So richten Sie die SAML-Integration zwischen der Blancco Management Console \ Blancco Cloud und Azure AD ein

Erstellungsdatum	Update Datum	betroffene Version	Fix version
10-10-2022		Management Console 5.2.0 or newer	

Beschreibung

In diesem Artikel werden wir uns die erforderlichen Schritte zur Einrichtung der SAML-Integration in der Management Console/Blancco Cloud und Azure AD ansehen.

Bevor wir uns mit den Einrichtungsschritten befassen, werden wir einige der Informationen/Details hervorheben, die als Teil dieser Einrichtung erforderlich sind, sowie einige Voraussetzungen.

SAML: Security Assertion Markup Language ist ein offener Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Parteien, insbesondere zwischen **einem Identity Provider** und **einem Service Provider**. SAML ist eine XML-basierte Auszeichnungssprache für Sicherheitsaussagen.

SAML SSO: SAML Single Sign-On ist ein Mechanismus, der SAML nutzt und es den Benutzern ermöglicht, sich bei mehreren Webanwendungen anzumelden, nachdem sie sich beim Identitätsanbieter angemeldet haben. Der Benutzer muss sich nur einmal anmelden. SAML SSO bietet eine schnellere, nahtlose Benutzererfahrung.

Identity Provider - Führt die Authentifizierung durch und übergibt die Identität und Berechtigungsstufe des Benutzers an den Dienstanbieter..

Service Provider - vertraut dem Identitätsprovider und autorisiert den angegebenen Benutzer für den Zugriff auf die angeforderte Ressource.

BMC SAML-Integration: Um die Azure AD SAML-Integration mit Blancco Cloud/Local BMC durchführen zu können, sind folgende Voraussetzungen erforderlich:

- **Blancco Cloud**:
  - Identity Provider, der das SAML-Protokoll verwendet, z. B. Azure AD.
  - Identity Provider Metadata als XML file.
  - Domain Name, e.g. Blancco.com

- **Local BMC**:
  - SSO-Zertifikat des Identity provider, das in eine JKS-Datei importiert wird, d. h. eine JKS-Datei, die die Signatur des Identity provider enthält nur erforderlich, wenn die Option "Signierte Authentifizierungsanforderung" bei der Erstellung der Metadaten-XML-Datei und des Identity provider-Zertifikats aktiviert ist.

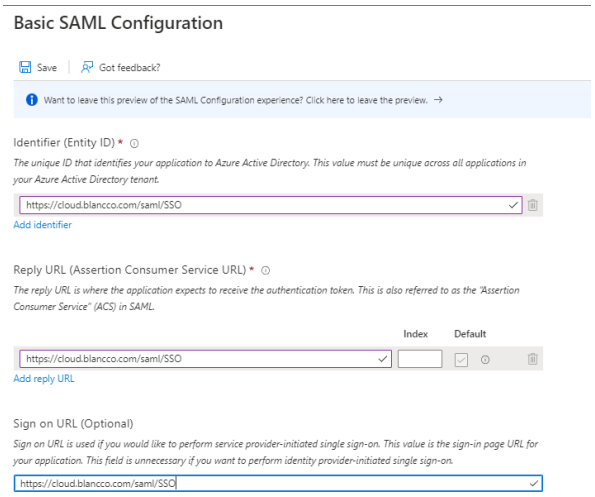
Schritt für Schritt Anleitung

Bevor Sie Änderungen in der Blancco Cloud/Blancco Management Console vornehmen, müssen Sie zunächst ein SSO-Zertifikat und XML-Metadaten generieren. Die folgenden Informationen beschreiben die Schritte, die für die Generierung erforderlich sind.

SSO-Zertifikat und XML-Metadaten-Datei generieren - Alle folgenden Schritte müssen im Microsoft Azure Admin-Konto ausgeführt werden:

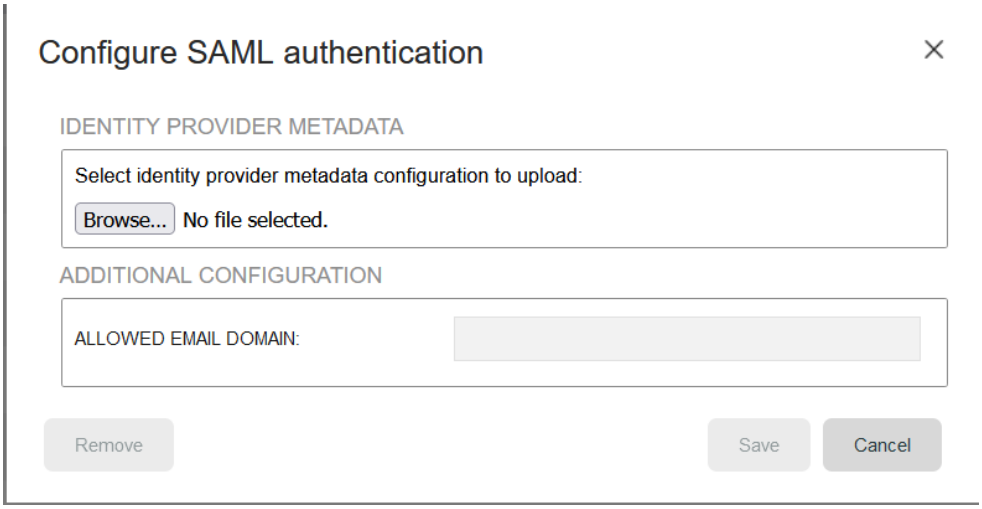
Melden Sie sich bei Ihrem Microsoft Azure-Konto an.

- Navigieren Sie zu Azure Active Directory Unternehmensanwendung Neue Anwendung Nicht-Galerie-Anwendung Fügen Sie Ihre eigene Anwendung hinzu Geben Sie der Anwendung in diesem Schritt einen Namen, z. B: Cloud Blancco Hinzufügen.
- Navigieren Sie nun zu der im obigen Schritt neu hinzugefügten Anwendung "Cloud Blancco" Klicken Sie auf Benutzer und Gruppe Benutzer hinzufügen Fügen Sie hier Benutzer hinzu, um den Zugriff für die SAML-Authentifizierung zu ermöglichen.
- Unter dem Abschnitt Verwalten für die Anwendung "Cloud Blancco" Wählen Sie "Single Sign On" Wählen Sie SAML Geben Sie die erforderlichen Details an, um die Metadaten-XML-Datei und das Zertifikat zu erzeugen.
- Erforderliche Details sind - Siehe beigefügten Screenshot als Referenz, die unten stehende URL ist korrekt, wenn Sie die Blancco Cloud verwenden, wenn Sie SAML mit einer lokal installierten Management-Konsole einrichten, passen Sie bitte die URL an, um auf Ihre Management-Konsolen-Installation zu verweisen.
  - Entity ID: https://cloud.blancco.com/saml/SSO
  - Reply URL: https://cloud.blancco.com/saml/SSO
  - SignOn URL: https://cloud.blancco.com/saml/SSO

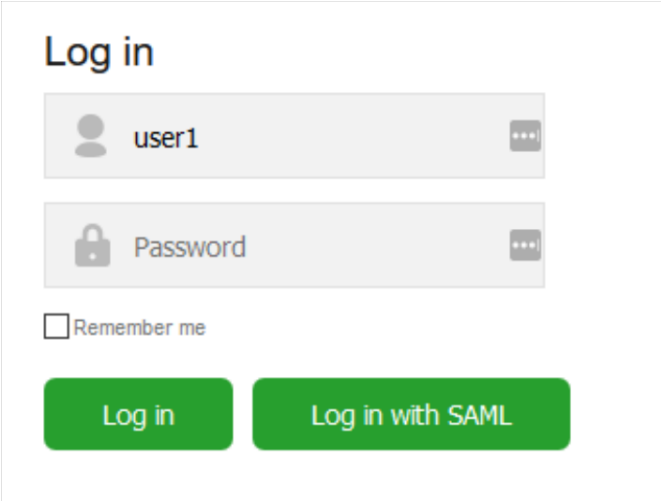


- Benutzerattribute und Ansprüche: Attribute/Ansprüche sind für Blancco Cloud nicht anwendbar, also überspringen Sie diese Einstellung.
- Es ist nicht möglich, die "signierte Authentifizierungsanfrage" mit der Blancco Cloud zu verwenden. Stellen Sie daher sicher, dass Sie die Option "signierte Authentifizierungsanfrage" deaktivieren, bevor Sie die Metadaten-Datei für die Verwendung mit der Blancco Cloud erstellen.
- Erstellen Sie nun die XML-Metadaten und die Zertifikatsdatei auf dem lokalen Rechner und fügen Sie die XML-Datei zur Blancco Cloud hinzu (https://cloud.blancco.com)

- Melden Sie sich bei der Blancco Cloud/Blancco Management Console mit einem Benutzerkonto an, das über Manager/Admin-Berechtigungen verfügt.
- In der Hauptgruppe -> Klicken Sie auf Gruppe verwalten -> SAML-Konfiguration.
  - Hochladen der Datei "Metadata.xml
  - Domänenname angeben.



  - Einstellungen Speichern
- Melden Sie sich vom Manager/Admin-Benutzerkonto ab und melden Sie sich mit einem Standard-Benutzerkonto an, indem Sie die jetzt angezeigte Schaltfläche Login with SAML verwenden



Zusätzliche Schritte für die Einrichtung der lokalen Managementkonsole

Wenn Sie die Option "Signierte Authentifizierungsanfrage" mit einer lokal installierten Management-Konsole verwenden, müssen auch die folgenden Schritte ausgeführt werden.

- Um SAML SSO Login mit Local BMC zu integrieren, wenn "Signed Authentication request" deaktiviert ist, kann der obige Abschnitt "Step by Step instruction" für die Integration verwendet werden.
- Wenn "Signierte Authentifizierungsanfrage" aktiviert ist, dann:
  - Kopieren Sie die JKS-Datei in das BMC-Installationsverzeichnis Obligatorisch, damit MC die Signaturschlüssel erkennt und lädt und sie in der SAML-Signatur verwendet.

Schritt-für-Schritt-Anleitung zur Erstellung einer JKS-Datei:

1. Führen Sie den folgenden Befehl im Verzeichnis JAVA HOME/bin aus, um eine JKS-Datei zu erstellen:
   a. keytool -genkeypair -alias my-service-provider -keypass password -keyalg RSA -keysize 2048 -keystore my-sso-keystore.jks
2. Importieren Sie das SAML SSO-Zertifikat in die JKS-Datei - Um die SSO-Zertifikatsdatei zu erhalten, folgen Sie dem Abschnitt "**So erzeugen Sie ein SSO-Zertifikat und eine XML-Metadaten-Datei**".
   a. keytool -import -trustcacerts -alias sso -file ./sso.crt -keystore ./my-sso-keystore.jks
3. Nach erfolgreichem Import - Kopieren Sie die JKS-Datei in das MC-Installationsverzeichnis.