VMware Workspace Portal 管理者ガイド

Workspace Portal 2.1

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、http://www.vmware.com/jp/support/pubs を参照してください。

JA-001537-00

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/）にあります
VMware の Web サイトでは最新の製品アップデートも提供されています。
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

VMware Workspace Portal 管理者ガイドについて 1

『VMware Workspace Portal 管理者ガイド』では、VMware Workspace™ Portal の使用およびメンテナンスについての情報と手順を説明します。Workspace を使用すると、組織のアプリケーションのリソース カタログをカスタマイズし、そのリソースに対して、セキュアなマルチ デバイスの管理対象ユーザー アクセスが可能になります。そのようなリソースには、Web アプリケーション、ThinApp パッケージとしてキャプチャされる Windows アプリケーション、Citrix ベース アプリケーション、View™ デスクトップおよびアプリケーション プールなどがあります。Workspace によってユーザーは一体感を体験でき、IT 部門には複数のデバイス間のすべてのサービスとアプリケーションに対して統一されたセキュリティと管理を提供できます。

対象者

『VMware Workspace Portal 管理者ガイド』は、企業の管理者を対象としています。この情報は、仮想マシン テクノロジ、ID 管理、Kerberos、ディレクトリ サービスに精通している、Windows または Linux のシステム管理者向けに記述されています。VMware ThinApp®、View、Citrix アプリケーション仮想化、および RSA SecurID などのその他の機能の実装を計画している場合は、それらのテクノロジの知識も役立ちます。

Workspace 管理者ガイドの概要

『VMware Workspace Portal 管理者ガイド』は、Workspace をインストールした後に使用します。

Workspace を管理するには、Workspace 管理コンソール を使用します。

Workspace 管理コンソール から実行する主要タスクは、リソースの使用資格をユーザーに付与することです。その他のタスクは、この主要タスクをサポートするものであり、どのユーザーまたはグループに、どのような条件でどのリソースの使用資格を付与するか細部にわたって制御できるようにします。

管理者として実行するタスクは、管理する予定のリソース タイプによって異なります。View デスクトップおよびアプリケーション プール、Windows アプリケーション（ThinApp パッケージ）、DaaS デスクトップ、Citrix ベース アプリケーション、Web アプリケーションを管理できます。実際に管理するリソース タイプは、組織のニーズに応じて異なります。リソース タイプに使用資格を付与するには、『VMware Workspace Portal でのリソースのセットアップ』ガイドの説明に従って、最初にそれぞれの事前構成タスクを実行する必要があります。

Workspace の概要（管理者向け） 2

Workspace では、一元的な管理コンソールで組織のカタログをカスタマイズし、カタログ内のリソースに対する使用資格を管理します。カタログには組織のアプリケーションとリソースが含まれます。

Workspace は、ユーザーの属性を検出し、アプリケーション全体にポリシーを適用します。ユーザーのワークスペースは、資格付与された一連のリソースで構成されます。Windows、Web、および Software-as-a-Service（SaaS）の各アプリケーションに単一のポータルからアクセスするための機能を含めてそれらのアプリケーションの提供をユーザーごとにカスタマイズできる一方で、アプリケーションへのセルフ サービス アクセスをユーザーに提供することもできます。

Workspace の管理サービス

Workspace のユーザー グループとリソース管理、認証、同期セットアップ、およびデータベース接続を別の Workspace 管理サービスから管理します。

- Workspace 管理コンソール インターフェイスで、リソースカタログをセットアップし、ユーザーおよびグループ、使用資格、レポートを管理します。ユーザー、リソース使用状況、および Workspace アプライアンスの健全性を監視するために、[ユーザー エンゲージメント] ダッシュボードと [システム診断] ダッシュボードを表示できます。Active Directory から割り当てられた管理者ユーザー ロールとしてログインします。管理コンソールに直接ログインする場合の URL は、https://<WorkspaceFQDN/>/SAAS/admin です。
- Connector Services Admin ページでは、ディレクトリの構成、AuthBroker のセットアップ、仮想デスクトップやリモート アプリケーションなどその他のエンタープライズ統合の管理を行います。これには、View 接続サーバ、ThinApp リポジトリ、Citrix 公開アプリケーション リソースとの統合のセットアップが含まれます。これらのページから、ディレクトリの同期状態とアラートを確認することもできます。セットアップ時に作成したユーザー名 **admin** および管理者パスワードを使用して、Workspace 管理者としてログインします。WorkspaceConnector Services Admin ページへのリンクは、https://<Workspace_FQDN> .com:8443 にあります。
- Appliance Configurator ページでは、Workspace データベースの管理、証明書の更新、Syslog の有効化、Workspace およびシステム パスワードの変更、その他のインフラストラクチャ管理を実行できます。Workspace をセットアップしたときに作成した管理者ユーザー名と管理者パスワードを使用して、Workspace 管理者としてログインします。Appliance Configurator ページへのリンクは、https://<Workspace_FQDN> .com:8443 にあります。[Appliance Configurator] ページは、Worksapce 管理コンソールの [設定] > [VA 構成] ページからアクセスすることもできます。

Workspace エンド ユーザー コンポーネント

ユーザーは Workspace App Portal （エージェントレス クライアント）を使用して、使用資格のあるリソースにアクセスできます。また、ユーザーは、Workspace for Windows から ThinApp パッケージとしてキャプチャされた仮想 Windows アプリケーションにアクセスできます。

表 2-1. Workspace ユーザー クライアントのコンポーネント

Workspace ユーザー コンポーネント	説明	使用可能なエンドポイント
Workspace アプリ ポータル	Workspace アプリ ポータルは、エージェントレス Web ベース アプリケーションです。ユーザーがブラウザでアクセスし、資格付与されたワークスペース アセットを使用する場合に使用されるデフォルトのインターフェイスです。このポータルを使用すると、ユーザーは View デスクトップおよび Workspace Web アプリケーションにアクセスできます。 ThinApp アプリケーションにアクセスする権限があるエンドユーザーが、Workspace for Windows プログラムがインストールされているアクティブな Windows システムを使用している場合、このアプリ ポータルから、使用資格のある ThinApp パッケージを表示および起動できます。 iOS デバイスでは、ユーザーは Safari などのブラウザ アプリを使用してこのポータルを開き、View デスクトップ、Workspace Web アプリケーション、および Citrix ベース アプリケーションにアクセスして使用できます。	Web ベースのアプリケーション ポータルは、Windows システム、Mac システム、iOS デバイス、Android デバイスなど、すべてのサポート対象システムのエンドポイントで使用できます。
Workspace for Windows	このプログラムがユーザーの Windows システムにインストールされていると、ユーザーは、ThinApp パッケージとしてキャプチャされた仮想 Windows アプリケーションで作業できます。	Windows システム

Workspace でサポートされる Web ブラウザ

Workspace 管理者コンソールは、Workspace をインストールするときにインストールされる Web ベース アプリケーションです。Workspace 管理コンソール は次のブラウザからアクセスして使用することができます。

- Internet Explorer 10 および 11（Windows システムの場合）
- Google Chrome 34.0 以降（Windows および Mac システムの場合）
- Mozilla Firefox 28 以降（Windows および Mac システムの場合）
- Safari 6.1.3 以降（Mac システムの場合）

エンド ユーザーは、次のブラウザから自分の Workspace アプリケーション ポータルにアクセスすることができます。

- Mozilla Firefox (最新版)
- Google Chrome (最新版)
- Safari (最新版)
- Internet Explorer 8 以降
- ネイティブ ブラウザおよび Google Chrome（Android デバイス）
- Safari（iOS デバイス）

Internet Explorer 8 で Workspace ページを表示すると、要素によってはページで適切に表示されない場合があります。最適な表示を得るため、新しいバージョンにアップグレードしてください。

[Workspace 管理コンソール] ダッシュボードを使用した、ユーザー、リソース、およびアプライアンスの健全性の監視

3

Workspace 管理コンソールには、ユーザー、リソース使用状況、および Workspace アプライアンスの健全性の監視に役立つ [ユーザー エンゲージメント] ダッシュボードおよび [システム診断] ダッシュボードが含まれます。

この章では次のトピックについて説明します。

Workspace で使用するリソースとユーザー

[ユーザー エンゲージメント] ダッシュボードには、ユーザーおよびリソースに関する情報が表示されます。サインインしたユーザー、使用中のアプリケーション、およびアプリケーションのアクセス頻度を表示できます。ユーザーとグループのアクティビティおよびリソース使用状況を追跡するレポートを作成できます。

[ユーザー エンゲージメント] ダッシュボードに表示される時刻は、ブラウザのタイム ゾーン設定に基づいています。ダッシュボードは、1 分ごとに更新されます。

手順

- ヘッダーには、その日にログインした一意のユーザー数、および 7 日間の毎日のログイン イベント数を示すタイムラインが表示されます。ログインしたユーザーのパーセンテージを表示する、今日のログイン ユーザー数は円で囲まれます。ログイン推移グラフには、その週のログイン イベントが表示されます。グラフのいずれかの点を指すと、その日のログイン数が表示されます。
- [ユーザー & グループ] セクションには、Workspace にセットアップされているユーザー アカウントの数およびグループの数が表示されます。ログインした最新のユーザーが表示されます。[全部のレポートを表示] をクリックすると、ある範囲の日数にログインしたユーザーを表示する監査イベント レポートを作成できます。
- [アプリケーションの人気度] セクションには、7 日間にアプリケーションが起動された回数をアプリケーション タイプ別に示す棒グラフが表示されます。特定の日を指すと、ツール ヒントに使用されたアプリケーションのタイプおよびその日に起動されたアプリケーションの数が表示されます。グラフの下のリストには、特定のアプリケーションが起動された回数が表示されています。1 日、1 週間、1 か月、または 12 週間のこの情報を表示するように選択するには、右側にあるドロップダウン メニューの矢印をクリックします。[全部のレポートを表示] をクリックすると、ある範囲の時間のアプリケーション、リソース タイプおよびユーザーのアクティビティ数を表示するリソース使用状況レポートを作成できます。
- [アプリの導入] セクションには、使用資格のあるアプリケーションを開いたユーザーのパーセンテージを示す棒グラフが表示されます。アプリケーションを指すと、ツール ヒントに実際の導入数と資格数が表示されます。
- 起動されているアプリケーションの円グラフには、起動されているリソースが全体に占めるパーセンテージが表示されます。この円グラフで特定のセクションを指すと、リソースのタイプ別に実際の数が表示されます。1 日、1 週間、1 か月、または 12 週間のこの情報を表示するように選択するには、右側にあるドロップダウン メニューの矢印をクリックします。

- [Workspace Client] セクションには、使用中の Workspace の Windows クライアント数が表示されます。

次に進む前に

[ダッシュボード] ドロップダウン メニューをクリックすると、[システム診断] ダッシュボードが表示されます。

Workspace のシステム情報および健全性の監視

Workspace の [システム診断] ダッシュボードには、環境に導入されている Workspace アプライアンスの健全性の詳細な概要および Workspace サービスに関する情報が表示されます。Workspace データベース サーバ、workspace-va 仮想マシン、および各仮想マシンで使用可能なサービス全体の健全性を表示できます。

[システム診断] ダッシュボードでは、インストールされている Workspace のバージョンなど、その仮想マシンのサービスのステータスを監視および表示する workspace-va 仮想マシンを選択できます。データベースや仮想マシンに問題がある場合は、マシンのステータスが赤色でヘッダー バーに表示されます。問題を表示するでは、赤色で表示されている仮想マシンを選択します。

手順

- ユーザー パスワードの有効期限が切れています。Workspace アプライアンスのルート ログイン パスワードおよびリモート ログイン パスワードの有効期限日が表示されます。パスワードの有効期限が切れている場合は、[設定] ページに移動して [VA 構成] を選択します。[システム セキュリティ] ページを開いてパスワードを変更します。
- 証明書。証明書の発行者、開始日、および終了日が表示されます。証明書を管理するには、[設定] ページに移動して [VA 構成] を選択します。[証明書のインストール] ページを開きます。
- Configurator - アプリケーション展開ステータス。Appliance Configurator サービスの情報が表示されます。[Web サーバ ステータス] には、Tomcat サーバが実行中かどうかが表示されます。[Web アプリケーション ステータス] には、[Appliance Configurator] ページにアクセスできるかどうかが表示されます。[アプライアンスのバージョン] には、インストールされている Workspace アプライアンスのバージョンが表示されます。
- Application Manager - アプリケーション展開ステータス。Workspace アプライアンスの接続ステータスが表示されます。
- Connector - アプリケーション展開ステータス。Connector Services Admin の接続ステータスが表示されます。接続に成功したことが表示されている場合は、Connector Services Admin ページにアクセスできます。
- Workspace FQDN。Workspace App Portal にアクセスするためにユーザーが入力した完全修飾ドメイン名が表示されます。ロード バランサが使用中の場合は、Workspace の FQDN はロード バランサを参照します。
- Application Manager - 統合コンポーネント。Workspace データベース接続、監査サービス、および接続の分析情報が表示されます。
- Connector - 統合コンポーネント。[Connector サービス管理] ページで管理されているサービスに関する情報が表示されます。ThinApp、View、および Citrix 公開アプリケーションのリソースに関する情報が表示されます。
- モジュール。Workspace で有効になっているリソースが表示されます。[有効] をクリックして、そのリソースの [Connector サービス管理] ページに移動します。

Workspace のユーザー認証の構成 4

Workspace のユーザー認証には、1 つ以上の ID プロバイダ インスタンスを使用する必要があります。これには、デフォルトの Workspace インスタンス、サードパーティ ID プロバイダ インスタンス、またはその両方の組み合わせを使用できます。ID プロバイダ インスタンスは、エンタープライズ ネットワーク内の Active Directory を使用してユーザーを認証します。

各自の Workspace 環境に対して ID プロバイダ インスタンスを構成して追加するには、Workspace が各自の Active Directory 環境に適切にアクセスできるように、いくつかの前提作業を実行する必要があります。

この章では次のトピックについて説明します。

Workspace のユーザー認証の概要

Workspace では、構成する認証方法、デフォルトのアクセス ポリシー セット、ネットワーク範囲、および ID プロバイダ インスタンスに基づいて、ユーザーを認証します。

Workspace で使用する ID プロバイダ インスタンスは、SAML 2.0 アサーションを使用して Workspace と通信するネットワーク内のフェデレーション機関を作成します。ID プロバイダ インスタンスは、エンタープライズ ネットワーク内の Active Directory を使用してユーザーを認証します。

Workspace でサポートされているユーザー認証方法は、Active Directory パスワード、Kerberos、および RSA SecurID です。ただし、お使いのサードパーティの ID プロバイダが、Workspace の展開で使用できるスマート カード ベースの認証などの追加の認証方法をサポートしている場合があります。

デフォルトでサポートされる Workspace 認証タイプ	説明
パスワード	まったく構成を行わないと、Workspace は Active Directory パスワード認証をサポートします。この方法では、Active Directory に対して直接、ユーザーを認証します。
Kerberos	Kerberos 認証によりドメイン ユーザーがシングル サインオンで Workspace にアクセスできるため、ドメイン ユーザーがエンタープライズ ネットワークへのログイン後に Workspace にログインする必要がなくなります。ID プロバイダ インスタンスは、キー配布センター（KDC）が配布する Kerberos チケットを使用して、ユーザー デスクトップ資格情報を検証します。
RSA SecurID	RSA SecurID 認証では、ユーザーがトークン ベースの認証システムを使用する必要があります。RSA SecurID は、エンタープライズ ネットワークの外部から Workspace にアクセスするユーザーに対して推奨される認証方法です。

Kerberos 認証または RSA SecurID 認証を実装するには、既存の ID プロバイダ インスタンスを使用するか、または各自の展開によって 1 つ以上の追加の ID プロバイダ インスタンスを展開できます。

ユーザーがログインする際に、Workspace は、ユーザーを認証する ID プロバイダ インスタンスを決定する必要があります。

その決定をするために、Workspace はデフォルトのアクセス ポリシー セットを評価し、そのセットの中から適用するポリシーを選択します。適用されたポリシーは、そのログイン イベントに必要な最小認証スコアを示します。次に、Workspace は、必要な最小認証スコアおよび方法の順序に基づいて利用可能な認証方法をフィルタしてソートします。方法の順序は、組織の要件に応じて設定できます。Workspace は、ポリシーの認証方法およびネットワーク範囲の要件を満たしている最初の ID プロバイダ インスタンスを選択し、そのインスタンスにユーザー認証要求を転送して認証を行わせます。認証が失敗した場合、リストの下方に向かって ID プロバイダ選択プロセスが続きます。

重要　ID プロバイダ インスタンスを削除またはリセットする場合は、対応する ID プロバイダ名を [ID プロバイダ] ページから削除する必要があります。

Workspace は ID プロバイダの選択プロセスを使用するようにさまざまな方法で展開できますが、その 1 つの例を次に示します。

外部に RSA SecurID 認証、内部にパスワード認証以上を使用した例

これは、同じ Workspace 展開環境で内部ユーザーに Active Directory パスワード認証方法または Kerberos 認証方法を、外部ユーザーに RSA SecurID 認証方法を使用するように Workspace を構成する方法の 1 つです。

- 内部ポリシー - Workspace 管理コンソール を使用して、Active Directory パスワードを認証方法として受け入れる最小認証スコアに基づいて、デフォルトのアクセス ポリシー セットにポリシーを作成します。Workspace が最初に Kerberos 認証でユーザーの認証を試みるようにするには、Kerberos 方式の認証スコープをパスワード方式の認証スコープよりも高く設定し、[認証方法] ページのリストの先頭に Kerberos を配置します。内部ユーザーのためのネットワーク範囲も割り当てます。
- 外部ポリシー - Workspace 管理コンソール を使用して、ユーザー認証に RSA SecurID 認証方法が確実に使用されるようにするための最小認証スコアに基づいて、デフォルトのアクセス ポリシー セットにポリシーを作成します。想定されるすべてのユーザーを含むネットワーク範囲も割り当てます（0.0.0.0 ～ 255.255.255.255）。

このように構成すると、エンタープライズ ネットワークの内側から Workspace にアクセスしようとするユーザーは Kerberos 認証またはパスワード認証を提供する ID プロバイダ インスタンスに振り分けられ、エンタープライズ ネットワークの外側のユーザーは RSA SecurID 認証を提供する ID プロバイダ インスタンスに振り分けられます。内部と外部のユーザーは、認証方法の構成方法によって、同じ ID プロバイダ インスタンスに転送される場合も、異なる ID プロバイダ インスタンスに転送される場合もあります。

ネットワーク範囲の追加または編集

特定の ID プロバイダ インスタンスに振り分ける IP アドレスのネットワーク範囲を追加できます。

ALL RANGES と呼ばれるデフォルトのネットワーク範囲には、インターネットで利用可能なすべての IP アドレス、つまり 0.0.0.0 から 255.255.255.255 が含まれます。Workspace 展開環境の ID プロバイダ インスタンスが 1 つの場合でも、デフォルト範囲を構成し、特定の IP アドレスを除外したり含めたりするために他の範囲を追加する必要が生じることがあります。展開環境に異なる認証方法を使用する ID プロバイダ インスタンスが複数ある場合は、複数のネットワーク範囲を定義する必要があります。「ID プロバイダ インスタンスの追加と構成 (P. 15)」を参照してください。

注意　デフォルトのネットワーク範囲 ALL RANGES とその説明「全範囲用のネットワーク」は、編集可能です。[ネットワーク範囲] ページの[編集] 機能を使用すると、テキストを別の言語に変更することを含めて、名前と説明を編集できます。

開始する前に

必要なネットワーク範囲計画を実行します。

- 組織のニーズに合わせて Workspace を Active Directory に統合する最適な方法を決定します。このような計画は展開環境内の ID プロバイダ インスタンス数に影響を及ぼし、必要なネットワーク範囲の数にも影響を与えます。
- ネットワーク トポロジに基づいて、Workspace 展開環境のネットワーク範囲を定義します。
- View モジュールが有効になっている場合にネットワーク範囲を追加するには、Horizon Client アクセスの URL およびネットワーク範囲のポート番号を記録します。詳細については、View のドキュメントを参照してください。

手順

1 Workspace 管理コンソール にログインします。

2 [設定] - [ネットワーク範囲] を選択します。

3 既存のネットワーク範囲を編集するか、新しいネットワーク範囲を追加します。

オプション	説明
既存の範囲の編集	編集する範囲で [編集] をクリックします。
範囲の追加	新しい範囲を追加するには、[+ ネットワーク範囲] をクリックします。

4 フォームを完成させます。

フォーム項目	説明
名前	ネットワーク範囲の名前を入力します。
説明	ネットワーク範囲の説明を入力します。
View ポッド	View ポッド オプションは、View モジュールが有効の場合のみ表示されます。 Client アクセスの URL ホスト。ネットワーク範囲に対して、正しい Horizon Client アクセスの URL を入力します。 Client アクセス ポート。ネットワーク範囲に対して、正しい Horizon Client アクセスのポートを入力します。 『VMware Workspace Portal ガイド』の「リソースのセットアップ」 の「View デスクトップ プールおよびアプリケーションへのアクセスの提供」の章を参照してください。
IP 範囲	IP 範囲を編集または追加し、必要なすべての IP アドレスを含め、不必要な IP アドレスが含まれないようにします。

次に進む前に

- 各ネットワーク範囲を ID プロバイダ インスタンスに関連付けます。「ID プロバイダ インスタンスの追加と構成 (P. 15)」を参照してください。
- ネットワーク範囲をアクセス ポリシー セットに適宜に関連付けます。第 5 章「アクセス ポリシー セットの管理 (P. 21)」を参照してください。

ユーザー認証方法の追加または編集

既存のユーザー認証方法を編集できます。サードパーティの ID プロバイダを追加すると、Workspace がデフォルトでサポートしていないユーザー認証方法を構成できます。認証方法を特定の Web アプリケーションに関連付けるアクセス ポリシーを作成することもできます。

Workspace でサポートされているユーザー認証方法は、Active Directory パスワード、Kerberos、および RSA SecurID です。スマート カード ベースの認証などの他の認証方法をサポートするサードパーティ ID プロバイダを追加することで、Workspace でその認証方法を実行できます。「ID プロバイダ インスタンスの追加と構成 (P. 15)」を参照してください。サードパーティの ID プロバイダ インスタンスを使用するための Workspace の構成に関連する作業の完全なリストについては、「サードパーティ ID プロバイダ インスタンスを 使用するように Workspace を構成する作業の概要 (P. 17)」を参照してください。

各方法の最小認証スコアと、[認証方法] ページにおけるその方法の順序は、ユーザー認証の ID プロバイダ インスタンスを選択するために Workspace が行うプロセスに大きな影響を与えます。ユーザーに一定の最小認証スコアの認証方法を使用して Web アプリケーションにアクセスさせる方法については、「Web アプリケーション固有のアクセス ポリシー セットの管理 (P. 22)」を参照してください。

指定されている認証方法を使用して Workspace が試みる回数は異なります。Workspace は、Kerberos 認証を 1 回のみ試みます。Kerberos によるユーザーのログインが失敗すると、リストの次の認証方法が試みられます。Active Directory パスワードまたは RSA SecurID 認証によるログインの最大失敗試行回数は 5 回です。ユーザーがログインに 5 回失敗すると、Workspace はリストの次の認証方法を使用してログインを試みます。すべての認証方法で失敗すると、Workspace はエラーメッセージを表示します。

開始する前に

- Workspace と統合する予定の認証システムを展開します。たとえば、RSA SecurID を Workspace 展開環境に統合する予定がある場合、RSA SecurID がネットワークにインストールされて構成されていることを確認します。
- 独自の基準を使用して、Workspace 環境で使用する予定の認証方法のセキュリティ レベルを、最もセキュリティが低いスケール 1 から最もセキュリティが高いスケール 5 で決定します。

手順

1 Workspace 管理コンソール にログインします。

2 [設定] - [認証方法] を選択します。

3 既存の認証方法を編集するか、新しい認証方法を追加します。

オプション	説明
既存の認証方法の編集	既存の認証方法を構成するには [編集] をクリックします。
新しい認証方法の追加	新しい認証方法を追加するには、[+ 認証方法の追加] をクリックします。たとえば、展開環境に新しいサードパーティ ID プロバイダ インスタンスを追加するという場合が考えられます。

4 認証方法の設定を編集します。

フォーム項目	説明
名前	この ID プロバイダ インスタンスの名前を入力します。
SAML コンテキスト	ドロップダウン メニューから適切な SAML コンテキストを選択します。 リストには、SAML 2.0 仕様に従って現在サポートされている SAML 認証コンテキストが含まれます。

フォーム項目	説明
認証スコア	デフォルトのアクセス ポリシー セットまたは Web アプリケーション固有のポリシー セットのためにアクセス ポリシーを作成する場合、最小認証スコアを設定します。ポリシーは、指定された認証スコア以上の認証方法を使用して Workspace（デフォルトのアクセス ポリシーの場合）または Web アプリケーション（Web アプリケーション固有のポリシーの場合）にアクセスすることをユーザーに求めます。 認証方法にあらかじめ決められているセキュリティ レベルに基づいて、認証スコアを適用します。
デフォルトの方法	認証方法をデフォルトとして設定するには、[デフォルトの方法] を選択します。 [デフォルトの方法] オプションは、[SAML コンテキスト] オプションに関連します。 次の状況は、デフォルトの方法として選択されている認証方法を Workspace が使用する例になります。 認証方法を追加する際に SAML コンテキストを選択します。その後に、サードパーティの ID プロバイダ インスタンスが送信する SAML コンテキストがその ID プロバイダ インスタンスに対して選択した SAML コンテキストに一致しない場合、Workspace は送信された SAML コンテキストを認識しません。認証の試行を終了する代わりに、Workspace はデフォルトの方法として選択されている認証方法を使用してユーザーの認証を試みます。

5 [保存] をクリックします。

次に進む前に

- 各認証方法を適切な ID プロバイダ インスタンスに関連付けます。「ID プロバイダ インスタンスの追加と構成 (P. 15)」を参照してください。
- 各アクセス ポリシーに適切な最小認証スコアを設定することにより、アクセス ポリシーを認証方法に関連付けます。

ID プロバイダ インスタンスの追加と構成

ID プロバイダ インスタンスを Workspace 展開環境に追加して構成することで、高可用性を実現し、追加のユーザー認証方法をサポートし、ユーザー IP アドレス範囲に基づいて柔軟にユーザー認証プロセスを管理できます。

高可用性を高めるため、Workspace の展開用に ID プロバイダ インスタンスを追加します。

開始する前に

- 必要な計画を実行します。
  - 組織のニーズに合わせて Workspace を Active Directory に統合する最適な方法を決定します。単一のドメインまたはマルチドメイン フォレストを構成できます。
  - 組織のニーズを満たすのに必要な認証タイプを決定します。たとえば、組織内のユーザーに対して Kerberos 認証を構成し、組織外のユーザーに対して RSA SecurID 認証を構成できます。この種類の構成は、両方の認証方法に単一の ID プロバイダ インスタンスを使用するか、またはそれぞれの認証方法に個別の ID プロバイダ インスタンスを使用して設定できます。
- 展開の概念実証フェーズで、Workspace を単一の Active Directory ドメインに展開します。
- Workspace 展開環境用の追加の ID プロバイダ インスタンスを作成します。
  - サードパーティの ID プロバイダ インスタンスを追加するには、次のタスクを実行します。サードパーティの ID プロバイダ インスタンスを使用するための Workspace の構成に関連する作業の完全なリストについては、「サードパーティ ID プロバイダ インスタンスを 使用するように Workspace を構成する作業の概要 (P. 17)」を参照してください。
    - サードパーティの ID プロバイダ インスタンスが SAML 2.0 に準拠し、Workspace がそれにアクセスできることを確認します。
    - Workspace がサードパーティのインスタンスからメタデータを取得する方法を決定し、サードパーティのインスタンスから適切なメタデータ情報をコピーして保存します。この情報は、構成中に Workspace 管理コンソール に貼り付けることができます。サードパーティのインスタンスから取得するメタデータ情報は、メタデータへの URL または実際のメタデータのいずれかです。
    - Workspace で追加の認証方法を使用できるようにするには、管理コンソール を使用して追加の認証方法を構成します。「ユーザー認証方法の追加または編集 (P. 14)」を参照してください。
- 管理コンソール を使用して、ネットワーク範囲を構成します。「ネットワーク範囲の追加または編集 (P. 13)」を参照してください。

手順

1 Workspace 管理コンソール にログインします。

2 [設定] - [ID プロバイダ] を選択します。

3 [ID プロバイダを追加] をクリックします。このオプションでは、Workspace で既存のサードパーティの ID プロバイダ インスタンスを登録できるようにするための情報を入力するよう求められます。

4 ID プロバイダ インスタンスの設定を編集します。

フォーム項目	説明
タイプ	サードパーティの ID プロバイダ インスタンスの場合は [手動] を選択します。 注意 VMware のテクニカル サポートから指示されない限り、[自動] を選択しないでください。
プロバイダ名	この ID プロバイダ インスタンスの名前を入力します。
説明	この ID プロバイダ インスタンスの説明を入力します。
ユーザー ストア	[ユーザー ストア] テキスト ボックスには、Workspace 展開環境で使用可能なユーザー ストアが表示されます。 この ID プロバイダ インスタンスに関連付けるすべてのユーザー ストアを選択します。
認証方法	[認証方法] テキスト ボックスには、Workspace 展開環境で使用可能なユーザー認証方法が表示されます。このリストには、デフォルトの認証方法とサードパーティの ID プロバイダをサポートするためにあらかじめ追加した方法が含まれます。新しい認証方法の追加は、この作業の前提条件として記載されています。選択する認証方法がリストにない場合は、その認証方法を前提条件に記載されているように追加します。 この ID プロバイダ インスタンスに関連付けられているユーザーのログイン時に Workspace が適用する認証方法を選択します。 注意 選択された認証方法が有効になっており、適切に構成されていることを確認します。Workspace のインストールと構成を参照してください。
次を使用して構成	[次を使用して構成] オプションは、サードパーティの ID プロバイダ インスタンスを追加し、ID プロバイダ タイプとして [手動] を選択する場合にのみ使用できます。URL ID の方法を選択します。 ■ Workspace が登録目的でサードパーティの ID プロバイダ インスタンスのメタデータを受信できるようにするには、[自動検出 URL] を選択し、[自動検出] テキスト ボックスにメタデータへの URL を入力します。 ■ [メタデータ XML] を選択し、ID プロバイダ インスタンスから XML メタデータをコピーして、それを [メタデータ XML] テキスト ボックスに貼り付けます。
ネットワーク範囲	[ネットワーク範囲] テキスト ボックスには、Workspace 展開環境内の既存のネットワーク範囲が一覧表示されます。 認証のためにこの ID プロバイダ インスタンスに振り分けるユーザーのネットワーク範囲を、その IP アドレスに基づいて選択します。

5 [保存] をクリックします。

6 必要な場合は、ID プロバイダ インスタンスの順序を変更します。

Workspace では、ID プロバイダ インスタンスのリストの上から下に向かって IP アドレスを検索します。1 つの IP アドレスが複数の ID プロバイダ インスタンスに割り当てられている場合、Workspace は、リスト最上位にある ID プロバイダ インスタンスを最初のインスタンスとして認識します。

a [ID プロバイダの順序を編集] をクリックします。

b 上下の矢印を使用して、ID プロバイダ インスタンスを適切な場所に移動します。

c [保存] をクリックします。

次に進む前に

- マルチ フォレスト環境用に Workspace を構成する場合は、Workspace ユーザーにそれぞれのドメインを通知し、ログイン時にドロップダウン メニューからドメインを選択する必要があることを説明します。[この設定を保存] チェック ボックスをオンにして、ログインするたびにプロンプトが繰り返し表示されないようにできることを通知します。
- サードパーティの ID プロバイダ インスタンスを追加した場合は、サードパーティの ID プロバイダ インスタンスを構成するために必要な Workspace の情報をコピーして保存します。「サードパーティの ID プロバイダ インスタンスの構成に必要な Workspace SAML 情報の取得 (P. 18)」を参照してください。

サードパーティ ID プロバイダ インスタンスを 使用するように Workspace を構成する作業の概要

サードパーティ ID プロバイダ インスタンスを使用するために Workspace を構成するには、構成全体でいくつかの特定の手順を実行する必要があります。

構成前の作業

Workspace 管理コンソールを使用してサードパーティ ID プロバイダ インスタンスを追加する前に、次の作業を完了します。

1 サードパーティの ID プロバイダ インスタンスが SAML 2.0 に準拠し、Workspace がそれにアクセスできることを確認します。

2 Workspace がサードパーティのインスタンスからメタデータを取得する方法を決定し、サードパーティのインスタンスから適切なメタデータ情報をコピーして保存します。この情報は、構成中に Workspace 管理コンソールに貼り付けることができます。サードパーティのインスタンスから取得するメタデータ情報は、メタデータへの URL または実際のメタデータのいずれかです。

3 サードパーティ ID プロバイダでサポートされている認証方法を Workspace で使用できるようにするには、管理コンソールを使用して追加の認証方法を構成します。「ユーザー認証方法の追加または編集 (P. 14)」を参照してください。

4 認証方法を編集するには、[デフォルトの方法] チェックボックスをオンにします。この操作を行うと、サードパーティの認証方法で問題が発生した場合に Workspace で該当の認証方法を使用できます。「ユーザー認証方法の追加または編集 (P. 14)」を参照してください。

構成

ID プロバイダ インスタンスを追加する場合は、サードパーティ ID プロバイダに固有の次の手順を実行します。「ID プロバイダ インスタンスの追加と構成 (P. 15)」を参照してください。

1 管理コンソール で、[設定] > [ID プロバイダ] ページに進み、[ID プロバイダを追加] ボタンをクリックして [タイプ] ドロップダウン メニューから [手動] を選択します。

2 Workspace で使用する予定のサードパーティ ID プロバイダ インスタンスでサポートされている認証方法を選択します。

3 [次を使用して構成] オプションを使用して、サードパーティ ID プロバイダ インスタンスのメタデータを Workspace に転送する方法（メタデータの URL を使用する方法またはメタデータをコピーして貼り付ける方法のいずれか）を選択します。

構成後の作業

Workspace SAML 情報を収集し、この情報をサードパーティ ID プロバイダ インスタンスに適用します。「サードパーティの ID プロバイダ インスタンスの構成に必要な Workspace SAML 情報の取得 (P. 18)」を参照してください。

1 Workspace 管理コンソールを使用して、サードパーティ ID プロバイダ インスタンスの構成に必要な SAML 情報を収集します。

2 Workspace から収集した SAML 情報を適用してサードパーティ ID プロバイダ インスタンスを構成します。

サードパーティの ID プロバイダ インスタンスの構成に必要な Workspace SAML 情報の取得

Workspace をサードパーティの ID プロバイダ インスタンスと統合する場合、Workspace 側で構成を実行した後に、サードパーティの ID プロバイダ側の構成に必要な SAML 証明書情報をコピーして準備する必要があります。

手順

1 管理コンソール にログインします。

2 [設定] - [SAML 証明書] を選択します。

3 Workspace に表示される SAML 署名証明書をコピーして保存します。

a [署名証明書] セクションにある、証明書情報をコピーします。

b 後でサードパーティの ID プロバイダ インスタンスを構成する際に使用するために、証明書情報をテキスト ファイルに保存します。

4 SAML SP メタデータをサードパーティの ID プロバイダ インスタンスが使用できるようにします。

a [SAML 証明書をダウンロード] ページで、[サービス プロバイダ（SP）メタデータ] をクリックします。

b それぞれの組織に最も適した方法を使用して、表示された情報をコピーして保存します。

ここでコピーされた情報は、後でサードパーティの ID プロバイダを構成する際に使用します。

方法	説明
ページの URL をコピー	サービス プロバイダ（SP）メタデータのページの URL をコピーして保存します。
ページの XML をコピー	ページのコンテンツをテキスト ファイルにコピーして保存します。

5 サードパーティ ID プロバイダ インスタンスから Workspace へのユーザー マッピングを確認します。

サードパーティ ID プロバイダを構成するときには、サードパーティ ID プロバイダ内の SAML アサーションを編集して Workspace ユーザーをマップします。

NameID の形式	ユーザー マッピング
urn:oasis:names:tc:SAML:2.0:nameid-format:emailAddress	SAML アサーション内の NameID 値は、Workspace 内のメール アドレス属性にマップされます。
urn:oasis:names:tc:SAML:2.0nameid-format:unspecified	SAML アサーション内の NameID 値は、Workspace 内のユーザー名属性にマップされます。

次に進む前に

必要に応じて、このタスクのためにコピーした情報を適用して、サードパーティの ID プロバイダ インスタンスを構成します。

デフォルトのアクセス ポリシー セットの編集

Workspace には、Workspace アプリケーション ポータルへのユーザー アクセスを制御するデフォルトのアクセス ポリシー セットが含まれています。ポリシー セットを編集して、必要に応じてポリシーを変更することができます。

デフォルトのアクセス ポリシー セット内の各ポリシーでは、Workspace がアプリケーション ポータルへのアクセスを許可するための一連の基準が満たされている必要があります。第 5 章「アクセス ポリシー セットの管理 (P. 21)」を参照してください。

次のアクセス ポリシー セットは、デフォルトのアクセス ポリシー セットを構成して Workspace アプリケーション ポータルへのアクセスを制御する方法の例として参考になります。手順については、「アクセス ポリシー セットの編集 (P. 24)」を参照してください。

デフォルトのアクセス ポリシー セットの例

この例では、デフォルトのアクセス ポリシー セットを編集する方法を示します。

ポリシー名	ネットワーク	最小認証スコア	TTL（時間）
内部	内部範囲	1	8
外部	全範囲	3	4

ポリシーは上記の順で評価されます。ポリシー セットのポリシーを上または下にドラッグして評価の優先順位を変更できます。

上記のポリシー セットの例を、次の使用例に適用します。

デフォルトのアクセス ポリシー、ブラウザの使用例

1
- 内部。内部（内部範囲）ネットワークから Workspace にアクセスするために、Workspace は Active Directory のパスワードによる認証方法をユーザーに提示します。Workspace が最初に Kerberos 認証でユーザーの認証を試みるようにするには、Kerberos 方式の認証スコープをパスワード方式の認証スコープよりも高く設定し、[認証方法] ページのリストの先頭に Kerberos を配置します。内部ユーザーのためのネットワーク範囲も割り当てます。ユーザーはブラウザを使用してログインし、ユーザー ポータルに 8 時間のセッションの間アクセスできます。
- 外部。外部（全範囲）ネットワークから Workspace にアクセスするには、ユーザーは SecurID（この例では認証スコア 3）を使用してログインする必要があります。ユーザーはブラウザを使用してログインし、4 時間のセッションの間、アプリケーション ポータルにアクセスできます。

2 ユーザーがリソースへのアクセスを試みると、Web アプリケーション固有のポリシー セットでカバーされている Web アプリケーションを除いて、デフォルトのポータル アクセス ポリシー セットが適用されます。

たとえば、そのようなリソースの有効時間（TTL）は、デフォルトのポータル アクセス ポリシー セットの TTL と一致します。アプリケーション ポータルにログインしているユーザーの TTL がデフォルトのポータル アクセス ポリシー セットに従って 8 時間である場合、ユーザーが TTL セッション中にリソースを起動しようとすると、アプリケーションはユーザーに再認証を求めずに起動します。

5 アクセス ポリシー セットの管理

デフォルトのアクセス ポリシー セットを構成し、ユーザーが Workspace アプリ ポータル にアクセスするために満たす必要がある基準を指定できます。ユーザーが指定した Web アプリケーションを起動するために満たす必要がある基準を指定する Web アプリケーション固有のアクセス ポリシー セットを作成することもできます。

アクセス ポリシーを適用するには、アクセス ポリシー セットの一部としてポリシーを作成します。アクセス ポリシー セットの各ポリシーでは、次の情報を指定できます。

- エンタープライズ ネットワークの内部または外部などのユーザーがログインできる場所。
- そのポリシーで使用できる認証方法を決定する最小認証スコア。
- ユーザーに提供されるアクセスの時間数。

注意　Workspace のアクセス ポリシーは、Web アプリケーションのセッションの持続時間の長さを制御しません。ポリシーは、ユーザーが Web アプリケーションを起動するのに必要な時間を制御します。

Workspace には、編集可能なデフォルトのアクセス ポリシー セットがあります。このアクセス ポリシー セットは、Workspace 全体へのアクセスを制御します。「デフォルトのアクセス ポリシー セットの編集 (P. 18)」を参照してください。特定の Web アプリケーションへのアクセスを制御するために、追加のアクセス ポリシー セットを作成できます。Web アプリケーションにアクセス ポリシー セットを適用しない場合は、デフォルトのアクセス ポリシー セットが適用されます。

この章では次のトピックについて説明します。

アクセス ポリシー設定の概要

アクセス ポリシー セットには 1 つ以上のアクセス ポリシーが含まれます。各アクセス ポリシーは、Workspace アプリ ポータル に対する全体としてのユーザー アクセスまたは指定された Web アプリケーションへのユーザー アクセスを管理するために構成できる設定値の集まりです。

各アクセス ポリシーは、ネットワーク範囲を最小認証スコアに関連付けます。適用されたポリシーの特定のネットワーク範囲内の IP アドレスからログインするユーザーには、そのポリシーの最小認証スコア以上の認証方法が提示されます。Workspace 展開環境における各 ID プロバイダ インスタンスもまた、ネットワーク範囲と認証方法を関連付けます。アクセス ポリシーを構成する際は、作成したネットワーク範囲と認証スコアのペアが、既存の ID プロバイダ インスタンスに対応していることを確認します。

アクセス ポリシーの作成時には、次の設定値を構成できます。

ネットワーク

各アクセスポリシーごとに、ネットワーク範囲を指定してユーザー ベースを決定します。ネットワーク範囲は、1 つ以上の IP 範囲から構成されます。アクセス ポリシー セットを構成する前に、管理コンソールの [ネットワーク範囲] ページでネットワーク範囲を作成します。

最小認証スコア

アクセス ポリシー セットの構成に先立ち、管理コンソールの [認証方法] ページを構成する際には、各認証方法に認証スコアを割り当てます。

Workspace でデフォルトでサポートされている認証方法は、Active Directory パスワード、Kerberos、および RSA SecurID です。サードパーティの ID プロバイダ インスタンスを Workspace 環境に統合する場合、Workspace はサードパーティ ID プロバイダがサポートする追加の認証方法をサポートするように拡張されます。

ユーザーが認証方法の 1 つを使用して Workspace にログインすると、Workspace によって認証の時間と認証に使用された方法が記録されます。

アクセス ポリシー セットが割り当てられた Web アプリケーションに、その後ユーザーがアクセスを試みると、Workspace により、ユーザーの現在の認証スコアとその Web アプリケーションへのアクセスに必要な認証スコアが比較されます。ユーザーの現在の認証スコアがリクエストされているアプリケーションで必要な認証スコアの最小スコアより低い場合、Workspace により、より強い認証を提供する ID プロバイダ インスタンスがユーザーにリダイレクトされます。ユーザーの現在の認証スコアが、要求されたアプリケーションで必要な最小認証スコア以上の場合、Workspace は有効時間の値を確認した後でアプリケーションを起動します。この後に示されている、有効時間についての説明を参照してください。次の状況では、Workspace はアプリ ポータルへのアクセスまたは Web アプリケーションの起動の要求を拒否します。

- 要求にポリシーが定義されていない。
- 最少認証スコアに認証を行う ID プロバイダ インスタンスが定義されていない。
- ユーザーがすべての認証方法で認証に失敗した。

有効時間

各アクセスポリシーごとに、有効時間（TTL）の値を割り当てます。TTL 値は、ユーザーが Workspace にアクセスするか、または特定の Web アプリケーションを起動した前回の認証イベント以来の最長時間を決定します。たとえば、Web アプリケーション ポリシーに TTL 値 <4> を指定すると、ユーザーが別の認証イベントを開始して TTL 値が延長される場合を除いて、Web アプリケーションを 4 時間起動できます。

Web アプリケーション固有のアクセス ポリシー セットの管理

Web アプリケーション固有のアクセス ポリシーを作成できます。たとえば、特定の Web アプリケーションについて、そのアプリケーションにアクセスできる IP アドレス、使用する認証方法、および再認証が必要になるまでの期間を指定するアクセス ポリシー セットを作成できます。

注意　ベスト プラクティスとして、Web アプリケーション固有のポリシーの最小認証スコアを、対応するネットワーク範囲を持つ、デフォルトのアクセス ポリシー セット内のポリシーの最小認証スコア以上に構成します。

次の Web アプリケーション固有のアクセス ポリシー セットは、指定した Web アプリケーションへのアクセスを制御するために作成できるポリシー セットの例です。第 5 章「アクセス ポリシー セットの管理 (P. 21)」を参照してください。

例 1：Web アプリケーション固有のポリシー セット

この例では、機密アプリケーションに対して作成および適用する可能性のあるポリシー セットを示します。

ポリシー名	ネットワーク	最小認証スコア	TTL（時間）
内部	内部範囲	1	8
外部	全範囲	3	4

ポリシーは上記の順で評価されます。ポリシー セットのポリシーを上または下にドラッグして評価の優先順位を変更できます。

上記のポリシー セットの例を、次の使用例に適用します。

厳密な Web アプリケーション固有のアクセス ポリシー セット、ブラウザの使用例

1 エンタープライズ ネットワークの外部から Workspace にアクセスするには、ユーザーは RSA SecurID を使用してログインする必要があります。この例では、RSA SecurID の最小認証スコアは 3 です。「デフォルトのアクセス ポリシー セットの編集 (P. 18)」の外部ポリシーの例を参照してください。ユーザーはブラウザを使用してログインし、デフォルトのアクセス ポリシー セットに指定されているように、4 時間のセッションまでアプリ ポータルにアクセスできます。

2 4 時間後に、ユーザーは例 1 の Web アプリケーション固有のポリシー セットが適用された Web アプリケーションを起動しようとします。

3 Workspace は、例 1 のポリシー セットのポリシーをチェックし、ユーザー リクエストが Web ブラウザと全範囲ネットワーク範囲から来ているため、全範囲ネットワーク範囲の外部ポリシーを適用します。

ユーザーは、機密アプリケーションの起動に適した認証スコアである最小認証スコア 3 でログインしていますが、ポリシーの TTL の期限が切れています。したがって、ユーザーは再認証にリダイレクトされます。再認証により、ユーザーには再度 4 時間のセッションが与えられ、アプリケーションの起動が許可されます。これに続く 4 時間、ユーザーは再認証する必要なしにアプリケーションを起動し続けることができます。

例 2：Web アプリケーション固有のポリシー セット

この例では、高機密アプリケーションに対して作成および適応する可能性のあるポリシー セットを示します。

ポリシー名	ネットワーク	最小認証スコア	TTL（時間）
ExtraSensitive	全範囲	レベル 3	1

上記のポリシー セットの例を、次の使用例に適用します。

非常に厳格な Web アプリケーション固有のアクセス ポリシー セットの使用例

1 ユーザーは、この例で認証レベル 1 になっているパスワード認証方法を使用してエンタープライズ ネットワークの内部からログインしています。「デフォルトのアクセス ポリシー セットの編集 (P. 18)」の内部ポリシーの例を参照してください。

これで、ユーザーはアプリ ポータルに 8 時間アクセスできます。

2 ユーザーは、例 2 のポリシー セットが適用された Web アプリケーションを直ちに起動しようとします。このためにはレベル 3 以上の認証が必要です。

3 ユーザーは、RSA SecurID 認証を要するレベル 3 以上の認証強度を提供する ID プロバイダにリダイレクトされます。

4 ユーザーがログインに成功すると、Workspace によりアプリケーションが起動され、認証イベントが保存されます。

ユーザーはこのアプリケーションを 1 時間継続して起動できますが、ポリシーに指定されているように 1 時間以内にレベル 3 以上の認証イベントを開始しなければ、1 時間後に再認証を求められます。

アクセス ポリシー セットの編集

Workspace 全体へのユーザーのアクセスを制御する既存のポリシー セットであるデフォルトのアクセス ポリシー セットは編集できます。また、以前に手動で作成した Web アプリケーション固有のポリシー セットも編集できます。

Web アプリケーション固有のアクセス ポリシー セット全体はいつでも削除できます。デフォルトのアクセス ポリシー セットは、永続的なものです。これは編集することはできますが、削除することはできません。

既存のデフォルト アクセス ポリシー セットまたは Web アプリケーション固有のアクセス ポリシー セットは、既存のポリシーをセットから削除するか、セット内の既存のポリシーを編集するか、または新しいポリシーをセットに追加することによって編集できます。アクセス ポリシー セットの概要については、第 5 章「アクセス ポリシー セットの管理 (P. 21)」を参照してください。

ポリシー セットの情報および例については、該当するトピックを参照してください。

- 「デフォルトのアクセス ポリシー セットの編集 (P. 18)」.
- 「Web アプリケーション固有のアクセス ポリシー セットの管理 (P. 22)」.

開始する前に

- 各自の環境に適した ID プロバイダを構成します。「ID プロバイダ インスタンスの追加と構成 (P. 15)」を参照してください。
- 各自の Workspace 展開環境に適したネットワーク範囲を構成します。「ネットワーク範囲の追加または編集 (P. 13)」を参照してください。
- 各自の展開環境に適した認証方法を構成します。「ユーザー認証方法の追加または編集 (P. 14)」を参照してください。

手順

1. Workspace 管理コンソール にログインします。
2. [ポリシー] - [アクセス ポリシー セット] を選択します。
3. (オプション) Web アプリケーション固有のアクセス ポリシー セットを完全に削除するには、そのポリシー セットに対して [削除] をクリックします。

   デフォルトのアクセス ポリシー セットに対して、[削除] オプションは使用できません。デフォルトのアクセス ポリシー セットは削除できません。
4. 構成する既存のポリシー セットの [編集] をクリックします。
5. (オプション) 必要に応じて、それぞれのテキスト ボックスでポリシー セットの名前と説明を変更します。

注意　Workspace では、[ポリシー セット名] および [説明] テキスト ボックスに英語でテキストが表示されます。テキストを異なる言語に変更するなど、このテキストは編集することができます。

---

6 (オプション) 必要に応じて、既存のポリシーを編集するか、既存のポリシーを削除するか、または新しいポリシーを追加します。

ベスト プラクティスとして、Web アプリケーション固有のポリシーの最小認証スコアを、対応するネットワーク範囲を持つ、デフォルトのアクセス ポリシー セット内のポリシーの最小認証スコア以上に構成します。

オプション	説明
既存のポリシーの編集	a 構成するポリシーの名前をクリックします。 b 必要に応じて、ポリシーの設定を変更します。 c [適用] をクリックします。
既存のポリシーの削除	a 削除するポリシーの名前をクリックします。 b [削除] をクリックします。
新しいポリシーの追加	a 新しいポリシーを追加するには、[+ アクセス ポリシー] をクリックします。 b 必要に応じて、ポリシーの設定を構成します。 c [追加] をクリックします。

7 [保存] をクリックします。

編集したアクセス ポリシー セットは直ちに有効になります。

次に進む前に

ポリシー セットがまだ適用されていない Web アプリケーション固有のアクセス ポリシー セットである場合は、そのポリシー セットを 1 つ以上の Web アプリケーションに適用します。

Web アプリケーション固有のアクセス ポリシー セットの追加

Web アプリケーション固有のポリシー セットを作成し、特定の Web アプリケーションへのユーザーのアクセスを制御できます。

アクセス ポリシー セットの概要については、第 5 章「アクセス ポリシー セットの管理 (P. 21)」を参照してください。Web アプリケーション固有のアクセス ポリシー セットの情報と例については、「Web アプリケーション固有のアクセス ポリシー セットの管理 (P. 22)」を参照してください。

開始する前に

- 各自の環境に適した ID プロバイダを構成します。「ID プロバイダ インスタンスの追加と構成 (P. 15)」を参照してください。
- 各自の Workspace 展開環境に適したネットワーク範囲を構成します。「ネットワーク範囲の追加または編集 (P. 13)」を参照してください。
- 各自の展開環境に適した認証方法を構成します。「ユーザー認証方法の追加または編集 (P. 14)」を参照してください。
- 特に Workspace を初期設定する際に Workspace 全体へのユーザーのアクセスを制御するデフォルトのポータル アクセス ポリシー セットの編集を計画している場合は、Web アプリケーション固有のポリシー セットを作成する前に構成します。

手順

1 Workspace 管理コンソール にログインします。

2 [ポリシー] - [アクセス ポリシー セット] を選択します。

3 [+ アクセス ポリシー セット] をクリックして、新しいポリシー セットを追加します。

4 それぞれのテキスト ボックスにポリシー セットの名前と説明を追加します。

5 [+ アクセス ポリシー] をクリックして、最初のポリシーを追加します。

6 必要に応じて、ポリシーの設定を構成します。

注意 ベスト プラクティスとして、Web アプリケーション固有のポリシーの最小認証スコアを、対応するネットワーク範囲を持つ、デフォルトのアクセス ポリシー セット内のポリシーの最小認証スコア以上に構成します。

7 [追加] をクリックします。

8 (オプション) ポリシー セットが組織のニーズに適合するまで、ポリシーを追加する手順を繰り返します。

9 [保存] をクリックして、ポリシー セットを保存します。

次に進む前に

ポリシー セットを 1 つ以上の Web アプリケーションに適用します。

Web アプリケーション固有のアクセス ポリシー セットの適用

Web アプリケーション固有のアクセス ポリシー セットを作成した後に、そのセットを特定の Web アプリケーションに適用して、これらのアプリケーションへのユーザーのアクセスを制御できます。

Workspace は、すべての新しい Web アプリケーションにデフォルトのアクセス ポリシー セットを適用します。デフォルトのアクセス ポリシー セットを上書きするには、Web アプリケーションに Web アプリケーション固有のポリシー セットを適用する必要があります。

開始する前に

Web アプリケーション固有のアクセス ポリシー セットがまだ作成されていない場合は作成し、特定の Web アプリケーションへのユーザーのアクセスを制御します。「Web アプリケーション固有のアクセス ポリシー セットの追加 (P. 25)」を参照してください。

手順

1 [カタログ] タブをクリックします。

2 [任意のアプリケーションの種類] - [Web アプリケーション] をクリックします。

3 Web アプリケーション固有のアクセス ポリシー セットを適用する Web アプリケーションをクリックします。

Web アプリケーションの情報ページが、デフォルトで選択される [資格] タブに表示されます。

4 [アクセス ポリシー] をクリックします。

5 [アクセス ポリシー セット] ドロップダウン メニューからアプリケーションに適用する Web アプリケーション固有のアクセス ポリシー セットを選択します。

6 [保存] をクリックします。

アクセス ポリシー セットは、アプリケーションへのユーザーのアクセスを制御するようになります。

ユーザーおよびグループの管理 6

ユーザーとグループ（Active Directory からインポートされたユーザーとグループ、ゲスト ユーザー、および Workspace グループを含む）を管理および監視できます。

Workspace 管理コンソール では、[ユーザー & グループ] ページで Workspace のユーザーとグループを中心としたビューが表示されます。たとえば、ユーザーの [資格] ページではユーザーにリソースの使用資格を付与でき、グループ [資格] ページではグループにリソースの使用資格を付与できます。また、[カタログ] ページを使用することで、Workspace のリソースを中心としたビューを確認することもできます。たとえば、リソースの [資格] ページでは、そのリソースの使用資格をユーザーまたはグループに付与できます。

この章では次のトピックについて説明します。

Workspace のユーザーとグループのタイプ

Workspace 管理コンソール を使用して、ユーザー、ゲスト ユーザー、グループを管理できます。

ユーザー

Workspace ユーザーは Active Directory からインポートされたユーザーです。Workspace ユーザー ベースは、ディレクトリ サーバの同期スケジュールに従って更新されます。

グループ

Workspace 管理コンソール に表示される可能性があるグループのタイプは、ディレクトリ サーバからインポートされたグループと、Workspace を使用して自分で作成した Workspace グループです。

グループ タイプ	説明
ディレクトリ サーバ グループ	Connector Services Admin Directory Sync、[グループを選択] ページを使用して Active Directory から Workspace にグループをインポートします。管理コンソール で、グループ名の横にあるロック アイコンはそのグループがディレクトリ サーバ グループであることを示します。Workspace を使用して、ディレクトリ サーバ グループを編集または削除することはできません。インポートされたディレクトリ サーバ グループは、ディレクトリ サーバの同期スケジュールに従って Workspace で更新されます。
Workspace グループ	Workspace 管理コンソール を使用して、Workspace グループを作成します。このグループをカスタマイズして、企業内で Workspace を最適な方法で使用できるようにします。ユーザーとグループの組み合わせを追加することで、Workspace グループを作成できます。追加するグループは、既存の Workspace グループか、ディレクトリ サーバからインポートされたグループのいずれかです。管理コンソール では、グループ名の横のチェック ボックスは、そのグループが Workspace グループであることを示します。Workspace を使用すると、Workspace グループの削除やグループ内のユーザーの変更を行うことができます。

グループのメンバーに対してアクセスおよび使用資格を付与するリソースを指定できます。各個人ユーザーの資格を定義するのではなく、グループに資格を付与することで、一連のユーザーに資格を付与できます。ユーザーは複数のグループに属することができます。たとえば、セールス グループと管理グループを作成した場合、セールス マネージャは両方のグループに属することができます。グループのメンバーに適用するモバイル ポリシー設定を指定できます。

Workspace グループの管理

グループの作成、グループのメンバーシップの変更、およびグループの削除は、Workspace グループにのみ適用する Workspace で実行できるタスクです。グループへのリソースの使用資格の付与は、Workspace グループと Active Directory グループの両方に対して実行できるタスクです。

手順

- Workspace グループを作成するには、[ユーザー & グループ] - [グループ] を選択して、[グループを作成] をクリックし、グループ名と説明を入力します。
- 1 つ以上の Workspace グループを削除するには、[ユーザー & グループ] - [グループ] を選択して、削除する Workspace グループに対応しているチェック ボックスをオンにし、[グループを削除] をクリックします。

  削除できるのは、Workspace グループだけです。Active Directory グループ名の横に表示されているロック アイコンは、そのグループが Active Directory グループであり、Workspace を使用してグループを編集や削除できないことを示しています。

Workspace のグループ メンバーシップの変更

Workspace のグループ メンバーシップを変更できます。

各ユーザーに個別に使用資格を付与するのではなく、グループを使用して複数のユーザーに同じリソースの使用資格を同時に付与します。

グループ ルールを使用して、特定の Workspace グループに属するユーザーを定義します。ユーザーは複数のグループに属することができます。たとえば、セールス グループと管理グループを作成した場合、セールス マネージャは両方のグループのメンバーになることができます。

手順

1 Workspace 管理コンソール にログインします。

2 [ユーザー & グループ] - [グループ] を選択します。

- グループ名の横のチェック ボックスは、そのグループが Workspace グループであることを示します。
- グループ名の横のロック アイコンは、そのグループがディレクトリ サーバ グループであることを示します。ディレクトリ サーバ グループは、ディレクトリ サーバで直接管理します。Workspace を使用して、ディレクトリ サーバ グループのメンバーシップを定義することはできません。

3 メンバーシップを変更する Workspace グループの名前をクリックします。

4 [このグループのユーザー] タブをクリックします。

グループの現在のメンバーであるユーザーのリストが表示されます。

5 [このグループのユーザーを変更] をクリックします。

6 ドロップダウン メニューからオプションを選択します。

オプション	操作
次のいずれか	グループ メンバーシップのいずれかの条件が満たされた場合にグループ メンバーシップを付与します。このオプションは OR 条件のように機能します。たとえば、「グループが次であるもの：セールス」と「グループが次であるもの：マーケティング」というルールに [次のいずれか] を選択すると、セールスとマーケティングのスタッフにこのグループのメンバーシップが付与されます。
次のすべて	グループ メンバーシップのすべての条件が満たされた場合にグループ メンバーシップを付与します。これは AND 条件のように機能します。たとえば、「グループが次であるもの：セールス」と「メールが次で始まるもの：'western_region'」というルールに [次のすべて] を選択すると、西部地域のセールス スタッフだけにこのグループのメンバーシップが付与されます。他の地域のセールス スタッフにメンバーシップは付与されません。

7 Workspace グループに 1 つ以上のルールを構成します。

ルールはネストできます。

オプション	操作
グループ	■ この Workspace グループに関連付けるグループを選択する場合は、[次であるもの] を選択します。テキスト ボックスにグループ名を入力します。入力すると、グループ名のリストが表示されます。 ■ この Workspace グループから除外するグループを選択する場合は、[次ではないもの] を選択します。テキスト ボックスにグループ名を入力します。入力すると、グループ名のリストが表示されます。
属性ルール	次のルールは、デフォルトの属性や、企業で構成され追加されたカスタム属性など、すべての属性で利用できます。属性の例としては、メールや電話が挙げられます。 注意　ルールでは大文字と小文字が区別されません。 ■ 入力した条件と完全に一致するディレクトリ サーバ エントリにグループ メンバーシップを付与する場合は、[次と一致するもの]を選択します。たとえば、同じ代表電話番号を共有する出張担当部署があるとします。その電話番号を共有するすべての従業員に対して旅行予約アプリケーションのアクセス権を付与する場合は、「電話番号が次と一致するもの：(555) 555-1000」といったルールを作成できます。 ■ 入力した条件に一致するディレクトリ サーバ エントリを除いてグループ メンバーシップを付与する場合は、[次と一致しないもの] を選択します。たとえば、いずれかの部署で代表電話番号を共有している場合に、その部署でソーシャル ネットワーキング アプリケーションにアクセスできないようにするには、「電話番号が次と一致しないもの：(555) 555-2000」といったルールを作成できます。 ■ 入力した条件で始まるディレクトリ サーバ エントリにグループ メンバーシップを付与する場合は、[次で始まるもの] を選択します。たとえば、組織のメール アドレスが sales_username@example.com のように部署名から始まるとします。セールス スタッフ全員にアプリケーションのアクセス権を付与する場合は、「メールが次で始まるもの：sales_」といったルールを作成できます。 ■ 入力した条件で始まるディレクトリ サーバ エントリを除いてグループ メンバーシップを付与する場合は、[次で始まらないもの] を選択します。たとえば、人事部のメール アドレスが hr_username@example.com という形式である場合は、「メールが次で始まらないもの：hr_」といったルールを設定すれば、人事部からのアプリケーションへのアクセスを拒否できます。この場合、それ以外のメール アドレスを使用するディレクトリ サーバ エントリからは、アプリケーションにアクセスできます。

オプション	操作
次のいずれか	このルールでグループ メンバーシップのいずれかの条件が満たされた場合にグループ メンバーシップが付与されます。ここではルールをネストする方法を説明します。たとえば、「グループが次であるもの：セールス」と「グループが次であるもの：カリフォルニア」の両方を指定するルールを作成できます。「グループが次であるもの：カリフォルニア」の場合に [次のいずれか] を選択して、「電話番号が次で始まるもの：415」、「電話番号が次で始まるもの：510」を指定します。グループ メンバーは、カリフォルニア セールス スタッフに所属し、電話番号が 415 または 510 のいずれかで始まる必要があります。
次のすべて	このルールですべての条件が満たされた場合にグループ メンバーシップが付与されます。ここではルールをネストする方法を説明します。たとえば、「グループが次であるもの：マネージャ」と「グループが次であるもの：カスタマ サービス」のいずれかを指定するルールを作成します。「グループが次であるもの：カスタマ サービス」の場合に、[次のすべて] を選択して、「メールが次で始まるもの：cs_」、「電話番号が次で始まるもの：555」を指定します。この場合、グループ メンバーには、マネージャまたはカスタマ サービス担当者のいずれかで、かつカスタマ サービス担当者の場合はメールが「cs_」で始まり、電話番号が「555」で始まるものに限定されます。

8 (オプション) この Workspace グループに対して追加または除外するユーザーを個別に指定するには、適切なチェック ボックスをオンにして、ユーザー名を入力します。

9 [次へ] をクリックしてから、[保存] をクリックします。

Workspace グループ情報

Workspace 管理コンソールを使用して、使用資格が付与されているリソース、メンバーシップ、適用されているモバイル ポリシー セットなど、グループについての詳細情報を表示できます。

手順

1 Workspace 管理コンソール にログインします。

2 [ユーザー & グループ] - [グループ] をクリックします。

このページには、Workspace 展開環境のすべてのグループのリストと、各グループの詳細情報が表示されます。

- グループ名の横のチェック ボックスは、そのグループが Workspace グループであることを示します。Workspace グループは、Workspace 内で定義および管理します。
- グループ名の横のロック アイコンは、そのグループがディレクトリ サーバ グループであることを示します。ディレクトリ サーバ グループは、組織のディレクトリ サーバで管理します。
- このページには、各グループの次の情報が表示されます。

情報のタイプ	説明
ユーザー数	グループ内のメンバー数。
アプリケーション数	グループ全体に資格付与されているリソース数。
ユーザー ストア	Active Directory グループが関連付けられているユーザー ストア。Workspace がマルチ フォレストの Active Directory 環境にデプロイされている場合を除き、展開環境には default という名前の単一のユーザー ストアが含まれます。

3 グループ名をクリックします。

グループの詳細ページが、ページ上部にグループ名を表示して、表示されます。

4 表示したい情報に対応するタブをクリックします。

オプション	説明
[資格]	グループの資格ページが表示されます。このページでは、以下を実行できます。 ■ グループのユーザーに使用資格が付与されているリソースのリストを表示します。 ■ [資格を追加] をクリックして、カタログで利用可能なリソースの使用資格をグループのユーザーに付与します。 ■ リスト内で使用資格が付与されたリソースの名前をクリックして、そのリソースの編集ページを表示します。 ■ [編集] ボタンを使用できるリソース タイプの場合、このボタンをクリックすると、そのタイプのリソースに対してグループのユーザーの使用資格を付与/解除したり、使用資格が付与された各リソースのオプションをカスタマイズできます。[資格] ページから、以下のように変更を加えることができます。 ■ Web アプリケーションについては、[編集] をクリックして、Web アプリケーションのグループの使用資格またはグループに使用資格が付与された各 Web アプリケーションの展開タイプを変更します。ユーザー ポータルにデフォルトで Web アプリケーションを表示するには、[自動] を選択します。ユーザーが使用できるアプリケーションを集めた App Center からユーザーの [マイアプリ] エリアに Web アプリケーションを追加できるようにするには、[ユーザーによるアクティブ化] を選択します。 ■ View デスクトップ プールおよびアプリケーション プールの場合は、Workspace システムと統合した View プールのグループの既存の使用資格を表示できます。View デスクトップ プールおよびアプリケーション プールの使用資格は、Workspace システムと統合された View 接続サーバ インスタンスで設定します。グループの [資格] ページで、View プールの使用資格を変更することはできません。 ■ ThinApp パッケージについては、[編集] をクリックして、ThinApp パッケージのグループの使用資格またはグループに使用資格が付与された ThinApp パッケージの展開タイプを変更します。ユーザー ポータルの [マイアプリ] エリアにデフォルトで ThinApp パッケージを表示するには、[自動] を選択します。ユーザーがアプリ カタログから [マイアプリ] エリアに ThinApp パッケージを手動で追加できるようにするには、[ユーザーによるアクティブ化] を選択します。 ■ Citrix 公開アプリケーションについては、Workspace システムと統合した Citrix ベース アプリケーションに対するグループの既存の使用資格を表示できます。Citrix ベース アプリケーションの資格は、Workspace システムと統合された Citrix 展開環境で設定します。 グループの [資格] ページで、Citrix ベース アプリケーションの資格を変更することはできません。 ■ [資格を解除] ボタンを使用できるリソース タイプの場合は、このボタンをクリックしてその特定のリソースを使用するグループ アクセスを削除できます。 注意 [プロビジョニングのステータス] 列は使用されません。デフォルトでは、このページでエントリが入力されている表の行は、[プロビジョニングのステータス] 列に [使用不可] と表示されており、この値は変更できません。
[このグループのユーザー]	グループのメンバーシップのページが表示されます。このページでは、以下を実行できます。 ■ グループに属しているユーザーのリストを表示します。 ■ 詳細ページを表示するユーザーの名前をクリックします。 ■ [このグループのユーザーの変更] をクリックして、 Workspace グループにメンバーシップを定義するルールを設定し、表示します。[このグループのユーザーの変更] オプションは、Workspace グループで利用できますが、ディレクトリ サーバ グループには利用できません。

Workspace ユーザーを管理

Workspace 管理コンソール を使用して、Active Directory からインポートしたユーザーを管理できます。

Workspace でのユーザー管理には、リソースの使用資格をユーザーに付与する、適切な Workspace グループにユーザーを追加する、プロビジョニングされたユーザーのワークスペースの状態を管理する、といったタスクがあります。

Workspace ユーザー情報

Workspace 管理コンソールを使用して、ユーザーに使用資格が付与されているリソース、グループ加入、プロビジョニングされているデスクトップ システムやモバイル デバイスなど、ユーザーについての詳細情報を表示できます。

ユーザー属性は、データ ノードのホスト名属性や、同期中にディレクトリ サーバから取得するよう Workspace を構成した追加属性など、表示可能なユーザー情報の 1 つです。個別ユーザーの追加ディレクトリ サーバ属性を表示することが役立つかどうかは、そのような属性を環境内でどのように使用するかによって異なります。これら追加属性は以下のように使用できます。

- Workspace グループのメンバーシップを変更します。たとえば、Active Directory でマネージャの属性を使用する場合、そのマネージャの属性を Workspace にマップできます。グループ ルールによって Workspace ユーザー レコードにマネージャの属性があるユーザーのみをメンバーにするようなグループを作成できます。
- 特定の属性要件で、ユーザーが Web アプリケーションにアクセスできるようにします。たとえば、財務アプリケーションの場合は、Workspace ユーザー レコードに従業員 ID 属性があるユーザーにアクセスを制限することが考えられます。

手順

1 Workspace 管理コンソール にログインします。

2 [ユーザー & グループ] - [ユーザー] を選択します。

すべての Workspace ユーザーがページに表示されます。

3 ユーザー名をクリックします。

ユーザーの詳細ページが表示されます。ユーザー名、メール アドレス、ロールがページ上部に表示されます。

4 (オプション) ユーザーのロールを変更するには、表示されているロールの名前（[ユーザー] または [管理者]）をクリックします。

ユーザーを管理者ロールに昇格させて、Workspace 管理コンソールにアクセスできるようにすることが可能です。管理者ロールが割り当てられても、引き続きユーザーとして Web からアプリケーション ポータルにアクセスできます。管理コンソールにアクセスするための URL は、Web クライアントにアクセスするための URL とは異なります。

以下の URL の場合、プレースホルダの <WorkspaceFQDN> は実際の値に置き換えます。

Web インターフェイス	必要なロール	URL 例
Workspace 管理コンソール	管理者	https://<WorkspaceFQDN>/admin
Workspace アプリ ポータル	ユーザー	https://<WorkspaceFQDN>/web

5 (オプション) [追加属性を表示] をクリックして、ディレクトリ サーバ属性など、ユーザーに割り当てられている追加属性を確認します。

6 表示したい情報に対応するタブをクリックします。

オプション	説明
[資格]	ユーザーの資格ページが表示されます。このページでは、以下を実行できます。 ■ ユーザーに使用資格が付与されているリソースのリストを表示します。 ■ [資格を追加] をクリックして、カタログで利用可能なリソースの使用資格をユーザーに付与します。 ■ リスト内で使用資格が付与されたリソースの名前をクリックして、そのリソースの編集ページを表示します。 ■ [編集] ボタンを使用できるリソース タイプの場合、このボタンをクリックすると、そのタイプのリソースに対してグループのユーザーの使用資格を付与/解除したり、使用資格が付与された各リソースのオプションをカスタマイズできます。[資格] ページから、以下のように変更を加えることができます。 ■ Web アプリケーションについては、[編集] をクリックして、Web アプリケーションのユーザーの使用資格またはユーザーに使用資格が付与された各 Web アプリケーションの展開タイプを変更します。ユーザー ポータルにデフォルトで Web アプリケーションを表示するには、[自動] を選択します。ユーザーが使用できるアプリケーションの集まりであるアプリ センターからユーザーの [My Apps] エリアに Web アプリを追加できるようにするには、[ユーザーによるアクティブ化] を選択します。 ■ View デスクトップ プールおよびアプリケーション プールの場合は、Workspace システムと統合した View プールのユーザーの既存の使用資格を表示できます。View デスクトップ プールおよびアプリケーション プールの使用資格は、Workspace システムと統合された View 接続サーバ インスタンスで設定します。ユーザーの [資格] ページで、View プールの使用資格を変更することはできません。 ■ ThinApp パッケージの場合は、[編集] をクリックして、ThinApp パッケージのユーザーの使用資格またはユーザーに使用資格が付与された ThinApp パッケージの展開タイプを変更します。ユーザー ポータルの [マイアプリ] エリアにデフォルトで ThinApp パッケージを表示するには、[自動] を選択します。ユーザーがアプリ カタログから [マイアプリ] エリアに ThinApp パッケージを手動で追加できるようにするには、[ユーザーによるアクティブ化] を選択します。 ■ Citrix 公開アプリケーションの場合は、Workspace システムと統合した Citrix ベース アプリケーションのユーザーの既存の使用資格を表示できます。Citrix ベース アプリケーションの資格は、Workspace システムと統合された Citrix 展開環境で設定します。 ユーザーの [資格] ページで、Citrix ベース アプリケーションの資格を変更することはできません。 ■ [資格を解除] ボタンを使用できるリソース タイプの場合は、このボタンをクリックしてそのリソースを使用するユーザー アクセスを削除できます。 注意 [プロビジョニングのステータス] 列は使用されません。デフォルトでは、このページでエントリが入力されている表の行は、[プロビジョニングのステータス] 列に [使用不可] と表示されており、この値は変更できません。
[グループ加入]	ユーザーが属しているグループのリストが表示されます。各グループ名は、ユーザーがメンバーになっているグループを表します。グループ名をクリックすれば、そのグループの詳細ページが表示されます。
[ワークスペース]	ユーザーのワークスペース ページが表示されます。このページでは、ワークスペースの現在のステータス情報を含む、ユーザーのデスクトップ システムにプロビジョニングされているデスクトップ ワークスペースを表示できます。 ■ デスクトップ システムの場合は、[削除] をクリックすれば、対応するシステムを Workspace から削除できます。Workspace からシステムを削除する理由としては、システムが紛失した、盗まれた、使用されないなどが考えられます。

Active Directory で同期されているユーザーとグループの変更

Workspace のセットアップ時に、Active Directory サーバに接続するための情報を入力し、どのユーザーを Workspace Directory に同期するかを指定する Active Directory のユーザー属性とフィルターを選択し、追加する Active Directory グループを選択しています。これらの設定は、Connector Services Admin の [ディレクトリ同期] ページで変更できます。

これらのページで実行し保存した変更は、次回のディレクトリ同期の後で Workspace 上で自動的に更新されます。「Workspace のユーザーを選択する設定の変更 (P. 34)」を参照してください。

[ユーザー属性をマップ] ページの変更

[ユーザー属性をマップ] ページには、Active Directory の属性と Workspace の属性間のマッピングが表示されます。ユーザーに関する追加情報を Active Directory から取得する場合は、ユーザー属性を [ユーザー属性をマップ] ページに追加します。

[ユーザー属性をマップ] ページにマッピングされたデフォルトのユーザー属性の 1 つは、アカウントを無効化する属性です。UserAccountControl 属性は Workspace が無効化された属性にマッピングされます。Active Directory の UserAccountControl 属性のフラグが UF_Account_Disable に設定されていると、Workspace ディレクトリのユーザーは無効になります。

アカウントが無効になると、ユーザーはログインしてアプリケーションとリソースにアクセスすることができません。ユーザーに使用資格が付与されているリソースはアカウントから削除されないため、フラグがアカウントから削除されても、ユーザーはログインして使用資格が付与されているリソースにアクセスすることができます。

Workspace のユーザーを選択する設定の変更

Workspace のセットアップ時に、Active Directory、ユーザー属性、および Workspace で使用する Active Directory ユーザーを選択するためのフィルタを指定します。Connector Services Admin ページからこれらの設定を更新できます。

開始する前に

新規ベース DN、含めるユーザー属性、含めるグループなど、変更する内容を確認します。

手順

1 Workspace 管理者パスワードを使用して Connector Services Admin にログインします。

2 適切な処理を実行します。

オプション	操作
サーバ ホスト、ベース DN、バインド パスワードなど、Active Directory サーバ情報を変更します。	a [ディレクトリ] をクリックします。 b 変更します。 c [保存] をクリックします。
Workspace ユーザー属性と Active Directory ユーザー属性のマッピングを変更します。	a [ユーザー属性をマップ] をクリックします。 b 変更します。 c [保存] をクリックします。
Workspace と同期している特定の Active Directory ユーザーを除外し、Workspace と同期している Active Directory グループを更新するフィルタを作成します。	a [ディレクトリ同期] をクリックします。 b [ディレクトリ同期ルールを編集] をクリックします。 c 必要に応じて [ユーザーを選択] ページで変更を加え、[保存] をクリックします。 d 必要に応じて [グループを選択] ページで変更を加え、[保存] をクリックします。 e [Workspace にプッシュ] をクリックします。 f [保存して続行] をクリックします。

7 Workspace カタログの管理

Workspace カタログは、ユーザーに使用資格を付与できる全リソースのリポジトリです。カタログで特定のリソース タイプが利用できるかどうかは、Workspace で有効になっているモジュールによって制御されます。

カタログを表示するには、Workspace 管理コンソール で [カタログ] タブをクリックします。[カタログ] ページで次のタスクを実行できます。

- 新規リソースをカタログに追加する。
- 現在ユーザーに使用資格を付与できるリソースを表示する。
- カタログ内の各リソースについての情報にアクセスする。

タイプによっては、[カタログ] ページを使用して直接カタログに追加できるリソースもあります。他のリソース タイプでは、管理コンソール 以外での操作が必要になります。リソースのセットアップについては、 『VMware Workspace Portal ガイド』の「リソースのセットアップ」を参照してください。

リソース	リソースをカタログに表示する方法
Web アプリケーション	Web アプリケーション モジュールを有効にします。管理コンソール を使用して、[カタログ] ページでアプリケーションの種類として [Web アプリケーション] を選択します。
ThinApp パッケージとしてキャプチャされた仮想 Windows アプリケーション	Connector Services Admin の [パッケージ化されたアプリ - ThinApp] ページで、ThinApp パッケージをカタログと同期します。管理コンソール を使用して、[カタログ] ページでアプリケーションの種類として [ThinApp パッケージ] を選択します。
View デスクトップ プール	Connector Services Admin の [View プール] ページで View プールをカタログと同期します。管理コンソール を使用して、[カタログ] ページでアプリケーションの種類として [View デスクトップ プール] を選択します。
View でホストされているアプリケーション	Connector Services Admin の [View プール] ページで View がホストするアプリケーションとカタログを同期します。管理コンソール を使用して、[カタログ] ページでアプリケーションの種類として [View でホストされているアプリケーション] を選択します。
Citrix ベース アプリケーション	Connector Services Admin の [公開アプリケーション - Citrix] ページで、Citrix ベース アプリケーションをカタログと同期します。管理コンソール を使用して、[カタログ] ページでアプリケーションの種類として [Citrix 公開アプリケーション] を選択します。

この章では次のトピックについて説明します。

Workspace リソース タイプの概要

資格とユーザーへの配布のためにカタログ内で定義できるリソース タイプは、Web アプリケーション、VMware ThinApp パッケージとしてキャプチャされる Windows アプリケーション、Citrix ベース アプリケーション、VMware View デスクトップ プール、および View でホストされているアプリケーションです。

特定のリソースの使用資格をユーザーに付与できるようにするには、そのリソースをカタログに格納する必要があります。リソースをカタログに格納する場合に使用する方法は、リソースのタイプによって異なります。

これらのリソースの情報、要件、インストールおよび構成については、 『VMware Workspace Portal ガイド』の「リソースのセットアップ」を参照してください。

Web アプリケーション

Workspace 管理コンソール の [カタログ] ページで、Web アプリケーションをカタログに直接格納します。[カタログ] ページに表示されている Web アプリケーションをクリックすると、そのアプリケーションについての情報が表示されます。表示されたページで Web アプリケーションを構成できます。たとえば、適切な SAML 属性を指定し、Workspace とターゲットの Web アプリケーション間にシングル サインオンを構成できます。Web アプリケーションが構成されると、その Web アプリケーションの使用資格をユーザーとグループに付与できるようになります。「カタログにリソースを追加 (P. 39)」を参照してください。

ThinApp パッケージ

次のタスクを実行することで、ThinApp パッケージとしてキャプチャされた Windows アプリケーションをカタログに格納します。

1 ユーザーがアクセスする ThinApp パッケージがまだ存在しない場合は、Workspace と互換性のある ThinApp パッケージを作成します。VMware ThinApp に関するドキュメントを参照してください。

2 ネットワーク共有を作成し、互換性のある ThinApp パッケージをそこに格納します。

3 ネットワーク共有上のパッケージと統合するように、Workspace を構成します。

これらのタスクを実行すると、仮想 Windows アプリケーションや、ネットワーク共有に追加した ThinApp パッケージがリソースとしてカタログで利用できるようになります。そして、リソースの使用資格をユーザーに付与できます。

Workspace によって配布および管理される ThinApp パッケージを起動および実行するには、Windows システム上に Workspace for Windows をインストールしておく必要があります。

Citrix 公開アプリケーション

次のタスクを実行することで、Citrix ベース アプリケーションをカタログに格納します。

1 まだ Citrix サーバを展開していない場合は、展開します。これには、Citrix ベース アプリケーションの使用資格をユーザーに付与することも含まれます。適切な Citrix のドキュメントを参照してください。

2 Citrix サーバと Workspace 展開環境を統合します。

これらのタスクを実行すると、Citrix サーバによってユーザーに使用資格を付与した Citrix ベース アプリケーションがカタログでリソースとして利用できるようになります。

View デスクトップ プール

次のタスクを実行して、 View デスクトップ プールと、それに対応する View デスクトップをカタログに格納します。

1 まだ View デスクトップ プールを VMware View に展開していない場合は、展開します。これには、ユーザーにデスクトップの使用資格を付与することも含まれます。VMware View のドキュメントを参照してください。

2 VMware View と Workspace 展開環境を統合します。

これらのタスクを実行すると、VMware View でユーザーに使用資格を付与した View デスクトップがカタログでリソースとして利用できるようになります。

View でホストされているアプリケーション

次のタスクを実行することで、View アプリケーション プールをカタログに格納します。

1 アプリケーション プールが View にリモート デスクトップ サービスとして展開されていることを確認してください。View のドキュメントを参照してください。

2 Workspace 展開環境を View に統合する

これらのタスクを実行すると、View でユーザーに使用資格を付与したホストされているアプリケーション プールがカタログでリソースとして利用できるようになります。

リソース カテゴリの使用の概要

カタログ リソースを検索するデフォルトの方法は、リソース タイプで検索する方法です。カテゴリで検索することもできます。

カテゴリで Workspace Catalog リソースを検索できるようにするには、カテゴリを作成してリソースに適用します。

リソース カテゴリの作成

Workspace リソース カテゴリは、作成した後すぐには適用しないでおくことも、作成と適用を同時に行うことも可能です。

手順

1 Workspace 管理コンソール にログインします。

2 [カタログ] タブをクリックします。

3 1 つ以上のリソースのチェックボックスをクリックします。

リソースを選択すると、[カテゴリの適用] ボタンがアクティブ化されます（この状態はカテゴリの作成に必須）。カテゴリの作成と適用を同時に行うには、新しいカテゴリの適用先となるすべてのリソースのチェックボックスをクリックします。カテゴリを作成した後すぐには適用しないでおく場合、選択したリソースに意味はありません。この場合、カタログ内の任意のリソースのチェックボックスをクリックできます。

4 [カテゴリの適用] をクリックします。

5 [カテゴリの検索] テキスト ボックスに、新しいカテゴリ名を入力します。

6 [カテゴリの追加...] をクリックします。

Workspace によって新しいカテゴリが作成されますが、適用は行われません。

7 (オプション) 選択したリソースにカテゴリを適用するには、新しいカテゴリ名のチェックボックスをクリックします。

Workspace によって、選択したリソースにそのカテゴリが適用されます。

次に進む前に

リソースにカテゴリを適用するのが妥当であれば、この操作を行います。「リソースへのカテゴリの適用 (P. 38)」を参照してください。

リソースへのカテゴリの適用

カテゴリを作成した後、そのカテゴリをカタログ内の任意のリソースに適用できます。

開始する前に

リソース カテゴリを作成します。

手順

1 Workspace 管理コンソール にログインします。

2 [カタログ] タブをクリックします。

3 カテゴリの適用先となるすべてのリソースのチェックボックスをクリックします。

4 [カテゴリの適用] をクリックし、適用するカテゴリの名前を選択します。

選択したリソースにそのカテゴリが適用されます。

カテゴリの除去または削除

リソースに対するカテゴリの関連付けを解除することも、カタログからカテゴリを永久的に除去することもできます。

カテゴリ ラベルを除去することによって、リソースに対するカテゴリの関連付けを解除できます。また、カタログから永久的にカテゴリを削除することも可能です。カテゴリを永久的に削除した時点で、カテゴリはカタログから消えます。[任意のカテゴリ] ドロップダウン メニューに表示されなくなり、これまでの適用先であるリソースのどれにもラベルとして表示されなくなります。

手順

1 Workspace 管理コンソール にログインします。

2 [カタログ] タブをクリックします。

3 1 つ以上のリソースのチェックボックスをクリックします。

リソースを選択すると、[カテゴリの適用] ボタンがアクティブ化されます（この状態はカテゴリの除去と削除に必須）。カテゴリ ラベルを 1 つ以上のリソースから除去するには、カテゴリ ラベルを除去するすべてのリソースのチェックボックスをクリックします。カテゴリを永久的に削除する場合、選択したリソースに意味はありません。この場合、カタログ内の任意のリソースのチェックボックスをクリックできます。

4 [カテゴリの適用] をクリックします。

オプション	説明
リソースからのカテゴリの除去	ラベルのチェックボックスが選択されています。そのチェックボックスをクリックして、選択したリソースからカテゴリ ラベルを除去します。
カテゴリの永久削除	カテゴリ上にマウスを合わせます。「x」が表示されます。この「x」をクリックし、カタログからカテゴリを永久的に除去します。

Workspace リソースへのアクセス

カタログにアクセスして、ユーザーに使用資格を付与できるリソース（Workspace Web アプリケーション、ThinApp パッケージ、Citrix ベース アプリケーション、View デスクトップ プール）の情報を表示できます。アプリケーション タイプ別またはカテゴリ別にリソースを表示できます。

開始する前に

- ユーザーに使用資格を付与したいリソース タイプに対応するリソース モジュールを有効にします。有効にできるモジュールとして、Web アプリケーション モジュール、モバイル管理モジュール、View モジュール、ThinApp パッケージ モジュール、および Citrix 公開アプリケーション モジュールがあります。

- 企業のニーズに合わせてリソースをカタログに追加します。第 7 章「Workspace カタログの管理 (P. 35)」を参照してください。
- カテゴリ別にリソースを表示するには、カテゴリを作成して適用します。「リソース カテゴリの使用の概要 (P. 37)」を参照してください。

手順

1 Workspace 管理コンソール にログインします。

2 [カタログ] タブをクリックします。

Workspace に、カタログ内のすべてのリソースが表示されます。

3 (オプション) ソート方法を変更するには、[アプリケーション] または [アプリケーション タイプ] をクリックします。

4 (オプション) 特定の種類別にリソースを表示するには、[任意のアプリケーション タイプ] ドロップダウン メニューからリソースの種類を選択します。

Workspace に追加されていないアプリケーションの種類は、ドロップダウン メニューに表示されません。

オプション	説明
[任意のアプリケーション タイプ]	カタログ内のすべてのリソースが表示されます。
[Web アプリケーション]	カタログ内の Web アプリケーションだけが表示されます。Web アプリケーションには、SaaS アプリケーションや、企業内で管理されている Web アプリケーションも含みます。
[ThinApp パッケージ]	ThinApp パッケージとしてキャプチャされた Windows アプリケーションだけが表示されます。Workspace の構成時に ThinApp パッケージを展開環境に追加してから管理コンソールにアクセスすると、ThinApp パッケージがカタログに表示されます。
[View デスクトップ プール]	View デスクトップ プールだけが表示されます。Workspace を VMware View に統合してから Workspace 管理コンソールにアクセスすると、View デスクトップ プールがカタログに表示されます。
[View でホストされているアプリケーション]	View でホストされているアプリケーションのみをリストします。Workspace を View に統合してから 管理コンソール にアクセスすると、View でホストされているアプリケーションがカタログに表示されます。
[Citrix 公開アプリケーション]	Citrix ベース アプリケーションのみが表示されます。Workspace を Citrix 展開環境に統合してから管理コンソールにアクセスすると、Citrix ベース アプリケーションがカタログに表示されます。

5 (オプション) 特定カテゴリ別にリソースを表示するには、[任意のカテゴリ] ドロップダウン メニューから 1 つまたは複数のカテゴリ名を選択します。

Workspace に、選択した条件を満たすすべてのリソースが表示されます。

- 1 つのカテゴリを選択した場合、Workspace にそのカテゴリ ラベルが付けられたすべてのリソースが表示されます。
- 複数のカテゴリを選択した場合、Workspace には選択したすべてのカテゴリ ラベルが付けられたリソースのみが表示されます。

6 特定のリソースの詳細を表示するには、そのリソースのアイコンをクリックします。

カタログにリソースを追加

Workspace 管理コンソール の [カタログ] ページを使用して、直接カタログに Web アプリケーションを追加することができます。

Web アプリケーションをカタログに追加する手順については、『VMware Workspace Portal でのリソースのセットアップ』ガイドで「Web アプリケーションへのアクセス」の章を参照してください。

以下では、このようなタイプのリソースをカタログに追加する場合の手順の概要を示します。

手順

1 Workspace 管理コンソール にログインします。

2 [カタログ] タブをクリックします。

3 [+ アプリケーションを追加] をクリックします。

4 リソース タイプ、およびアプリケーションの場所に応じてオプションをクリックします。Android ワークスペース イメージをインポートする場合は、この手順でオプションをクリックする必要はありません。

リンク名	リソース タイプ	説明
[Web アプリケーション ...クラウド アプリケーション カタログより]	Web アプリケーション	Workspace では、クラウド アプリケーション カタログで使用できるいくつかのデフォルトの Web アプリケーションにアクセスできます。それらはカタログにリソースとして追加できます。
[Web アプリケーション ... 新規作成]	Web アプリケーション	適切なフォームに入力することで、リソースとしてカタログに追加する Web アプリケーションのアプリケーション レコードを作成できます。
[Web アプリケーション ... ZIP または JAR ファイルをインポート]	Web アプリケーション	Workspace で構成済みの Web アプリケーションをインポートできます。この方法は、ステージング環境から本番環境に Workspace の環境を展開する際に使用することをお勧めします。そのような場合は、ステージング環境から ZIP ファイルで Web アプリケーションをエクスポートします。それからその ZIP ファイルを本番環境にインポートします。

5 画面の指示に従ってカタログへのリソースの追加を完了します。

ユーザー、グループ、またはカタログ リソースを検索

8

Workspace 管理コンソールの検索テキスト ボックスを使用して、カタログ内の Workspace のユーザー、グループ、またはリソースを検索します。

手順

1 Workspace 管理コンソール にログインします。

2 検索テキスト ボックスに文字列を入力します。

たとえば、電子メールアドレスが mycompany.com であるすべてのユーザーを検索するには、**`mycompany.com`** と入力します。

[検索結果] ページに、次のルールに従って、3 つのタブに返された結果が表示されます。

[ユーザー] タブ	入力した文字列は、Workspace ユーザーの名、姓、またはユーザー プリンシパル名の任意の語の開始文字に一致します。
[グループ] タブ	入力した文字列は、グループの名前または説明の任意の語の開始文字に一致します。
[カタログ] タブ	入力した文字列は、カタログ リソースの名前または説明の任意の語の開始文字に一致します。

注意　最大 100 件の結果がレコード タイプごとに返されます。たとえば、100 ユーザーを超えるレコードに文字列が見つかると、最大 100 件の結果が [ユーザー] タブに表示されます。この最大値は変更できません。

9 Workspace レポートの表示

Workspace では、ユーザー、リソース、監査イベントについてのレポートなど、さまざまなレポートを生成できます。レポートは、Workspace 管理コンソールの [レポート] タブに表示されます。

Workspace を使用して、さまざまなレポートを生成できます。

表 9-1. Workspace のレポート タイプ

Workspace レポート	説明
最近のアクティビティ	このレポートでは、過去にユーザーが Workspace で実行した処理のタイプが日、月、または 12 週間単位で示されます。[イベントを表示] をクリックすると、アクティビティの日付、時刻、およびユーザーの詳細を表示できます。
リソース使用状況	このレポートでは、全リソースのリストに加え、ユーザー数やライセンス数など、各リソースの詳細情報も示されます。
リソース資格	このレポートでは、指定したリソースのユーザーの資格のリストが示されます。
グループ メンバーシップ	このレポートでは、指定したグループのメンバー リストが示されます。
ユーザー	このレポートでは、Workspace の全ユーザーのリストに加え、各ユーザーについてメール アドレス、ロール、グループ加入などの詳細も示されます。
同時ユーザー	このレポートは、同時に開いたユーザー セッションの数を示します。
監査イベント	このレポートでは、過去 30 日間にログインしたユーザーなど、指定した検索条件に関係する監査イベントのリストが示されます。この機能は、トラブルシューティングの際に役立ちます。「監査イベント レポートを生成 (P. 43)」を参照してください。

監査イベント レポートを生成

指定した監査イベントのレポートを生成できます。

監査イベント レポートは、トラブルシューティングの方法として役立つことがあります。

開始する前に

監査を有効にします。「Workspace の管理設定の概要 (P. 45)」を参照してください。

手順

1 Workspace 管理コンソール にログインします。

2 [レポート] - [監査イベント] を選択します。

3 監査イベントの条件を選択します。

監査イベントの条件	説明
ユーザー	このテキスト ボックスでは、監査イベントの検索を特定のユーザーによって生成された対象に限定できます。
タイプ	このドロップダウン リストでは、監査イベントの検索を特定の監査イベント タイプに限定できます。ドロップダウン リストには、可能性がある監査イベント タイプが必ずしもすべて表示されるわけではありません。リストに表示されるイベント タイプは、自身の Workspace 環境で発生したことがあるイベント タイプだけです。LOGIN、LAUNCH など、すべて大文字で表示されている監査イベント タイプはアクセス イベントであり、これらでデータベースが変更されることはありません。その他の監査イベント タイプはデータベース内に変更をもたらします。
操作	このドロップダウン リストでは、検索対象を特定の操作に限定できます。リストには、データベースに特定の変更を加えるイベントが表示されます。[タイプ] ドロップダウン リストでアクセス イベントを選択したら、それは操作イベントではないことを表すため、[操作] ドロップダウン リストで操作を指定しないようにします。
対象	このテキスト ボックスでは、検索対象を特定のオブジェクトに限定できます。オブジェクトとしては、グループ、ユーザー、デバイスなどがあります。オブジェクトは、名前または ID で特定されます。
日付の範囲	これらテキスト ボックスでは、「___ 日前から ___ 日前まで」の形式で検索対象を日付範囲で限定できます。最大の日付範囲は 30 日です。たとえば、90 日前から 60 日前は有効な範囲ですが、90 日前から 45 日前は 最大範囲の 30 日を超えているので無効な範囲です。

4 [表示] をクリックします。

指定した条件に従って、監査イベント レポートが表示されます。

注意 監査サブシステムの再起動時に、監査イベント ページにエラー メッセージが表示され、レポートが生成されないことがあります。レポートが生成されないことを示すそのようなエラー メッセージが表示された場合は、数分待ってからやり直します。

5 監査イベントの詳細については、その監査イベントの [詳細の表示] をクリックして参照してください。

10 Workspace の管理者設定の構成

Workspace をインストールし、初期構成を実行したら、いくつかの管理設定を構成できます。

この章では次のトピックについて説明します。

Workspace の管理設定の概要

Workspace の管理に関するさまざまな設定を構成できます。

Workspace 管理コンソールを使用して管理設定にアクセスします。

設定	説明
VA 構成	[設定] - [VA 構成]を選択して、[Appliance Configurator] ページに移動します。これらのページでは、Workspace データベース、SSL 証明書、および外部 syslog サーバの設定の更新および変更、Workspace とシステムのパスワードの変更、ログ ファイルの表示が可能です。
ライセンス	[設定] - [ライセンス] を選択して、Workspace ライセンス キーを入力します。
SMTP	[設定] - [SMTP]を選択して、SMTP 設定を入力します。
パスワードの回復	[設定] - [パスワードのリカバリ] を選択して、[パスワードを忘れた場合] をクリックした場合にユーザーのログイン ページに表示される [パスワードを忘れた場合] リンクの動作を構成します。
ユーザー ストア	[設定] - [ユーザー ストア] を選択して、信頼関係がないマルチフォレスト Active Directory 展開のユーザー ストアを構成します。Workspace のインストールと構成 ガイドの「Workspace との Active Directory 接続の管理」の章を参照してください。
ネットワーク範囲	[設定] - [ネットワーク範囲] を選択して、組織のネットワーク範囲を構成し、IP アドレス範囲を ID プロバイダ インスタンスに関連付けられるようにします。「ネットワーク範囲の追加または編集 (P. 13)」を参照してください。
認証方法	[設定] - [認証方法] を選択して、デフォルトの認証方法を構成するか、Workspace で直接サポートされていないがサードパーティの ID プロバイダで間接的にサポートされている認証方法を追加します。「ユーザー認証方法の追加または編集 (P. 14)」を参照してください。
ID プロバイダ	[設定] - [ID プロバイダ] を選択して、既存の ID プロバイダ インスタンスを編集するか、新しい ID プロバイダ インスタンスを追加します。 Workspace の初回のインストールには、デフォルトの ID プロバイダ展開環境が含まれます。 必要に応じて Workspace のデフォルトの ID プロバイダを編集し、認証方法を選択してネットワーク アドレス範囲を追加します。 高可用性を高めるため、Workspace の展開用に ID プロバイダ インスタンスを追加します。 [ID プロバイダ] ページに複数の ID プロバイダ インスタンスが表示されている場合は、インスタンスの順序を編集できます。IP アドレスを複数の ID プロバイダ インスタンスに割り当てる場合は、順序が重要です。 ID プロバイダ インスタンスの追加および編集や ID プロバイダ インスタンスの順序の編集については、「ID プロバイダ インスタンスの追加と構成 (P. 15)」を参照してください。
リモート アプリ アクセス	[設定] - [リモート アプリ アクセス] を選択して、アプリケーションを Workspace に登録できるクライアントまたはテンプレートを作成します。

設定	説明
SAML 証明書	[設定] - [SAML 証明書] を選択して、SAML 署名証明書を表示します。Web アプリケーションでユーザー認証に SAML アサーションを使用する必要がある場合は、Workspace と Web アプリケーションの両方において、ローカルで利用できる同一の SAML 署名証明書のコピーが必要です。
承認	ライセンス承認を有効または無効にするには、[設定] - [承認]を選択します。ライセンス管理システムと Workspace の間で同期されます。
監査	監査イベント レポートのための情報収集を有効または無効にするには、[設定] - [監査] を選択します。監査イベント レポートには、[レポート] タブでアクセスできます。
Citrix 公開アプリケーション	[設定] - [Citrix 公開アプリケーション] を選択して、Workspace カタログで利用できる Citrix ベース アプリケーション用の Workspace のグローバル アプリケーション配信設定を編集します。 単一の Citrix ベース アプリケーションの設定を編集する手順については、 『VMware Workspace Portal ガイド』の「リソースのセットアップ」 を参照してください。
カスタム ブランディング	[設定] - [カスタム ブランディング] を選択して、Workspace インターフェイスのブランディングをカスタマイズします。「Workspace ブランディングのカスタマイズ (P. 46)」を参照してください。

Workspace ブランディングのカスタマイズ

さまざまなインターフェイスに現われるロゴ、フォント、Web クリップおよび背景をカスタマイズすることができます。これには、Workspace 管理コンソール、ユーザーおよび管理者のサインイン画面、およびモバイル デバイス上のアプリケーション ポータルの Web ビューなどがあります。

アプリケーション ポータルおよび Workspace 管理コンソール の Web ビューで使用されるブランディングは、カスタマイズすることができます。

手順

1 Workspace 管理コンソール にログインします。

2 [設定] - [カスタム ブランディング] を選択します。

3 必要に応じて、フォーム内の設定を編集します。

表 10-1. カスタム ブランディング構成

フォーム項目	説明
	ブランド名およびロゴ
ロゴ	[ロゴ] オプションでは、ユーザーのアプリケーション ポータルおよび管理コンソールに表示されるロゴを変更することができます。 アップロードするイメージの推奨最小サイズは、350 x 100 ピクセルです。350 x 100 ピクセルより大きいイメージをアップロードすると、イメージは 350 x 100 ピクセルのサイズに合わせて調整されます。有効なフォーマットは JPEG、PNG、または GIF です。 [変更] をクリックし、新しいイメージをアップロードして現在のロゴを置き換えます。[確認] をクリックすると、直ちに変更が行われます。
お気に入りアイコン	お気に入りアイコン オプションでは、Web ブラウザで使用されているお気に入りアイコンを変更できます。このオプションは、デスクトップ デバイスとモバイル デバイスの両方に適用されます。 お気に入りアイコンの最大サイズは 16 × 16 px です。有効なフォーマットは JPEG、PNG、GIF、または ICO です。 [変更] をクリックし、新しいイメージをアップロードして現在のお気に入りアイコンを置き換えます。変更の確認を求めるメッセージが表示されます。[確認] をクリックすると、直ちに変更が行われます。
会社名	会社名オプションは、デスクトップ デバイスとモバイル デバイスの両方に適用されます。このオプションでは、Web ブラウザ画面タイトルで製品名の前に表示される会社名を変更できます。 既存の会社名の上に新しい会社名を入力して、名前を変更します。
製品名	製品名オプションは、デスクトップ デバイスとモバイル デバイスの両方に適用されます。このオプションでは、Web ブラウザ画面タイトルで会社名の後に表示される名前を変更できます。 既存の名前の上に製品会社名を入力して、名前を変更します。
	サインイン画面

表 10-1. カスタム ブランディング構成 (続き)

フォーム項目	説明
背景の色	サインイン画面の背景に表示される色。 既存の色コードの上に新しい 16 進数の色コードを入力して、背景の色を変更します。 背景の色を強調するには [背景を強調] をオンにします。 背景の色にあらかじめデザインされた三角形パターンを設定するには [背景のパターン] をオンにします。
マストヘッドの色	サインイン画面の見出しエリアに表示される色。 既存の色コードの上に新しい 16 進数の色コードを入力して、マストヘッドの色を変更します。 マストヘッドの色にあらかじめデザインされた三角形パターンを設定するには [マストヘッドのパターン] をオンにします。
イメージ（オプション）	色の代わりにイメージを背景に追加するには、イメージをアップロードします。 イメージの最大サイズは 1400 × 900 px です。有効なフォーマットは JPEG、PNG、または GIF です。
ロゴ	[アップロード] をクリックし、新しいロゴをアップロードしてサインイン画面の現在のロゴを置き換えます。[確認] をクリックすると、直ちに変更が行われます。 アップロードするイメージの推奨最小サイズは、350 x 100 ピクセルです。350 x 100 ピクセルより大きいイメージをアップロードすると、イメージは 350 x 100 ピクセルに合わせて調整されます。有効なフォーマットは JPEG、PNG、または GIF です。
ポータル（Web ビュー）	
背景の色	Web ポータル画面の背景に表示される色。 既存の色コードの上に新しい 16 進数の色コードを入力して、背景の色を変更します。新しい色コードを入力すると、アプリケーション ポータルのプレビューで背景の色が変更され、アプリケーション ポータルに背景の色がどのように表示されるかが示されます。ただし、[背景イメージを含める] チェックボックスがオンの場合、プレビューで背景の色が表示されないことがあります。 背景の色を強調するには [背景を強調] をオンにします。 背景の色にあらかじめデザインされた三角形パターンを設定するには [背景のパターン] をオンにします。
名前とアイコンの色	アプリケーション ポータル画面にリストされているリソース名に使用されるフォントの色。リソースの名前は、リソースのアイコンのすぐ下に表示されます。 既存の色コードの上に 16 進数の色コードを入力して、フォントの色を変更します。新しい色コードを入力すると、アプリケーションリ ポータル プレビューでアプリ名テキストが変更され、アプリケーション ポータルにテキストがどのように表示されるかが示されます。
レタリング効果	MyApps 画面のテキストに使用するレタリングの種類を選択します。
イメージ（オプション）	色の代わりにイメージをアプリケーション ポータル画面の背景に追加するには、イメージをアップロードします。
ポータル（モバイルおよびタブレット ビュー）	
背景の色	既存の色コードの上に 16 進数の色コードを入力して、モバイル デバイスから表示される [マイアプリ] 画面の背景色を変更します。
タイトル バーの色	既存の色コードの上に 16 進数の色コードを入力して、モバイル デバイスから表示されるタイトル バーの色を変更します。 タイトル バーの色にあらかじめデザインされた三角形パターンを設定するには [タイトル バーのパターン] をオンにします。
タイトルの色	既存の色コードの上に 16 進数の色コードを入力して、タイトル バーの見出しに使用するフォントの色を変更します。
名前の色	アプリケーション ポータル画面にリストされているリソース名に使用されるフォントの色。リソースの名前は、リソースのアイコンのすぐ下に表示されます。 既存の色コードの上に 16 進数の色コードを入力して、アプリケーション名のフォントの色を変更します。
レタリング効果	MyApps 画面のテキストに使用するレタリングの種類を選択します。
起動プログラムとカタログの両方に同じ値を使用します。	モバイル デバイスの [マイアプリ] 画面ビューに使用されるのと同じブランド デザインを [App Center] 画面ビューに使用するには、このボックスをオンにします。[App Center] 画面を別のデザインにするには、このボックスをオフのままにして、[App Center] 画面の背景、タイトル バーの色、およびタイトルの色を設定します。
初回のユーザー ツアー	

表 10-1. カスタム ブランディング構成 (続き)

フォーム項目	説明
初回のユーザー ツアー	アプリケーション ポータルの初回起動時には、ワークスペースの機能に関するスライドショーが表示されます。 この機能を無効にするにはこのチェックマークを削除してください。
	モバイル デバイス
Web クリップ アイコン	Workspace アイコンは、ユーザーが App Portal の URL をブックマークとしてモバイル デバイスのホーム画面に保存すると表示されます。この Web クリップ アイコンによって Workspace App Portal が起動されます。 イメージの最大サイズは 512 × 512 px です。有効なフォーマットは JPEG または PNG です。 [変更] をクリックし、新しいイメージをアップロードして現在の Web クリップ アイコンを置き換えます。変更の確認を求めるメッセージが表示されます。[確認] をクリックすると、直ちに変更が行われます。
Web クリップ タイトル	Workspace Web クリップ アイコンに付随するタイトル。タイトルの長さは 20 文字未満にする必要があります。

4 [保存] をクリックします。

Workspace のカスタム ブランディングを更新して [保存] をクリックすると、5 分以内に更新内容が適用されます。

次に進む前に

各種インターフェイスでブランディングの変更の見栄えを確認します。

インデックス