

Inhaltsverzeichnis

1. Handbuch:Erweiterung/LDAP Authentication	2
2. Benutzerverwaltung	4
3. Gruppenverwaltung	4
4. Login	4

Handbuch:Erweiterung/LDAP Authentication

Eine [freigegebene Version](#) dieser Seite, [freigegeben](#) am *30. Juli 2020*, basiert auf dieser Version.

LDAP bedeutet Lightweight Directory Access Protocol (leichtgewichtiges Verzeichnisprotokoll). Dies kann zur zentralen Authentifizierung genutzt werden. Diese Erweiterung ermöglicht die Anbindung von BlueSpice (und MediaWiki) an einen LDAP-Server zur zentralen Authentifizierung.

Wichtig! Aufgrund einer Sicherheitslücke bei Active Directory wird dringend die Verwendung einer gesicherten Verbindung (mit SSL/TLS-Verschlüsselung) zur Benutzerauthentifizierung empfohlen. Microsoft veröffentlicht im März 2020 einen Patch, der keine ungesicherten Verbindungen mehr zulässt:

<https://portal.msrc.microsoft.com/de-de/security-guidance/advisory/ADV190023>
<https://support.microsoft.com/de-de/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirement-for-windows>

Betroffen ist jede Software, die LDAP-Abfragen über nicht gesicherte Verbindungen herstellt. Dies betrifft je nach Einstellungen ggf. auch BlueSpice MediaWiki. Sofern Ihr System so konfiguriert ist, dass es bereits eine gesicherte Verbindung verwendet, ist nichts zu tun.

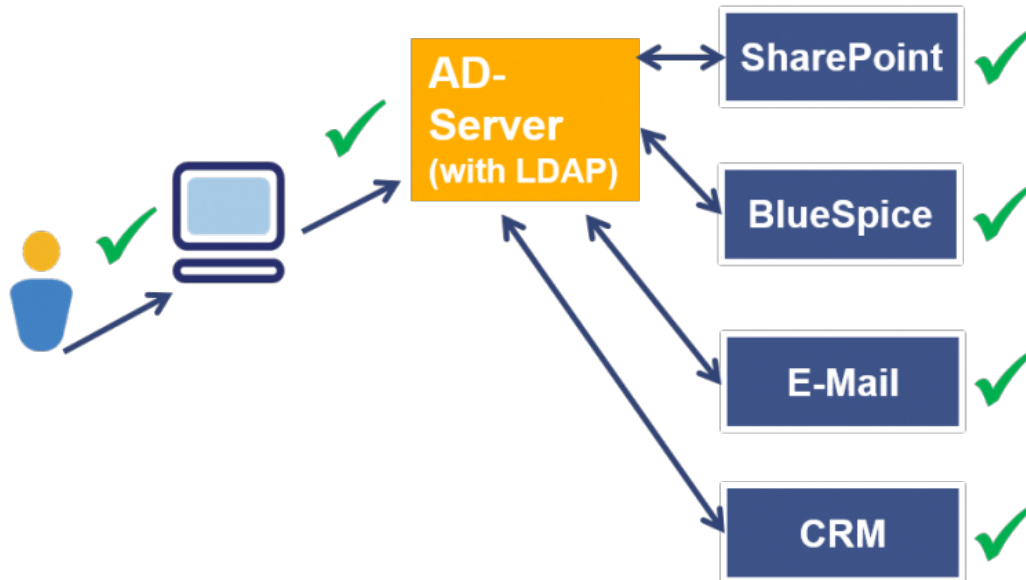
Sollten BlueSpice und Active Directory über eine nicht gesicherte Verbindung kommunizieren, muss das System nachkonfiguriert werden, um erreichbar zu bleiben. Bitte prüfen Sie Ihre Konfigurationen und kontaktieren Sie uns bei Fragen zu diesem Thema.

Inhaltsverzeichnis

1 BlueSpice mit LDAP	3
2 Konfigurationsmöglichkeiten	3
3 Nach der Konfiguration von LDAP zu beachten:	4
4 Weblinks	4

BlueSpice mit LDAP

Die MediaWiki-Erweiterung "[LDAP Authentication](#)" ist standardmäßig in BlueSpice free vorhanden, jedoch **nicht standardmäßig aktiviert**. Um das Wiki an LDAP anzubinden ist eine Aktivierung der Extension und deren Konfiguration notwendig.



Konfigurationsmöglichkeiten

LDAP	Anbindung an ein AD ohne Gruppensynchronisierung
LDAP mit Gruppensynchronisierung	Haben Sie für Ihr Unternehmen bereits definierte Benutzergruppen angelegt, können diese für das Wiki übernommen werden. Die entsprechenden Gruppen sind dann mit dem Gruppennamen automatisch im Wiki vorhanden und Sie können dort noch den Gruppen die entsprechenden Wiki-Rechte zuweisen.
Comfort Sign-on	wie LDAP mit Gruppensynchronisierung Um die Anbindung an eine zentrale Authentifizierung zusätzlich weiter auszubauen, gibt es die Möglichkeit ein Single Sign-On einzurichten. Damit ist der Benutzer direkt bei der Anmeldung am PC auch gleichzeitig am Wiki angemeldet.

Nach der Konfiguration von LDAP zu beachten:

- Das Wiki schreibt nicht in das LDAP-Verzeichnis zurück.
Das bedeutet, dass z.B. Passwortänderungen im Wiki zum Konflikt führen können, im besten Fall aber beim nächsten [Login](#) von LDAP überschrieben werden.
- User dürfen niemals im Wiki händisch angelegt werden, dies führt zum Konflikt, selbst wenn man die Konvention der Groß- und Kleinschreibung der LdapAuthentication befolgt.
- Über die [Benutzerverwaltung](#) lassen sich keine Benutzer im LDAP-Verzeichnis anlegen.
- Standardmäßig findet keine initiale und/oder aktive Synchronisierung mit dem LDAP-Verzeichnis statt. User tauchen erst nach dem erstmaligen Login im Wiki auf.
- Eine Gruppenzuweisung ist über das Wiki möglich.

für die LDAP Konfiguration mit Gruppensynchronisierung gilt zudem:

- Auch hier ist das AD die führende Instanz, d.h. Gruppen werden aus dem AD übernommen.
Vorsicht: Die entsprechende Gruppe muss mit dem identischen Namen, wie sie im AD-Verzeichnis heißt, im [Gruppenmanager](#) des Wikis angelegt werden, um die Gruppenzuweisung zu garantieren.
- Gruppen dürfen im Wiki nicht händisch dem User zugewiesen werden. Nehmen Sie bitte die Zuweisung über das LDAP-Verzeichnis vor.
- Gruppen, denen ein User im LDAP-Verzeichnis nicht angehört, werden ihm im Wiki nicht angezeigt.
- Die Zuweisung des Users zu Gruppen findet während der Login-Routine beim jeweiligen User statt, auch hier gilt: kein automatischer Abgleich mit dem Verzeichnis im Hintergrund.
- Eine Gruppenzuweisung über das Wiki ist nicht möglich. Ausnahmen sind die Gruppen sysop, bot und bureaucrat. Diese können über das Wiki zugewiesen werden und werden auch nicht dem User entzogen.

für die LDAP Konfiguration mit Comfort Sign-on gilt zudem:

- Browservoraussetzungen: kompatibel mit Internet Explorer, Edge und Google Chrome.
- Voraussetzung: Aufruf des Wikis über https, nicht http.
- Die Webseite muss entsprechend dem lokalen Intranet zugewiesen sein (Gruppenrichtlinie)

Weblinks

Dokumentation auf [Mediawiki.org](https://mediawiki.org)

Benutzerverwaltung

Weiterleitung nach:

- [Referenz:BlueSpiceUserManager](#)

Gruppenverwaltung

Weiterleitung nach:

- [Referenz:BlueSpiceGroupManager](#)

Login

Das Wiki ist mit einer Benutzeranmeldung ausgestattet. Je nach Konfiguration des Wikis können sich Nutzer entweder selbständig anmelden oder können nur nach Anmeldung über einen Systemadministrator das Wiki benutzen.

Inhaltsverzeichnis

1	Registrieren und anmelden - muss das sein?	6
2	Vorteile der verpflichtenden Anmeldung	6
3	Erstellung eines Benutzerkontos	6
3.1	Benutzerkonto selbst anlegen	6
3.2	Vergabe des Benutzerkontos durch Administratoren	7
3.3	Anmeldung mit Captcha	7
4	So melde ich mich an	8
5	So melde ich mich ab - Logout	9

Registrieren und anmelden - muss das sein?

In einem öffentlichen Wiki ist das Anlegen eines Benutzerkontos generell überflüssig. Oft ist ein Wiki jedoch eine Plattform für spezielle Interessenten, Gruppen oder Firmen. Nicht jeder soll bei so einem Wiki mitschreiben dürfen bzw. ist es gerade bei Unternehmen auch wichtig, dass von Extern gar kein Zugriff auf das Wiki stattfinden darf. Selbst bei öffentlichen Wikis ist es oft notwendig, dass gewisse Bereiche vor Veränderungen geschützt werden. Dadurch wird ein Rechtemanagement und damit auch eine Anmeldung mit einem Benutzerkonto notwendig. Dementsprechend ergeben sich verschiedene Varianten für die Anmeldung:

- Anmeldung ist *nicht* notwendig
- Anmeldung ist *notwendig*, der Benutzer kann *sich selbst registrieren*
- Anmeldung ist *notwendig*, der Benutzer wird *durch einen Administrator registriert*

Vorteile der verpflichtenden Anmeldung

Mit einem Benutzerkonto erhalten Sie Zugriff auf wichtige Funktionen:

- Eine Benutzerseite, auf der Sie sich vorstellen können. Diese ist verknüpft mit einer Diskussionsseite, auf der andere mit Ihnen Kontakt aufnehmen können.
- Eine [Beobachtungsliste](#), die Änderungen an Artikel anzeigt, die einen besonders interessieren.
- Die Möglichkeit, die eine [Anpassung der Funktionalität](#) von BlueSpice Wiki an Ihre Bedürfnisse ermöglicht.
- Eine [Signatur](#), um in Diskussionen mit Ihrem Namen zu unterschreiben.

Erstellung eines Benutzerkontos

Abhängig von der Konfiguration Ihres Wikis gibt es verschiedene Möglichkeiten, ein Benutzerkonto zu registrieren. Wenden Sie sich an Ihren Wiki-Administrator, um zu erfahren, wie Sie in Ihrem Fall ein Konto erstellen.

Benutzerkonto selbst anlegen

Wir nennen ein Wiki, für das Benutzer ihr Konto selbst anlegen können, *halb-offen*.



Anmelden

Du hast kein Benutzerkonto? [Neues Benutzerkonto anlegen.](#)

Zur Anmeldung müssen Cookies aktiviert sein.

Benutzername:

Passwort:

Mit diesem Browser dauerhaft angemeldet bleiben (maximal 180 Tage)

[Die Anmeldedaten vergessen?](#)

Über den *Link Neues Benutzerkonto anlegen* gelangt man zum Registrierungsformular. Notwendige Angaben hierfür sind

- Benutzername
- Passwort (und Wiederholung des Passwortes)
- E-Mail-Adresse

Vergabe des Benutzerkontos durch Administratoren

Die andere Möglichkeit ist die eines geschlossenen Wikis, d.h. es werden Benutzer nur durch einen Administrator zugelassen. Dieser legt das Konto für die Benutzer über die [Benutzerverwaltung](#) an und sendet die Zugangsdaten per Email. Mit diesen Daten können sich Nutzer dann anmelden und nachträglich das vom Admin gesetzte Passwort ändern.

Anmeldung mit Captcha

Viele Wikis kämpfen mit Spam. Um bei der Anmeldung schon die ersten Maßnahmen gegen nicht-menschliche Bots zu treffen, kann ein CAPTCHA eingebaut werden. Neben den normalen Angaben kann der Benutzer optional auch seinen bürgerlichen Namen, zusätzlich zu seinem gewählten Nutzernamen, angeben. Eine Bestätigung von z.B. **Nutzungsbedingungen** für das Wiki kann ebenfalls abgefragt und durch Setzen eines Häkchens gefordert werden.

Benutzerkonto anlegen

Haben Sie bereits ein Benutzerkonto? [Anmelden](#).

Zum Schutz gegen die automatisierte Erstellung von Benutzerkonten bitten wir Sie, die folgenden beiden Wörter in das untenstehende Feld einzugeben:



Benutzername:

Passwort:

Passwort wiederholen:

E-Mail-Adresse:

Die Angabe einer E-Mail-Adresse ist optional, ermöglicht aber die Zusendung eines Ersatzpasswortes, sofern Sie Ihr Passwort vergessen haben.

Bürgerlicher Name:

Optional. Damit kann Ihr bürgerlicher Name Ihren Beiträgen zugeordnet werden.

Hiermit akzeptiere ich die [Nutzungsbedingungen](#)

Mit diesem Browser dauerhaft angemeldet bleiben (maximal 180 Tage)

Nach Abschluss des Registrierungsprozesses bekommen Benutzer eine automatische Mail zur **Verifizierung der Angaben** zugesandt. Damit wird verhindert, dass sich Nutzer mit falschen Mail-Adressen registrieren. Nach Bestätigung über den darin enthaltenen Link ist die Anmeldung im Wiki möglich.

So melde ich mich an

Ist nun ein Benutzerkonto angelegt, ist die Anmeldung über den Anmelde-Link im Hauptmenü möglich.

Hinweis: Hierfür müssen Browser-Cookies zugelassen sein.

Anmeldung via LDAP und Single Sign-on

Mit BlueSpice besteht grundsätzlich die Möglichkeit der Anbindung an Active Directory / LDAP. BlueSpice free enthält dazu die Erweiterung [LDAPAuthentication](#).

Ebenso ist mit BlueSpice ein Single Sign-on möglich: Mit diesem Verfahren muss sich der Benutzer z.B. einer Firma nicht mehr im Wiki anmelden. Die Anmeldung erfolgt automatisch mit der Authentifizierung am Computer des Arbeitsplatzes.

So melde ich mich ab - Logout

Die Abmeldung erfolgt über das Benutzermenü in der Kopfleiste:

