

The dotCMS SAML Authentication Module has been tested to work with **dotCMS 4.3 and dotCMS 5.** The module is also compatible with **dotCMS Enterprise and dotCMS Cloud.**

The SAML Authentication Module is compatible with the 3 primary IdPs - ADFS, Shibboleth, and Okta. The module uses openSAML Library version 3, and applies OneLogin's open source SAML Java Toolkit to turn dotCMS into an SP that can be connected to various IdPs.

Authenticated Applications and the Digital Age

Most enterprises in the digital age are focused on investing their efforts in delivering an excellent customer experience on the public facing side. This includes the acquisition of new customers, driving brand awareness, executing campaigns, and promoting products and services. But that's just the tip of the iceberg.

Campaigns

Brand Awarness

Promotions

Website
Customer Acquisition

Customer Service

Billing & Payment

Customer Portal
Customer Experience

Product Data

Account Management

Training & Support

Logistics
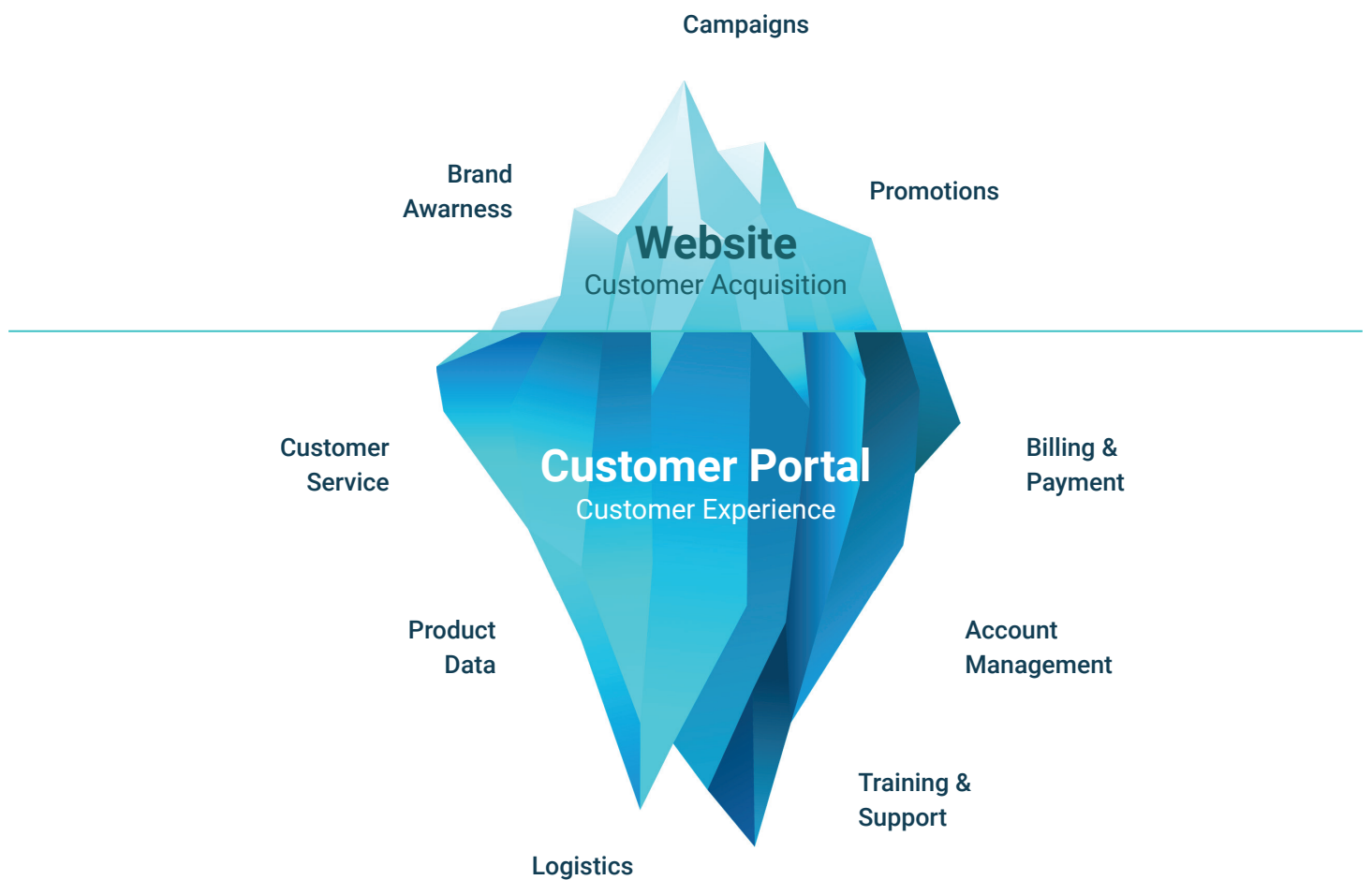
With customers now expecting to interact with brands through multiple touchpoints, this is an excellent opportunity for brands to distinguish themselves from the competition and truly **deliver a hyper-personalized customer experience with secure interaction** that comes in line with the latest GDPR legislation around privacy rights. This will really help to nourish customer relations.

When it comes to authenticated **business applications that allows you to have secure touch points** during the customer cycle, we're referring to the following applications:

- **Intranets** (used by sales representatives to enhance the sales process when they're with consumers)
- **Extranets**
- **B2B portals**
- **B2C portals**
- **Community portals**

If we take a look at the figure below, we can see that many industries are using the above mentioned applications.

BUSSINESS	INTRANET	EXTRANET	B2C PORTAL	B2B PORTAL	COMMUNITY PORTAL
Finserv	✔	✔	✔		
Retail	✔		✔	✔	
Manufacturing	✔	✔	✔	✔	
Higher Ed	✔	✔			✔
Government	✔		✔	✔	
NGO	✔	✔			✔
Technology	✔	✔	✔		✔
Publising	✔	✔	✔		
Healthcare	✔	✔	✔	✔	

As for authenticated access in the context of dotCMS, it concerns the following two points:

- **Content authoring and publishing**

- **Content consumption**

The former is about providing a convenient, user-friendly, secure and safe environment for content creators and marketers to create and deliver experiences to consumers. The latter is about providing the same environment for both direct and indirect content consumption.

Direct content consumption: is where content is consumed on a website built by dotCMS.

Indirect consumption: is when content is being pulled from the central dotCMS content repository to be utilized on either a single page app or a third party application over a secure RESTful API.

dotCMS delivers secure flexibility by supporting LDAP (Active Directory, Oracle LDAP, Open LDAP), OAuth 1 and 2, and, most recently, SAML. All of which are available out-of-the-box.
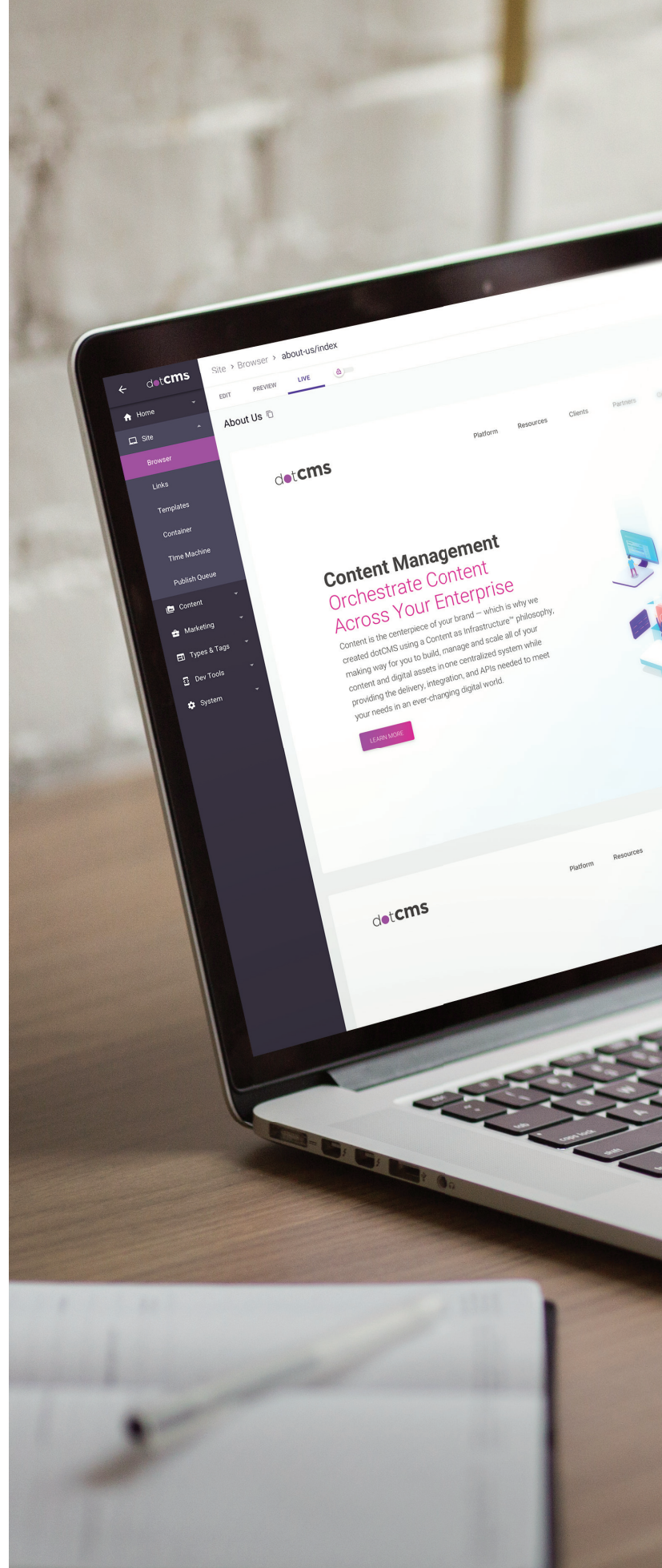
Introduction to SAML

Security Assertion Markup Language (SAML) is an SSO login standard which **eliminates the need for multi-factor authentication** (application specific-passwords), resulting in the following advantages:

- **Users don't need** to remember or renew passwords

- **It prevents** the use of weak passwords

- **There's no need** to type in login credentials

As the name suggests, SAML is an XML-based markup language that is used in the context of security assertion.

It allows service providers to grant their users access to the services they provide, while also being able to control what privileges, including features, functions and tools, a user can have access to.

SAML rose to prominence due to growing number of SaaS applications that were being delivered to both employees and consumers, prompting the need for a more streamline login procedure for utilizing multiple SaaS applications - the average enterprise uses 91 SaaS applications.[2]

SAML has become a standard for many cloud-based providers **including Google, Salesforce.com and WebEx.**

How Does SAML Work?

A SAML SSO involves three parties:

- The end user

- A cloud-based application service provider (SP) (i.e. dotCMS)

- An Identity service provider (IdP)

The IdP keeps the information about the users in a database. When a user connects with an SP via SSO, the SP communicates with the IdP to delegate authentication - this happens when the SP recognizes the username. Once the IdP validates and confirms the username against its databases, it then sends a SAML assertion to the SP. The SP then authorizes the user to gain access to the application.

The SAML exchanges user authorization and user authentication information via the relevant signed digital security certificates and PKI (Public Key Infrastructure). This ensures the integrity of the data remains intact, eliminating the possibility of password theft/reuse.

User connects to service provider to access application

Service provider authentication to Identify Provider

User gets access to app from Service Porvicer

IdP Validates User

UDB: Universal Database

The User

Service Provider

Identify Provider
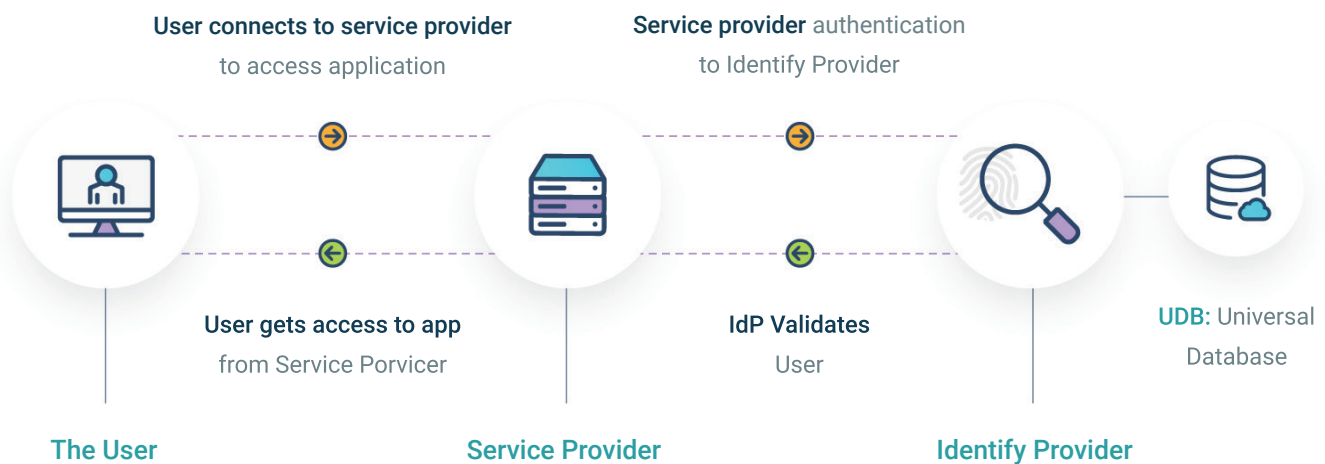
How the SAML Authentication Plugin Simplifies & Secures Multi-site Management

One of the main features of dotCMS, that has benefited many of our enterprise clients including the likes of Telus, Aon, Thompson Reuters and RBC Royal Bank is its multi-site capability.

dotCMS acts as a central repository for all your content; and the decoupled API-driven environment enables you to **easily distribute and push your content to a multitude of channels and devices, without having to resort to duplication.**

With the addition of the SAML plugin, it will **help dotCMS users to simplify and secure** their multi-site management in the following ways:

01. Streamlined Maintenance

Operating multiple sites through dotCMS **reduces the load on IT having to look after the platform, and gives more control to marketers and business users** to deliver a more personalized one-to-one customer experience. From an IT perspective, the SAML plugin will provide developers with instantaneous access to the back-end of multiple sites. dotCMS can be installed either on-premise or via the cloud, with the latter providing developers access through any device that has an internet connection.

02. Content Management

The multi-site and multi-domain set up of dotCMS provides users with an **intuitive authoring experience where they can update content on multiple sites via a single moderation**. With the addition of the SAML plugin, dotCMS administrators can assign what sites and channels a user can update, giving you better user management and more control to how content is distributed.

03. Assign Who Can Create New Sites

The NoCode feature in dotCMS allows non-technical users and marketers to create and configure a new site in an instant. Again, with the addition of the SAML plugin, dotCMS administrators can assign which users can create new sites, **eliminating the scenario of an irrelevant site being created in error.**

04. Standardization

The content-as-a-service model of dotCMS allows marketers to operate multiple sites which adhere to branding guidelines, ensuring you achieve consistency across the board through all your applications. The SAML plugin enables site administrators to **control what users can do on a site in terms of design and branding.** This also works well for official site documentation like privacy policy and terms and conditions.

05. Internationalization

For many enterprises, they will engage with businesses, consumers and employees on an international level. To achieve this brands must operate **multiple sites that contain localized content for the country or region they are serving,** in many cases, they will also be operating sites in multiple languages - a feature that dotCMS provides. Since international organizations will have hundreds, maybe thousands of users, the new SAML plugin can enable you to manage these large number of users into different groups easily. **Each group can be assigned to either a country or region,** depending on the nature of your organization.

06. Better Administration

The SAML plugin comes with its own user interface, which is separate from the host. From this interface, dotCMS administrators can **change SP and IdP configurations and enable and disable user access.** Administrators can make these changes in a matter of a few clicks.

07. Better User Experience

The absence of having to remember multiple username and passwords can allow for a better user experience. **Workers** who need to access multiple sites such as an intranet or B2B portal **can improve their productivity as result of not having to input their username and password each time they log on** to a site, whatever device they're on.

How dotCMS Utilizes the SAML Plugin

The full-featured SAML module that has been developed for dotCMS allows administrators to **utilize a single IdP to centrally manage all dotCMS user access accounts and allow users to access multiple sites** on a single installation.

The primary function of the module is to **save users from having to log into multiple sites to access both content and data.** The automated login feature is activated when a user logs into one participating site that is associated with the dotCMS installation. This allows them to have automatic access to subsequent sites based on their SAML configuration.

Without the SAML module, businesses and organizations who have multiple separate domains and subdomains with encrypted information will have to resort to having to log into each site, hampering productivity as a result.

In a recent dotCMS webinar:
Alex Sterling,
Ethode's Full Stack Developer:

provided a complete demonstration into how to install the SAML plugin from dotCMS' root directory and how to operate the SAML interface.[3]

What Features Are Included in the SAML Module for dotCMS?

Ethode, who helped dotCMS develop the SAML module, have enhanced the plugin to use version 3 of the openSAML Library. In addition, the SAML plugin utilizes OneLogin's open source SAML Java Toolkit to enable SAML support for dotCMS.

When the SAML module is running, it turns dotCMS into an SP, enabling it to connect with various IdPs. **The new SAML module has been extensively tested and is compatible with the three primary IdPs:** Shibboleth, ADFS, and Okta.

01. Shibboleth

is a middleware solution that is primarily used by governments, universities, and public institutions to deliver an **open-source solution for identity management.**

02. ADFS

is Microsoft's Active Directory Federation Service. It runs on Windows Server OS to **provide users with SSO access to various external systems and applications.**

03. Okta

is a third-party enterprise-grade IdP solution that was **built with the cloud in mind.** It is also compatible with many on-premise applications.

Also, the SAML configuration info has moved away from the host content type. The plugin enables dotCMS administrators to edit and configure user permissions via a new, easy-to-use intuitive interface that is separate from the host interface. **Any configurations that are made via the interface are saved onto a JSON file, rather than a content type.** This enables push-publishing to be more safer and secure.

This new interface provides dotCMS administrators with a range of tools to configure SAML properties including enabling and disabling user access and changing both SP and IdP configurations by either per host or globally.

03

Primary IdPs
compatible with the new
SAML module

01 — *Shibboleth*

02 — *ADFS*

03 — *Okta*

Middleware Solurion

To deliver an

Open-Source
Solution

Microsoft's Active Dirextory Federation Service

Provide SSO access to

External
systems & apps

Thrid-part Colution for Cloud

Compatible with

On-Premise
Apps
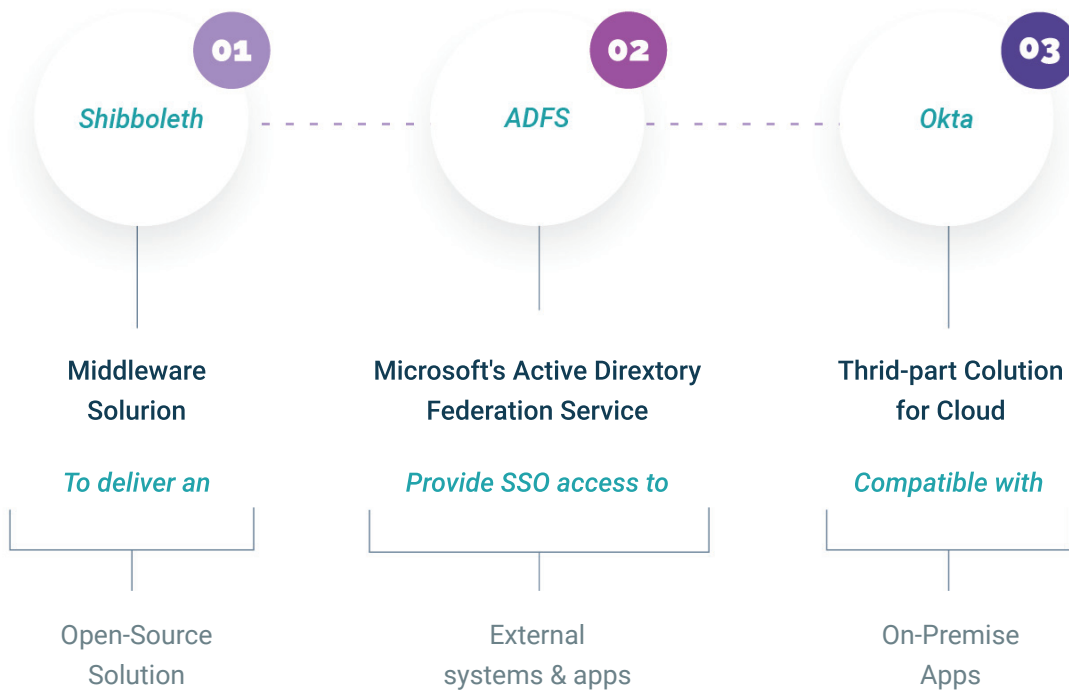
Other notable features of the SAML plugin, as mentioned by Ethode [4], include:

01. **SSO and SLO** (SP-Initiated and IdP-Initiated)

02. **Assertion and nameId encryption**

03. **Assertion signatures**

04. **Message signatures:** AuthNRequest, LogoutRequest, LogoutResponses

05. Enablement of **Assertion Consumer Service endpoint**

06. Enablement of a **Single Logout Service endpoint**

07. **Publishing the SP metadata** (which can also be signed)

The SAML Module That Goes Beyond dotCMS

Besides being able to provide a seamless login experience between all dotCMS developed applications on a single installation, the integration capabilities of dotCMS allows you to extend the SAML plugin to other separate services that utilize the same IdP.

dotCMS is a best-of-breed solution that can integrate with any marketing technology or suite application.

The API-driven environment of dotCMS allows you to easily plug in any tool or functionality, and remove it when not required.

dotCMS has no intentions on being a "jack-of-all-trades" solution, it wanted to allow users to gain access to the best available tools without having to endure a vendor lock-in.

By extending the SAML functionalities to other services beyond dotCMS, brands can further reduce the inconvenience of memorizing multiple credentials, increasing productivity as a result.

Seamless Enterprise-Grade Security at Your Fingertips

To summarise, the new SAML plugin for dotCMS provides both users and administrators the following advantages:

01.

Improved Usability: Users only need one set of credentials to access all dotCMS instances at the same time.

02.

Strong Security: The SAML plugin provides dotCMS with a secure SSO protocol that is trusted by the most security-conscious enterprises, including Google and WebEx.

03.

Integration with Third Parties: dotCMS, with the SAML plugin installed, can integrate with other separate services that are using the same IdP. This minimizes the burden on users even further.

04.

Speed: SAML is fast, requiring only one redirect.

05.

User Management: SAML centralizes user account management and authentication.

SAML plugin's advantages for dotCMS:

01. Improved Usability

02. Strong Security

03. Integration with Third Parties
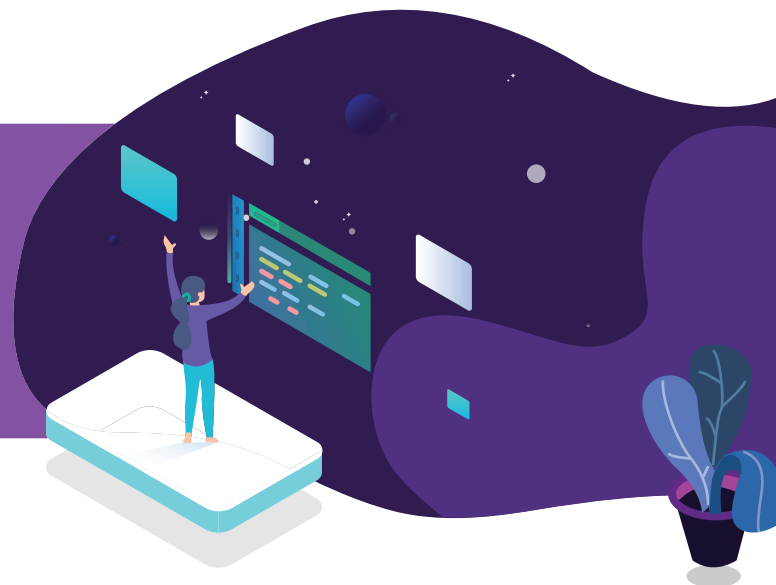
04. Speed

05. User Management

About
dotCMS

Is an open-source Java, customer experience orchestration hub for companies that want to drive business outcomes with their websites and other content-driven applications. dotCMS provides the technology to deliver connected and continuous customer experiences that business teams can orchestrate. **Extensible, scalable, and with headless content management capabilities, organizations can rapidly build their Digital Experience Platform and drive innovation** while their marketing and business teams drive customer experiences for every touchpoint, in every customer journey, on any device — all from a single system.
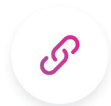
Founded in 2003, dotCMS is a privately owned U.S. company with offices in Miami (Florida), Boston (Massachusetts), and San José (Costa Rica). With a global network of certified implementation partners and an active open-source community, **dotCMS has generated more than a half-million downloads and over 10,000 implementations and integration projects in over 70 countries.** Notable dotCMS customers include: Telus, Standard & Poors, Hospital Corporation of America, Royal Bank of Canada, DirecTV, Nomura Bank, Thomson Reuters, China Mobile, Aon, DriveTest Ontario, and ICANN.

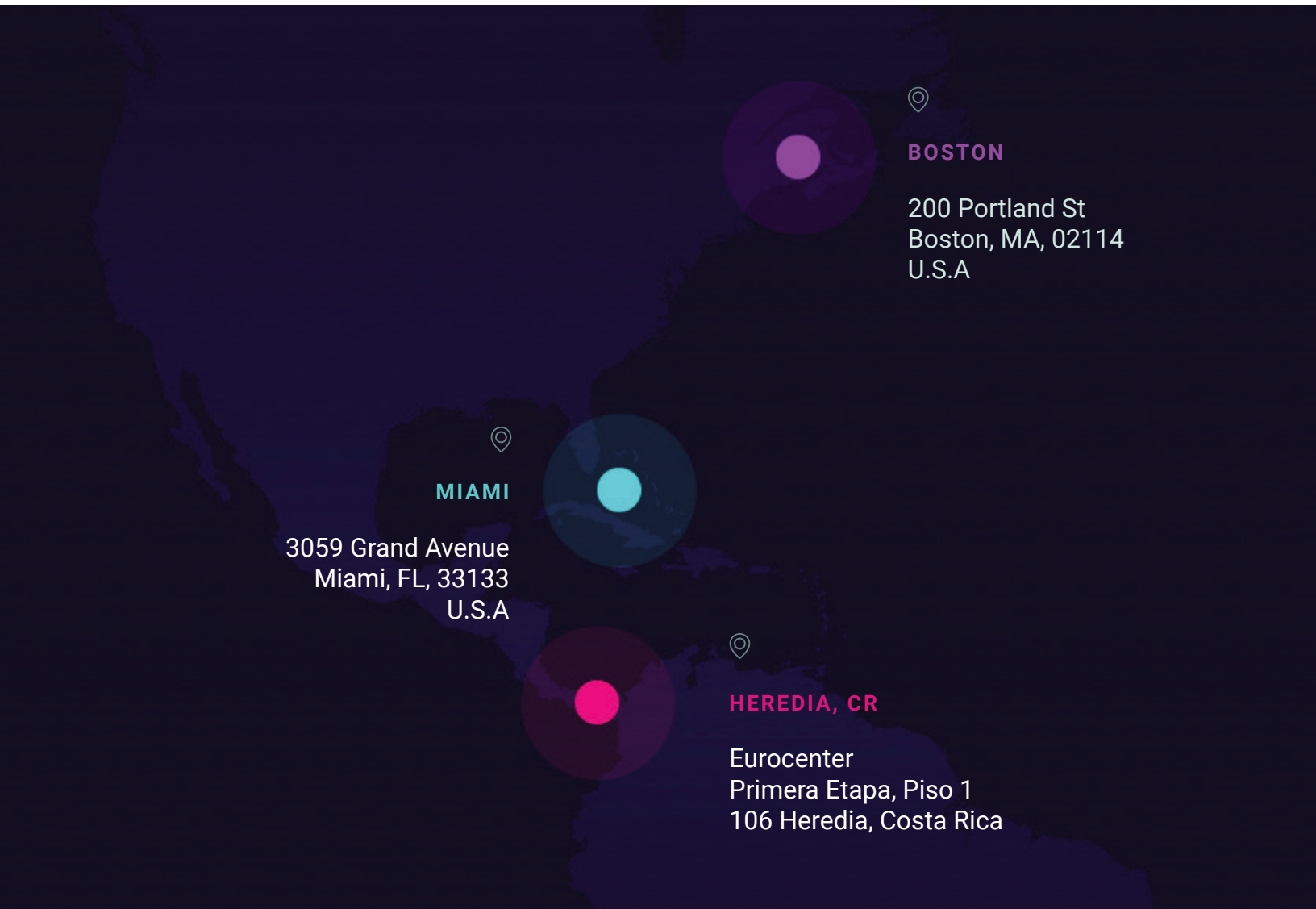### SCHEDULE A
dotCMS demo at dotcms.com

Contact
dotCMS

Web:
dotcms.com

Phone:
+1 - 305 - 900 - 2001

Email:
info@dotcms.com

BOSTON

200 Portland St
Boston, MA, 02114
U.S.A

MIAMI

3059 Grand Avenue
Miami, FL, 33133
U.S.A

HEREDIA, CR

Eurocenter
Primera Etapa, Piso 1
106 Heredia, Costa Rica

About
Ethode

Ethode is a full-cycle web development company headquartered in Northern Ohio with employees across the United States. We specialize in providing Web and Mobile Application architecture, development, testing, and product management services to our clients throughout the U.S.

Ethode was founded by developers that share a passion for quality development. We pride ourselves on customer service, dedication to excellence, and a culture that focuses on innovation and creative problem solving.

{ethode}

Our mission is to use our innovation and creativity to help make the world a more joyous place to live.

Web:
ethode.com

Phone:
(888) 336-3395

Email:
welcome@ethode.com

References

[1] "2017 CEO Survey: CIOs Must Scale Up Digital Business - Centro Computer." http://www.centrocomputer.it/interna/present.nsf/0/0d7bb84dac83a778c12581fe00298aca/$FILE/Gartner%202017%20ceo%20survey.pdf.

[2] "The average enterprise uses 91 marketing cloud services" https://chiefmartec.com/2017/06/average-enterprise-uses-91-marketing-cloud-services/.

[3] "Authenticated Applications & Secure Sign-On Through SAML" - https://www.dotcms.com/landing-pages/webinars/authenticated-applications-secure-sign-on-through-saml-thank-you?submissionGuid=edbb2c1dea24-4891-a0f9-6d6a51ecf4a5

[4] "SAML Module Enables 1-Login for multiple dotCMS sites - Ethode." https://www.ethode.com/blog/saml-module-enables-1-login-for-multiple-dotcms-sites.