Salesforce

Tolleiv Nietsch - 2024-09-09 - Applikation verbinden

Was ist „Salesforce“?

Salesforce ist eine führende cloudbasierte Kundenbeziehungsmanagement (CRM)-Plattform, die von Unternehmen verwendet wird, um Kundenbeziehungen zu verwalten, Vertriebsprozesse zu optimieren und Geschäftsinformationen zu zentralisieren. Die Anwendung bietet eine breite Palette von Tools und Funktionen, darunter:

- Kontaktverwaltung
- Vertriebsautomatisierung
- Marketingautomatisierung
- Kundensupport
- Analytik und Berichterstattung

Unternehmen nutzen Salesforce, um Kundenkontakte zu verfolgen, Verkaufschancen zu managen, Marketingkampagnen zu steuern, Kundenservice zu verbessern und Daten zu analysieren, um bessere Geschäftsentscheidungen zu treffen. Salesforce erleichtert die Zusammenarbeit im Team und die Integration von verschiedenen Geschäftsprozessen, was es zu einem wichtigen Werkzeug für Unternehmen jeder Größe und Branche macht.

Bare.ID-Instanz mit „Salesforce“ verbinden

- Die vorkonfigurierte Verbindung macht die Integration von Salesforce in Bare.ID besonders einfach. Abschließend muss Bare.ID nur noch als Login-Provider in der Salesforce -Applikation hinterlegt werden.

Salesforce als Applikation mit Bare.ID verbinden

- Melde Dich mit einem Administrator-Konto bei Bare.ID unter app.bare.id an.
- Wähle auf der Willkommensseite die Instanz aus, für die Salesforce als Applikation verbunden werden soll.
- Klicke in der Navigation links auf "Applikationen".

- Klicke auf den Button "**APPLIKATIONEN VERBINDEN**".

Es öffnet sich die Seite "**APPLIKATIONEN VERBINDEN**" mit einer Übersicht an Applikationen, die bereits vorkonfiguriert sind

- Wähle die Salesforce-Applikation durch Klick auf das entsprechende Icon.

Es öffnet sich die Seite "Salesforce verbinden"

- Setze alle Optionen und fülle die Felder wie gewünscht:

- **Client ID:** Trage eine eindeutige Client-ID ein. Diese muss beim Einrichten in Personio eingetragen werden.
- **Beschreibung:** Füge eine kurze Beschreibung für die Verbindung hinzu, um sie bei der Verwaltung besser identifizieren zu können.
- Option **Zugriff beschränken:** Setze den Schalter aktiv, um nur Nutzern der Bare.ID-Instanz eine Anmeldung an Personio zu ermöglichen, die über die entsprechende applikationsspezifische Rolle verfügen.

- Option **Verbindung aktiviert**: Aktiviere oder deaktiviere die Verbindung zur Applikation. Lasse die Option zum Testen der Verbindung aktiv. Nur im aktiven Zustand können sich Nutzer über Bare.ID an der Applikation anmelden.
- **Client Secret:** Ein sicheres Passwort wird nach dem Speichern automatisch generiert. Dieses muss beim Einrichten in Personio eingetragen werden.
- **Instanz-Name:** Trage den Namen der Personio-Instanz aus der URL ein. Bei "https://mycompany.personio.de/" also "mycompany".
- Klicke auf den "SPEICHERN"-Button, um die Angaben zu speichern und die ausgewählte Applikation mit der ausgewählten Bare.ID-Instanz zu verbinden.

Nach dem erfolgreichen Speichern der Verbindung wird die Erfolgsmeldung "Applikation hinzugefügt" eingeblendet. Die Verbindung zur Applikation wird jetzt in der Übersichtsliste aller Applikationen aufgeführt und kann zur Bearbeitung ausgewählt werden.

Bare.ID in Salesforce konfigurieren

Aktivieren Sie Salesforce als Identitätsanbieter

1. Legen Sie fest, welches Zertifikat Sie verwenden möchten, um die Kommunikation zwischen Ihrer Organisation und dem Serviceanbieter zu ermöglichen. Sie können das Standardzertifikat verwenden oder ein eigenes erstellen. Siehe Zertifikate und Schlüssel.
    - Standardmäßig verwendet ein Salesforce-Identitätsanbieter ein selbstsigniertes Zertifikat, das mit dem SHA-256-Signaturalgorithmus generiert wurde. Fahren Sie mit Schritt 2 fort, wenn Sie das Standardzertifikat verwenden möchten.
    - Wenn Sie ein neues selbstsigniertes Zertifikat erstellen möchten, befolgen Sie die Anweisungen unter Generieren eines selbstsignierten Zertifikats und fahren Sie dann mit Schritt 2 fort.
    - Befolgen Sie zum Erstellen eines von einer Zertifizierungsstelle signierten Zertifikats die Anweisungen im Thema Generieren eines von einer Zertifizierungsstelle signierten Zertifikats in der Salesforce-Hilfe und fahren Sie dann mit Schritt 2 fort.
2. Geben Sie unter "Setup" im Feld "Schnellsuche" den Text

Identitätsanbieter
ein und wählen Sie dann **Identitätsanbieter** aus.

3. Klicken Sie auf **Identitätsanbieter aktivieren**.
4. Wählen Sie im Dropdown-Menü ein Zertifikat aus.
5. Speichern Sie Ihre Änderungen.

Erfüllen Sie die Voraussetzungen zum Integrieren von Serviceanbietern.

Geben Sie Ihrem Serviceanbieter Informationen zu Ihrer Konfiguration von Salesforce als Identitätsanbieter. Je nachdem, was von Ihrem Serviceanbieter unterstützt wird, können Sie diese Informationen als Metadaten in einer XML-Datei oder als Zertifikat freigeben. Führen Sie zum Zugreifen auf diese Informationen die folgenden Schritte aus.

1. Geben Sie unter "Setup" im Feld "Schnellsuche" den Text Identitätsanbieter ein und wählen Sie dann **Identitätsanbieter** aus.
2. Klicken Sie auf **Metadaten herunterladen**, sofern von Ihrem Serviceanbieter Metadaten unterstützt werden. Klicken Sie auf **Zertifikat herunterladen**, sofern von Ihrem Serviceanbieter Zertifikate unterstützt werden.

Rufen Sie die Konfigurationsinformationen von Ihrem Serviceanbieter ab:

- ACS-URL (Assertion Consumer Service): Der URL, unter dem der Identitätsanbieter SAML-Antworten sendet.
- Einheiten-ID: Die eindeutige Kennung des Serviceanbieters.
- Thematyp: Gibt an, wo entsprechend der Erwartung des Serviceanbieters Salesforce Benutzeridentitätsinformationen in SAML-Behauptungen sendet. Salesforce kann Benutzerinformationen im Betreff der Behauptung oder in einem benutzerdefinierten Attribut senden.
- Sicherheitszertifikat: Erforderlich, wenn der Serviceanbieter die Anmeldung über Salesforce initiiert und seine SAML-Anforderungen signiert.

Konfigurieren Sie die erzwungene Authentifizierung, um zusätzlichen Schutz für vertrauliche Ressourcen hinzuzufügen. Bei der erzwungenen Authentifizierung müssen Benutzer, die bereits bei Salesforce angemeldet sind, ihre Anmeldeinformationen erneut eingeben, wenn sie versuchen, auf einen Serviceanbieter zuzugreifen.

Geben Sie eine akzeptierte SAML-Anforderung zur erzwungenen Authentifizierung an Ihren Serviceanbieter weiter, um die erzwungene Authentifizierung zu konfigurieren. Über diese Anforderung informiert der Serviceanbieter Salesforce, dass sich der Benutzer neu authentifizieren muss. Es gibt kein zusätzliches Setup in Ihrer Organisation. Wenn

Salesforce als Identitätsanbieter fungiert, wird die erzwungene Authentifizierung automatisch unterstützt.

Integrieren Sie Ihren Serviceanbieter als SAML-aktivierte verbundene Anwendung.

Ordnen Sie den Benutzern der verbundenen Anwendungen die Salesforce-Benutzer zu.

1. Geben Sie unter "Setup" im Feld "Schnellsuche" den Text Benutzer ein und wählen Sie dann **Benutzer** aus.
2. Suchen Sie nach dem gewünschten Benutzer und klicken Sie neben dem Namen auf **Bearbeiten**.
3. Geben Sie unter "Single Sign-On-Informationen" in Verbund-ID einen Kennzeichner ein, der vom Serviceanbieter erkannt werden kann. Geben Sie beispielsweise den Benutzernamen ein, der für die Anmeldung beim Serviceanbieter verwendet werden soll.
4. Speichern Sie Ihre Änderungen.

Bare.ID ist jetzt als Login-Provider für Salesforce eingerichtet.