Red Hat Single Sign-On 7.4

リリースノート

Red Hat Single Sign-On 7.4 向け

Last Updated: 2023-08-23

Red Hat Single Sign-On 7.4 リリースノート

Red Hat Single Sign-On 7.4 向け

法律上の通知

概要

このガイドは、Red Hat Single Sign-On のリリースノートとして作成されています。

目次

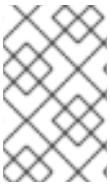
多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

第1章 RED HAT SINGLE SIGN-ON 7.4.0.GA

1.1. 概要

Red Hat は、Red Hat Single Sign-On (RH-SSO) のバージョン 7.4 のリリースを発表します。RH-SSO は Keycloak プロジェクトをベースとしており、OpenID Connect、OAuth 2.0、SAML 2.0 などの一般的な標準仕様に基づいて Web SSO 機能を提供することで、Web アプリケーションのセキュリティーを保護します。RH-SSO サーバーは OpenID Connect または SAML ベースの ID プロバイダー (IdP) として機能し、エンタープライズユーザーディレクトリーまたはサードパーティー IdP が標準仕様ベースのセキュリティートークンを使用してアプリケーションを保護できるようにします。



注記

IBM Z および IBM Power Systems 向けの Red Hat Single Sign-On は、OpenShift 環境でのみサポートされます。IBM Z および IBM Power Systems でのベアメタルインストールはサポートされていません。

以下の注記は RH-SSO 7.4 リリースに適用されます。

1.2. 新機能または改善された機能

1.2.1. 認証の改善

RH-SSO は、WebAuthn (W3C Web Authentication) のサポートを提供するようになりました。WebAuthn のサポートを追加すると、認証フロー設定および認証情報管理がよりリファクタリングされるようになります。この変更により、管理者は認証フローを設定する際の柔軟性と、希望する認証方法を選択する際の柔軟性が向上します。

認証および認証情報管理の改善により、さまざまな利点があります。

1.2.1.1. 二要素認証

管理者が二要素認証を設定し、二要素認証に複数の選択肢を選択することが簡単になりました。たとえば、管理者は、OTP と WebAuthn を認証フローの選択肢として設定できます。これにより、ユーザーは認証中にこれらのメカニズムを選択できます。

1.2.1.2. パスワードレス認証

管理者は、簡単に、パスワードレス認証を設定できるようになりました。この機能は、二要素認証メカニズムおよびパスワードレス認証メカニズムとして使用できる WebAuthn に便利です。パスワードがないと、認証中に WebAuth で認証を行うユーザーはパスワードを指定する必要はありません。パスワードレスと二要素認証を簡単に組み合わせることができます。

1.2.1.3. ID ファースト認証

管理者は、認証中にユーザーが最初のフォームにユーザー名のみを提供できるように認証フローを設定できます。RH-SSO はターゲットユーザーの推奨認証メカニズムを検出し、それを基に認証フォームを表示することができるため、この変更により柔軟性が向上します。

1.2.1.4. 条件付きオーセンティケーター

RH-SSO は、認証フローの特定の場所に条件を追加できます。そのため、指定した条件が満たされる場

合に限り、ユーザーは認証メカニズムで認証する必要があります。これは、たとえば、特定のロールのメンバーに二要素認証が必要であることを示しています。もう 1 つの例は、2 要素認証情報が設定されたユーザーに二要素認証メカニズムが必要であることです。

1.2.1.5. OPTIONAL 認証実行要件への変更

条件付きオーセンティケーターを追加することで、認証実行の OPTIONAL 要件を削除できました。条件付きオーセンティケーターはより柔軟で、OPTIONAL 認証要件で以前に許可されたすべてのサポートを可能にします。OPTIONAL 認証実行を使用する場合、認証フローは自動的に移行されます。

詳細は、アップグレードガイド を参照してください。

1.2.1.6. 認証情報の管理

RH-SSO データベースに保存されているユーザー認証情報の形式が変更になりました。また、複数の OTP 認証情報や複数の WebAuthn 認証情報など、すべてのユーザーが同じタイプの複数の認証情報を持つこともできます。認証時に、使用する認証情報と認証メカニズムを選択できます。

管理者は、特定のユーザーの認証情報と、ターゲット認証情報に関連付けられパブリックメタデータを確認できます。たとえば、管理者はユーザーパスワードのハッシュ化に使用したハッシュアルゴリズムを確認できます。管理者は、一部のユーザー認証情報を削除したり、一部の認証情報の優先度を変更したりして、ターゲットユーザーに対して優先されるようにすることができます。

1.2.1.7. ユーザーの認証情報管理

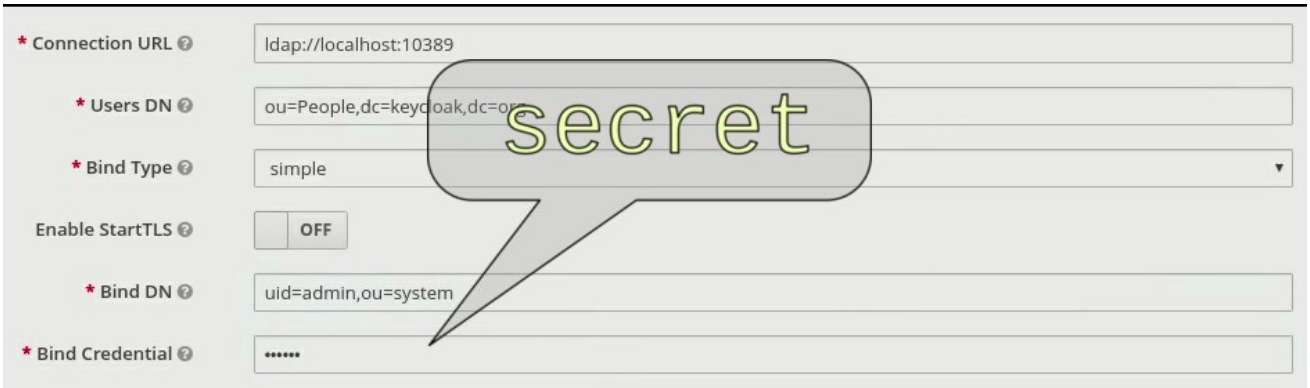
ユーザーは、アカウントコンソールですべての認証情報を表示し、認証情報を追加または削除できます。テクノロジープレビュー機能である新規アカウントコンソールセクションを参照してください。現在サポートされているアカウントコンソールのユーザーアカウントサービスは、この機能をサポートしません。以前の RH-SSO バージョンと同様の方法で OTP をサポートします。

詳細は サーバー管理ガイド の 認証フロー を参照してください。

1.2.2. シークレットの Vault

本リリースでは、RH-SSO はシークレットを保存し、取得するための Vault を追加します。Vault は、セキュアな自動アクセスを提供し、クリアテキスト値のストレージを除外します。Vault を使用すると、データベースには実際のシークレットではなく Vault エントリーへの参照が含まれます。また、Vault を使用することで、RH-SSO 管理者から Vault 管理者へのシークレットの管理が行われます。

複数の設定フィールドには、ユーザーが直接値を入力する必要があるのではなく、外部 Vault から値を取得できます。フィールドは LDAP バインドパスワード、SMTP パスワード、およびアイデンティティープロバイダーシークレットです。



RH-SSO は、OpenShift シークレット、Elytron 認証情報ストア、またはカスタム Vault からシークレットを読み取る機能を提供します。

1.2.2.1. OpenShift Vault

RH-SSO は、OpenShift シークレットの Vault 実装をサポートします。これらのシークレットはデータボリュームとしてマウントでき、フラットなファイル構造を持つディレクトリーとして表示され、各シークレットはシークレット名の付いたファイルで表され、そのファイルの内容はシークレットの値になります。

1.2.2.2. Elytron 認証情報ストア

RH-SSO には、キーストアベースの Elytron 認証ストアからシークレットを読み取る新しい組み込み Vault プロバイダーが含まれます。認証情報ストアの作成および管理は、Elytron サブシステムまたは elytron-tool.sh スクリプトを使用して Elytron によって処理されます。

1.2.2.3. カスタム Vault

Vault SPI が導入され、拡張機能がカスタム Vault からシークレットにアクセスできるように導入されました。

詳細は サーバー管理ガイド および サーバー開発者ガイド を参照してください。

1.2.3. WebAuthn (プレビュー)

RH-SSO は、W3C Web Authentication (WebAuthn) の限定的なサポートを提供します。これは WebAuthn の Relying Party (RP) として機能します。

WebAuthn が有効な場合、管理者は WebAuthn ポリシーを設定できます。これにより、管理者は使用できる WebAuth オーセンティケーターデバイスと、それに必要な証明書を制限できます。管理者は、WebAuthn の 2 要素オーセンティケーターまたは WebAuthn パスワードレス認証に異なる設定を設定できます。管理者は、特定のユーザーに WebAuthn 認証情報の設定や認証フローの設定を要求することを許可されています。これは、WebAuth 認証がすべてのユーザーに必要になるか、2 要素メカニズムなどとして許可されるようにするためです。上記のリリースノートの認証の改善セクションで説明されているように、この分野には多くの柔軟性があります。

注記

WebAuthn はテクノロジープレビューであるため、完全にサポートされていません。この機能はデフォルトでは無効になっています。この機能の成功は、オーセンティケーター、ブラウザー、およびプラットフォームをサポートするユーザーの WebAuthn によって異なります。この WebAuthn サポートを使用する場合は、これらのエンティティーが WebAuthn 仕様をサポートするエクステントを明確にしてください。

ユーザーは、次のセクションで説明されているように、新しいアカウントコンソールでのみ WebAuthn 認証情報を管理できます。

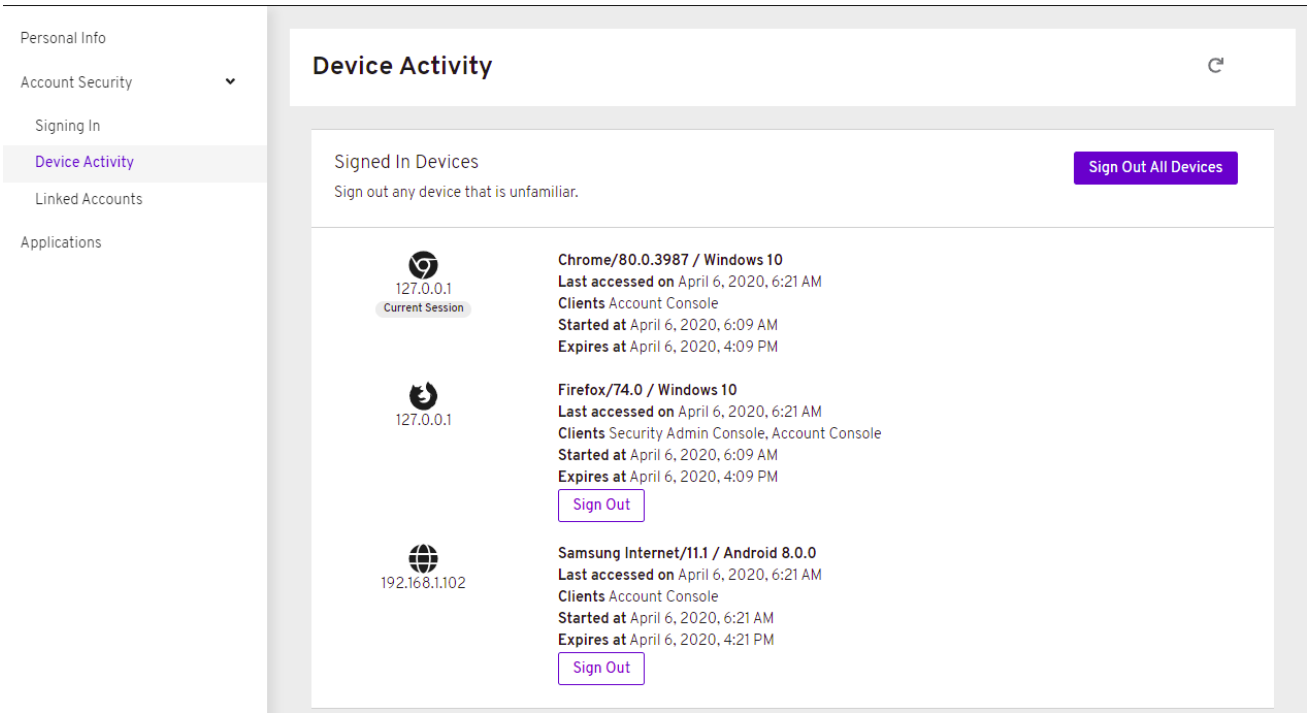
1.2.4. 新規アカウントコンソール (プレビュー)

ユーザーアカウントサービスは、テクノロジープレビューにおける新規のアカウントコンソールとして大幅に改善されています。既存のユーザーアカウントサービスは引き続きサポートされます。

試しにこのコンソールを使用するには、以下を行います。

1. システムプロパティーを使用して RH-SSO サーバーを起動し、新規の Account Console および新しい Account REST API を有効にします。
   standalone -Dkeycloak.profile.feature.account_api=enabled -Dkeycloak.profile.feature.account2=enabled
2. 管理コンソールにログインします。
3. レルム設定、テーマを選択します。
4. Account Theme を **rhsso-preview** に変更します。

Manage Account を選択すると、新しいアカウントコンソールが表示されます。以下はサンプルの画面です。



この新しいコンソールは、React および PatternFly 4 をベースにしています。これにより、PatternFly CSS 変数 を使用して簡単なスタイルすることができます。また、ページを削除し、独自のページを追加することもできます。完全なドキュメントは今後のリリースで提供されます。

1.2.5. 新しいデフォルトホスト名プロバイダー

この新しいデフォルトホスト名プロバイダーにより、以下の改善点が追加されました。

- プロバイダーを固定ベース URL に変更する必要はありません。
- フロントエンドおよびバックエンドリクエストの異なるベース URL のサポート
- RH-SSO がリバースプロキシーを介して異なるコンテキストパスで公開される場合のコンテキストパスの変更のサポート

1.2.6. その他の改善

RH-SSO には、本リリースで追加のマイナーリリース機能が含まれています。これらの機能のほとんどは、Financial-grade API (FAPI) のサポートに関連する高度な OpenID Connect/OAuth2 の概念およびアルゴリズムのサポートを改善します。RH-SSO は FAPI を完全にはサポートしていませんが、以下の変更がその方向に進んでいます。

- MP-JWT クライアントスコープ。Eclipse MicroProfile 仕様の後にトークンを簡単に発行できます。
- 署名付きのクライアントシークレット JWT を使用したクライアント認証でサポートされるアルゴリズム。HS384 アルゴリズムおよび HS512 アルゴリズムが既存の HS256 アルゴリズムに追加されました。
- 署名済み JWT または Basic 認証を使用した OIDC ID ブローカーのクライアント認証。OIDC 仕様のすべてのクライアント認証方法がサポートされます。
- ID ブローカーの変更により、ID プロバイダーで特定ユーザーの初回ログイン時に RH-SSO ユーザーの自動作成を簡単に無効にできるようになりました。詳細は サーバー管理ガイド の ユーザーの自動作成の無効 を参照してください。
- 秘密鍵署名 JWT を使用したクライアント認証の追加署名アルゴリズムのサポート。
- 署名済み JWT を使用したクライアント認証の追加署名アルゴリズムのサポート。サポートされるすべてのアルゴリズムは、RS256、RS384、RS512、PS256、PS384、PS512、ES256、ES384、および ES512 です。
- PS256 トークン署名のサポート
- JavaScript アダプターの PKCE サポート。
- ユーザーロケールの処理が改善
- 管理エンドポイント/コンソールでのクライアントおよびロールのページネーションサポート

1.2.7. 既存のテクノロジープレビュー機能

以下の機能は引き続きテクノロジープレビューのステータスになります。

- トークンの交換
- 詳細な認可パーミッション

1.3. 削除された機能または非推奨の機能

これらの機能のステータスが変更になりました。

- Red Hat Single Sign-On 7.2 でテクノロジープレビュー機能として導入されたクロスサイトレプリケーションは、最新の RH-SSO 7.6 リリースを含む Red Hat SSO 7.x リリースでサポート機能として利用できなくなりました。Red Hat は、この機能がサポートされていないため、お使いの環境でこの機能を実装したり、使用したりすることは推奨しません。また、この機能のサポート例外は考慮されず、受け入れられなくなりました。
  クロスサイトレプリケーションの新しいソリューションについて議論されており、Keycloak (RHBK) の Red Hat ビルドの将来のリリースで暫定的に検討されています。これは、Red Hat SSO 8 の代わりに導入される製品です。詳細は近日中にお知らせいたします。
- Red Hat Enterprise Linux 6 (RHEL 6) での Red Hat Single Sign-On (RH-SSO) のサポートは非推奨になり、RH-SSO の 7.5 リリースは RHEL 6 ではサポートされなくなります。RHEL 6 は 2020 年 11 月 30 日にライフサイクルの ELS フェーズに入り、RH-SSO が依存する Red Hat JBoss Enterprise Application Platform (EAP) は、EAP7.4 リリースで RHEL 6 のサポートを終了します。お客様は、RHEL 7 または 8 バージョンに RH-SSO 7.5 のアップグレードをデプロイする必要があります。

- Spring Boot アダプターは非推奨となり、RH-SSO の 8.0 以降のバージョンには含まれません。このアダプターは、RH-SSO 7.x のライフサイクル期間、メンテナンスされます。ユーザーは Spring Security に移行して、Spring Boot アプリケーションを RH-SSO と統合する必要があります。
- RPM からのインストールは非推奨になりました。Red Hat Single Sign-On は、7.x 製品の有効期間中も引き続き RPM を提供しますが、次のメジャーバージョンでは RPM は配信されません。製品は、引き続き ZIP ファイルからのインストールと、OpenShift でのインストールを引き続きサポートします。
- 承認サービスの Drools ポリシーが削除されました。
- 管理 REST エンドポイントおよびコンソールを使用したスクリプトのアップロードが非推奨となりました。これは今後のリリースで削除されます。

1.4. 修正された問題

本リリースでは、1100 を超える問題が修正されました。修正された問題の詳細は、https://issues.redhat.com/issues/?filter=12346377 を参照してください。

1.5. 既知の問題

本リリースには、リンク先に記載される 既知の問題 と、特に以下の重要な問題が含まれています。

- KEYCLOAK-13589 - Can't add user in admin console when 'Email as username' is enabled (メールをユーザー名にが有効になっている場合に管理コンソールでユーザーを追加できない)
- KEYCLOAK-13635 - Cannot create mappers which require certain characters like $ ($ などの特定の文字が必要なマッパーを作成できない)
- KEYCLOAK-13668 - Group-Based Policy not working for new clients (新規クライアントのグループベースポリシーが機能しない)
- KEYCLOAK-13581 - Client pagination with reduced permissions results in an empty response (権限を減らしたクライアントページネーションで空の応答が発生する)

1.6. サポートされる設定

RH-SSO Server 7.4 でサポートされる機能および設定は、Red Hat Single Sign-On でサポートされる設定 を参照してください。

1.7. コンポーネントのバージョン

RH-SSO 7.4 でサポートされるコンポーネントバージョンの一覧は、Red Hat Single Sign-On Component Details を参照してください。

1.8. RED HAT OPENSHIFT の RED HAT SINGLE SIGN-ON メータリングラベル

メータリングラベルを Red Hat Single Sign-On に追加し、OpenShift Metering Operator を使用して Red Hat サブスクリプションの詳細を確認できます。

注記

メータリングラベルは、Operator がデプロイおよび管理する Pod に追加しないでください。

Red Hat Single Sign-On では、以下のメータリングラベルを使用できます。

- **com.redhat.component-name: "SSO"**
- **com.redhat.component-type: application**
- **com.redhat.component-version: 7.4.10**
- **com.redhat.product-name: "Red_Hat_Runtimes"**
- **com.redhat.product-version: 2020/Q2**

関連情報

- OpenShift Container Platform でのメータリングの設定および使用