システム管理者ガイド
管理コンソールマニュアル

（最終更新日：2016 年 12 月 15 日）

NTT Communications

目 次 –The table of contents -

はじめに

このたびは、NTT コミュニケーションズ株式会社が提供する「Workspace Mobility (D-Type)」についてご導入いただき、誠にありがとうございます。

Workspace Mobility は、スマートデバイス対応のセキュアなモバイルワークを実現するためのプラットフォームです。各種業務アプリケーション（Microsoft Exchange Server や Office365、Web アプリケーション）と連携して、メールやカレンダー、連絡先、TO-DO、添付ファイル、Web アプリケーションをスマートデバイスから安全にご利用いただけます。

本書は、Workspace Mobility の構築が完了した後、システム管理者が行う作業を記載した管理コンソールのマニュアルガイドです。

※対象クライアントのサポート OS バージョンについては、Workspace Mobility のオフィシャルサイトを確認願います。

http://www.ntt.com/workspace-d/

※本マニュアルおよび FAQ については、Workspace Mobility のサポートサイトを確認願います。

http://support.ntt.com/workspace-d/

注意事項（必ずご確認ください）

・管理コンソールへのアクセスには VPN（UNO）回線経由でのアクセスに限定されます。

インターネットからのアクセスは出来ませんのでご注意ください。

・本マニュアルに掲載されている内容以外の設定についてはサポート対象外となります。

・サービス利用不可になることを避けるため、「サポート対象外」もしくは「初期設定値のまま変更しないでください」という記載がある設定／操作は実施しないでください。

・故意や正常な操作に関わらず、本マニュアルに記載されていない操作を実施することによる不具合について、当社および関連会社には一切責任を負うものはありません。

（特に P14、P21 に記載している Connector タブの操作上の注意をご確認ください。サービスがご利用出来なくなります）

※理由１：日本の通信規格に合っていない仕様やセキュリティ面を考慮し、不必要だと判断する設定内容

※理由２：誤って設定変更を行い、お客様 AD サーバとの連携がとれなくなる等、トラブル回避のため

・事前に登録されている「SYSADM」アカウントは弊社サポートに必要なアカウントとします。

これらのアカウントを削除されますと、弊社サポートを受けられません。

・事前に登録されている「USERADM」アカウントはお客様アカウントとします。

ログイン PW は開通案内にて通知しますが、セキュリティ面を考慮し、初回ログイン時にお客様側で変更していただきます。

本書の表記規則

一般の表記

表記例	意味
メニューの[ファイル(F)]-[開く(O)]	メニューのコマンドの選択経路をあらわします。この例では、[ファイル(F)]メニューに含まれている[開く(O)]コマンドをあらわしています。
<OK>ボタン、<次へ(N)>ボタン <OK>または<適用>ボタン	コマンドボタン名は、山カッコ（<>）で囲んであらわします。
「ファイル名」、「入力値」、「画面名」、「ダイアログ名」、「参照場所」	構文中の鍵カッコ（「」）で囲んである部分は、ファイル名や入力値などをあらわします。また、画面名やダイアログ名、参照する場所などを示す場合も鍵カッコ（「」）で囲んであらわします。
チェックする、チェックしない、チェックをはずす	メニューのコマンドやダイアログのチェックボックスなどを ON（または OFF）することをあらわします。

スマートデバイス操作の表記

表記例	意味
タップ	タッチパネルを指先で 1 回軽くたたくことです。
フリック	タッチパネルを指先で軽くはじくことです。
ピンチイン	タッチパネルに 2 本の指を付け、2 本の指を近づけることです。
ピンチアウト	タッチパネルに 2 本の指を付け、2 本の指を離すことです。

キー操作の表記

表記例	意味
[SHIFT]キー	キーは、大カッコ（[]）で囲んであらわします。
[F]→[O]キー	キーが右矢印（→）で区切られている場合は、それぞれのキーを順に押すことをあらわします。この例では、[F]キー、[O]キーを順に押すことをあらわしています。
[Ctrl]+[A]キー	2 つのキーの間にあるプラス記号（+）は、最初のキーを押しながら 2 番目のキーを押すことをあらわします。 この例では、[Ctrl]キーを押しながら[A]キーを押すことをあらわしています。
矢印キー	[→]キー、[←]キー、[↑]キー、[↓]キーの総称です。

記号の表記

記号	意味
	「注意事項」を意味します。使用方法などに関する注意事項や設定を行う際の注意事項を説明しています。
	「関連」を意味します。 設定を行う際の関連箇所を説明しています。
※	「注釈」を意味します。 簡単な補足説明などのコメントを記述しています。

1. Workspace Mobility 用語とポイント

この章では、Workspace Mobility のシステムを管理するために必要な用語や押さえていただきたい情報、基本的な動作・挙動についての概念について記載します。

1.1 本書で使用される用語

❑ コラボレーションシステム

Workspace Mobility が連携できるグループウェア（MS Exchange Server/Office365 Exchange Online）のこと

❑ Workspace Mobility サーバ

Workspace Mobility を利用する上で必要なサーバコンポーネントの 1 つ。Workspace Mobility に関する各種設定を行う Web 管理コンソール画面の表示、スマートデバイスの端末認証、Connector サーバとの連携を行います。

❑ Connector サーバ

Workspace Mobility を利用する上で必要なサーバコンポーネントの 1 つ。コラボレーションシステムと連携し、メール、カレンダー、連絡先、TO-DO 等の情報を同期するサーバ

❑ クライアントアプリ

Workspace Mobility を利用する上で必要なクライアントコンポーネント。スマートデバイスにインストールして利用するクライアントアプリケーションを指します。（推奨 OS バージョン：iOS ver8.2 以上、Android ver4.4 以上）

❑ トップ画面

クライアントアプリを起動した際、最初に表示される Workspace Mobility のメイン画面

※ デフォルトのトップ画面には、「受信トレイ」、「未読」、「カレンダー」、「連絡先」、「TO-DO」、「添付ファイル」のアイコンが表示されます。

❑ セキュア・コンテナ

メール、カレンダー、連絡先、TO-DO 等の業務データを暗号化し、保存する安全な領域のこと。スマートデバイス内に生成され、セキュア・コンテナ以外の領域とは論理的に分離されます。

❑ App Box Gateway

Workspace Mobility に Web アプリケーション環境を提供するサーバコンポーネント。自社用の SFA、CRM、EPR、グループウェア等を従業員に利用させたい場合に必要なサーバ。

❑ App Box

App Box Gateway が提供する Web アプリケーション環境のこと

1.2 ユーザーとデバイスの考え方

Workspace Mobility では、「ユーザー」と「デバイス」の２つの考え方があります。それぞれの考え方を表 1.2.1 に示します。

表 1.2.2 ユーザーとデバイスの考え方

項目	説明	登録方法
ユーザー	本サービスの利用権限を有する利用者を指します。権限には「User」、「Super user」、「Admin」の３種類の権限が存在し、各ユーザーは付与された権限に応じたサービス利用を行います。（権限の詳細については「1.2 ユーザー権限について」を参照） システムへのユーザー登録は、連携先 Active Directory のアカウント情報（アカウント名／パスワード）同期によって自動で実施されます。アカウント同期は、ユーザーによるクライアントアプリ初回ログイン時に実施されるため、管理コンソール上でユーザー作成をする必要はありません。	クライアントアプリログイン時に自動登録 （AD サーバ情報を同期・システム登録）
デバイス	本サービスにおいてユーザーが利用するスマートデバイスを指します。デバイスはユーザーに紐づいてシステムに登録され、複数デバイスの 1 ユーザーへの紐づけや、1 デバイスの複数ユーザーへの紐づけも可能です。 クライアントアプリ初回ログイン時の自動登録／ユーザー紐づけだけでなく、管理コンソールから手動でデバイス登録／ユーザー紐づけも実施することができます。	① クライアントアプリログイン時に自動登録 ② 管理コンソールから手動登録 ※詳細は「2.5 デバイスの登録と許可」を参照

1.3 ユーザー権限について

Workspace Mobility には、「Admin」、「Super user」、「User」の 3 種類のユーザー権限が存在します。それぞれ表 1.3.1 に示すような権限を持っています。必要に応じてユーザーに権限を付与します。1 ユーザーに複数の権限を付与することも可能です。

表 1.3.1 ユーザー権限の種類

項目	役割	Workspace Mobility 利用権限	管理権限
User	Workspace Mobility を利用する権限を持っています。クライアントアプリを使用するユーザーは、この権限が必要です。任意のグループ名も使用できます。	○	×
Super user	Admin が指定した項目及びユーザーのデバイスに対する管理権限を持っています。任意のグループ名も使用できます。	×	○ （一部）
Admin	Workspace Mobility システム全体の管理者権限を持っています。管理コンソール画面のすべての設定変更が可能です。任意のグループ名も使用できます。	×	○

1.4 複数デバイス、複数ユーザーの動作について

Workspace Mobility は、1 ユーザーが複数のデバイスを利用することができます。1 デバイスを複数ユーザーで利用することもできます。

注意

1 ユーザーで複数デバイスを利用する場合、最後に同期したデバイスにのみ新着通知が送信されます。

1 デバイスに、別ユーザーがログインすると、既存ユーザー情報が全て消去されます。

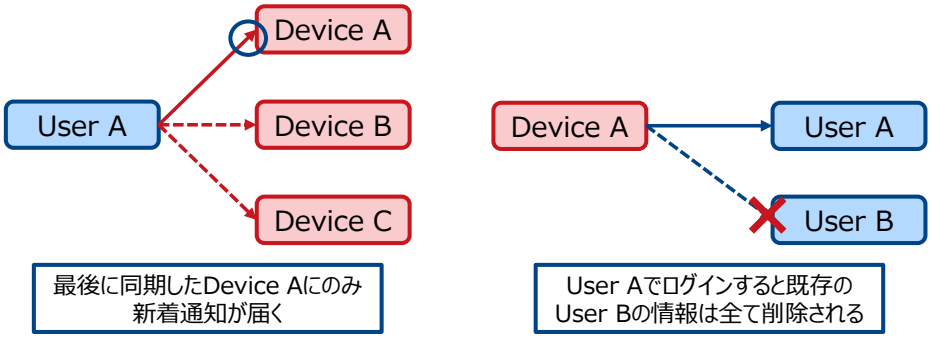


図 1.4.1 複数デバイス、複数ユーザーの動作

1.5 グループについて

グループは、ポリシーを作成し、適用対象とする範囲のことをいいます。本項では、本サービスにおけるグループの概念について説明します。

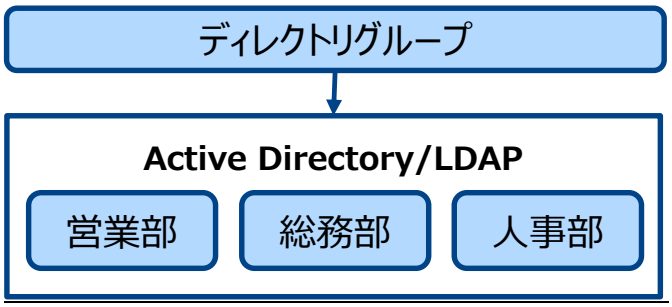


図 1.5.1 グループ

ディレクトリグループ

Active Directory/LDAP で管理されたグループに対して、ポリシーを割り当てることができるグループです。グループ単位で管理者を割り当てる場合、Active Directory/LDAP 内のユーザーに Super user 権限を付与することで、そのグループの管理者とすることができます。Super user 権限を付与するには、そのユーザーを Active Directory/LDAP 内にある「Superuser」グループに追加します。

1.6 ロックおよびワイプについて

本サービスではいくつかの種類のロックおよびワイプが存在するため、ロックおよびワイプの基本的な概念動作について記載します。

1.6.1 ロック（停止）

Workspace Mobility では、ロックは、ユーザーロックとデバイスロックの 2 種類があります。

表 1.6.1 ロックの種別

ロック種別	説明
ユーザーロック	ユーザーがロックされます。ユーザーが複数のデバイスを使用している場合は、すべてのデバイスでデータ同期ができなくなります。
デバイスロック	デバイスがロックされます。 ユーザーが複数のデバイスを利用している場合、ロックされたデバイスからのみデータ同期ができなくなります。

1.6.2 ワイプ（消去）

ワイプは、デバイス上のデータを消去することです。Workspace Mobility では、複数のワイプ種別があります。ワイプを設定する前に必ず、評価を実施してください。

注意

ワイプは、前提条件によりワイプの実行方法が異なります。必ず、事前に評価を実施して、ワイプの設定および実行するようにしてください。

ワイプの種別と実行条件

以下の表に、ワイプの種別と実行条件について記載します。なお、ワイプが実行された後は、自動的にデバイスロックが実行されます。

表 1.6.2 ワイプの種別

ワイプ範囲	説明
セキュア・コンテナ領域のワイプ	セキュア・コンテナ領域内にある同期データ等が消去されます。 デバイス上のクライアントアプリ自体は消去されません。
デバイス全体のワイプ	デバイス全体のデータ領域を消去し、工場出荷状態に戻します。 ※Workspace Mobility ではサポートしておりません。デバイス全体のワイプが必要な場合は、別途 MDM サービスをご契約いただく必要がございます。

表 1.6.3 セキュア・コンテナ領域のワイプ実行条件

ワイプ種別	トリガー	ワイプ範囲
リモートワイプ（管理者）	システム管理者が管理コンソール画面よりワイプ実行	セキュア・コンテナ領域
ローカルワイプ	Workspace Mobility のパスワードミス上限により自動的にワイプ実行	セキュア・コンテナ領域
リモートワイプ（利用者）	利用者自身によるワイプ実行	セキュア・コンテナ領域

2. Workspace Mobility 導入後作業

この章では、Workspace Mobility 導入後、システム管理者に実施していただく作業について記載します。

2.1 Workspace Mobility の管理コンソールへのアクセス

以下の手順にて、管理コンソールにアクセスができる事を確認してください。

2.1.1 管理コンソールへのログイン

1. Web ブラウザにて、https://[Workspace Mobility サーバの FQDN]:8088/ にアクセスしてください。
2. 図 2.2.1 が表示されます。[Username]にシステム管理者のアカウント ID を入力してください。
3. [Password]にパスワードを入力し、<Login>をクリックしてください。

・Username：USERADM
・Password：申込時にお客様に指定頂いたパスワード
（※初回ログイン後、システム管理者にてパスワード変更を実施してください。）

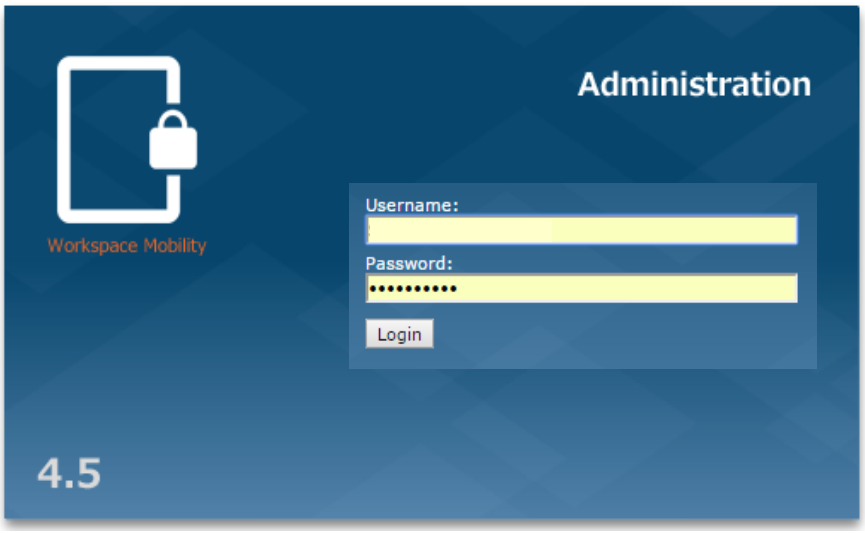


図 2.1.1 ログイン画面

管理コンソールのトップ画面（図 2.1.2）が表示される事を確認してください。

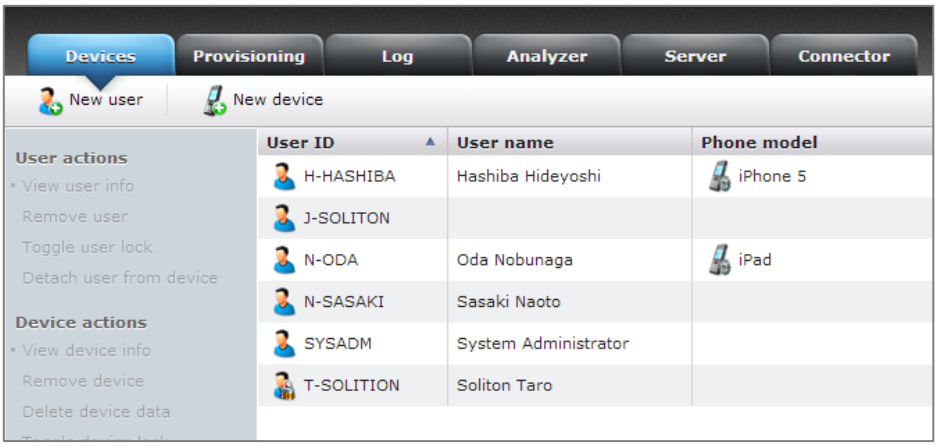


図 2.1.2 トップ画面

2.1.2 管理コンソールからのログアウト

1. 管理コンソールの右上にある赤い[×]アイコンをクリックしてください。

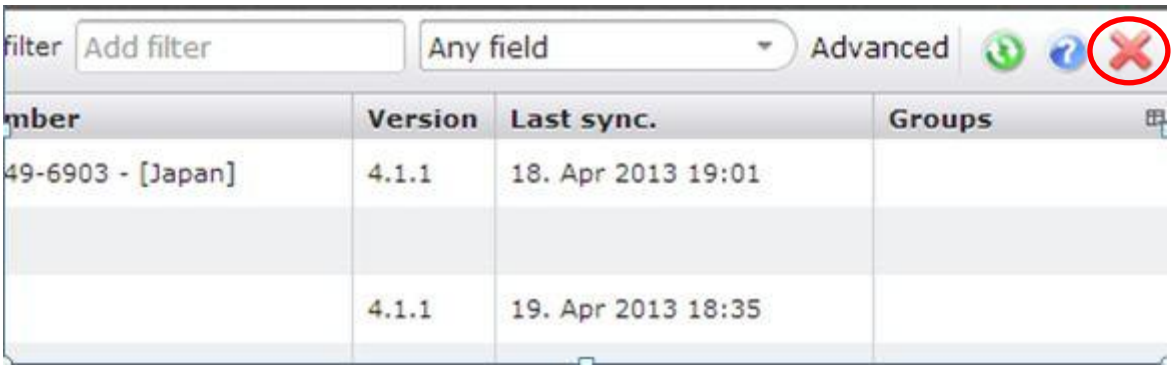


図 2.1.3 ログアウト操作

2. ログアウトが完了すると、ログイン画面が表示されます。

2.2 管理者向け設定

Workspace Mobility の運用開始前に、管理コンソールにて実施するシステム管理者向けの設定について、以下に記載します。

2.2.1 システム管理者のパスワード変更

Workspace Mobility では、ユーザーは Active Directory/LDAP で管理されているため、ユーザーのパスワードを管理コンソールで管理する必要はありません。Workspace Mobility 上で管理されているシステム管理者については、定期的にパスワードを変更してください。

注意

※User ID のうち、「SYSADM」、「SUPERADM」は削除、およびパスワード変更しないでください。当該アカウントは弊社サポートに必要なアカウントとなります。アカウントの削除／パスワード変更があった場合は、弊社サポートを受けられません。

※パスワード変更は「USERADM」のみとしてください。本アカウントを削除してしまうと、Active Directory/LDAP との連携に失敗した場合、Workspace Mobility 管理コンソールに一切ログインできなくなります。

1. 管理コンソールに、システム管理者でログインしてください。

2. [Devices]タブ-(パスワードを変更するユーザー)-[View user info]をクリックしてください。

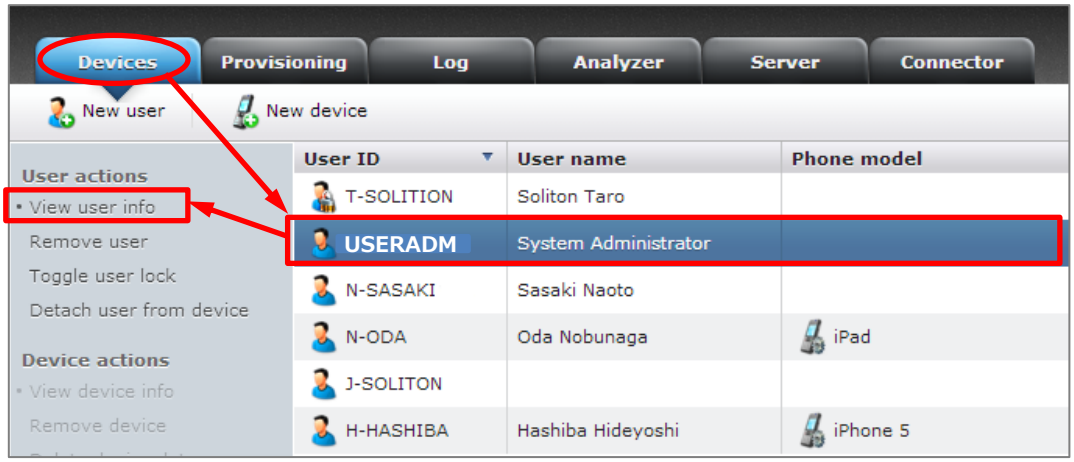


図 2.2.1 ユーザー情報の表示

3. 図 2.2.2 が表示されます。<Edit password>をクリックしてください。

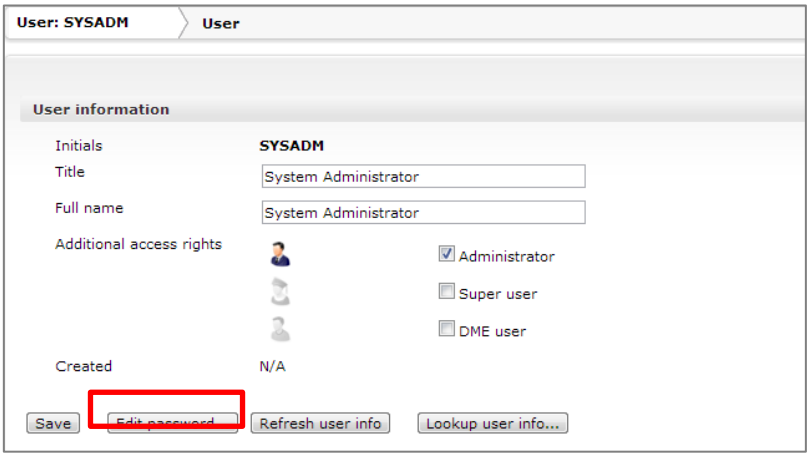


図 2.2.2 ユーザー情報

4. 図 2.2.3 が表示されます。[New password]、[Password again]に新しいパスワードを入力し、<Accept>をクリックしてください。パスワードが変更されます。

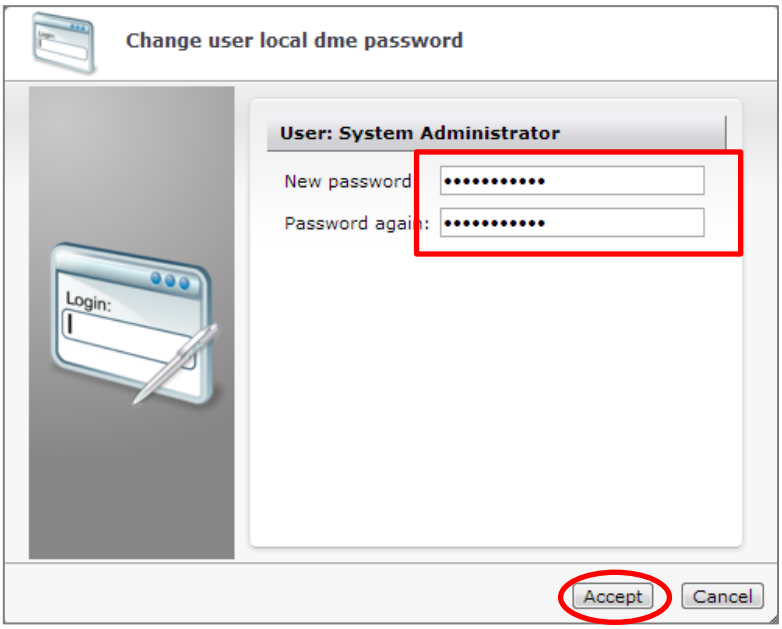


図 2.2.3 パスワード変更

2.2.2 Active Directory サーバ連携設定

本サービスは Active Directory のユーザーアカウント／パスワードを利用してクライアントアプリケーションへのログインを行うため、Active Directory サーバとの連携設定を実施してください。

注意

- **連携設定を完了させるためには、Active Directory サーバ側に所定の設定を実施済みである必要があります。詳細は、別紙「Workspace Mobility お客様システム事前設定ガイド AD サーバ／Exchange サーバ」を参照ください。**
- **本設定は「Connector1」と「Connector2」の両方に実施する必要があります。Connector1 の設定完了後、必ず Connector2 にも設定を行ってください。**

1. 管理コンソールに、システム管理者でログインしてください。
2. [Connector]タブより、「Connector1」をクリックしてください。

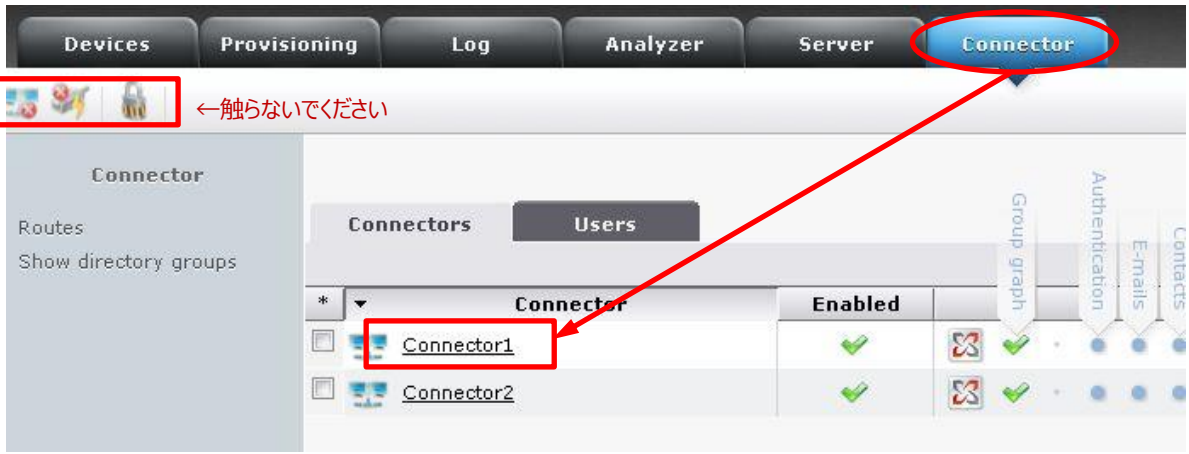


図 2.2.4 Connector 画面

注意

本サービスでは「図 2.2.4 Connector 画面」における左上の 3 つのアイコン（ ）はサポート対象外となり、利用しません。サービスが利用できなくなりますので、絶対にクリックしないでください。
上記操作を実施することによる不具合について、当社および関連会社には一切責任を負うものはありません。

3. 画面左の[Domain]をクリックし、Connector settings 画面を表示してください。
4. 「Directory server」の項目へ下記情報を参照して設定値を入力し、[Test readout]をクリックしてください。

表 2.2.1 Directory server 設定値

対象項目	入力値
Domain info directory server	Active Directory サーバの IP アドレス
User for domain info queries	DME_Server
Password	「DME_Server」アカウントに設定したパスワード

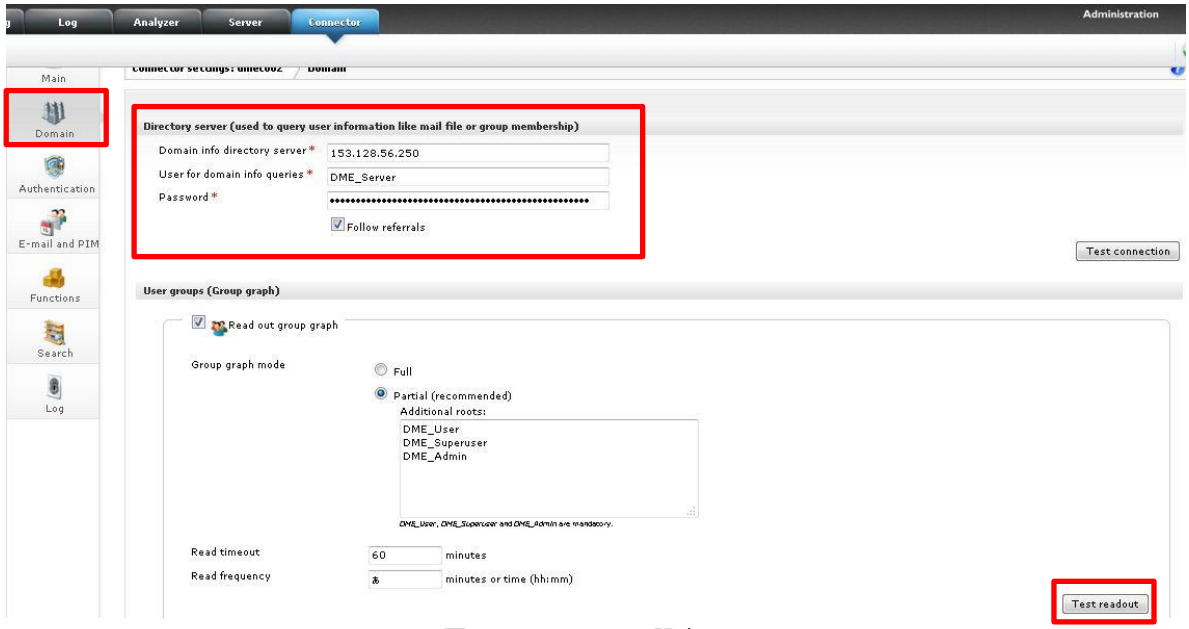


図 2.2.5 Domain 設定画面

5. [Test group graph]が表示されるので、[Save]をクリックします。

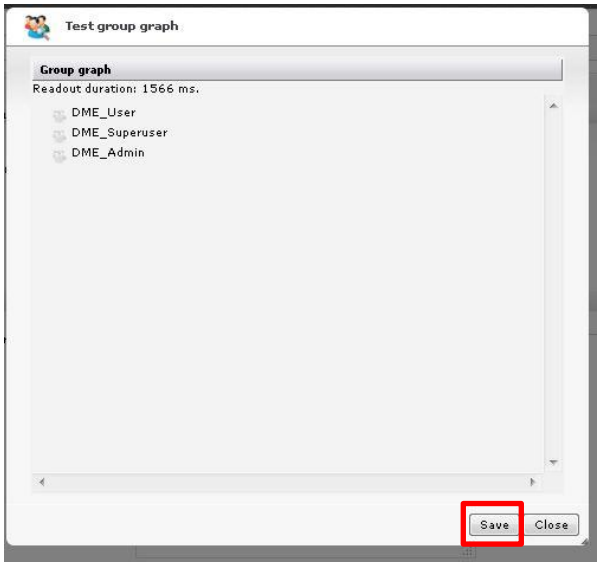


図 2.2.6 Test Group graph 画面

注意

「Test group graph」画面に、「DME_User」、「DME_Superuser」、および「DME_Admin」が表示されない場合、もしくはエラーになる場合は、別紙「お客様システム事前設定ガイド」を再度ご確認ください。

6. 画面左上の[Authentication]をクリックし、「Authentication」の項目へ下記情報を参照して設定値を入力し、[Save]をクリックしてください。
7. Save 後、入力値が正しいことを確認するため、画面右下の[Test login]をクリックしてください。

表 2.2.2 Authentication 設定値

対象項目	入力値
LDAP Server	AD サーバの IP アドレス
AD domain	AD ドメイン名
Administrator user name	AD サーバの管理者アカウント名
Administrator Password	上記管理者アカウントのパスワード

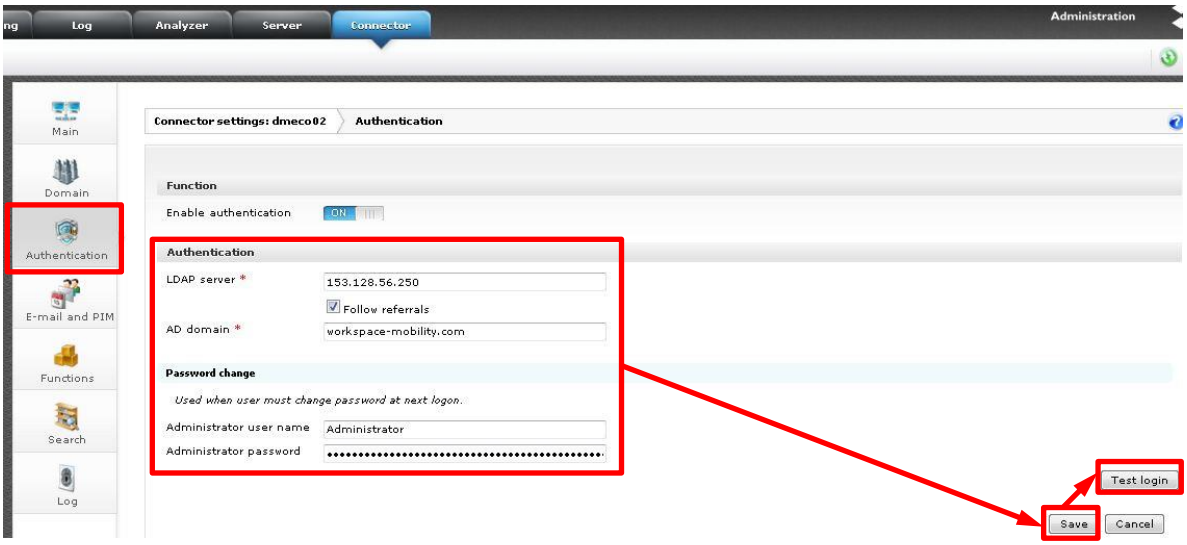


図 2.2.7 Authentication 設定画面

8. 「Test authentication」画面が表示されるので、「Username」に前項で設定した管理者アカウント名を、「Password」にそのパスワードを入力し、[Test]をクリックしてください。

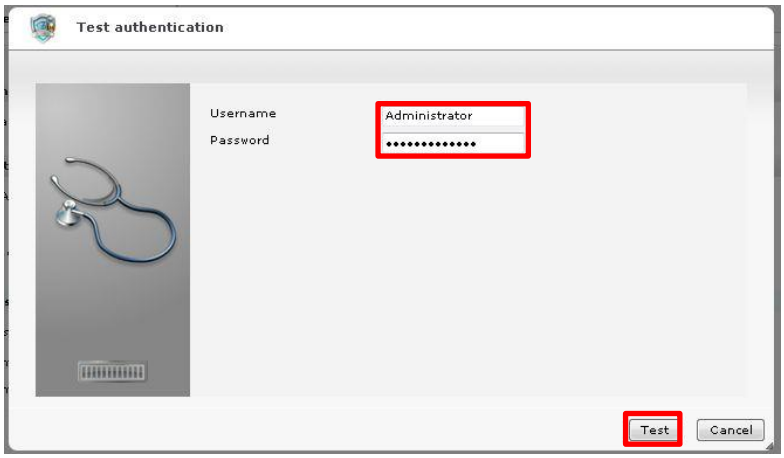


図 2.2.8 Test authentication 画面

9. 「Result of test」画面が表示されます。正常に処理された場合、「Authentication succeeded」が表示されるので、[Cancel]をクリックします。

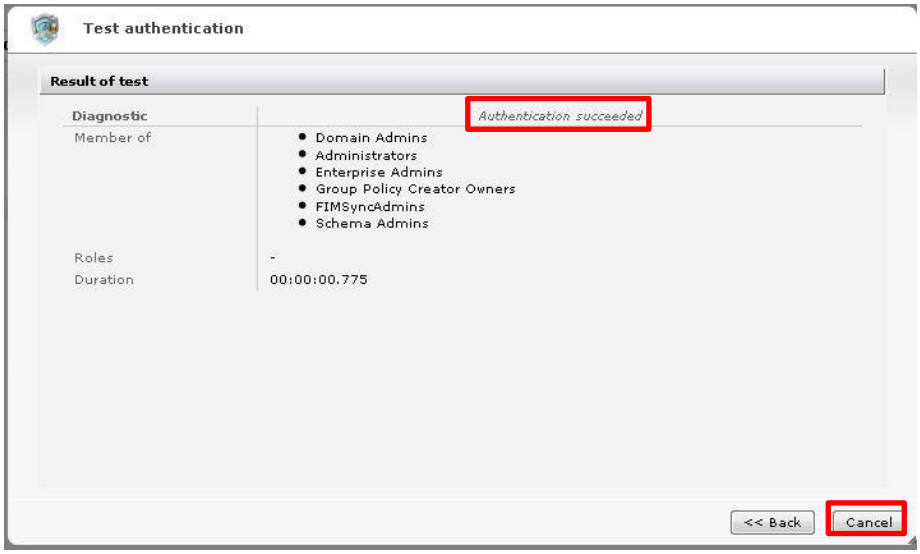


図 2.2.9 Result of test 画面

注意

「Authentication succeeded」が表示されない場合や、エラーになる場合は、入力したアカウント名またはパスワードが間違っている場合があります。[Back]をクリックし、再度ご確認ください。

アカウント名・パスワードが正しくてもエラーが発生する場合、弊社までお問い合わせください。

10. Connector2 の設定を行うため、「Connector」タブをクリックします。

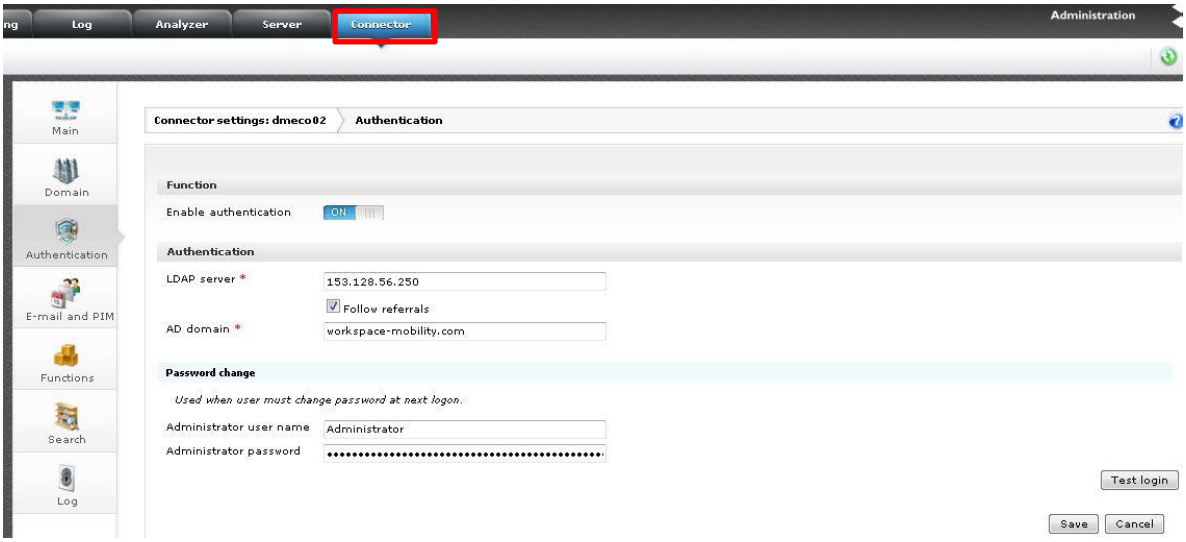


図 2.2.10 Authentication 設定画面

11. 「Connector 2 」をクリックしてください。

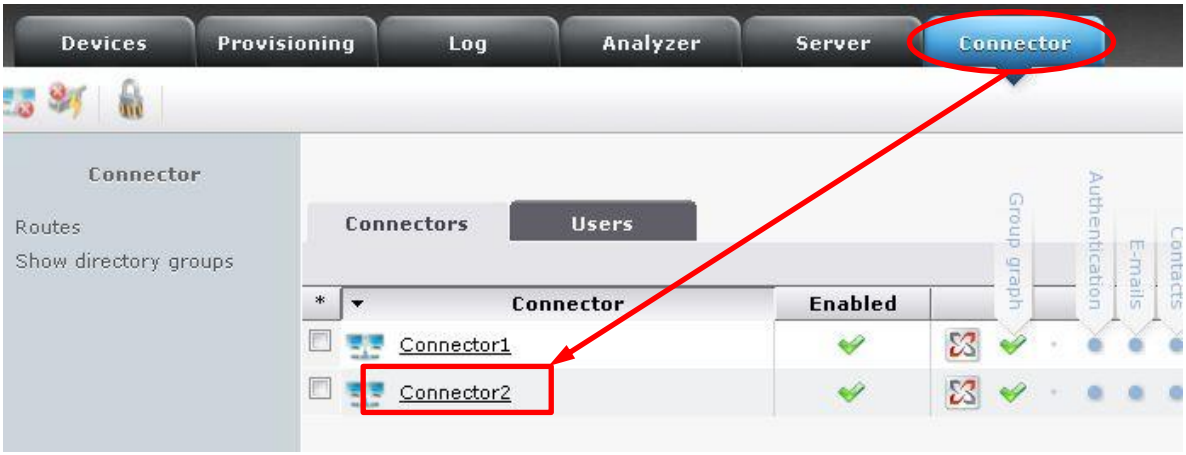


図 2.2.11 Connector 画面

12. 画面左の[Domain]をクリックし、Connector settings 画面を表示してください。
13. 「Directory server」の項目へ下記情報を参照して設定値を入力し、[Test readout]をクリックしてください。

表 2.2.3 Directory server 設定値

対象項目	入力値
Domain info directory server	Active Directory サーバの IP アドレス
User for domain info queries	DME_Server
Password	「DME_Server」アカウントに設定したパスワード

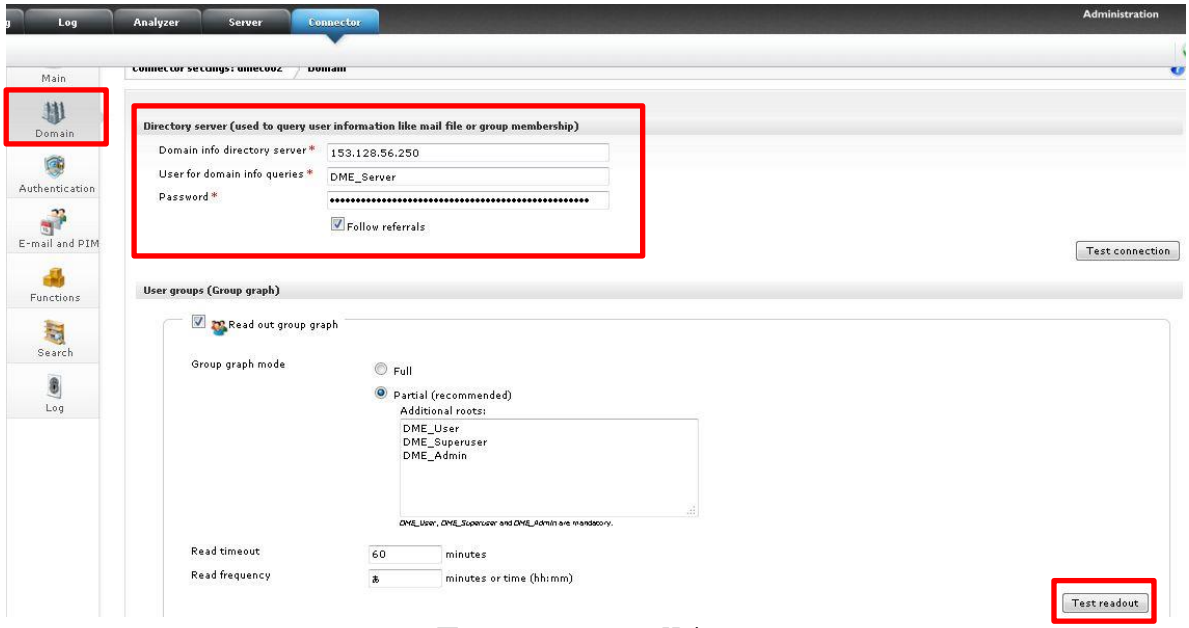


図 2.2.12 Domain 設定画面

14. [Test group graph]が表示されるので、[Save]をクリックします。

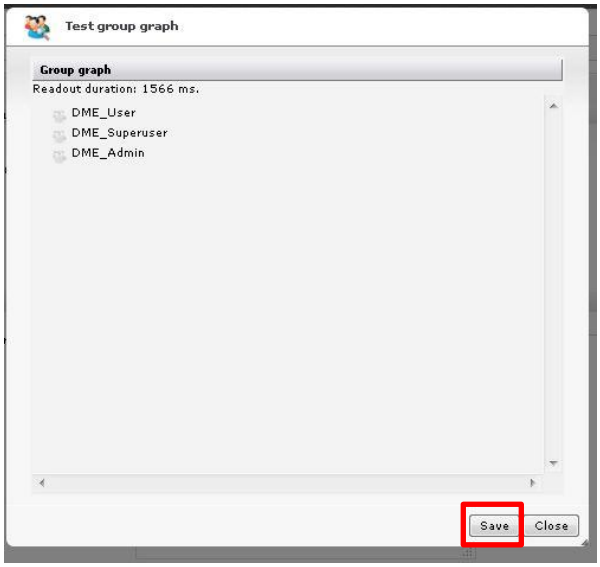


図 2.2.13 Test Group graph 画面

注意

「Test group graph」画面に、「DME_User」、「DME_Superuser」、および「DME_Admin」が表示されない場合、もしくはエラーになる場合は、別紙「お客様システム事前設定ガイド」を再度ご確認ください。

15. 画面左上の[Authentication]をクリックし、「Authentication」の項目へ下記情報を参照して設定値を入力し、[Save]をクリックしてください。

16. Save 後、入力値が正しいことを確認するため、画面右下の[Test login]をクリックしてください。

表 2.2.4 Authentication 設定値

対象項目	入力値
LDAP Server	AD サーバの IP アドレス
AD domain	AD ドメイン名
Administrator user name	AD サーバの管理者アカウント名
Administrator Password	上記管理者アカウントのパスワード

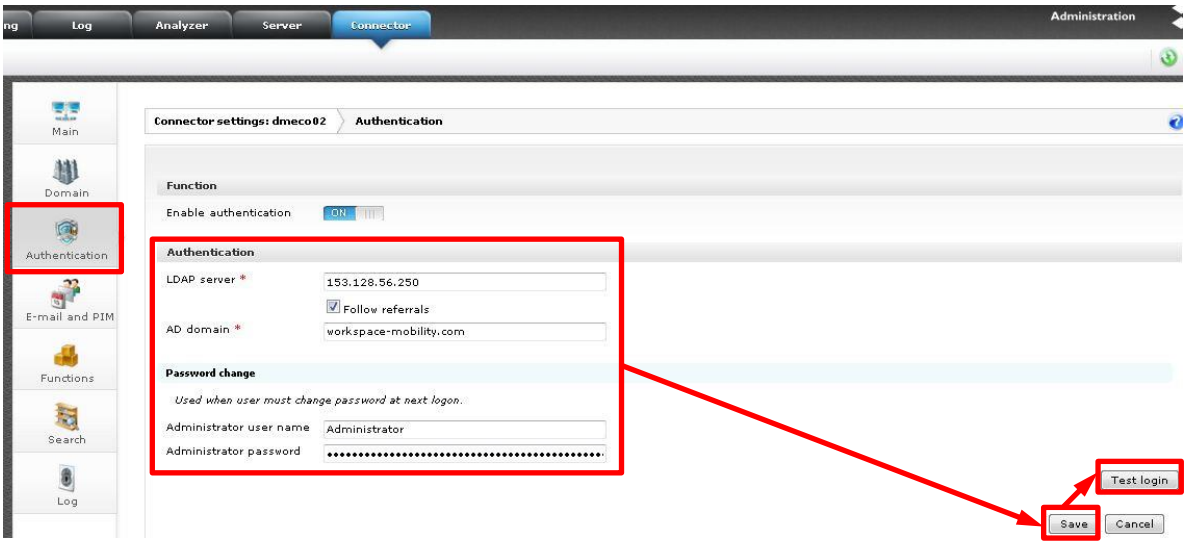


図 2.2.14 Authentication 設定画面

17. 「Test authentication」画面が表示されるので、「Username」に前項で設定した管理者アカウント名を、「Password」にそのパスワードを入力し、[Test]をクリックしてください。

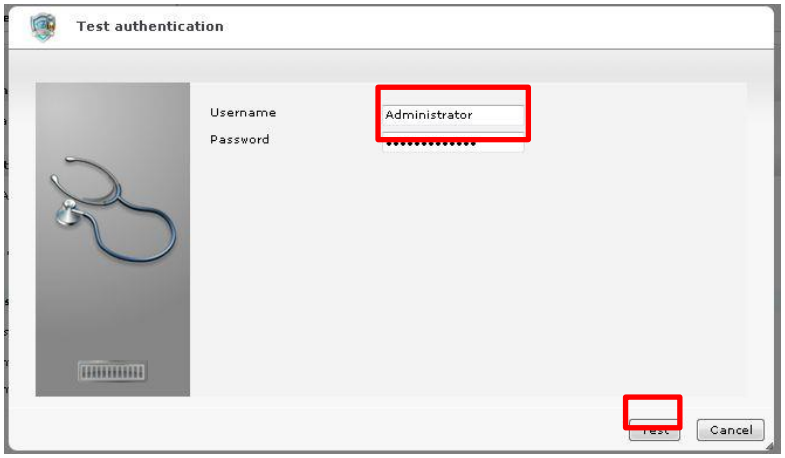


図 2.2.15 Test authentication 画面

18. 「Result of test」画面が表示されます。正常に処理された場合、「Authentication succeeded」が表示されるので、[Cancel]をクリックします。

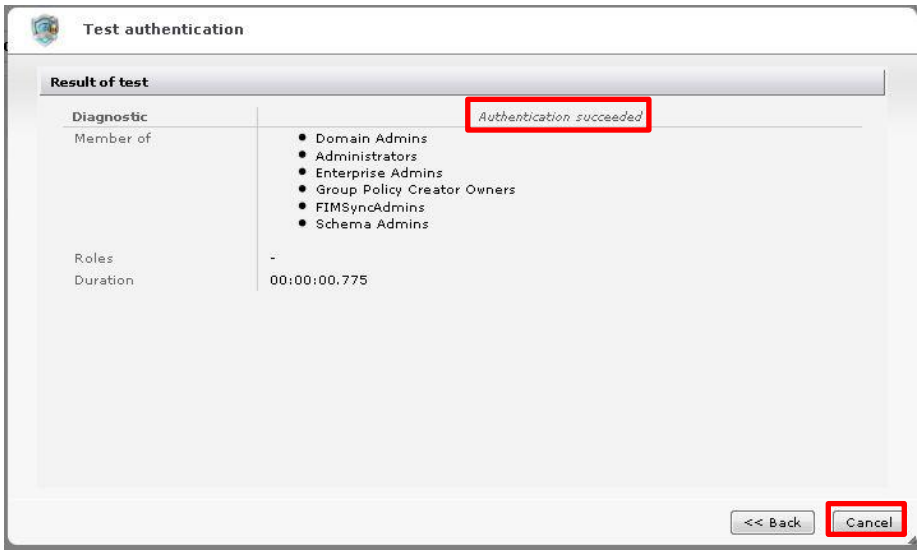


図 2.2.16 Result of test 画面

注意

「Authentication succeeded」が表示されない場合や、エラーになる場合は、入力したアカウント名またはパスワードが間違っている場合があります。[Back]をクリックし、再度ご確認ください。

アカウント名・パスワードが正しくてもエラーが発生する場合、弊社までお問い合わせください。

2.2.3 Exchange サーバ連携設定

本サービスで利用する Exchange サーバとの連携設定を行います。

注意

- **連携設定を完了させるためには、Exchange サーバ側に所定の設定を実施済みである必要があります。詳細は、別紙「Workspace Mobility お客様システム事前設定ガイド AD サーバ／Exchange サーバ」を参照ください。**
- **本設定は「Connector1」と「Connector2」の両方に実施する必要があります。Connector1 の設定完了後、必ず Connector2 にも設定を行ってください。**

1. 管理コンソールに、システム管理者でログインしてください。
2. [Connector]タブより、「Connector1」をクリックしてください。

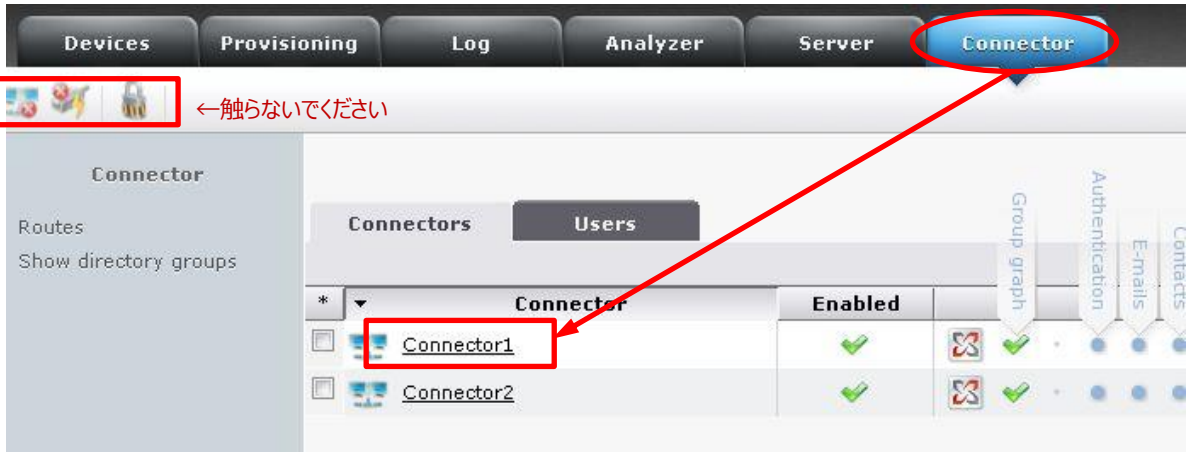


図 2.2.17 Connector 画面

注意

本サービスでは「図 2.2.17 Connector 画面」における左上の 3 つのアイコン（ ）はサポート対象外となり、利用しません。サービスが利用できなくなりますので、絶対にクリックしないでください。
上記操作を実施することによる不具合について、当社および関連会社には一切責任を負うものはありません。

3. 画面左の[E-mail and PIM]をクリックし、General (Exchange)画面を表示してください。
4. General (Exchange)タブ内の項目へ下記情報を参照して設定値を入力し、[Save]をクリックしてください。
5. Save 後、入力値が正しいことを確認するため、画面右下の[Test connection]をクリックしてください。

表 2.2.5 General (Exchange)設定値

対象項目	入力／選択値
Server	Exchange サーバの IP アドレス（※1）
Exchange domain	AD サーバのドメイン名（※2）
Protocol	Exchange2007 ご利用の場合：Exchange2007 (Web service) Exchange2010/Office365 ご利用の場合：Exchange2010 (Web service)
Auth.scheme	NTLM
Mailbox naming scheme	E-mail address

※1：Office365 をご利用の場合は、「outlook.office365.com」を入力ください。

※2：Office365 をご利用の場合は、メールアドレスで使用しているドメイン名（@以降）を入力ください。

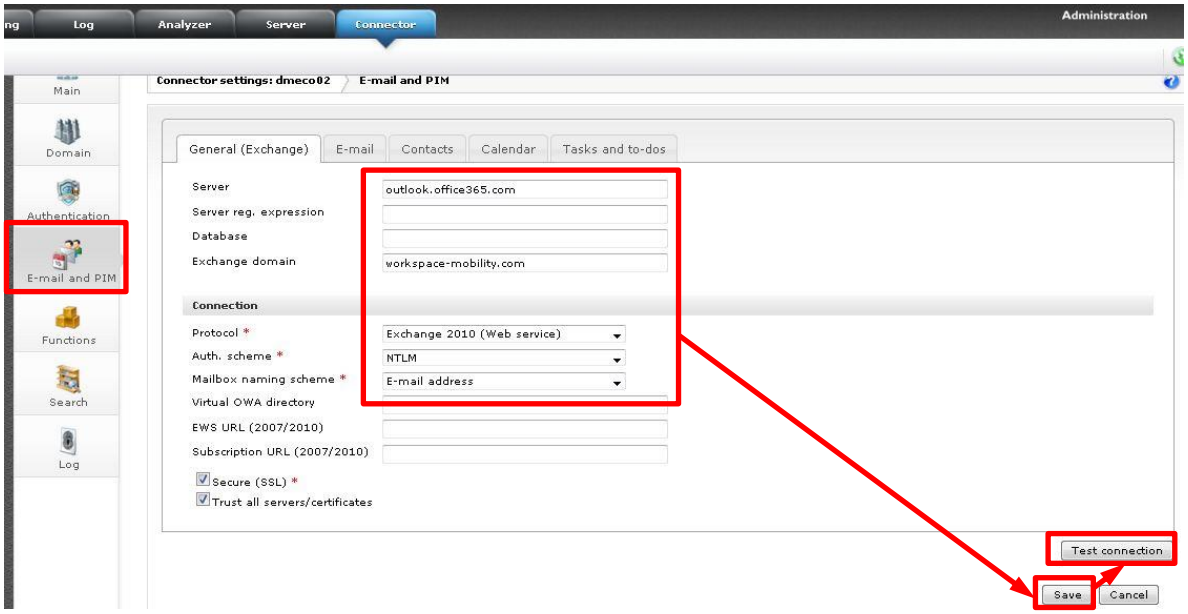


図 2.2.18 Connector 画面

6. Test functions 画面が表示されるので、「E-mails」、「Contacts」、および「Calendar」にチェックを入れます。その後、「Username」に「DME_User」グループに所属しているアカウント名を、「Password」にそのアカウントのパスワードを入力し、[Test]をクリックします。

図 2.2.19 Test functions 画面

7. Result of test の画面が表示されます。正常に処理された場合は、各項目の「Diagnostic」が表示されますので、[Cancel]をクリックします。

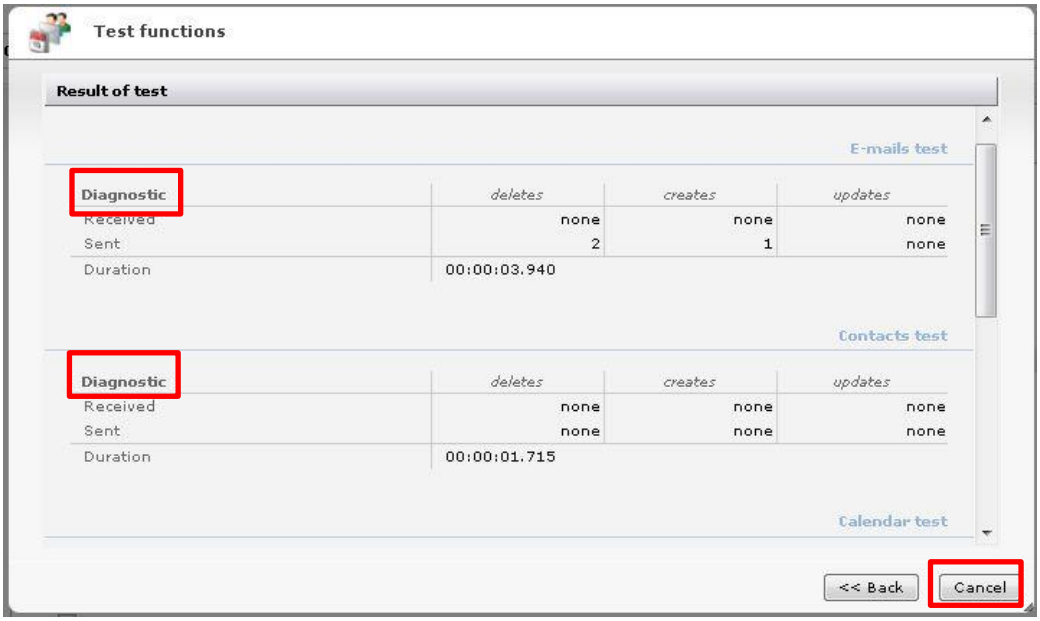


図 2.2.20 Result of test 画面

注意

「Diagnostic」が表示されない場合や、エラーになる場合は、入力したアカウント名または

パスワードが間違っている場合があります。[Back]をクリックし、再度ご確認ください。

アカウント名・パスワードが正しくてもエラーが発生する場合、弊社までお問い合わせください。

8. 画面左下の「Search」をクリックし、Global address book search 画面を表示します。
9. Global address book search タブ内の項目へ下記情報を参照して設定値を入力し、[Save]をクリックしてください。

表 2.2.6 Global address book search 設定値

対象項目	入力／選択値
Enable GAB search	ON
Server	AD サーバの IP アドレス
AD domain	AD ドメイン名
Search DN	AD ドメイン LDAP 識別名（※1） →「DC=XXX,DC=YYY」の記載ルールで入力

※1：LDAP 識別名はドメイン名が「workspace-mobility.com」の場合、「DC=workspace-mobility,DC=com」の記載になります。

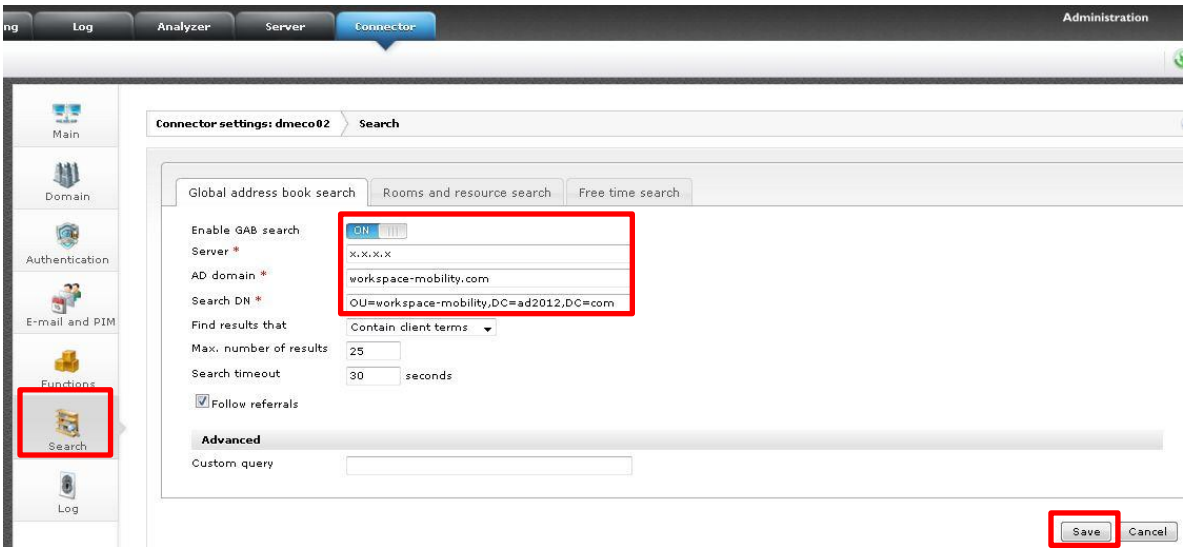


図 2.2.21 Global address book search 設定画面

10. Connector2 の設定を行うため、「Connector」タブをクリックします。

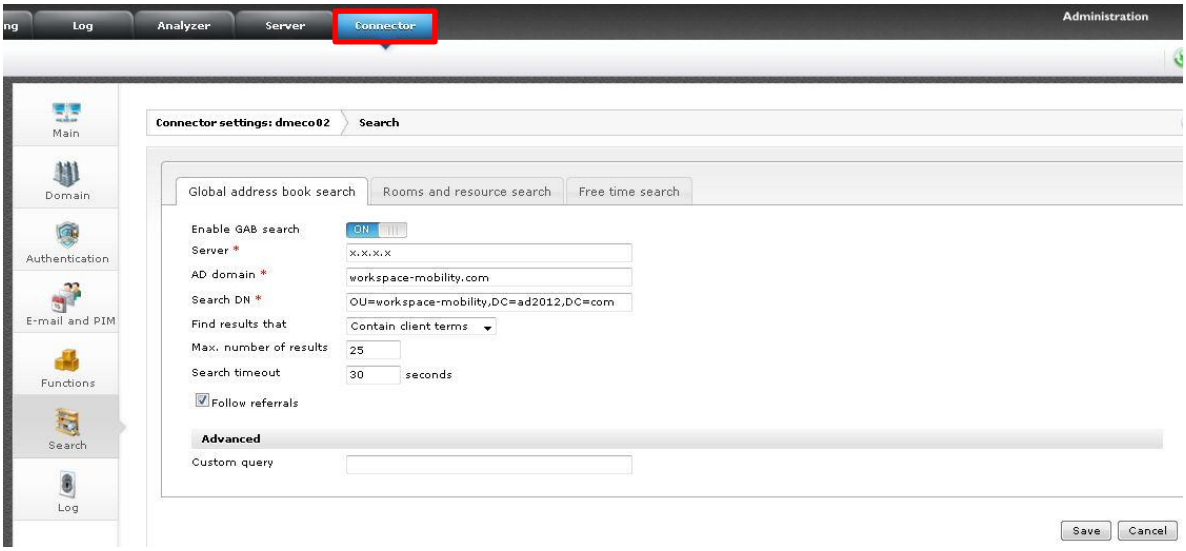


図 2.2.22 Authentication 設定画面

11. 「Connector 2 」をクリックしてください。

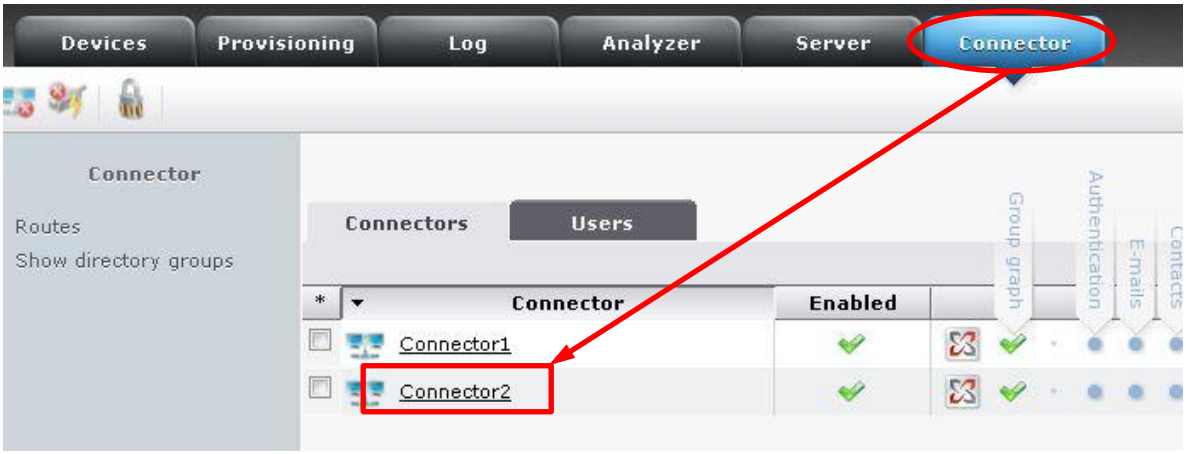


図 2.2.23 Connector 画面

12. 画面左の[E-mail and PIM]をクリックし、General (Exchange)画面を表示してください。
13. General (Exchange)タブ内の項目へ下記情報を参照して設定値を入力し、[Save]をクリックしてください。
14. Save 後、入力値が正しいことを確認するため、画面右下の[Test connection]をクリックしてください。

表 2.2.7 General (Exchange)設定値

対象項目	入力／選択値
Server	Exchange サーバの IP アドレス（※1）
Exchange domain	AD サーバのドメイン名（※2）
Protocol	Exchange2007 ご利用の場合：Exchange2007 (Web service) Exchange2010/Office365 ご利用の場合：Exchange2010 (Web service)
Auth.scheme	NTLM
Mailbox naming scheme	E-mail address

※1：Office365 をご利用の場合は、「outlook.office365.com」を入力ください。

※2：Office365 をご利用の場合は、メールアドレスで使用しているドメイン名（@以降）を入力ください。
AD が複数ある場合は、空欄で構いません。システム側で自動的に識別します。

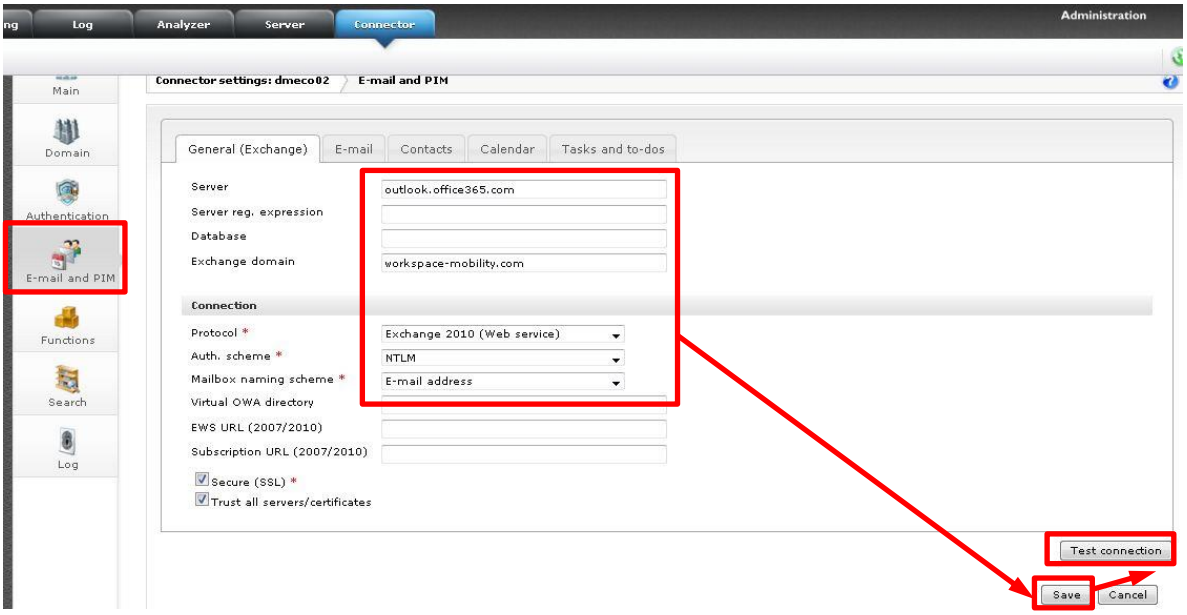


図 2.2.24 Connector 画面

15. Test functions 画面が表示されるので、「E-mails」、「Contacts」、および「Calendar」にチェックを入れます。その後、「Username」に「DME_User」グループに所属しているアカウント名を、「Password」にそのアカウントのパスワードを入力し、[Test]をクリックします。

図 2.2.25 Test functions 画面

16. Result of test の画面が表示されます。正常に処理された場合は、各項目の「Diagnostic」が表示されますので、[Cancel]をクリックします。

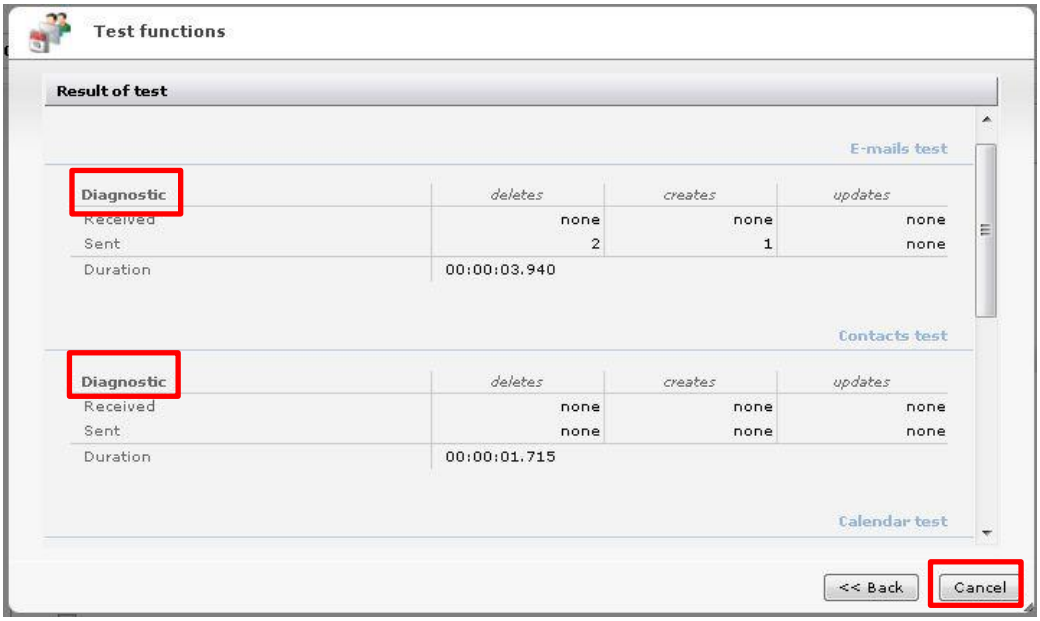


図 2.2.26 Result of test 画面

注意

「Diagnostic」が表示されない場合や、エラーになる場合は、入力したアカウント名または

パスワードが間違っている場合があります。[Back]をクリックし、再度ご確認ください。

アカウント名・パスワードが正しくてもエラーが発生する場合、弊社までお問い合わせください。

17. 画面左下の「Search」をクリックし、Global address book search 画面を表示します。
18. Global address book search タブ内の項目へ下記情報を参照して設定値を入力し、[Save]をクリックしてください。

表 2.2.8 Global address book search 設定値

対象項目	入力／選択値
Enable GAB search	ON
Server	AD サーバの IP アドレス
AD domain	AD ドメイン名
Search DN	AD ドメイン LDAP 識別名（※1） →「OU=XXX,DC=XXX」の記載ルールで入力

※1：LDAP 識別名はドメイン名が「workspace-mobility.com」の場合、「OU=workspace-mobility,DC=com」の記載になります。

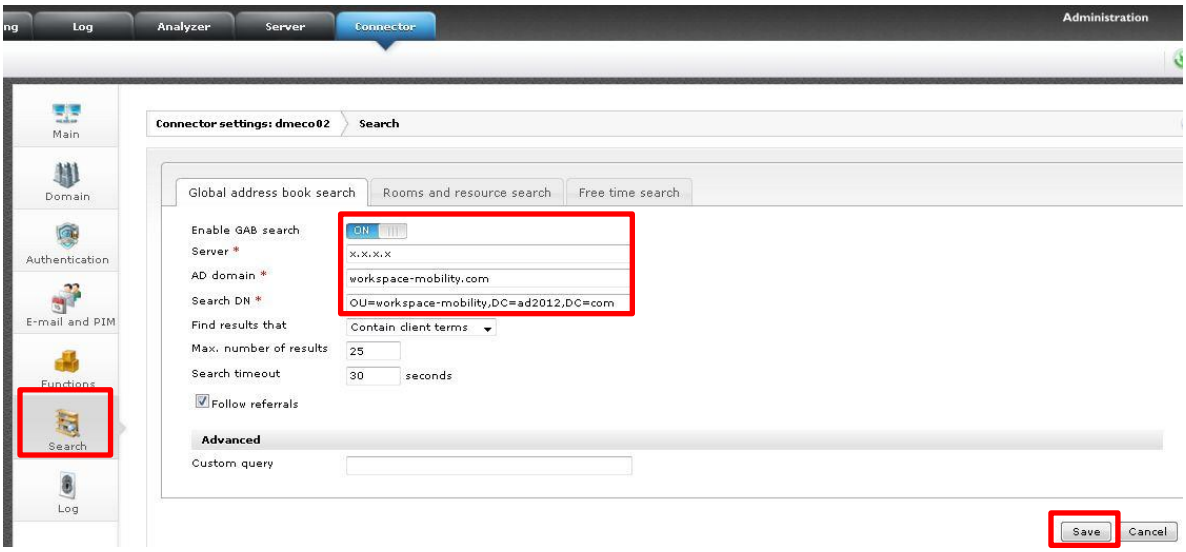


図 2.2.27 Global address book search 設定画面

2.3 グループ作成の検討

グループ作成について検討します。グループの概念については、1.5 項を参照してください。

グループ作成が不要な場合

図 2.3.1 のように、システム管理者 1 名、設定ポリシーが 1 つである場合グループ作成は不要です。

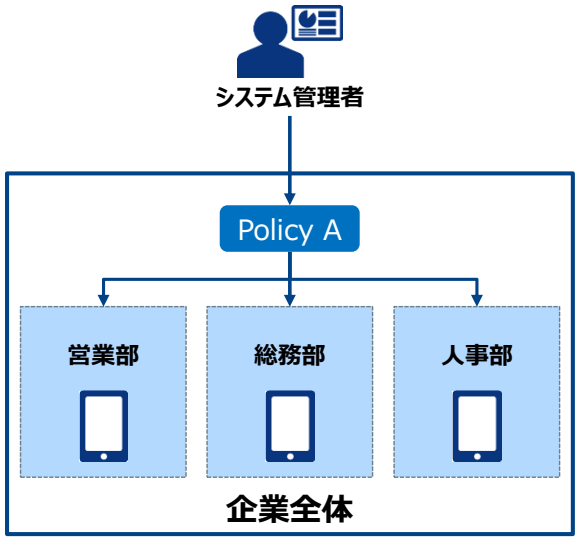


図 2.3.1 グループ作成が不要な場合

グループ作成が必要な場合

図 2.3.2 のように、部署や拠点ごとに管理者やポリシーを割り当てる場合は、グループ作成が必要です。

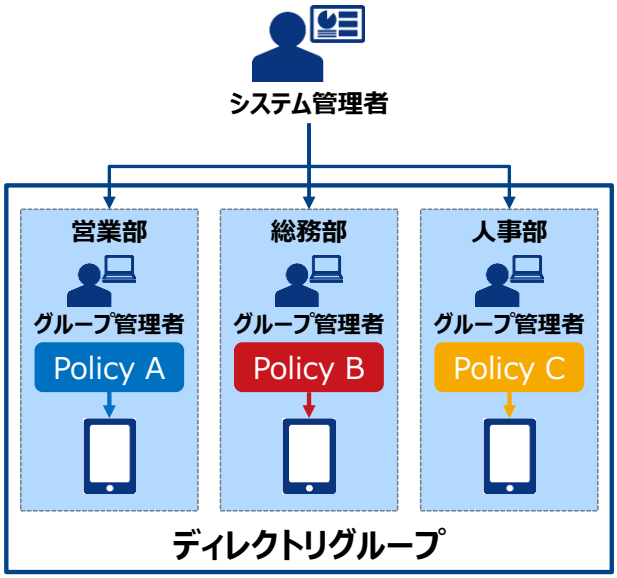


図 2.3.2 グループ作成が必要な場合

2.3.1 ディレクトリグループの追加

Active Directory/LDAP に基づくグループを追加する場合は、以下の手順を実施してください。

Active Directory/LDAP グループの読み込み設定

ディレクトリグループによるグループを追加する場合、まず、Workspace Mobility が利用する Active Directory/LDAP グループを認識する必要があります。Workspace Mobility が Active Directory/LDAP グループを読み込むためには、以下の手順を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Connector]タブより、「Connector1」をクリックしてください。

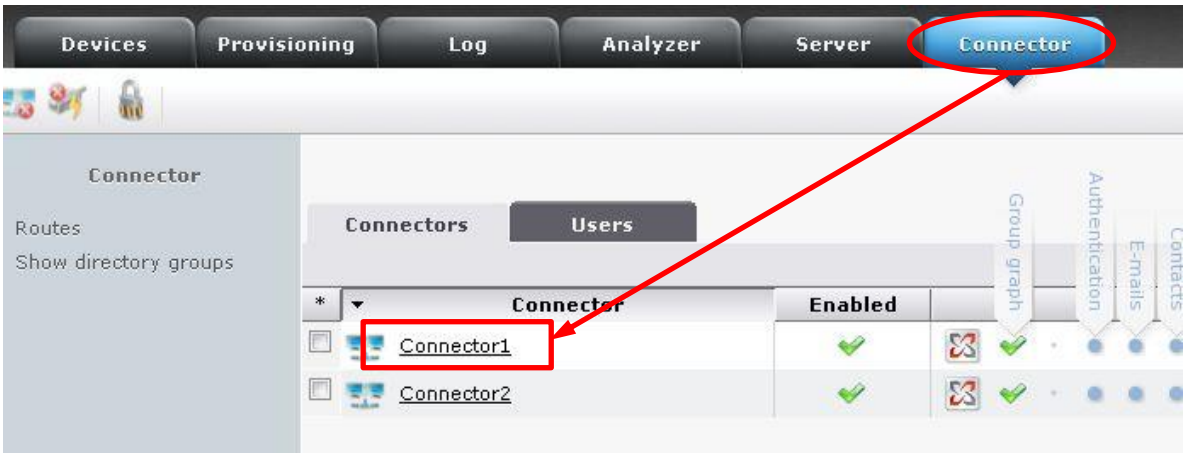


図 2.3.3 Connector 画面

3. 「Domain」をクリックし、画面下部に移動してください。

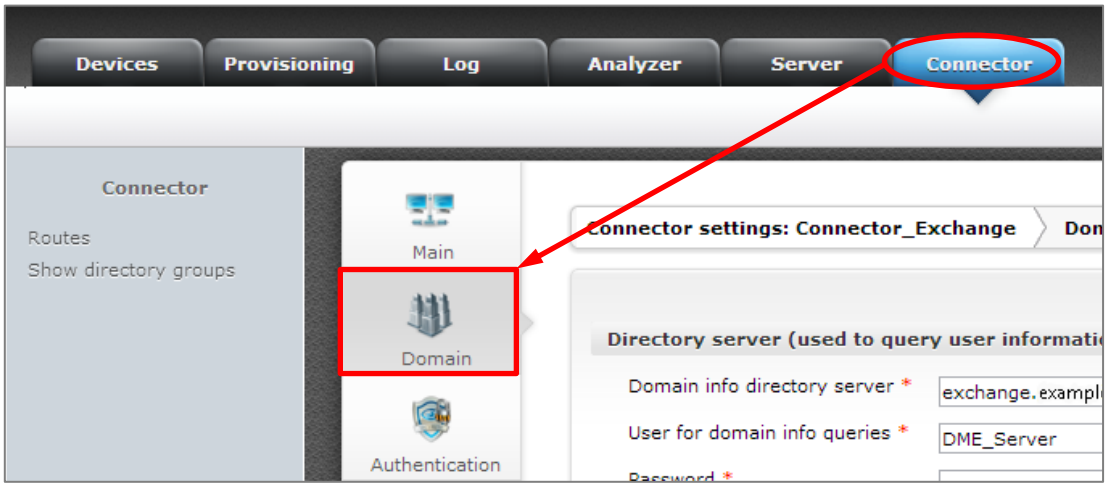


図 2.3.4 Domain 設定画面

4. 「User Groups」の設定項目で「Partial」が選択されていることを確認し、[Additional roots]内に管理対象としたい Active Directory/LDAP グループ名を追加し、<Test readout>をクリックしてください。
※グループ名の追加はテキスト入力形式です。

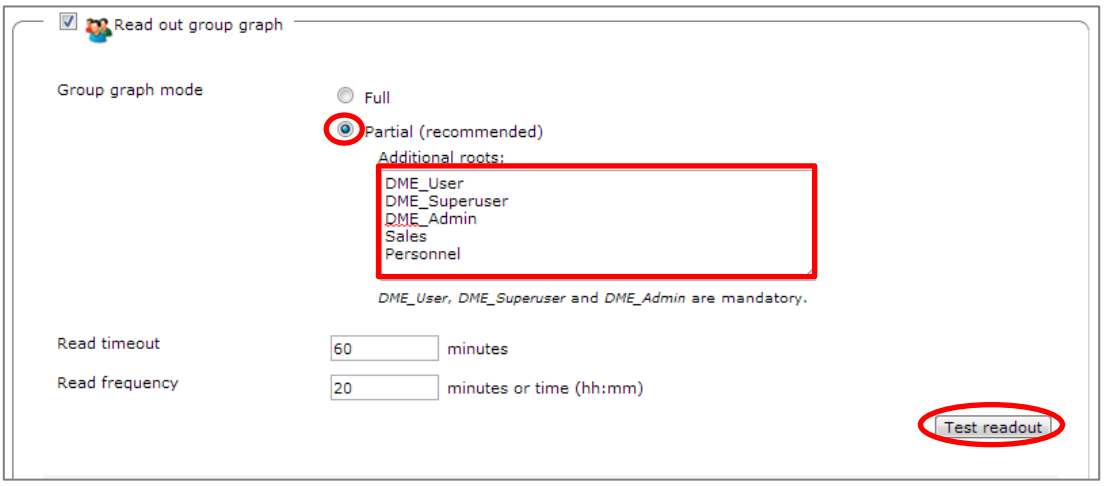


図 2.3.5 User groups (Group graph)

5. 図 2.3.6 が表示されます。追加した Active Directory/LDAP グループ名が正しく表示されている事を確認し、<Save>をクリックしてください。

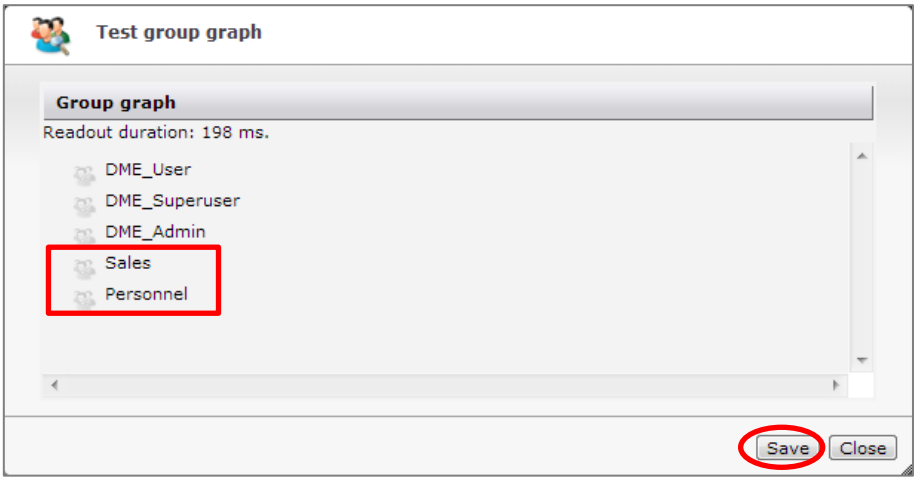


図 2.3.6 Test group graph

ディレクトリグループの追加

1. 管理コンソールに、システム管理者でログインしてください。
2. 管理コンソールにて、[Server]タブ-[Group management] をクリックしてください。

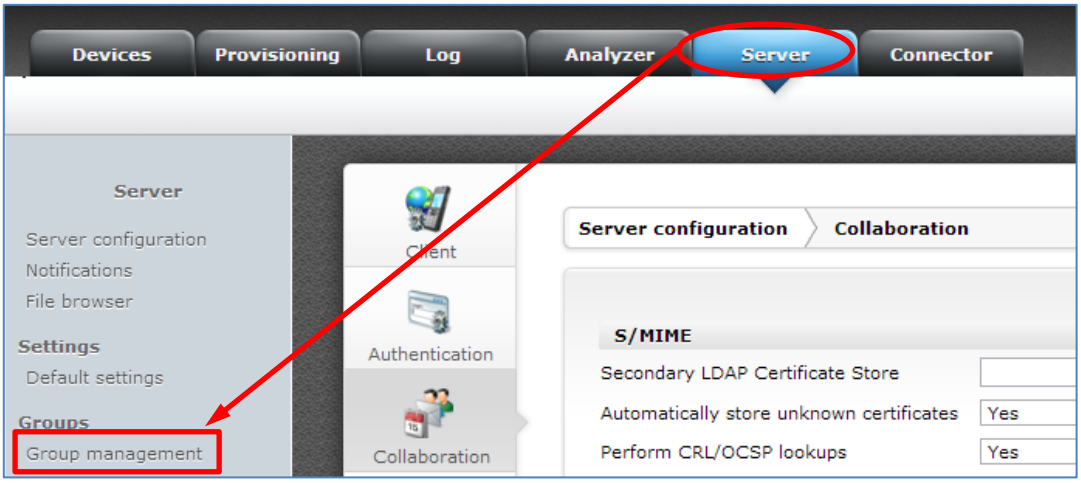


図 2.3.7 Server タブ

3. 図 2.3.8 が表示されます。<Add Group>をクリックしてください。

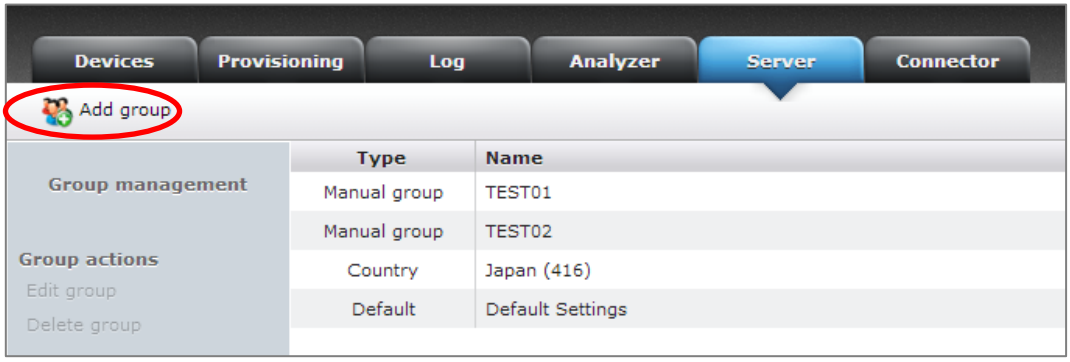


図 2.3.8 Group management

4. 図 2.3.9 が表示されます。[Group type]に[Directory group]を選択し、[Directory group]に新規に作成したい Active Directory/LDAP グループ名を選択し、<Save>をクリックしてください。なお、該当 Active Directory/LDAPグループ名がリストに表示されない場合は、「2.3.1ディレクトリグループの追加」における「Active Directory/LDAP グループの読み込み設定」を参照してください。

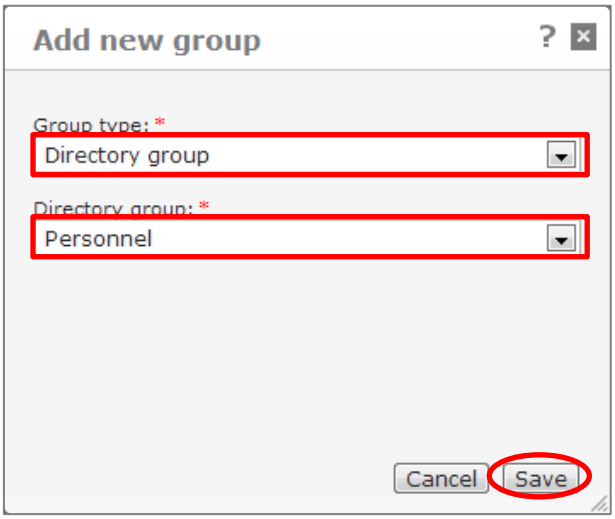


図 2.3.9 Add new group

5. 図 2.3.10 が表示されます。追加したグループが表示されていることを確認してください。

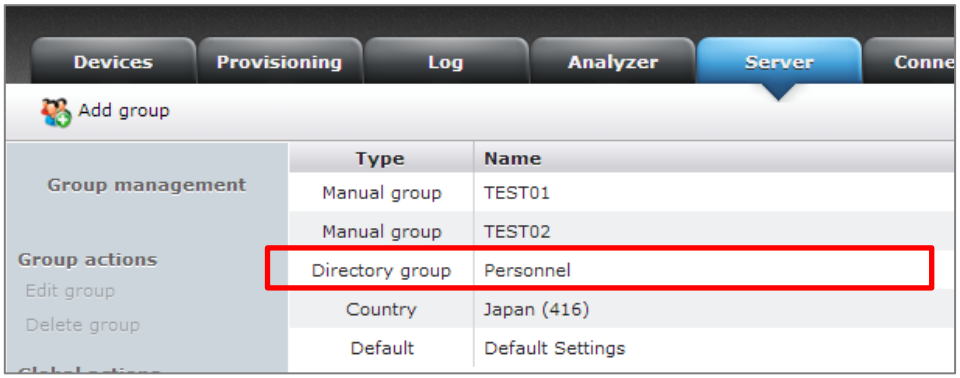


図 2.3.10 グループ作成完了

----------【以下参考】----------

管理者（Super user）権限の割り当て

1. Active Directory サーバに管理者権限のユーザーでログオンしてください。
2. [スタート]-[管理ツール]-[Active Directory ユーザーとコンピューター]をクリックしてください。
3. 図 2.3.11 が表示されます。左ペインにある[Users]ディレクトリをクリックし、管理者とするユーザーを右クリックして[グループの追加]をクリックしてください。

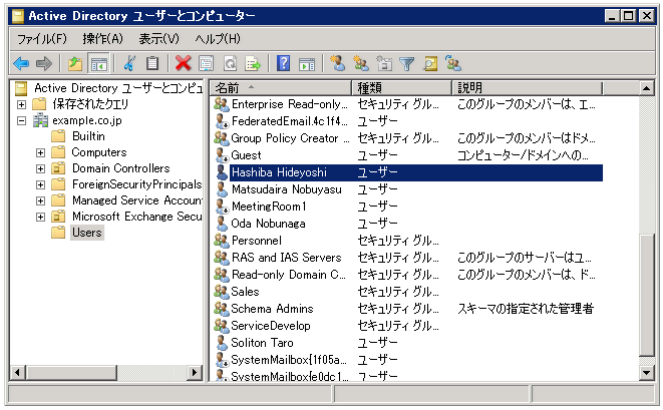


図 2.3.11 Active Directory ユーザーとコンピューター

4. 図 2.3.12が表示されます。[選択するオブジェクト名を入力してください(E)]に「DME_Superuser」と入力し、<OK>をクリックしてください。

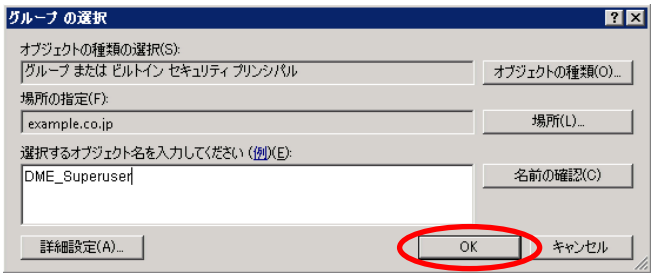


図 2.3.12 グループの選択

5. 図 2.3.13 が表示されます。<OK>をクリックしてください。

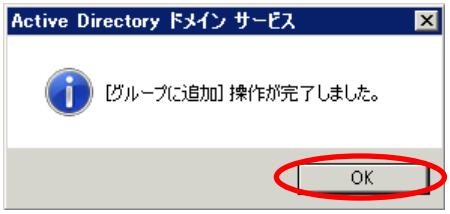


図 2.3.13 Active Directory ドメインサービス

2.4 各種ポリシー設定

ユーザーへ展開する前に、本項のポリシー設定を実施してください。各種ポリシーは後から変更する事もできますが、予め設定しておく事を推奨します。（各種ポリシーのパラメータについては、4.設定パラメータの項目を参照してください。）

注意

ポリシーを変更する前に、ユーザーがポリシーに当たる項目を変更した場合、ポリシーがユーザーの設定を上書きしない場合があります。可能な限り、ユーザーへの展開前にポリシーを作成してください。

2.4.1　全体のポリシー設定

Workspace Mobility を使用する端末全体にポリシーを割り当てる場合は、以下の手順を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Server]タブ-[Default settings]をクリックしてください。画面が切り替わったら[Settings]パネルをクリックします。

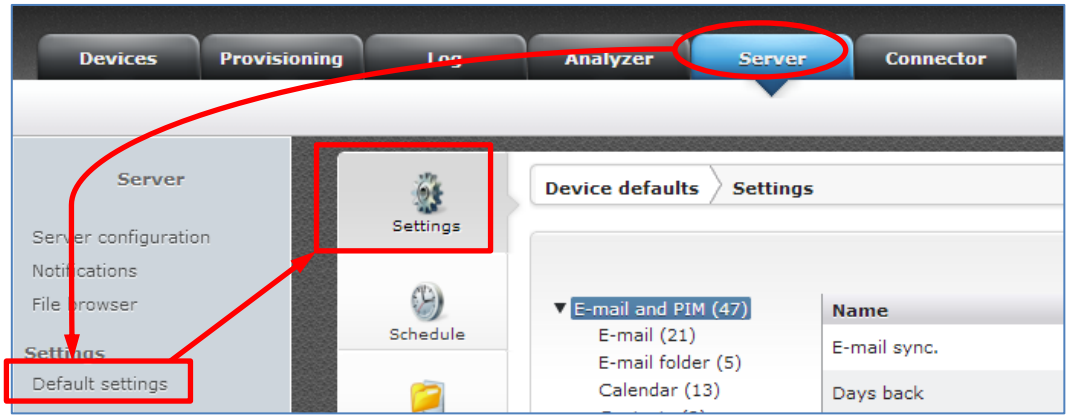


図 2.4.1 Settings

3. メールやスケジュールなどの設定の項目がありますので、必要に応じて変更してください。

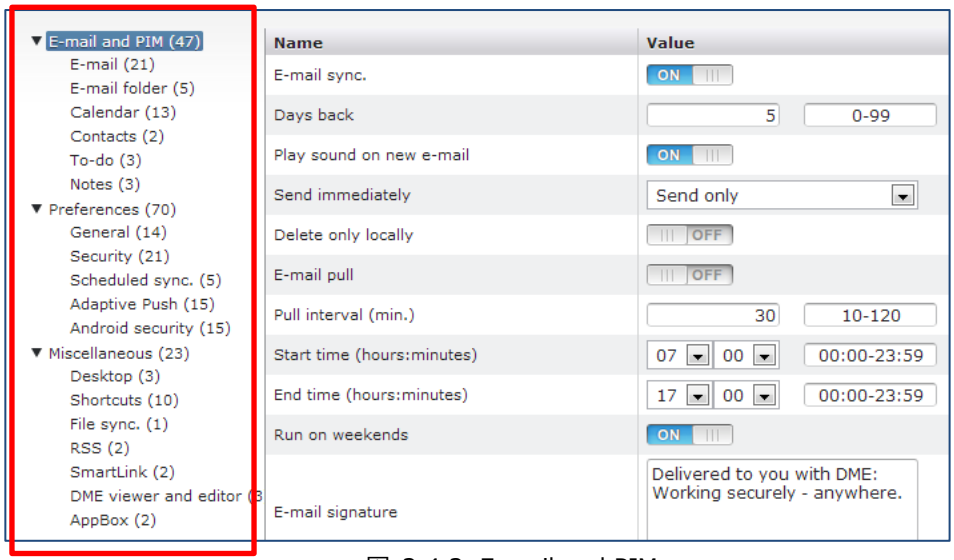


図 2.4.2 E-mail and PIM

4. 項目を選択して「Value」に必要な値を入力してください。最後に、<Save>をクリックして設定を保存してください。

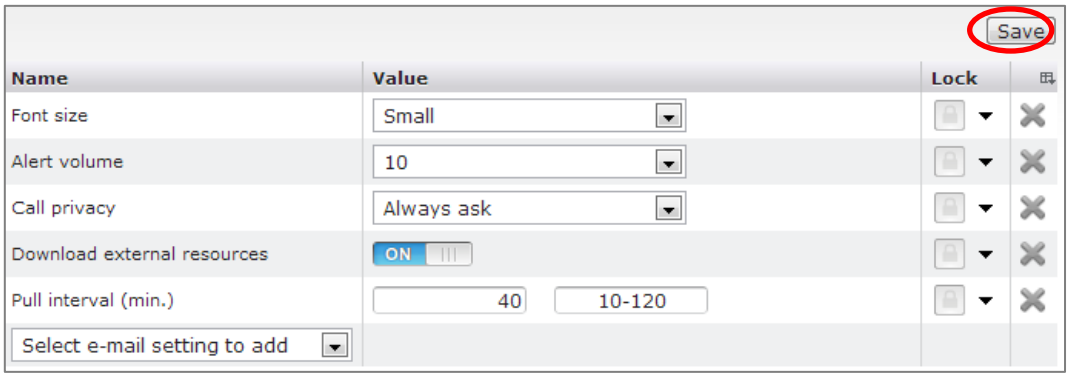


図 2.4.3 Settings

5. 図 2.4.4 が表示されます。<Save>をクリックして設定を保存してください。

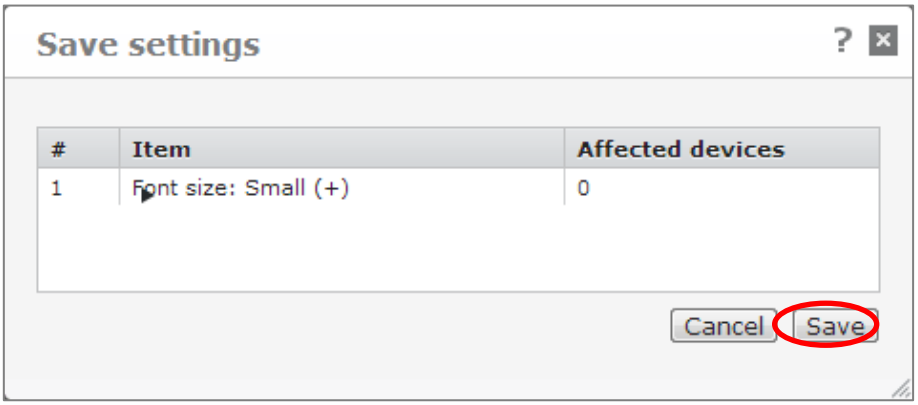


図 2.4.4 Save settings

2.4.2 ポリシー変更のロック

Workspace Mobility における User または Super user 権限を持ったユーザーは、ポリシーを変更することができます。そこで、Workspace Mobility 全体のポリシーを設定する前段階として、システム管理者の意に沿わないポリシーをユーザーが設定してしまわないように予め、システム管理者がポリシー変更のロックをかける事を推奨します。

1. Workspace Mobility 管理コンソールに、システム管理者でログインしてください。
2. [Server]タブ-[Default settings]をクリックしてください。

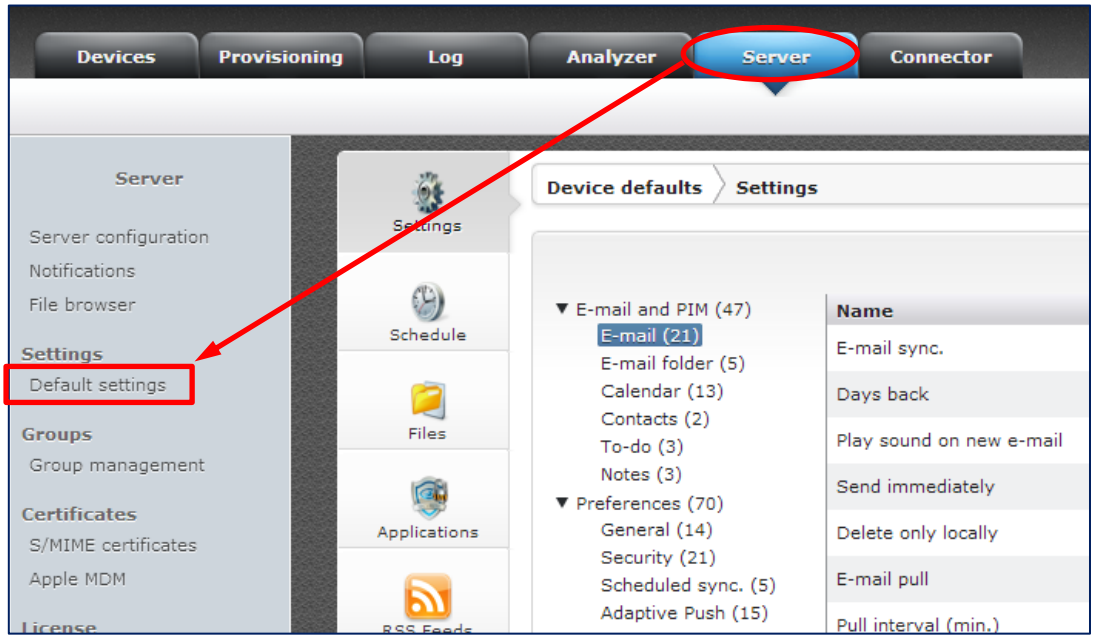


図 2.4.5 Default settings 画面

3. 利用者によるクライアントアプリ側でのポリシー変更をさせたくない場合、各ポリシー項目の右の鍵マークをクリックし、[Device lock]を[ON]に設定してください。
   Super user 権限アカウントによるポリシー変更をさせたくない場合、[Super user]を[ON]に設定してください。
   最後に、<Save>をクリックしてください。

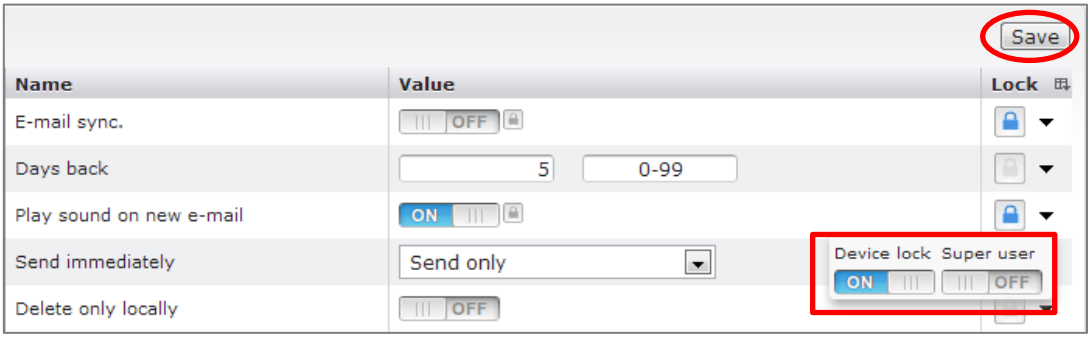


図 2.4.6 ポリシー変更ロック画面

4. <Save>をクリックして設定を保存してください。

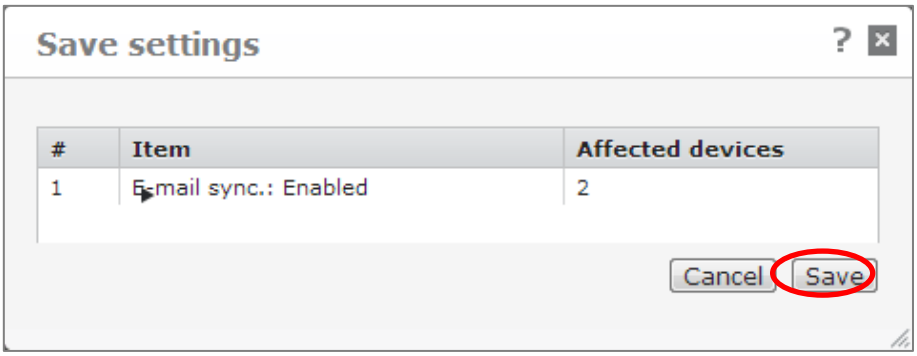


図 2.4.7 Save settings

2.4.3　グループ単位のポリシー設定

作成したグループにポリシーを割り当てる場合は、以下の手順を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Server]タブ-[Group management]をクリックしてください。

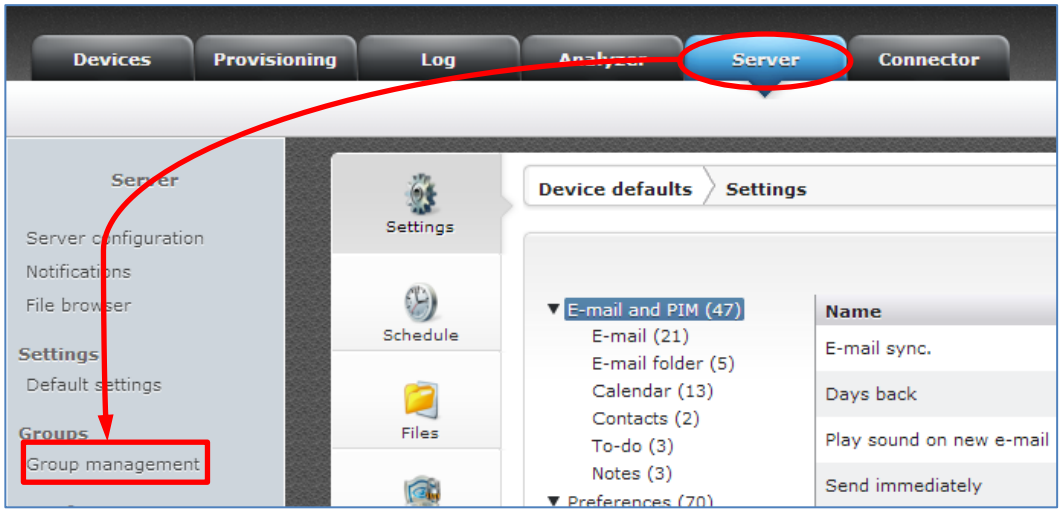


図 2.4.8 Group management

3. 作成したグループを選択して、[Edit group]をクリックしてください。

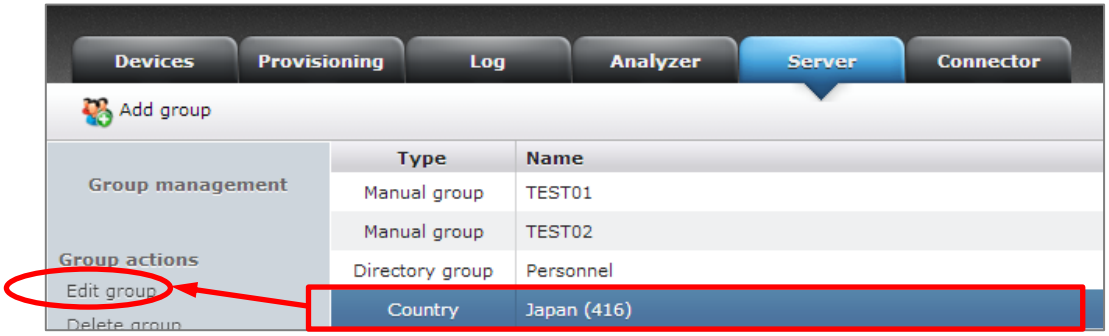


図 2.4.9 Edit group

4. [Settings]パネルを選択して必要な項目を設定してください。最後に、<Save>をクリックして設定を保存してください。

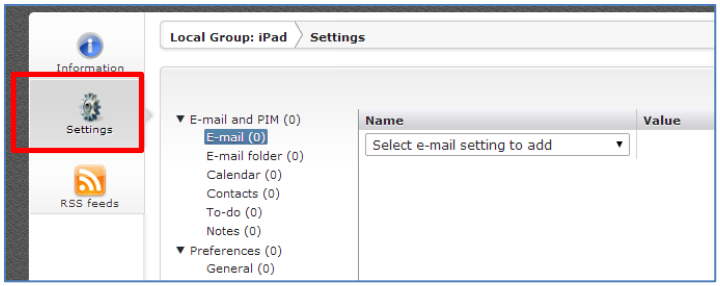


図 2.4.10 Edit group

2.4.4　デバイス単位のポリシー設定

デバイスごとにポリシーを設定する場合は、以下の手順を実施してください。

注意

本項の作業を実施するには、管理コンソール上に設定対象となるデバイスが登録されている必要があります。デバイスの登録についての詳細は、「2.5　デバイスの登録と許可」を参照ください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Devices]タブクリックし、設定するデバイスを選択してください。選択後、[View device info]をクリックします。

図 2.4.11　Devices タブ

3. 画面が切り替わったら、[Settings]パネルを選択してください。

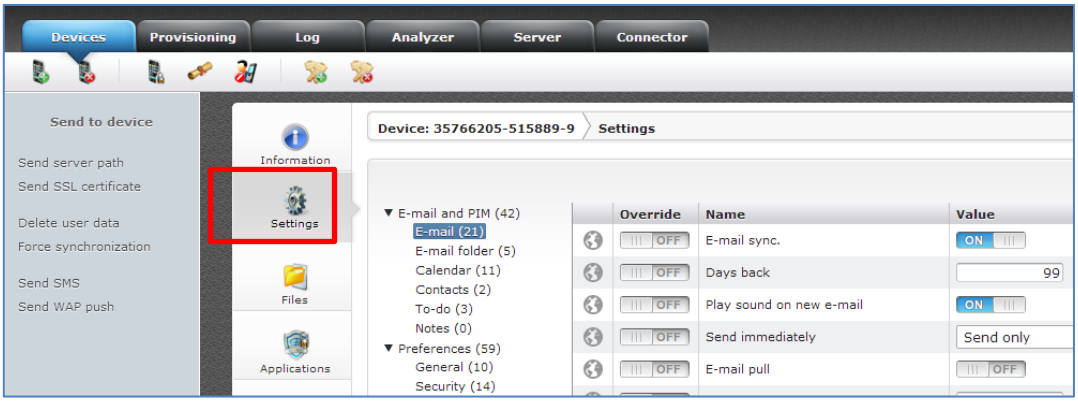


図 2.4.12　E-mail and PIM

4. 項目を選択して「Value」に必要な値を入力してください。最後に、<Save>をクリックして設定を保存してください。

2.5 デバイスの登録と許可

デバイスの登録方法は、大きく分けて「ユーザー認証に通ったデバイスすべて自動で登録し Workspace Mobility の利用を許可する」、「事前登録したデバイスのみ Workspace Mobility の利用を許可する」、「Workspace Mobility に接続してきたデバイスを管理者が承認すると Workspace Mobility の利用を許可する」方法の三種類があります。

ポリシーに従って、いずれかの方法を選択してください。

表 2.5.1 デバイス登録の方法

デバイス登録方法	内容
ユーザー認証に通ったデバイスすべて自動で登録し Workspace Mobility の利用を許可する	ユーザー認証に通ったデバイスすべての Workspace Mobility の利用を許可します。1 ユーザーにつき複数のデバイスを利用できるため、意図しないライセンスの消費が発生する可能性があります。（1 ユーザーで複数デバイスを利用する場合、利用するデバイス数分のライセンスを消費します）
事前登録したデバイスのみ Workspace Mobility の利用を許可する	事前に登録したデバイスのみ Workspace Mobility の利用を許可します。事前に IMEI 番号または、MAC アドレスを Workspace Mobility 管理コンソールに登録する必要があります。
Workspace Mobility に接続してきたデバイスを管理者が承認すると Workspace Mobility の利用を許可する	デバイスを初めて Workspace Mobility に接続すると、Workspace Mobility 管理コンソール上でロック状態のデバイスが登録されます。管理者が許可したいデバイスのロックを解除すると Workspace Mobility の機能が利用できるようになります。

2.5.1 ユーザー認証に通ったデバイスすべて自動で登録し Workspace Mobility の利用を許可する場合（初期値）

ユーザー認証に通ったデバイスすべての Workspace Mobility の利用を許可する場合は、デフォルトの設定のため、事前作業はありません。各デバイスにクライアントアプリをインストールした後、クライアントアプリ上で ID、パスワードを入力しログインすれば利用できます。

2.5.2 事前登録したデバイスのみ Workspace Mobility の利用を許可する場合

あらかじめ登録したデバイスのみ Workspace Mobility の利用を許可する場合は、認証されていないデバイスを登録できないように設定の変更をする必要があります。設定の変更後、利用を許可するデバイスを Workspace Mobility に登録し、その後デバイスからアクセスします。

事前登録したデバイスのみを許可するための設定

事前登録したデバイスのみを許可するためには、以下の手順を実施してください。

1. Workspace Mobility 管理コンソールに、システム管理者でログインしてください。
2. [Server]タブ-[Authentication]をクリックしてください。

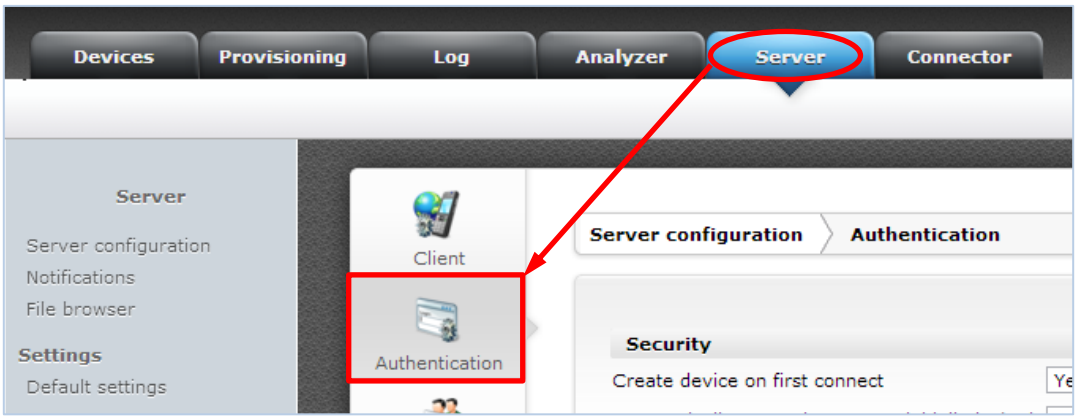


図 2.5.1 Server タブ

3. 図 2.5.2 が表示されます。「Create device on first connect」を「No」に設定し、<Save Configuration>をクリックしてください。

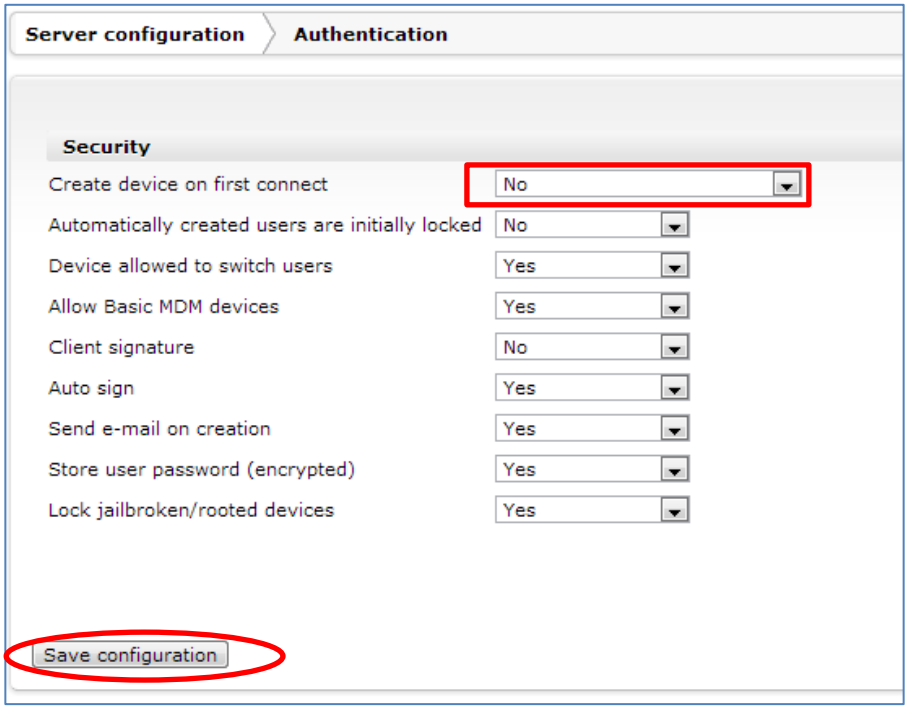


図 2.5.2 Authentication

端末の事前登録方法

接続を許可する端末の事前登録方法は、1 台ずつ登録する方法と CSV ファイルから複数台を一括登録する方法があります。

1 台ずつ個別に登録する場合

デバイスを 1 台ずつ個別に登録する場合は、以下の手順を実施してください。

1. [Devices]タブ-[New device]をクリックしてください。

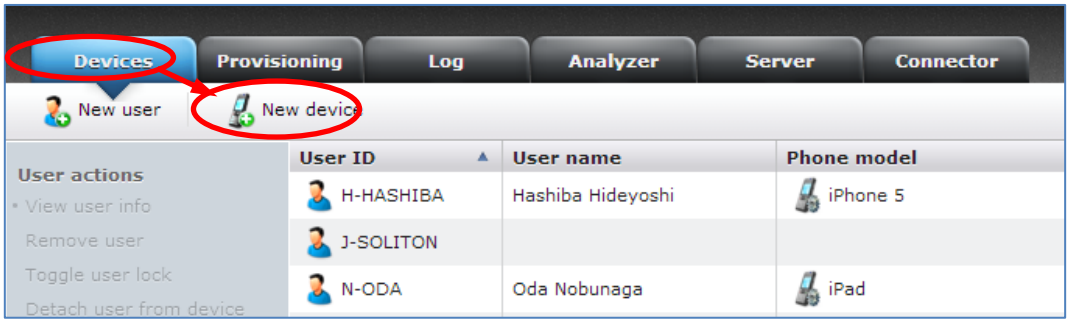


図 2.5.3 Devices タブ

2. 図 2.5.4 画面が現れます。表 2.5.2 を参照して、デバイス情報を入力し、<Create new device>をクリックしてください。

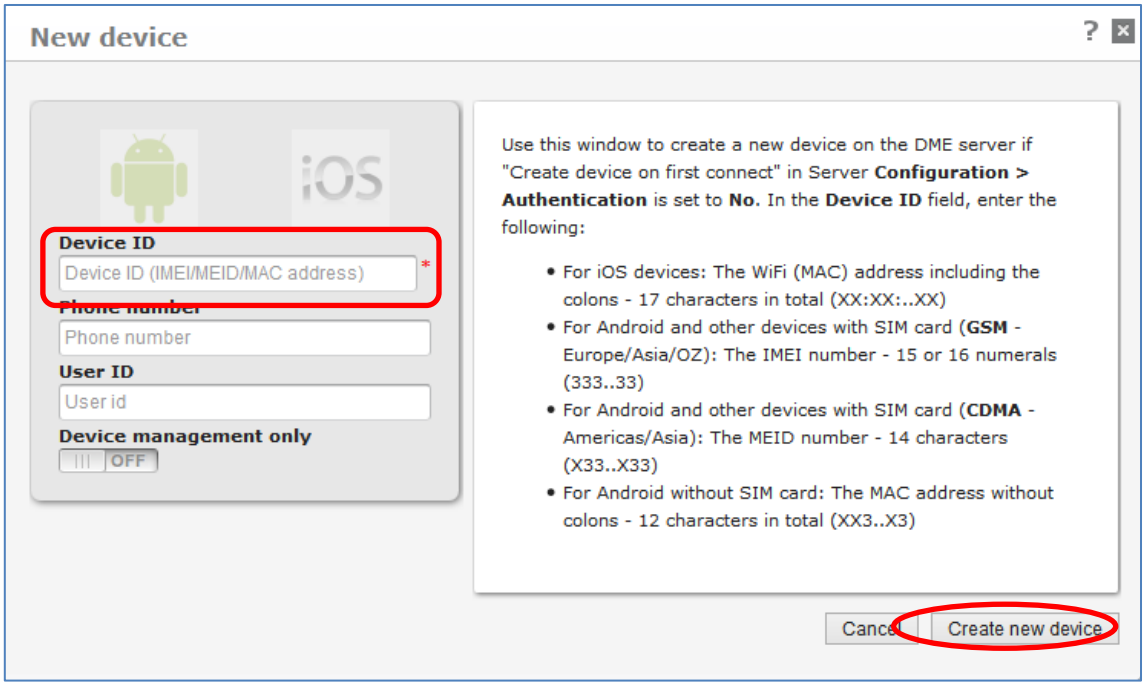


図 2.5.4 New device

表 2.5.2 デバイス登録情報

項目	内容
Device ID (terminalID)	下記の値を入力してください。 ● iOS の場合： SIM の有無に関係なく Wi-Fi (MAC)アドレス(17 桁)*1 ● Android の場合： 電話番号がある場合(au)：MEID 番号 (14 桁) *2 電話番号がある場合(docomo、SoftBank)：IMEI 番号(15 桁) *3 電話番号がない場合(タブレット等)：Wi-Fi MAC アドレス*4 の”：”を省いたもの(12 桁)
Phone number	電話番号がある場合、電話番号を入力します。
User ID	紐づけるユーザーが既に決まっている場合、ユーザーID を入力します。
Device management only	MDM 機能は未提供のため、[OFF]のまま変更しないでください。

表中の注意

*1 iOS の WiFi (MAC)アドレスの確認の方法

端末より設定> 一般>情報>Wi-Fi アドレス

*2 Android 端末(au 端末)

設定> タブレット情報>端末の状態> MEID

*3 Android 端末(docomo、ソフトバンク端末)

設定> タブレット情報>端末の状態> IMEI

*4 Android タブレット端末の MAC アドレスの確認の方法

設定> タブレット情報>端末の状態> Wi-Fi MAC アドレス

一括で登録する場合

CSV ファイルは以下の形式である必要があります。必須項目は terminalID のみです。他の項目は初回ログイン時に自動で Workspace Mobility サーバ側で取得するため、terminalID のみでの登録を推奨します。

注意

作成する CSV ファイルは、カンマ区切りではなく、セミコロン（;）で区切ってください。

1. CSV ファイルを作成します。1 行目に
「terminalID;dmeVersion;inUse;lastUsed;lastUserID;Locked;phoneModel;phoneNumber;platform;userID;userType」を入力し、2 行目以降に実際の値をセミコロン区切りで記載してください。
※任意項目を入力しない場合は、セミコロンのみ入力してください。

```
terminalID;dmeVersion;inUse;lastUsed;lastUserID;Locked;phoneModel;phoneNumber;platform;userID;userType
00a3293990c95075d25788195c2d7ad4;;;;;;;;;
fce687316e37a8c5063238093d04aaf8;;;;;;;;;
```

表 2.5.3 デバイス登録情報

項目	内容	必須/任意/不要
terminalID	下記の値を入力してください。 ● iOS の場合： Wi-Fi アドレス*1":"有りを MD5 ハッシュ変換したもの(32 桁) 例) 00a3293990c95075d25788195c2d7ad4 ※MD5 ハッシュ変換する機能は本サービスでは提供しないため、外部ツールを利用ください。 ● Android の場合： 電話番号がある場合(au)：MEID 番号*2(14 桁) 電話番号がある場合(docomo、SoftBank)：IMEI 番号*3 (15 桁) 電話番号がない場合(タブレット等)：Wi-Fi MAC アドレス*4 の":"を省いたもの(12 桁)	必須
dmeVersion	入力しないでください。（セミコロンのみ入力ください）	不要
inUse	入力しないでください。（セミコロンのみ入力ください）	不要
lastUsed	入力しないでください。（セミコロンのみ入力ください）	不要
lastUserID	入力しないでください。（セミコロンのみ入力ください）	不要
Locked	入力しないでください。（セミコロンのみ入力ください）	不要
phoneModel	デバイスのモデル名を入力します。デバイスが初めて全システム情報の同期を実行したときに、デバイスにより値が更新されます。例)iPhone5c	任意
phoneNumber	電話番号があれば電話番号を記入します。国番号を含めて入力下さい。 例)+819012345678	任意
platform	プラットフォーム名を入力します。デバイスが初めて全システム情報の同期を実行したときに、デバイスにより値が更新されます。 例)iOS	任意
User ID	紐づけるユーザーが既に決まっている場合、ユーザーID を入力します。 例)YAMADA	任意
userType	入力しないでください。（セミコロンのみ入力ください）	不要

表中の注意

*1 iOS の MAC アドレスの確認の方法
端末より設定> 一般>情報>Wi-Fi アドレス

*2 Android 端末(au 端末)
設定> タブレット情報>端末の状態> MEID

*3 Android 端末(docomo、ソフトバンク端末)
設定> タブレット情報>端末の状態> IMEI

*4 Android タブレット端末の MAC アドレスの確認の方法
設定> タブレット情報>端末の状態> Wi-Fi MAC アドレス

1. [Devices]タブ-[Import devices]をクリックしてください。

2.6.

5 Import devices

2. 図 2.5.5 が表示されます。<Upload>ボタンをクリックし、作成した CSV ファイルを選択して<Select devices>をクリックしてください。

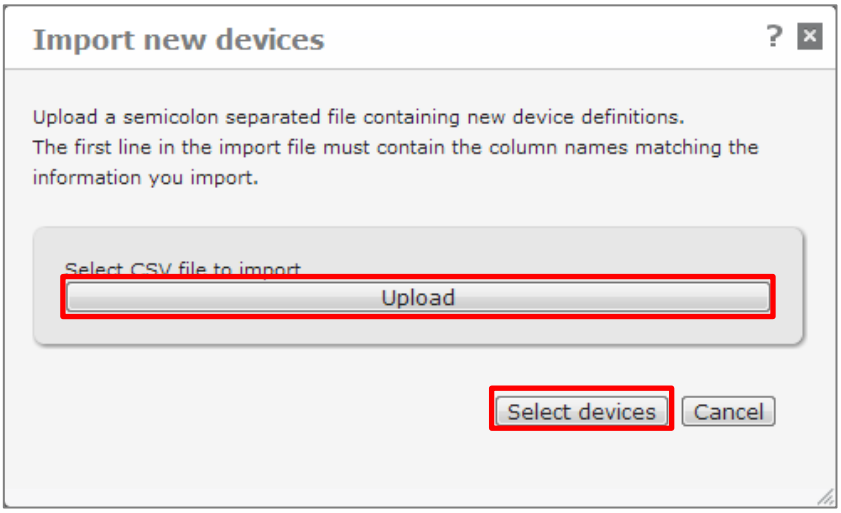


図 2.5.5 Import new devices

3. 図 2.5.6 が表示されます。アップロードするデバイスにチェックを入れ、<Import>をクリックしてください。

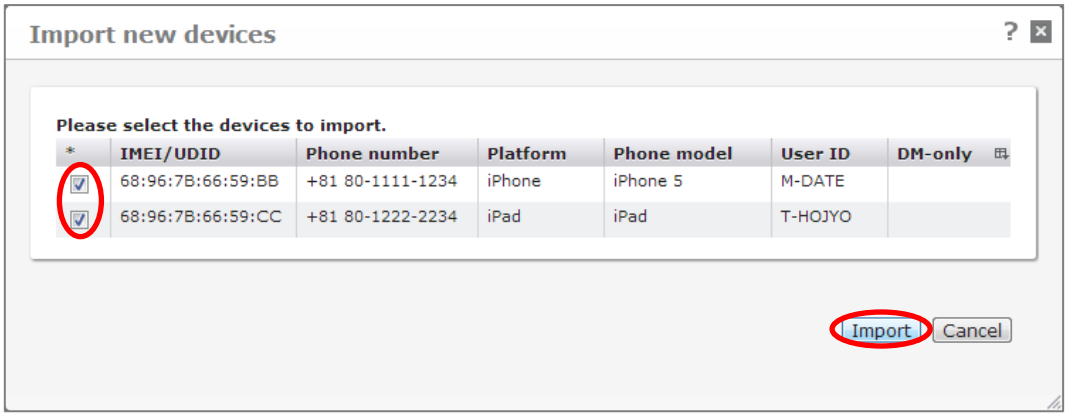


図 2.5.6 Import new devices

4. 図 2.5.7 が表示されます。Devices タブにインポートしたデバイス情報が表示されます。

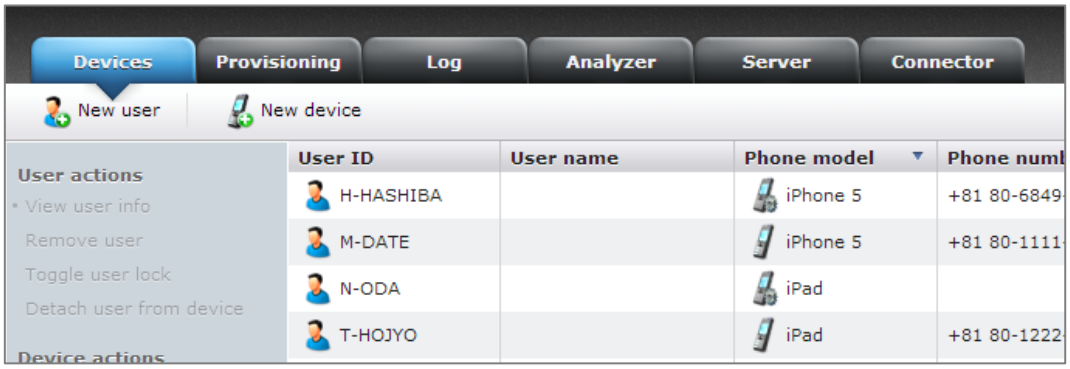


図 2.5.7 Devices タブ

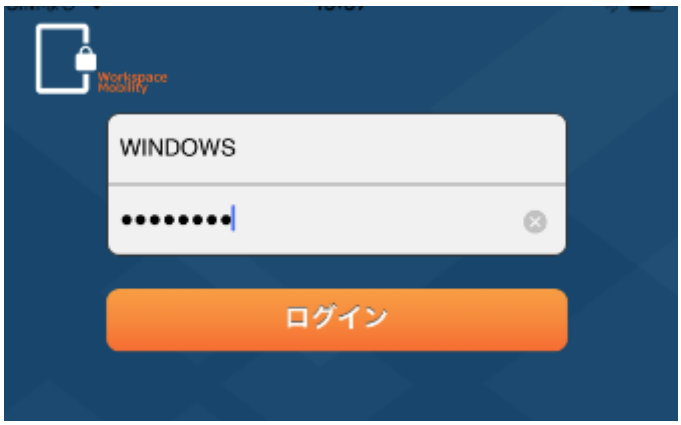
クライアントアプリでのログイン

デバイス登録後、クライアントアプリよりログインすると、デバイス登録がされている端末の場合のみユーザーのログインに成功します。デバイス登録がない場合、管理コンソールのログに「Not allowed to create device」と表示されます。

クライアント端末側での画面遷移は以下のとおりとなります。

1. ログイン画面が表示されます。ドメインアカウントの「ユーザー名」と「パスワード」を入力し、<ログイン>をタップします。

※ ユーザー名は大文字で表示されます。



2. 「サーバーホスト名」入力画面が表示されます。「ホスト名」の欄に、お客様毎にお知らせした Workspace Mobility サーバのホスト名を入力して、<接続のテスト>をタップします。「接続成功」と通知されたら、画面右上の <完了>をタップします。

※サーバーホスト名について分からない場合は、システム管理者にお問い合わせください。

（サーバーホスト名の例： n000000000.ws-d.jp）

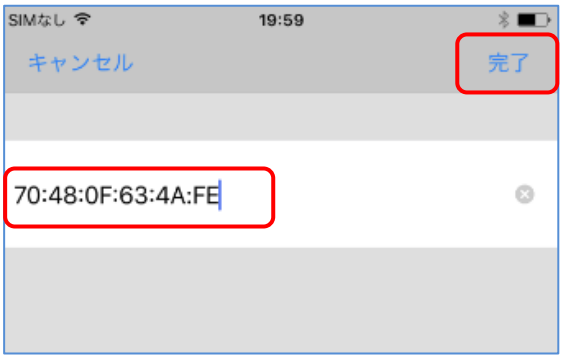
3. 「ようこそ」画面にて、ご利用端末の電話番号を入力します。（任意項目です。Wi-Fi 専用端末は対象外となります。）

※お客様毎の運用ポリシーに従って SMS メッセージ送信およびデバイス管理用に電話番号を認識します。

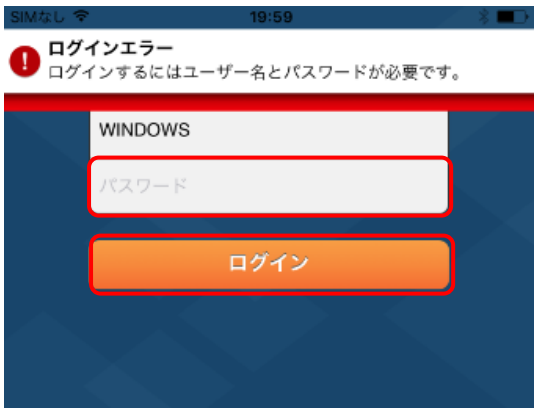
4. ログインエラーが表示されるので、「Wi-fi アドレスの入力」をタップします。

※iOS端末でのみ必要です。Android端末では本エラーは発生せず、ログイン成功しますのでご利用を開始して下さい。

5. 端末の Wi-fi アドレスをペーストし、「完了」をタップします。



6. 画面遷移によりログインエラーが表示されるので、再度パスワードを入力し、「ログイン」をタップします。



7. 同期が開始されるので、利用を開始して下さい。

2.5.3 システム管理者の承認にて Workspace Mobility の利用を許可する場合

Workspace Mobility に接続してきたデバイスを自動で登録し、管理者が承認すると Workspace Mobility の利用を許可する場合は、端末初期接続時にロック状態で登録されるように設定する必要があります。管理者が許可したいデバイスのロックを解除すると Workspace Mobility の機能が利用できるようになります。

初めに登録時にデバイスにロックをかける

デバイス登録時にロックをかけるためには、あらかじめ以下の設定を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Server]タブ-[Server Configuration]-[Authentication]をクリックしてください。

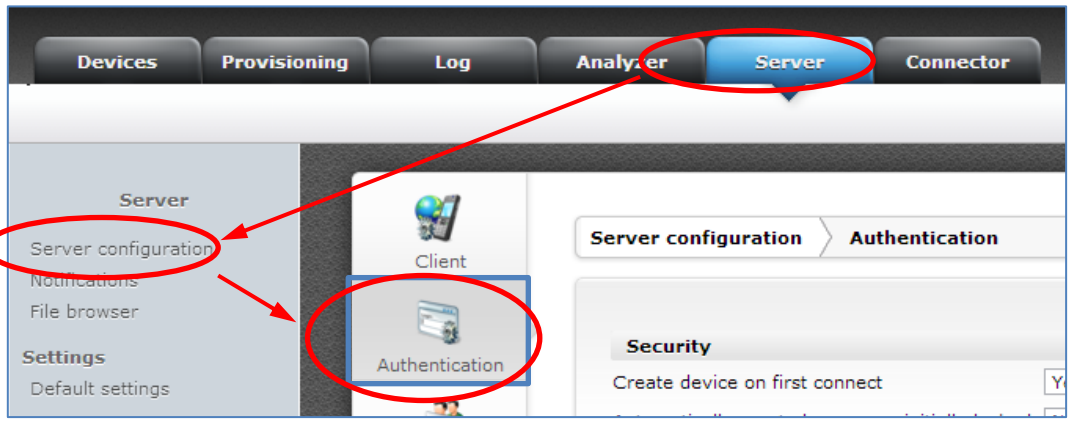
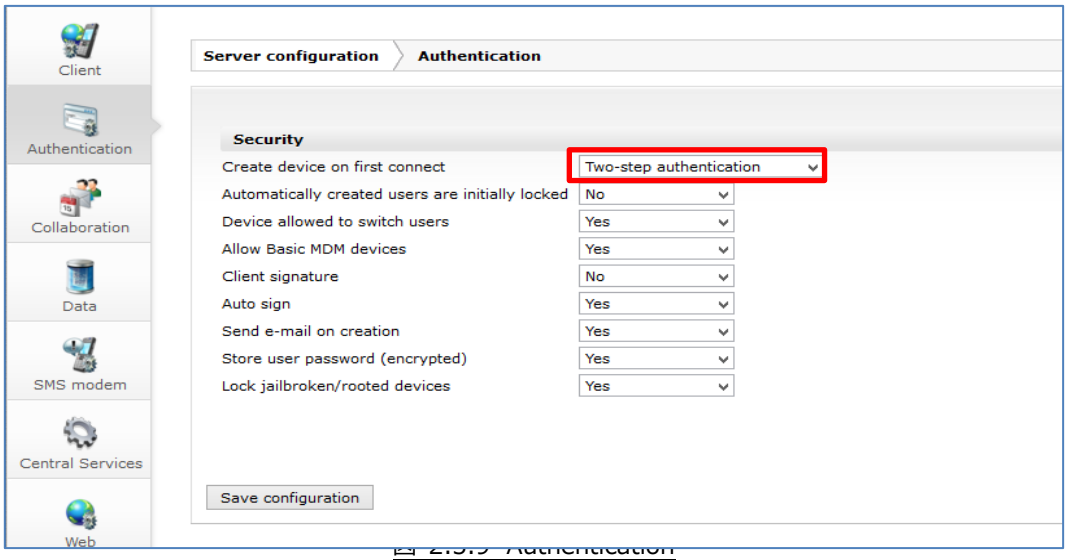


図 2.5.8 Authentication 設定画面

3. 図 2.5.9 が表示されます。「create device on first connect」を「Two-step authentication」にしてください。
4. 「Sava configuration」をクリックしてください。



2.5.5 Authentication

デバイスのロック解除

「Two-step authentication」に設定後、クライアントアプリから Workspace Mobility に接続すると、ユーザーはログインに失敗しますが、Workspace Mobility Server 上ではロックされたデバイスが登録され管理者に通知されます。管理者はユーザーが利用できるようにするため、デバイスのロックを解除する必要があります。

デバイスのロックを解除するためには、以下の手順を実施してください。

1. [Devices]タブ-ロック解除対象のデバイスを選択状態にし[Toggle Device blocking]をクリックしてください。

図 2.5.10 Devices タブ

2. 図 2.5.11 が表示されます。<Yes>をクリックしてください。

図 2.5.11 Toggle device blocking

3. 図 2.5.12 が表示されます。デバイスから鍵マークがなくなった事を確認してください。

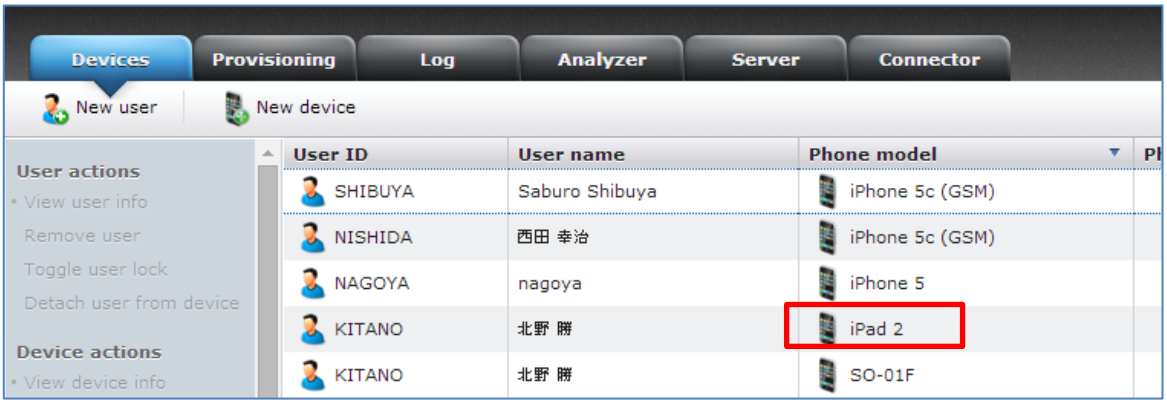


図 2.5.12 ロック解除されたデバイス

2.5.4 デバイス登録時のその他追加設定（[Authentication]パネル）

[Server]タブ-[Authentication]で使用できるその他の設定項目について説明します。

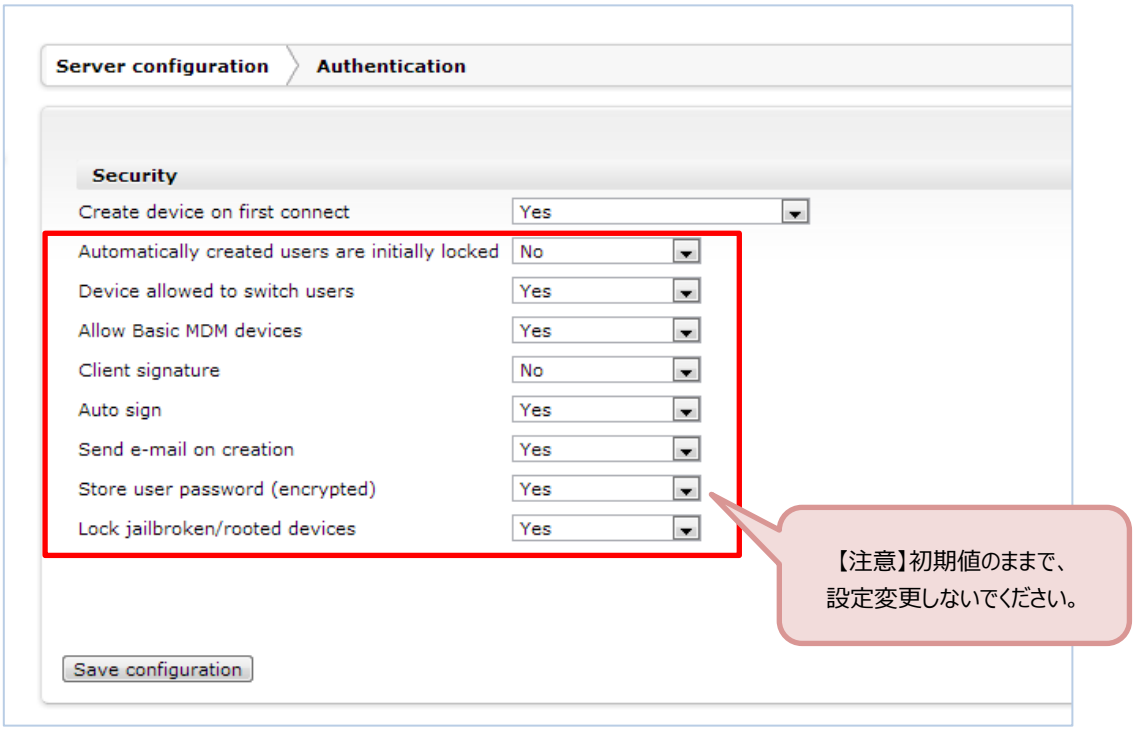


図 2.5.13 Authentication

----------【以下参考】----------

Automatically created users are initially locked

（※本設定項目は初期設定値のまま、お客様側で変更しないでください）

このフィールドを[Yes]に設定すると、ユーザーがロックされた状態で登録されます。

したがって、管理者が[Devices]タブでロックを解除するまで、ユーザーは Workspace Mobility が同期できません。このフィールドを[No]に設定すると、ユーザーはロックされずに登録されるため、すぐに Workspace Mobility を使用できます。デフォルトは[No]です。

[Yes]： ユーザー登録時にロック状態になります。

[No]： ユーザー登録時ロックされません。

Device allowed to switch users

（※本設定項目は初期設定値のまま、お客様側で変更しないでください）

このフィールドを[Yes]に設定すると、デバイス所有者の変更を許可します。つまり、1 つの端末でユーザーを切り替えて Workspace Mobility にログインできます。

このフィールドを[No]に設定すると、デバイスがユーザーに関連付けられ、ログインするユーザーが[Devices]タブに登録されたユーザーと異なる場合は利用できません。

[Yes]： ユーザーの切り替えを許可します。
[No]： ユーザーの切り替えを許可しません。

Client signature

（※本設定項目は初期設定値のまま、お客様側で変更しないでください）

このフィールドでは、クライアントとサーバ間に署名付きの通信が必要かどうかを指定できます。クライアントの署名とは、ユーザーの LDAP/AD 認証を開始する前に、クライアントがシステムの有効なユーザーであることをサーバが確認するプロセスです。これにより、LDAP システムに対する DoS 攻撃を防止します。

クライアントの署名は、Workspace Mobility Server が発行する公開鍵と秘密鍵を基礎に成り立っています。各クライアントがサーバから一意の鍵を受け取ります。クライアントが Workspace Mobility に接続すると、クライアントがサーバに提示した鍵をサーバが検証します。鍵が検証されない場合は、アクセスが即座に拒否されます。

[No]： サーバとクライアント間の通信に署名されることを前提としません。
[Compatible]： サーバが互換性のあるクライアントに対してのみ、サーバとクライアント間の通信に署名されている必要があるとみなします。互換性のあるクライアントとは、上述のプラットフォームで実行されるクライアントアプリのバージョン 2.0 以上です。この設定は、Workspace Mobility の前バージョンからのアップグレード中など、移行段階でのみ使用することを推奨します。すべてのクライアントに証明書がインストールされている場合は、このフィールドを[Yes]に変更する必要があります。
[Yes]： クライアントからサーバへのすべての接続が、DSS（Digital Signature Standard：デジタル署名標準）に従って署名されます。つまり、接続を確立して LDAP でユーザーのルックアップを実行するには、サーバが公開鍵と秘密鍵の仕組みを用いて、クライアントが実際にシステムに対して既知であることを検証する必要があります。

Auto sign

（※本設定項目は初期設定値のまま、お客様側で変更しないでください）

このフィールドを[Yes]に設定すると、初めて接続するときに、署名されていないデバイスに証明書（キーペア）が配布されます。[Client signature]が有効な場合は（上記を参照）、既存の対応するデバイスすべてに署名するまでの移行期間にこの設定を有効にすることができます。

このフィールドを[No]に設定すると、[Devices]タブの Add client signing key タブ機能を使用して、デバイスのキーペアを生成する必要があります。

[Yes]： 自動で証明書の割り当てを行う
[No]： 手動で証明書の割り当てを行う

Send e-mail on creation （※サポート対象外）

（※本設定項目は初期設定値のまま、お客様側で変更しないでください）

このフィールドを[Yes]に設定すると、デバイスが作成されたとき、デバイスのユーザーが変更されたとき、または新しいデバイス署名キーが生成されたときに、管理者にメールが送信されます。これにより、Workspace Mobility 管理者が変更

内容を確認したり、ロックされたデバイスのロックを解除したり、デバイスの新しいキーを生成できます。

[Yes]： デバイスが新規登録された際に、事前に設定された管理者宛てにメールで通知する
[No]： 通知メールを出しません

Store user password (encrypted)

（※本設定項目は初期設定値のまま、お客様側で変更しないでください）

このフィールドを[Yes]に設定すると、各ユーザーの受信トレイのパスワードが暗号化されて、ローカル Workspace Mobility データベースに保存されます。パスワードはユーザーが初めてデバイスを同期したときに保存されます。これにより、Workspace Mobility_Server ユーザーにアクセスを許可しなくても、Workspace Mobility がユーザーのパスワードを用いて受信トレイをスキャンできます。パスワードは受信トレイのスキャンのみに使用されます。

この設定を[Yes]から[No]に変更すると、保存されたパスワードがすべて消去されるためご注意ください。再度[Yes]に設定すると、個々のユーザーのパスワードを収集するプロセスが新たに開始します。このプロセスを実行するには、まず、JBoss アプリケーションサーバでアクティブなユーザーセッションがタイムアウトする必要があります。これには約 20 分かかります。この間、ユーザーがクライアントアプリから接続を確立することはできません。

[Yes]： 各ユーザーの受信トレイのパスワードが暗号化されて、ローカルデータベースに保存されます。
[No]： ローカル Workspace Mobility データベースに保存されません。

Lock jailbroken/rooted devices

（※本設定項目は初期設定値のまま、お客様側で変更しないでください）

Workspace Mobility はクライアントから、Jailbreak されたクライアント（iOS）、root 化されたクライアント（Android）、何の影響も受けていないクライアントに関する情報を取得します。それぞれ、(Jailbroken)または(Rooted)をデバイス名に追加することにより、クライアントがデバイスの Jailbreak や root 化について報告します（例えば、iPhone 3GS (Jailbroken)）。

このフィールドを[Yes]に設定すると、Jailbreak または root 化されたと報告されたすべてのデバイスがロックされます。この設定を有効にすると、Jailbreak または root 化された既存デバイスが次回 Workspace Mobility サーバにアクセスしたときにすべてロックされ、デバイスが Jailbreak または root 化されている場合は、新規デバイスがロック済みとして作成されます。

この設定を有効にし、再度無効にした場合は、ロックされたデバイスのロックを手動で解除する必要があります。

※ ロックされた Jailbreak/root 化されたデバイスを手動でロック解除した場合は、デバイスがサーバに接続したときに再度ロックすることはできません。このため、ユーザーがこのようなデバイスを通常のデバイスと同様に使用できます。

[Yes]： Jailbreak または root 化されたと報告されたすべてのデバイスがロックされます。（初期設定値）
[No]： Jailbreak または root 化された端末はロックされません。

3. Workspace Mobility 運用管理

この章では、クライアントを運用する上で、システム管理者にて実施が必要な手順について記載します。

3.1 ライセンスの確認と更新

Workspace Mobility を使用するユーザーやデバイス、ライセンス ID 等の確認方法について記載します。

3.1.1 ライセンス使用状況の確認

ライセンスの使用状況を確認するためには、以下の手順を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Server]タブ-[Manage License]をクリックしてください。

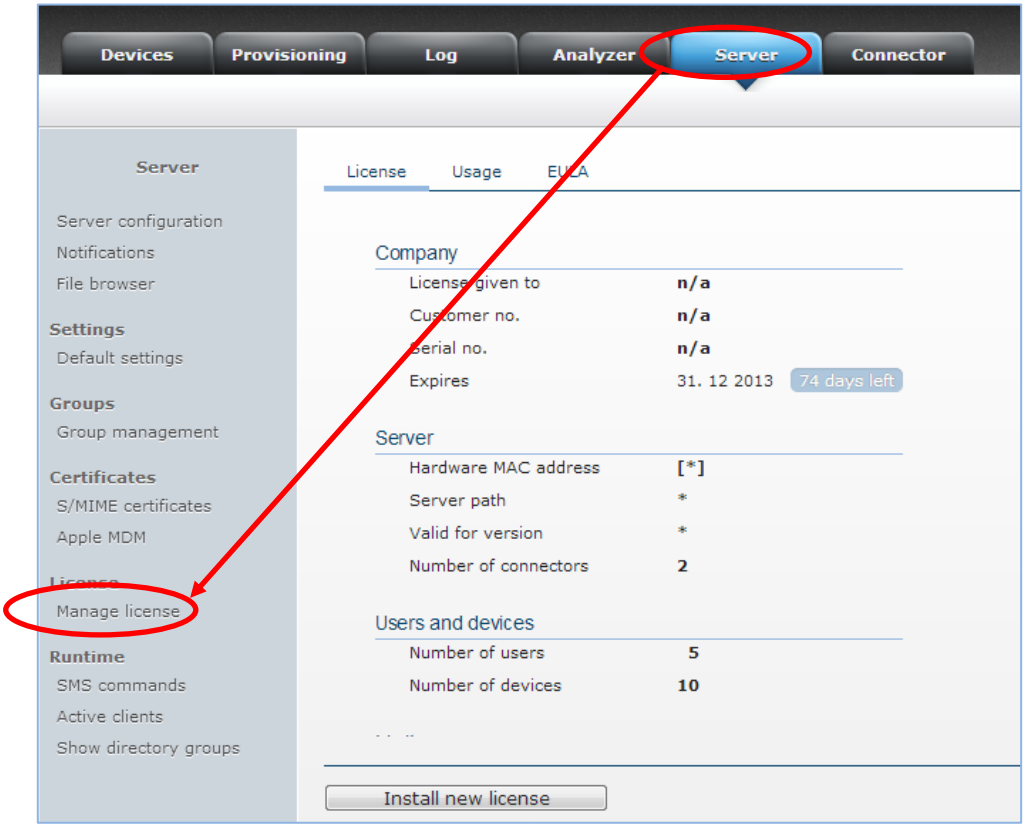


図 3.1.1 Manage License

3. [Usage]をクリックしてください。利用可能ライセンス数と現在の使用ライセンス数が表示されます。

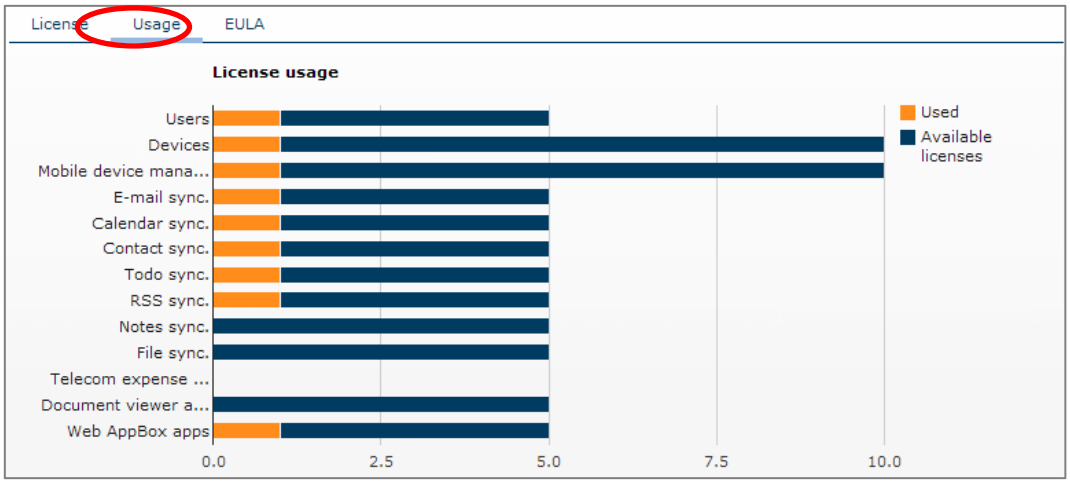


図 3.1.2 License Usage

4. ライセンス数の追加・削除・変更の際は、弊社営業担当までご連絡ください。

表 3.1.1 ライセンス項目説明

カテゴリ	項目	説明	メモ
Company	License given to	発行対象者	-
	Customer no.	カスタマー番号	-
	Serial no.	シリアル番号	-
	Expires	有効期限	-
Server	Hardware MAC address	Workspace Mobility サーバの MAC アドレス	-
	Server path	サーバ PATH	-
	Valid for version	対象 Workspace Mobility バージョン	-
	Number of connectors	コネクタ数	利用するコネクタ台数
Users and devices	Number of users	ユーザーライセンス数	利用するユーザー数
	Number of devices	デバイスライセンス数	利用するデバイス数
Limits	No. devices with Mobile Device Management (MDM)	MDM デバイスライセンス数	利用するデバイス数
	No. users with Document viewer and editor	Viewer and Editor ライセンス数	利用するユーザー数
	No. users with Web AppBox apps	AppBox ライセンス数	利用するユーザー数
	No. users with E-mail sync.	メールライセンス数	利用するユーザー数
	No. users with Contact sync.	連絡先ライセンス数	利用するユーザー数
	No. users with Calendar sync.	カレンダーライセンス数	利用するユーザー数
	No. users with Todo sync.	To-do ライセンス数	利用するユーザー数
	No. users with Notes sync.	メモライセンス数	利用するユーザー数
	No. users with File sync.	ファイル同期ライセンス数	利用するユーザー数
	No. users with RSS sync.	RSS ライセンス数	利用するユーザー数
	No. users with Telecom expense management	電気通信経費管理ライセンス数	利用するユーザー数

※ ユーザーを追加する場合、Active Directory/LDAP やコラボレーションシステム（Exchange、Office365）に対し、設定変更作業が必要です。未実施の場合、ユーザーのログインや各種データ同期に失敗する場合があります。

コラボレーションシステムの設定については、「導入の手引き」を参考に「DME_Test」ユーザーと同じ手順で、ユーザー作成等の設定を実施してください。

表 3.1.2 ライセンス項目説明

項目	説明	メモ
Number of Users	ユーザーライセンス数	-
Number of Tokens	デバイスライセンス数	-
Number of Menu Actions	Menu Action 登録最大数	-

3.2 デバイス情報の確認

各種デバイス情報を確認するためには、以下の手順を実施します。

3.2.1 デバイスの一般情報の確認

登録デバイスの一般情報を確認する場合は、以下の手順を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Devices]タブ-(確認するデバイス)-[View device info]をクリックしてください。

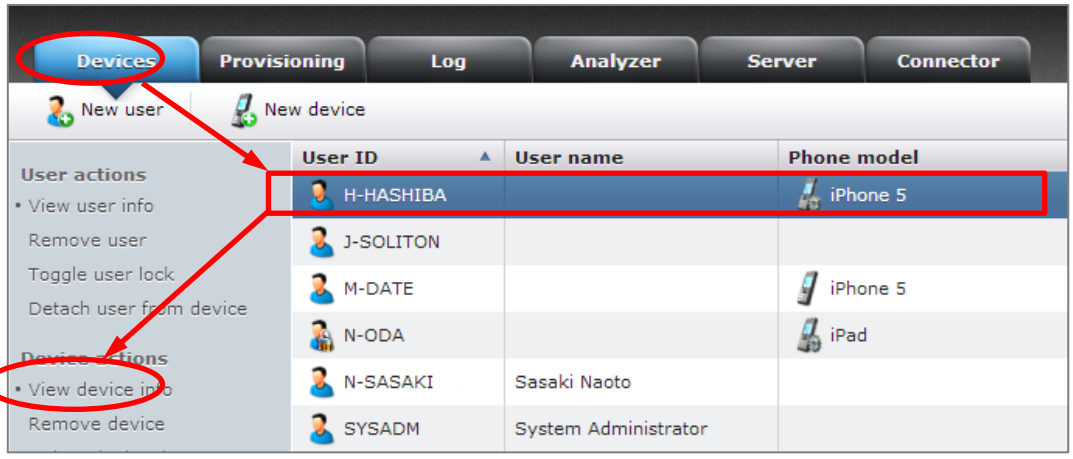


図 3.2.1 Devices タブ

3. 図 3.2.2 が表示されます。[Information]にデバイス情報が表示されます。

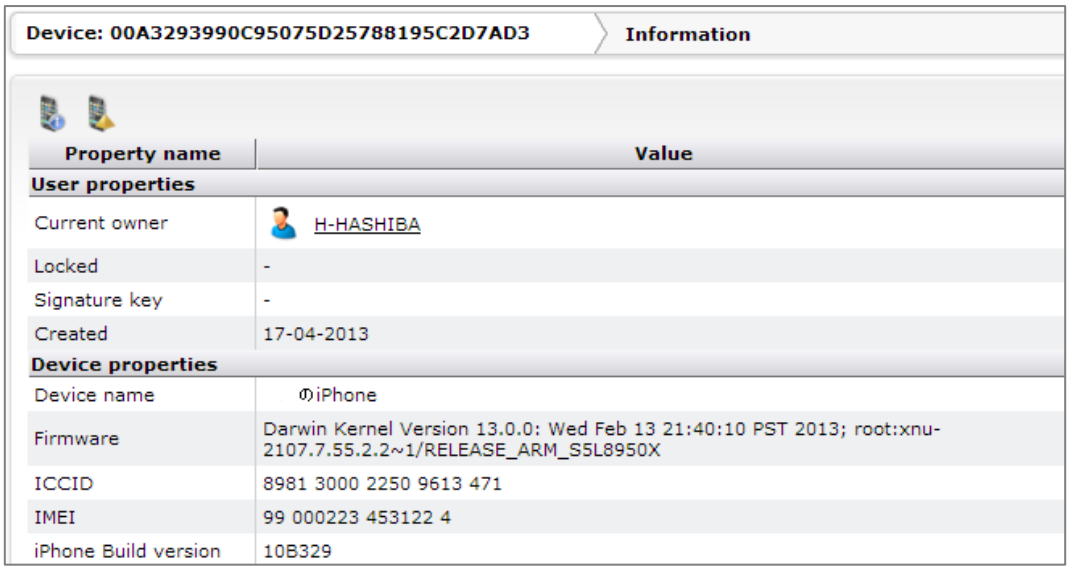


図 3.2.2 Information

3.2.2 デバイスに設定されているポリシーの確認

デバイスに設定されているポリシーを確認するためには以下の手順を実施してください。どのグループのポリシーが適用されているかもあわせて確認する事ができます。

1. [Devices]タブ-(確認するデバイス)-[View device info]をクリックしてください。

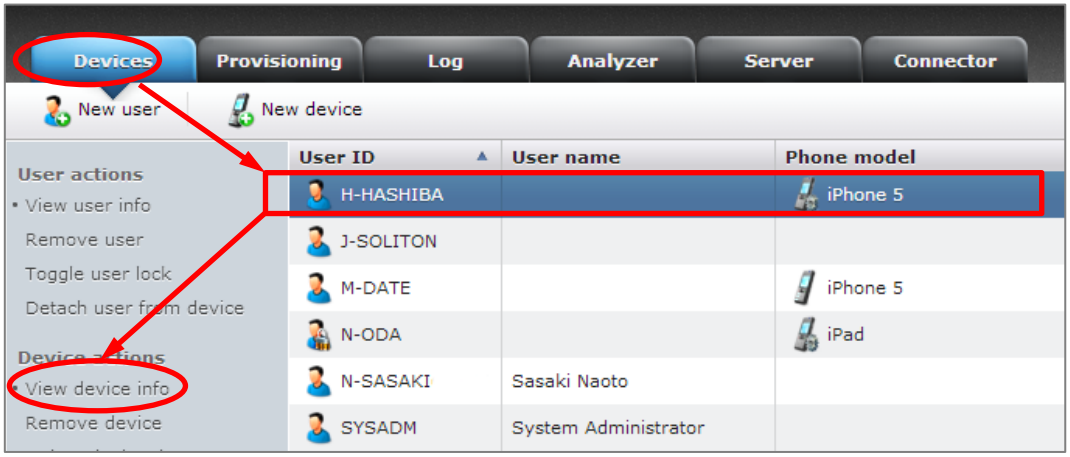


図 3.2.3 Devices タブ

2. 図 3.2.4 が表示されます。[Settings]をクリックしてください。

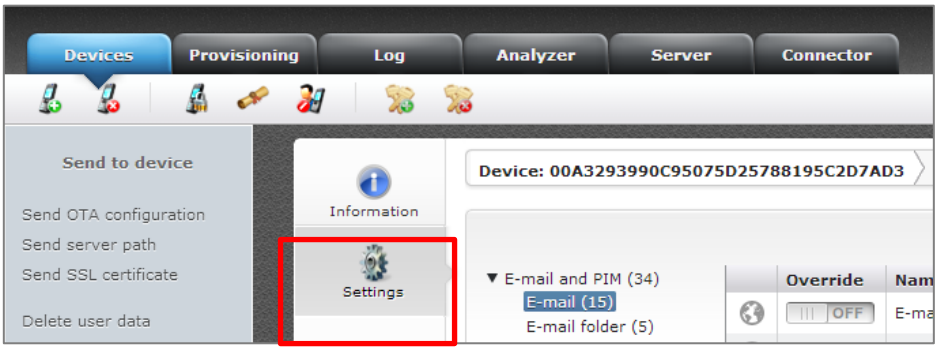


図 3.2.4 Settings 画面

3. 図 3.2.5 が表示されます。本画面より、デバイスに設定されているポリシーを確認してください。

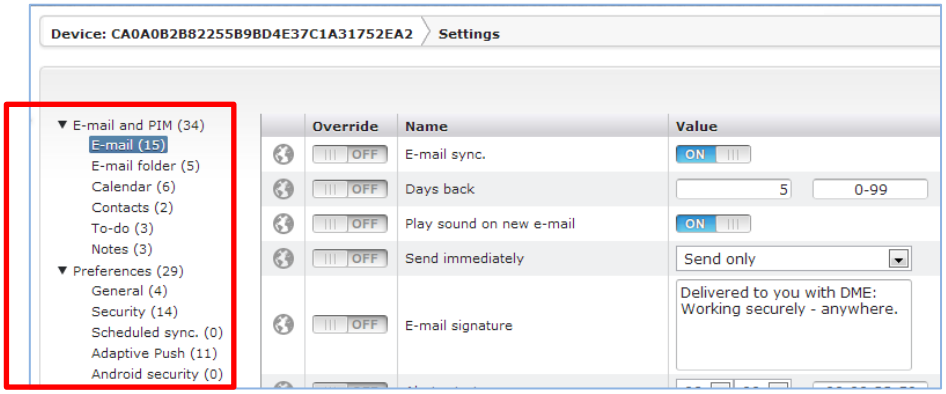


図 3.2.5 Device settings

3.2.3 ユーザートラフィックの確認

ユーザー毎のトラフィックを確認する事により、各ユーザーの使用状況が把握することができます。

ユーザー毎のトラフィックを確認するためには、以下の手順を実施してください。

1. [Analyzer]タブをクリックし、「Filter」にて検索期間を指定し、<Show period>をクリックしてください。

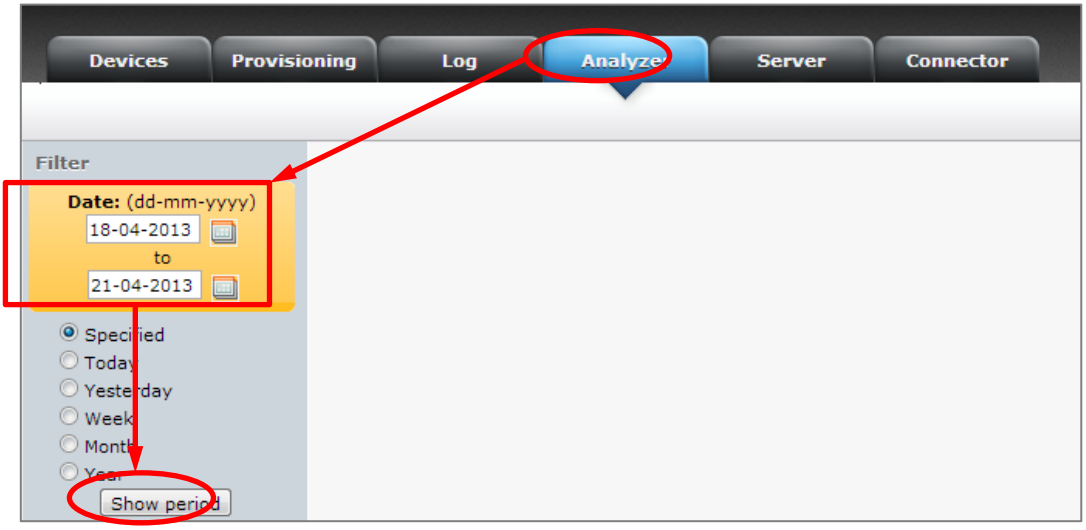


図 3.2.6 Analyzer

2. 図 3.2.7 が表示されます。「Requests」の量を確認し、トラフィックを確認します。

※「Requests」は、クライアントアプリから Workspace Mobility サーバへの通信要求数を示します。

「Data」はクライアントアプリからの通信でやりとりされたデータ量を示します。

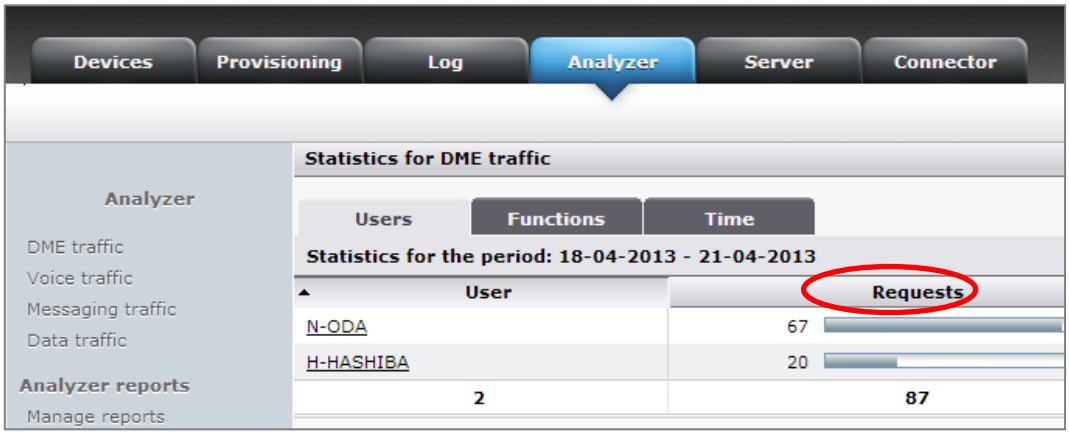


図 3.2.7 Statistics for Workspace Mobility traffic

3.3 ユーザー・デバイスの削除

あるユーザーが Workspace Mobility を使用しなくなった、もしくはデバイスを使用しなくなった場合は、該当するユーザーやデバイスを管理コンソールから削除します。

注意

予め、以下の作業を実施してから本作業を実施してください。実施せずに Workspace Mobility 管理コンソールから削除しても、通信時に自動で再登録されてしまう場合があります。

- **Active Directory/LDAP にて、削除するユーザーを DME_User グループから削除してください。**
- **デバイス側にてクライアントアプリのアンインストールを実施してください。**

3.3.1 ユーザーの削除手順

ユーザーを削除するためには、以下の手順を実施してください。

※ユーザーを削除した場合、当該ユーザーに紐づいたデバイス情報も一緒に削除されます。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Devices]タブ-(削除するユーザー)-[Remove user]をクリックしてください。

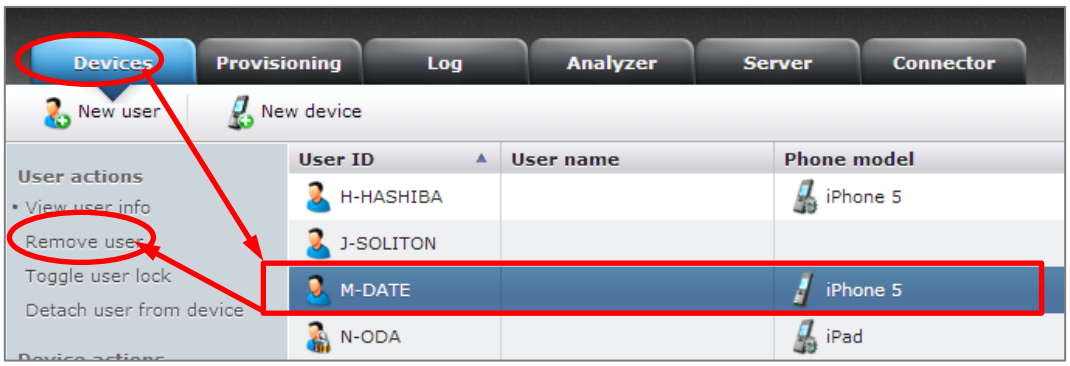


図 3.3.1 Devices タブ

3. 図 3.3.2 が表示されます。<Yes>をクリックしてください。

図 3.3.2 Remove user

4. Devices タブのデバイス一覧より、該当ユーザー情報のみが削除されたことを確認してください。

3.3.2 デバイスの削除手順

デバイスを削除するためには、以下の手順を実施してください。

1. [Devices]タブ-(削除するデバイス)-[Remove device]をクリックしてください。

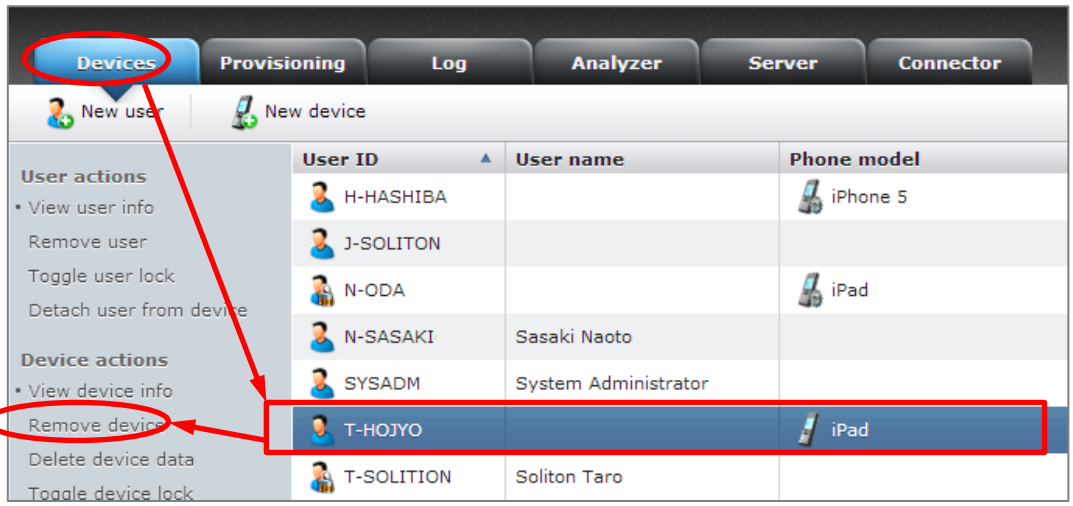


図 3.3.3 Devices タブ

2. 図 3.3.4 が表示されます。<Yes>をクリックしてください。

図 3.3.4 Remove device

3. Devices タブのデバイス一覧より、デバイス情報のみが削除されたことを確認してください。

3.4 同期に関するポリシー

Workspace Mobility では、多くの設定項目により様々なポリシーが作成できます。本項では、主にコラボレーションシステムとの同期に関するポリシー変更手順について記載します。
なお、本項では、すべて「Default settings」のポリシーを変更する場合として記載しています。グループの設定を変更する際は「2.4.3 グループ単位のポリシー設定」を参照し、グループ項目から変更してください。

3.4.1 通知を実行する時間帯の設定

コラボレーションシステムをスキャンした結果、例えば新着メールなどの変更があった場合や Workspace Mobility の設定でデバイスに影響のある変更があった場合、デバイスへ通知を行います。通知を行う時間帯を設定・変更したい場合は、以下の手順を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Server]タブ-[Notifications]-[Schedule]をクリックしてください。

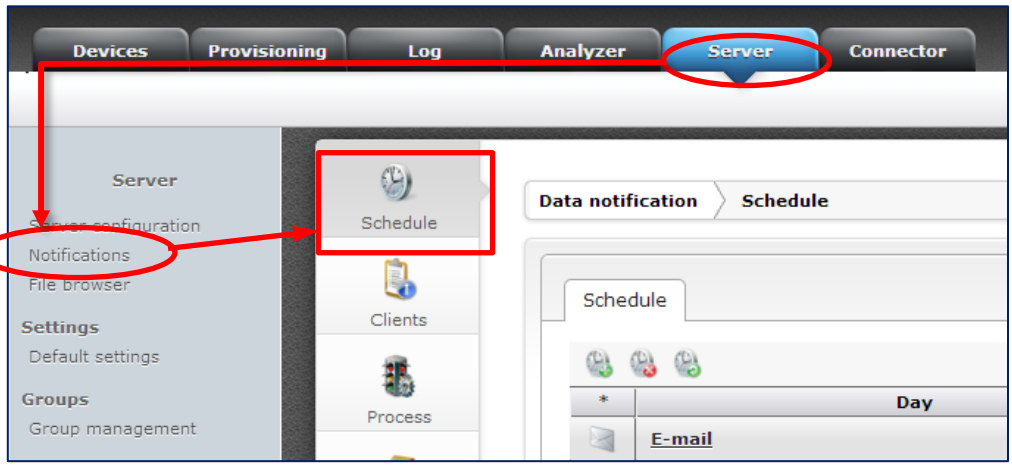


図 3.4.1 Schedule 設定画面

3. 図 3.4.2 が表示されます。変更する場合は既存のスケジュールをクリックしてください。新規の場合は、<New schedule>アイコンをクリックしてください。

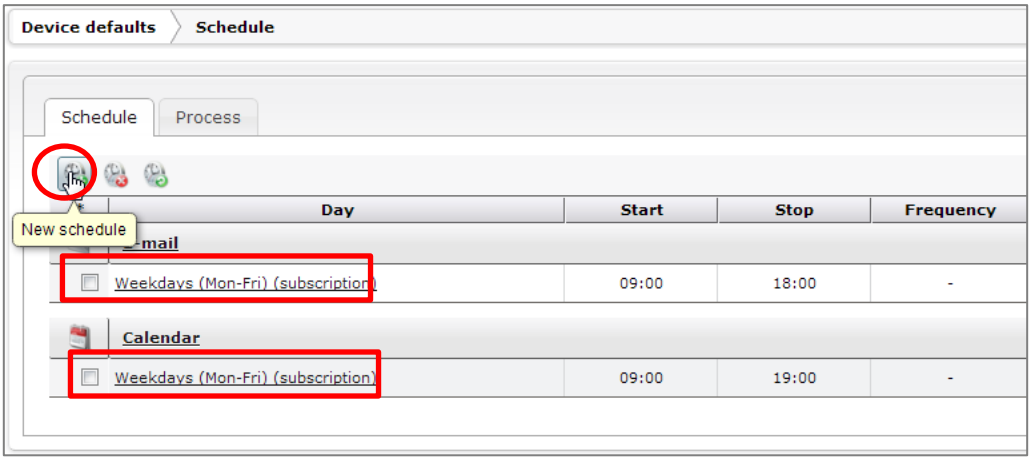


図 3.4.2 Schedule

4. 新規作成の場合は、図 3.4.3 が表示されます。通知する曜日、および通知時間を選択します。

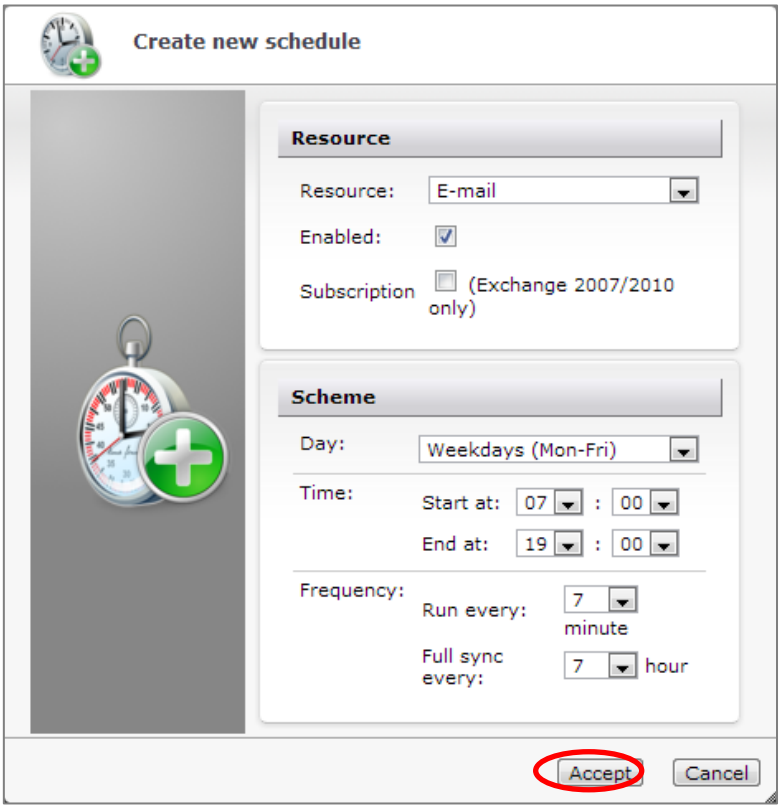


図 3.4.3 Create new schedule

Resource

- Resource…… スキャンスケジュールを設定するリソースを選択します。
- Enabled …… 作成するスキャンスケジュールの有効 / 無効を設定します。
- Subscription …… ※サポート対象外となります。有効にしないでください。

Scheme

- Day ……スキャンを実行する曜日を選択します。
- Time……スキャンを実行する時刻を指定します。
- Frequency
  - ➢ Run every 特定のリソースに変更が無いか確認する「高速スキャン」の実施頻度です。
  - ➢ Full sync every ユーザーが指定した期間全体のスキャンを実施します。カレンダーまたは ToDo にのみ適用されます。

5. <Accept>をクリックしてください。スケジュールが追加・変更されます。

3.4.2　同期に応答しないデバイスへの最大通知数

同期に応答しないデバイス（例えば休暇中のユーザーの端末など）に、サーバが通知を送信する回数を指定できます。指定した回数の通知を送信した後は、サーバが当該デバイスへの通知の送信を停止します。

注意

通知回数が上限に達した場合は、端末側で手動同期を実行するまで通知が表示されません。

通知回数はデバイスがサーバにアクセスするたびにリセットされます。そのため、最大通知数を超えて通知がされなくなったデバイスは、Workspace Mobility にログインするなどしてサーバに接続すると通知されるようになります。

1. [Server]タブ-[Default Settings]-[Settings]パネルを選択し、［Preference］-［Adaptive Push］をクリックします。

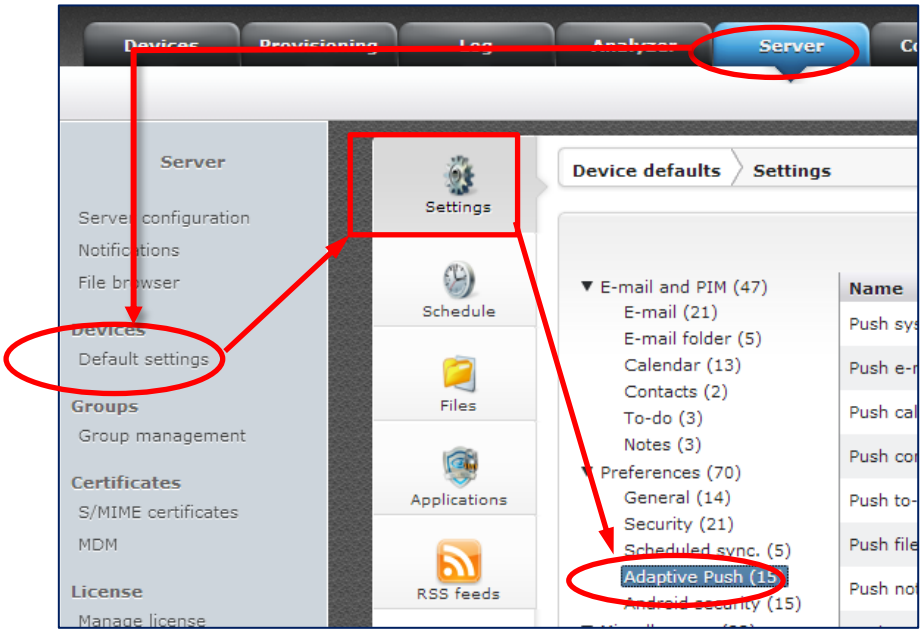


図 3.4.4 Adaptive push 設定画面

2. [Max. notifications if no response from a device] で変更できます。デフォルトは 5 回です。

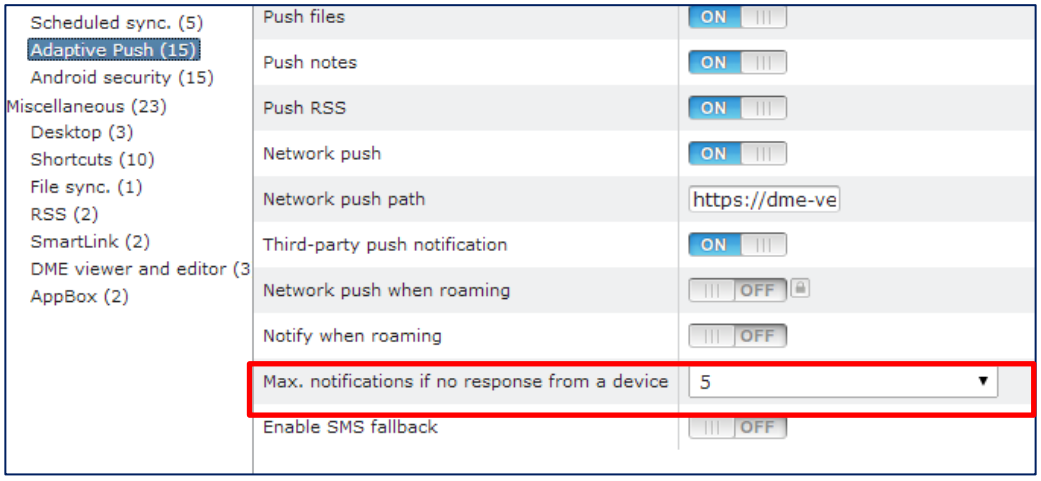


図 3.4.5 Adaptive push 設定画面

3.4.3　同期する日数の設定

クライアントアプリで何日前までのメールを同期し、クライアントアプリ上で閲覧可能とするかのこと指定することができます。同期日数（範囲）を変更するには、以下の設定を行ってください。

注意

Workspace Mobility に同期するメールは 1,000 件以下になるよう調整してください。デバイススペックにも依存しますが、1,000 件を超えると同期に時間がかかり、またクライアントアプリが不安定になることがあります。受信するメールが多い場合は、同期日数の値を小さくすることを推奨します。

1. [Server]タブ-[Default settings]をクリックしてください。

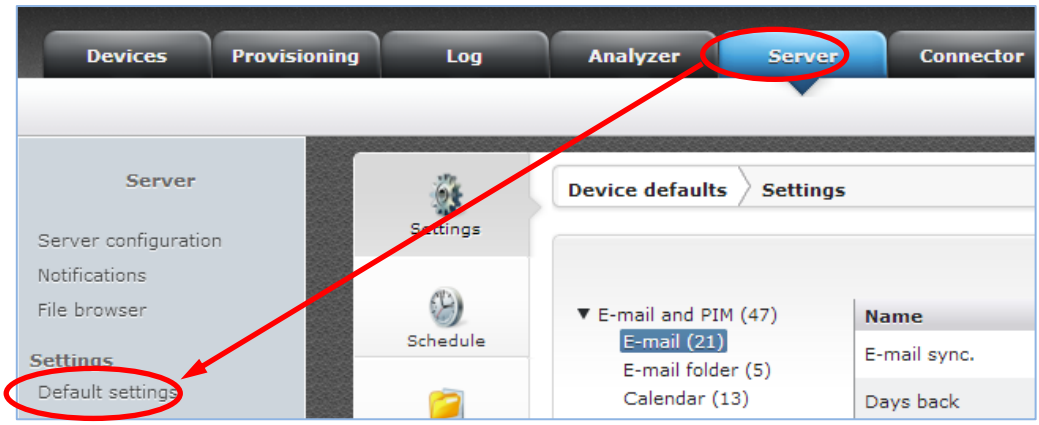
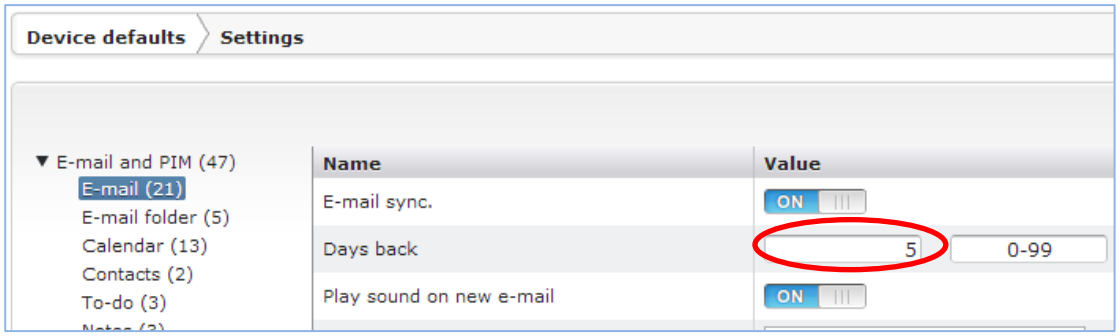


図 3.4.6 Default settings

2. メールの同期日数を変更する場合は、[E-mail]にて「Days back」を変更してください。
デフォルトでは過去 5 日間のメールが同期され閲覧できるようになっています。



3. メールフォルダの同期日数を変更する場合は、[E-mail folder]にて、「Days back in folder (default value)」を変更してください。

4. カレンダーの同期日数を変更する場合は、[Calendar]にて、「Days back」「Days forward」を変更してください。
「Days forward」は何日先までのカレンダーを同期するかの設定です。

5. To-do の同期日数を変更する場合は、[To-do]にて、「Days back」「Days forward」を変更してください。

3.4.4　メール署名の設定・変更

クライアントアプリからメール送信する際の署名を設定・変更する場合は、以下の手順を実施してください。

1.　[Server]タブ-[Default settings]をクリックしてください。

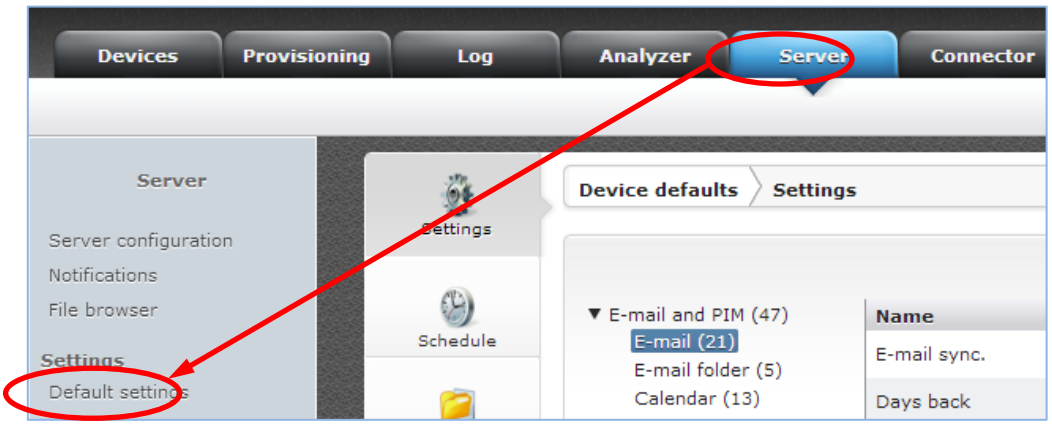


図 3.4.7 Default settings

2.　[E-mail]にて、「E-mail signature」を変更し、<Save>をクリックしてください。

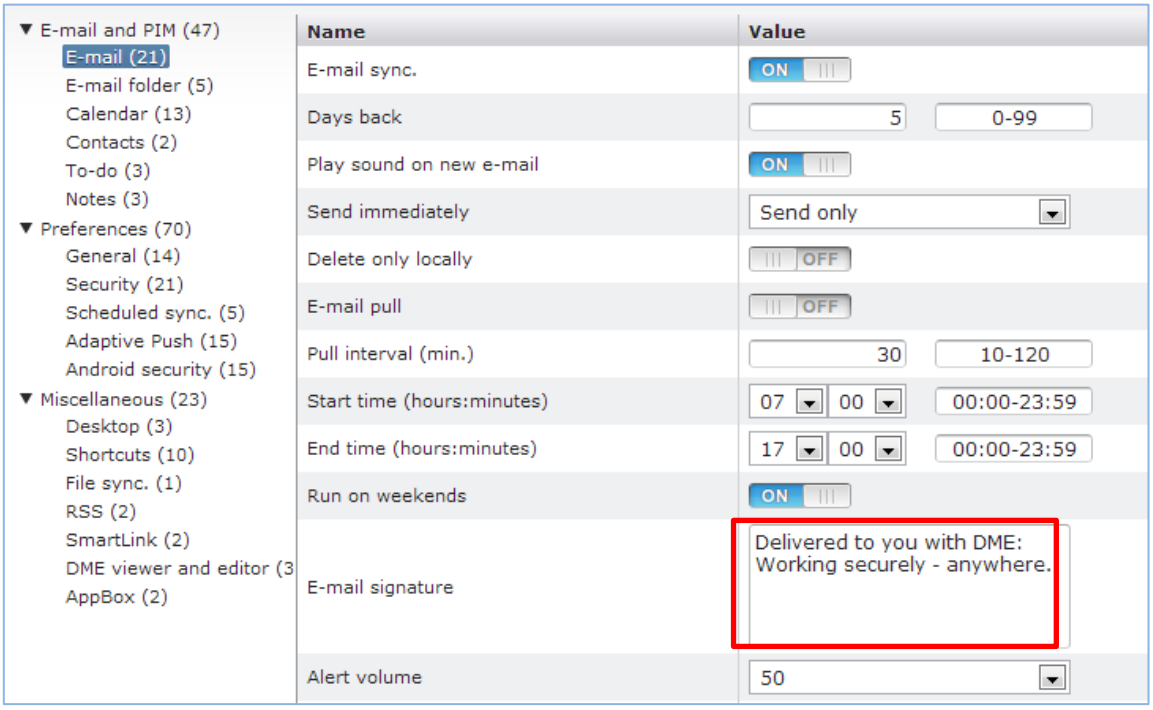


図 3.4.8 E-mail

3.5 パスワードに関するポリシー

3.5.1 クライアントアプリのログインのパスワード試行回数上限時ワイプ

Android、iOS デバイスにて、Workspace Mobility ログインのパスワード試行回数の上限値を超過した場合、ローカルワイプを実施することができます。（※セキュア・コンテナ領域を消去します。デバイスを初期化するものではありません。）

1. [Server]タブ-[Default settings]-[Settings]-[Security]をクリックしてください。

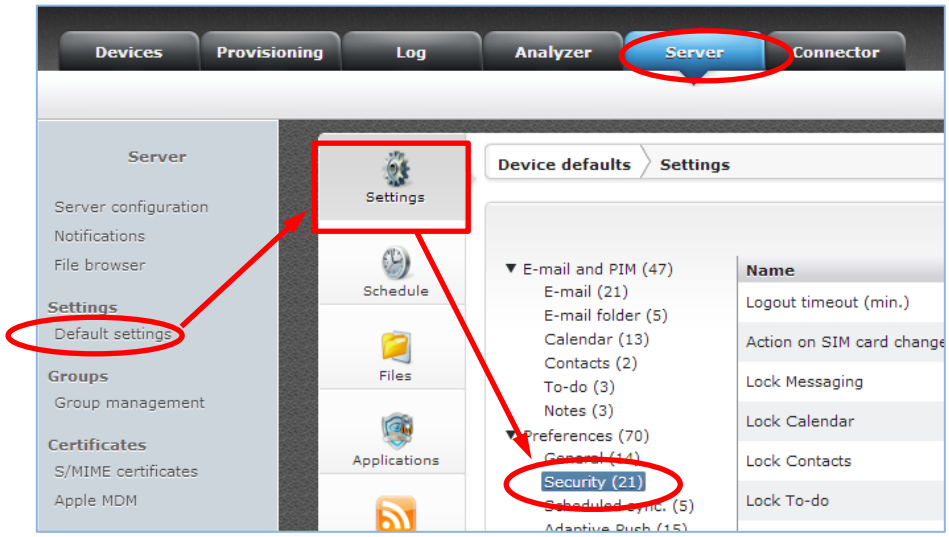


図 3.5.1 Settings 画面

2. 図 3.5.2 が表示されます。「Limit on password attempts (0 = no limit)」の値にパスワード試行回数の上限値を入力してください。「0」の場合は、上限値の設定はなしとなります。<Save>をクリックし、設定を保存してください。

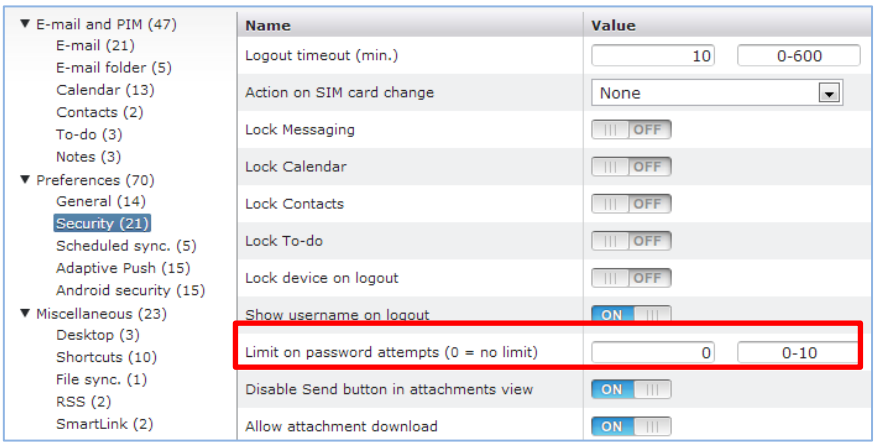


図 3.5.2 Security

注意

OS･デバイス種別によるワイプ範囲を確認し、事前評価の上、設定を実施してください。特に Android にて、セキュア･コンテナ領域のワイプを実行するためには、[Corporate Device]が OFF になっている必要があります。ON の場合、デバイス端末全体をワイプ（消去）することになります。（サポート対象外）

3.6 盗難・紛失時の対応

Workspace Mobility では、デバイスの盗難・紛失時にデバイスまたはユーザーをロック、もしくはセキュア・コンテナ領域のみをワイプするなど、使用方法に応じて柔軟な対応ができます。

3.6.1 デバイスロック（停止）

デバイスをロックするためには、以下の手順を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Devices]タブ-(ロック対象のデバイス)-[Toggle device blocking]をクリックしてください。

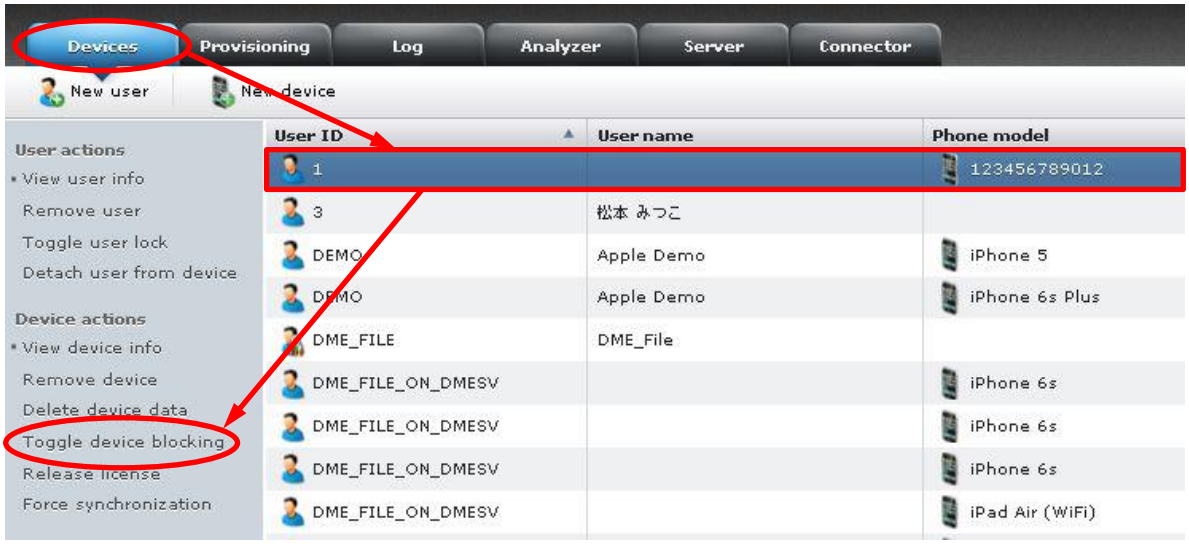


図 3.6.1 Devices タブ

3. 図 3.6.2 が表示されます。<Yes>をクリックしてください。

図 3.6.2 Toggle device blocking

4. デバイスのアイコンに鍵のマークがつきます。

図 3.6.3 Devices タブ

3.6.2 デバイスロック解除

デバイスをロックした場合、ユーザーは Workspace Mobility のコンテンツにアクセスできなくなり、正しいパスワードを入れてもログインできなくなります。

デバイスのロックを解除するためには、以下の手順を実施してください。

1. [Devices]タブ-(ロック解除対象のデバイス)-[Toggle device blocking]をクリックしてください。

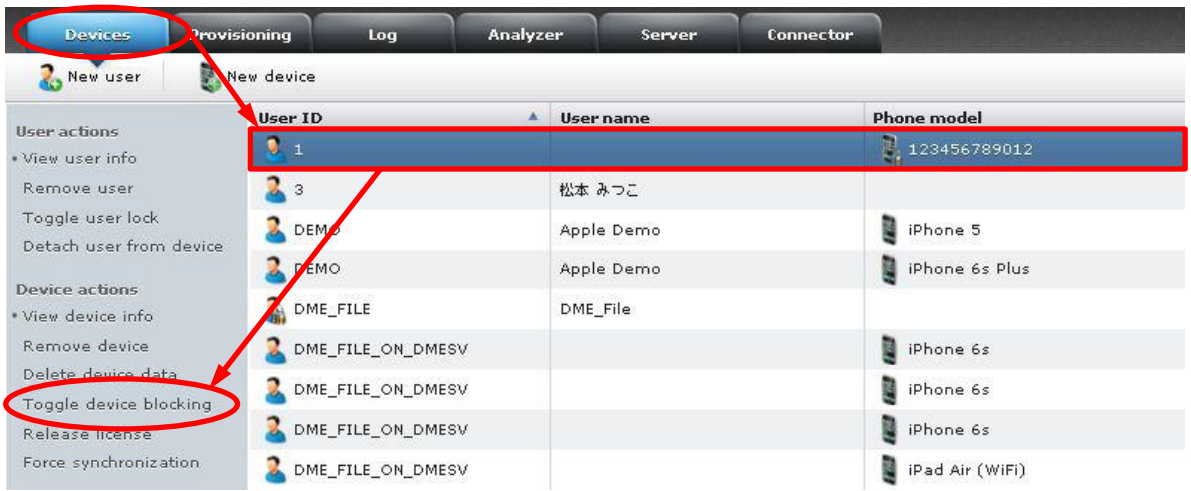


図 3.6.4 Devices タブ

2. 確認メッセージが現れます。<Yes>をクリックしてください。

図 3.6.5 Toggle device blocking

3. デバイスのアイコンから鍵のマークが消えている事を確認してください。

図 3.6.6 Devices タブ

3.6.3 リモートワイプ（Android）

セキュア・コンテナ領域のワイプ（消去）

Android にて、セキュア・コンテナ領域のワイプを実行するためには、[Corporate Device]が OFF になっている必要があります。セキュア・コンテナ領域をワイプするためには、以下の手順を実施してください。

注意

セキュア・コンテナ領域のワイプを実行するためには、[Corporate Device]が[OFF]になっている必要があります。[Corporate Device]が[ON]になっていると、デバイス端末全体を初期化することになるのでご注意ください。（デバイス全体の初期化についてはサポート対象外となります）

1. [Devices]タブ-(対象のデバイス)-[Delete device data]をクリックしてください。

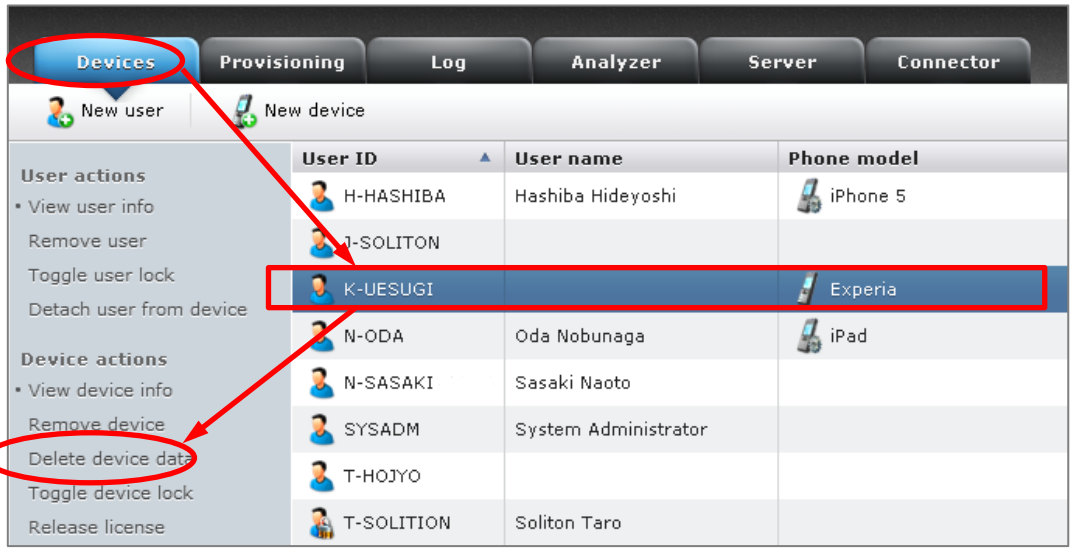


図 3.6.7 Devices タブ

2. 図 3.6.8 が表示されます。「Destroy all device data」を選択して<Send>をクリックしてください。

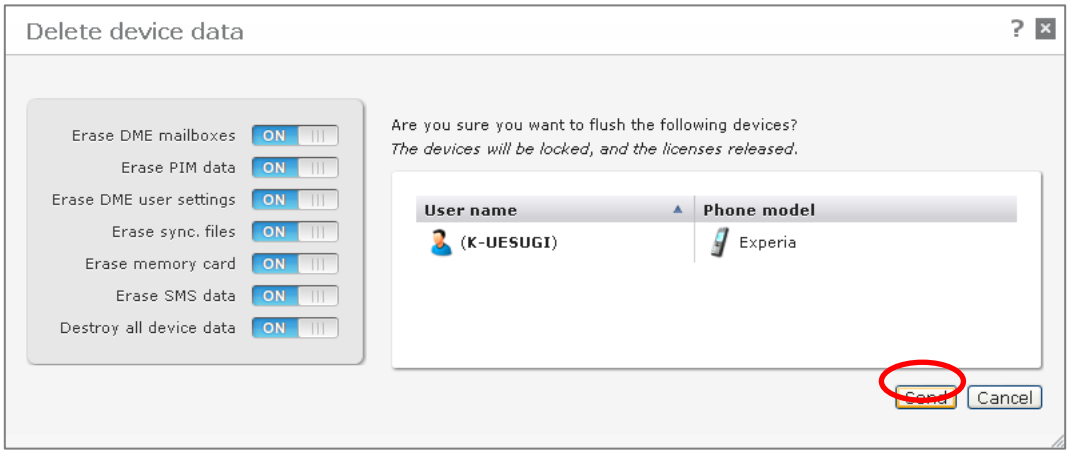


図 3.6.8 Delete device data

3. Android デバイスの Workspace Mobility 内のデータ領域が削除され、ユーザーは強制的に Workspace Mobility からログアウトします。デバイスロックもかかるため、正しいユーザーID、パスワードでログインしてもクライアントアプリからログインする事はできません。

3.6.4 リモートワイプ（iOS）

セキュア・コンテナ領域のワイプ（消去）

iOS にてセキュア・コンテナ領域のみをワイプするためには、以下の手順を実施してください。

1. [Devices]タブ-(対象のデバイス)-[Delete device data]をクリックしてください。

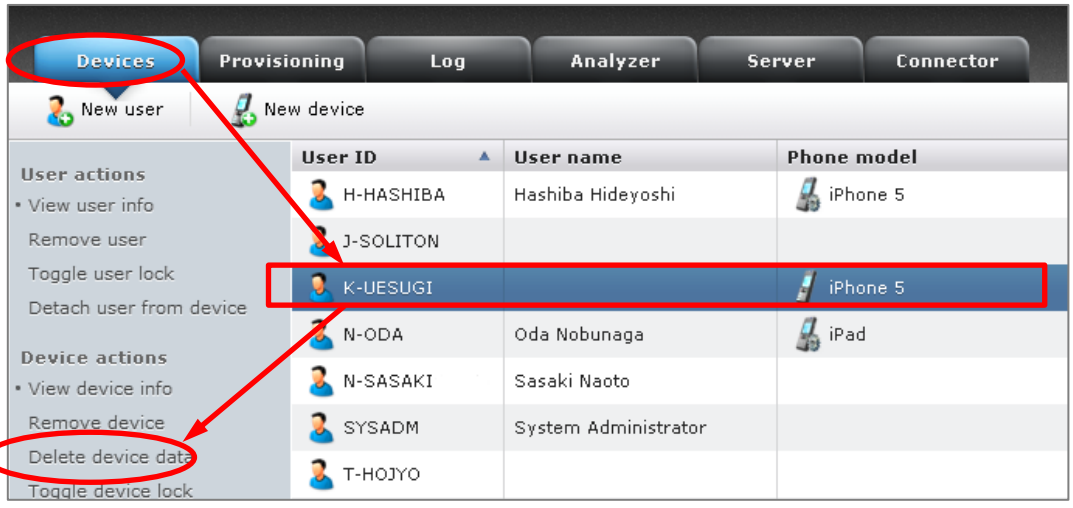


図 3.6.9 Devices タブ

2. 図 3.6.10 が表示されます。「Destroy all device data」を選択して<Send>をクリックしてください。

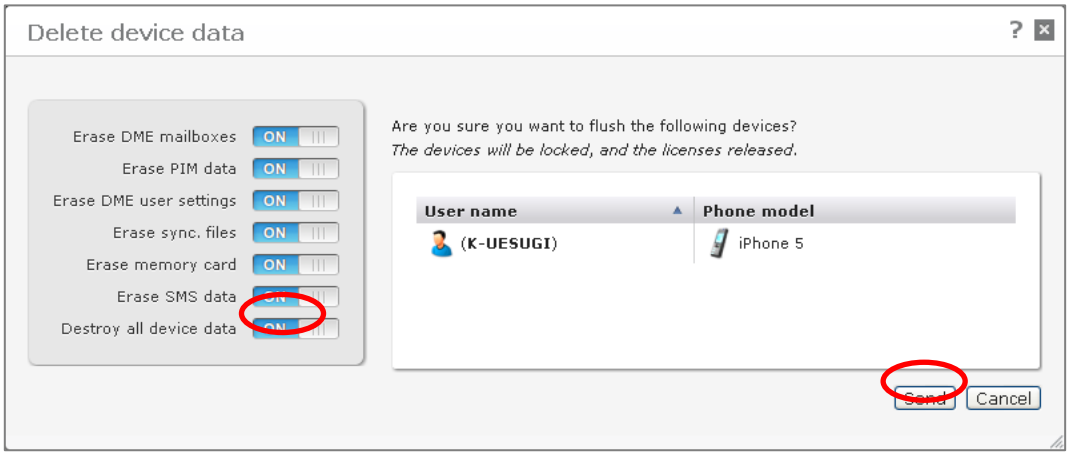


図 3.6.10 Delete device data

3. iOS デバイスのクライアントアプリデータ領域が削除され、ユーザーは強制的に Workspace Mobility からログアウトします。デバイスロックもかかるため、正しいユーザーID、パスワードを入力してもクライアントアプリからログインする事はできません。

3.6.5 利用ユーザー自身によるセルフワイプ（ユーザー作業）

Workspace Mobility では、利用ユーザー自身が Workspace Mobility サーバにアクセスして、自身のデバイスをワイプする事ができます。ユーザー自身がワイプする場合は、セキュア・コンテナ領域のワイプになります。ユーザー自身がワイプを実施するためには、以下の手順を実施してください。

1. https://[Workspace Mobility サーバの FQDN]:[ポート]/ にアクセスし、自身のユーザーID、パスワードを入れて<Login>をクリックしてください。ポートにはデフォルトで 5011 が使用されます。

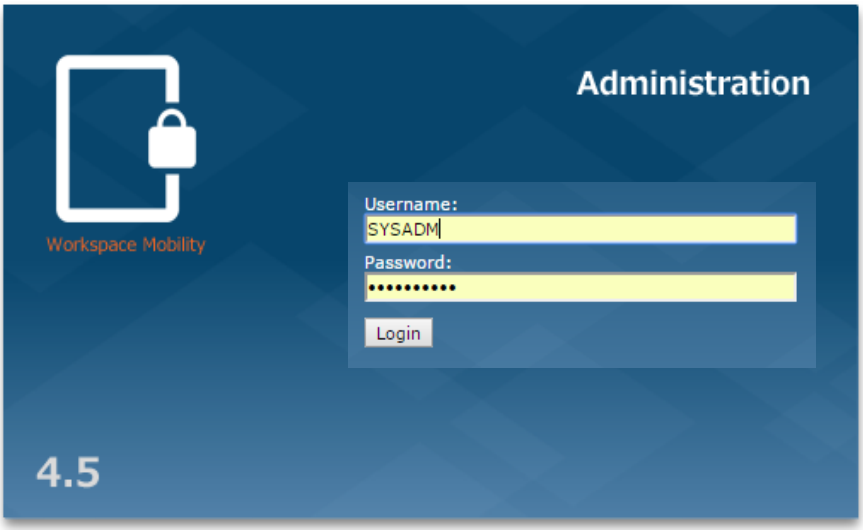


図 3.6.11 ログイン画面

2. 図 3.6.12 が表示されます。消去するデバイスを選択して<Delete device data>をクリックしてください。

図 3.6.12 My Workspace Mobility トップ画面

3. 図 3.6.13 が表示されます。「Destroy all device data」を ON にして<Send>をクリックしてください。

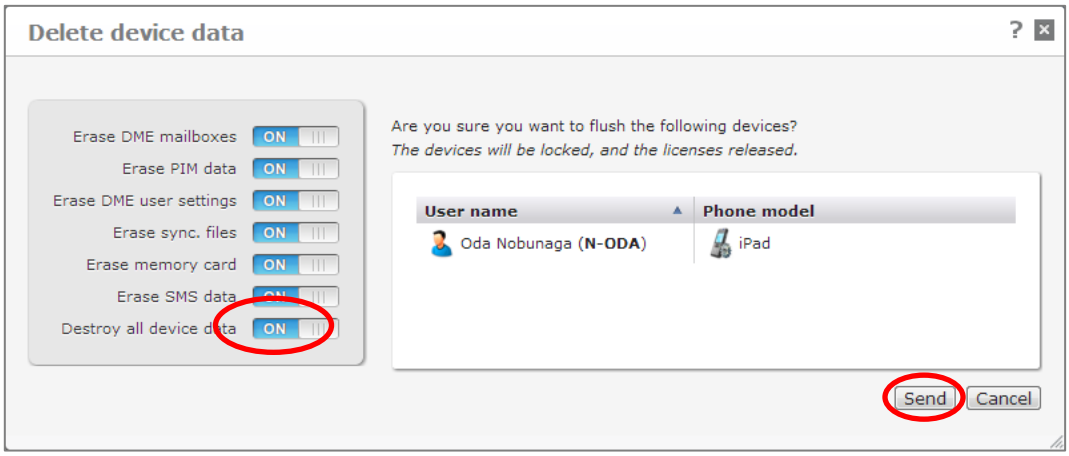


図 3.6.13 Delete device data

4. iOS デバイスのクライアントアプリデータ領域が削除され、ユーザーは強制的に Workspace Mobility からログアウトします。デバイスロックもかかるため、正しいユーザーID、パスワードでログインしてもクライアントプリからログインする事はできません。

3.6.6 デバイスのワイプ後の対応

ワイプを実行すると、デバイスは強制的にロックされ、ワイプが実行されます。デバイスが盗難・紛失から発見されたなど、再度そのデバイスを使用する場合は、デバイスロックの解除を行う必要があります。

ロックの解除方法は、「3.6.2 項 デバイスロック解除」を参照してください。

3.7 ログ確認

3.7.1　Workspace Mobility 管理コンソールのログ表示

管理コンソールには、Workspace Mobility サーバでのログを表示する事ができます。ログを表示する場合は以下の手順を実施してください。

1. 管理コンソールに、システム管理者でログインしてください。
2. [Log]タブをクリックしてください。

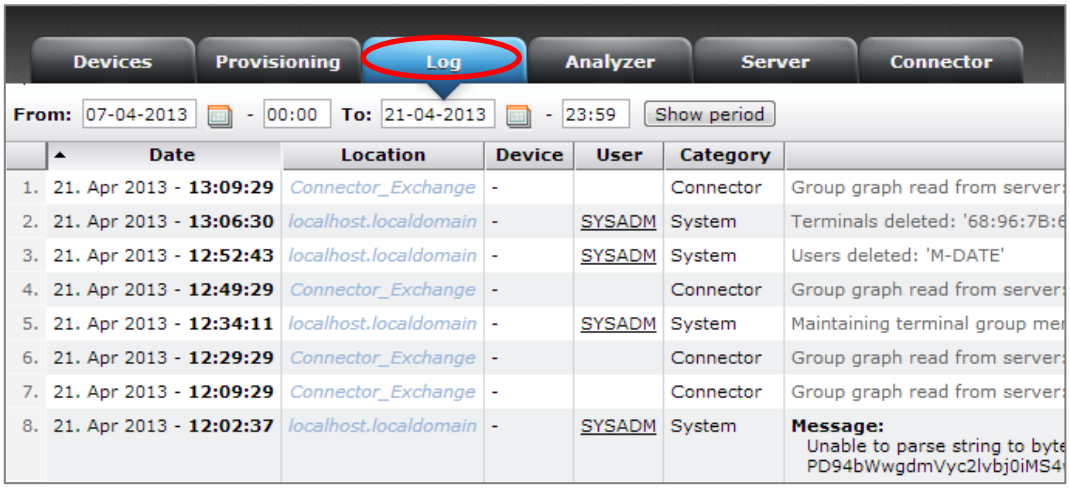


図 3.7.1　Log タブ

3. 右上にログのページ番号と、1 ページに表示させるログの数が表示されていますので、表示の調整をおこなってください。

図 3.7.2　ログの表示

3.8 Monitor の表示

Monitor では Workspace Mobility Server のプロパティおよび Workspace Mobility サーバが依存する様々なサービスを表示できます。

さらに、サーバと Connector のパフォーマンスに関する統計とトレンドを確認できます。

Monitor を確認する際は、 [Server]タブ-[Server configuration] -[Monitor]をクリックしてください。

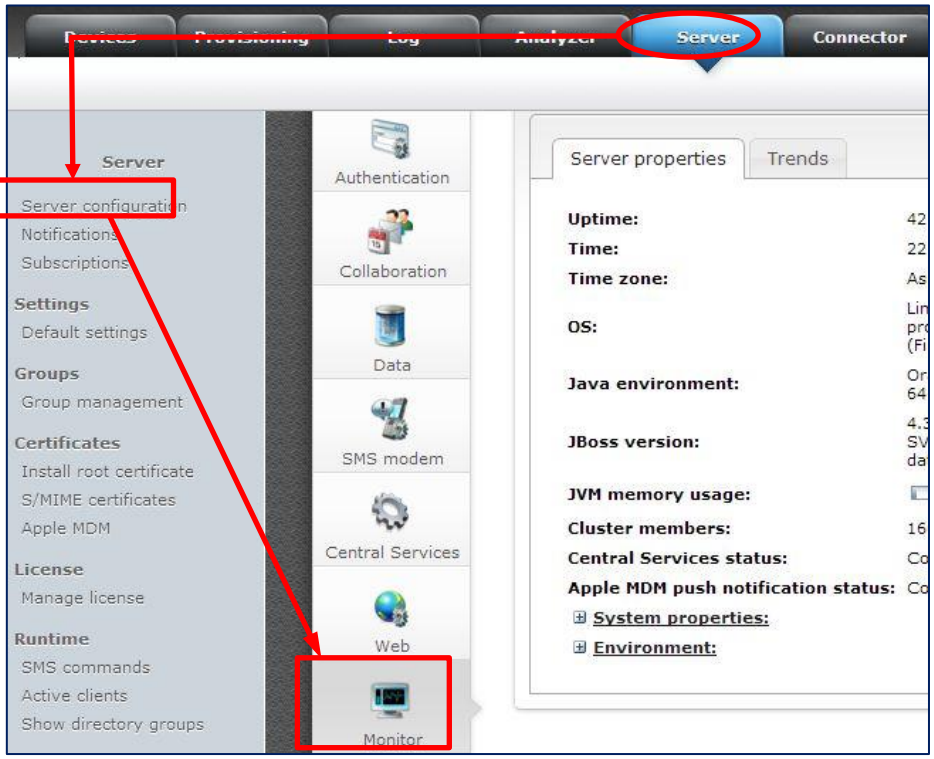
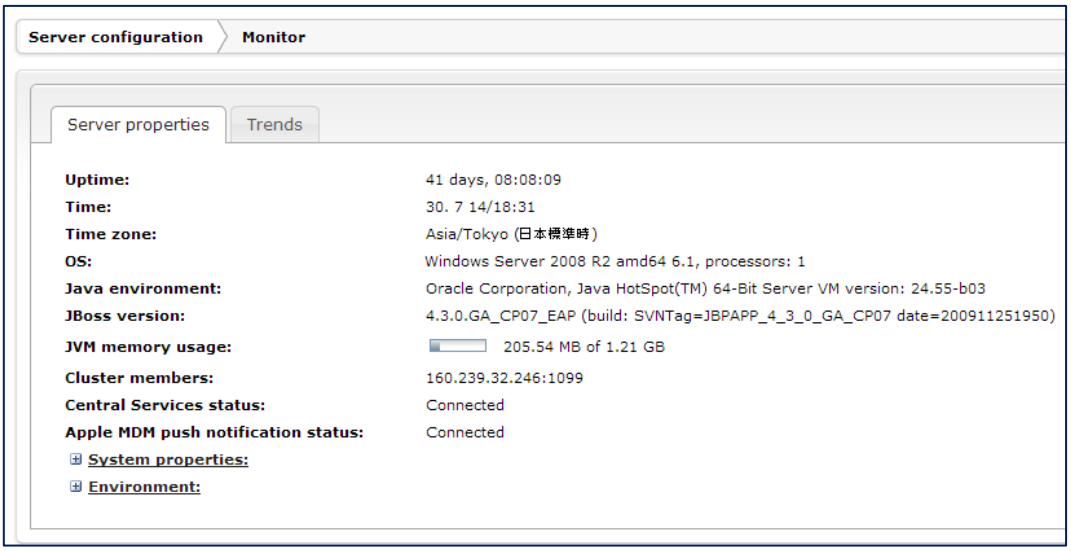


図 3.8.3 Monitor

3.8.1　Monitor で確認できる情報



- [Uptime]

  Workspace Mobility サーバが実行されている時間です。日数プラス時間、分、秒が表示されます。

- [Time]

  現在のサーバ時刻です。

- [Time zone（タイムゾーン）]

  サーバの現在のタイムゾーンです。

- [OS]

  Workspace Mobility がインストールされているオペレーティングシステムの完全な名前です。

- [Java environment]

  サーバにインストールされている Java のバージョンです。

- [JBoss version]

  Red Hat の Java アプリケーションサーバ JBoss のバージョンです。ただし、Workspace Mobility 3.5 以降では JBoss の Enterprise Edition が使用されます。以前のバージョンでは Community Edition が使用されていました。

- [JVM memory usage]

  JVM（Java Virtual Machine：Java 仮想マシン）のメモリ使用状況です。

例えば、1.15 GB of 1.22 GB と表示される場合は、次のように解釈できます。JVM の Java オブジェクトが使用可能なメモリの最大サイズが 1.22GB です。JVM 自体もメモリを消費しますが、これは含まれません。1.22GB のうち、実際に JBoss と Workspace Mobility が使用しているのは 1.15GB です。パフォーマンス上の理由で、JVM は必要になるまで、（使用しなくなった Java オブジェクトなどから）メモリを解放しません。したがって、実際よりも高いメモリ使用率が表示されることがよくあります。

[Cluster members]

このフィールドに、Workspace Mobility クラスタのオンラインのアクティブなメンバーの IP アドレスが表示されます。最初に表示されるサーバがクラスタのプライマリサーバ（マスターノード）です。マスターノードがダウンした場合は、リストの 2 番目のサーバが処理を引き継ぎ、マスターノードになります。元のマスターノードがオンラインに復帰した場合でもこれは変わりません。

Workspace Mobility に複数サーバが設定されていない場合は、このフィールドに現在のサーバのみが表示されます。

[Central Services status]

Workspace Mobility Server が Workspace Mobility セントラルサービスに接続するように設定されている場合は、このフィールドに接続が成功したかどうかが表示されます（[Connected]）。特に、これは Apple プッシュ通知サービスに影響します。

[Apple MDM push notification status] ※未サポート

Apple MDM APNS 証明書がサーバにインストールされている場合は、このフィールドに[Connected]と表示されます。その場合は、iOS デバイスのエンロールメントと設定を行うことができます。

[System properties]

クリックしてこのフィールドを展開できます。ここには、サーバにインストールされている Java システムについての情報（Java がレポートしたもの）が表示されます。

[Environment]

クリックしてこのフィールドを展開できます。ここには、Java がレポートしたサーバ環境についての情報が表示されます。

4. サポート

この章では、本サービスのサポートについて記載します。

4.1 クライアント障害対応

クライアントにて障害と思われる事象が発生した場合は、以下の手順を実施ください。

本ページの手順にて解決しない場合は、弊社サポートまでご連絡ください。

4.1.1 Workspace Mobility へログインできない、または同期に失敗する

クライアントアプリからログインできない場合、もしくはログインできても同期に失敗する場合、以下の可能性があります。

- 入力したユーザー名、パスワード、接続先サーバのパスのいずれかの値が間違っている
- 管理コンソール上でユーザー、もしくはデバイスにロックがかかっている
- AD/LDAP の DME_User グループにユーザーがメンバーとして追加されていない
- AD/LDAP との連携に失敗している
- Exchange との連携に失敗している
- DME のライセンスが不足している
- 回線が不安定など、通信に問題がある

※ 複数台同時にログインできない場合は、DME サーバや Connector サーバ側に問題がある可能性があります。その際は 4.2 サーバ障害対応をご確認ください。

4.2 サーバ障害対応

サーバにて障害と思われる事象が発生した場合は、以下の手順を実施ください。

4.2.1　サーバ障害の確認

管理コンソールに接続してみる

管理用 PC のブラウザを起動し、ご使用中の Workspace Mobility サーバの管理コンソールが表示されるか確認します。

Workspace Mobility 管理コンソールにてエラーが発生した場合、原因はさまざまなものが考えられますが、セッションが切れてしまっている事によって起こる事が多くあります。そのため、一度 Web ブラウザを閉じてから再度 Workspace Mobility 管理コンソールにログインできるかをお試しください。

アクセスできない場合、可能であれば別回線のネットワーク（スマートデバイスなどの回線等）から再度 Workspace Mobility 管理コンソールへアクセスしてみてください。

なお、ログイン画面は表示されるが、正しいユーザー名、正しいパスワードを指定してもログインできない場合、DB が使用できない状況の場合があります。

アクセスできない場合は弊社サポートまでご連絡ください。ログインできた場合は以下の手順にへ進んでください。

管理コンソールにて Connector サーバの接続確認を行う

管理コンソールにログインし、[Connector]タブを選択します。Connector サーバの[Enabled]欄が緑のチェックになっているか確認してください。

以下の状態の場合、Workspace Mobility のシステム障害の可能性がございます。

恐れ入りますが弊社サポートまでご連絡ください。

- [Enabled]がグレー　　：Connector サーバが停止しているため使用できない状態。
- [Enabled]が赤丸に×　：Connector サーバがアクセス可能だったが、現状何らかの理由で使用できない。

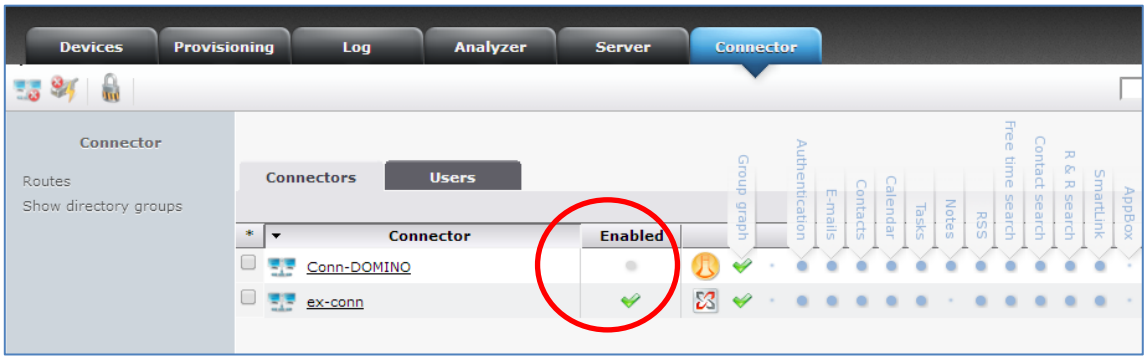


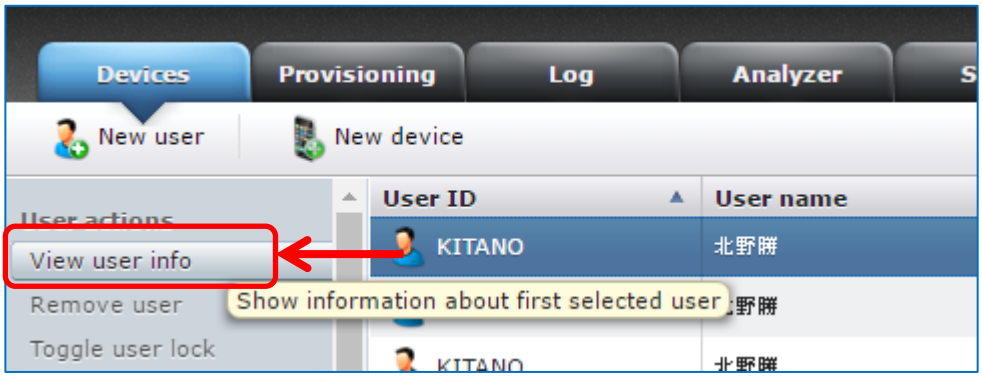
図 4.2.1 Connector サーバ管理画面

- [Enabled]が緑のチェックの場合、次ページの確認を実施してください。

AD/LDAP ユーザー情報の取得が行えるか確認を行う

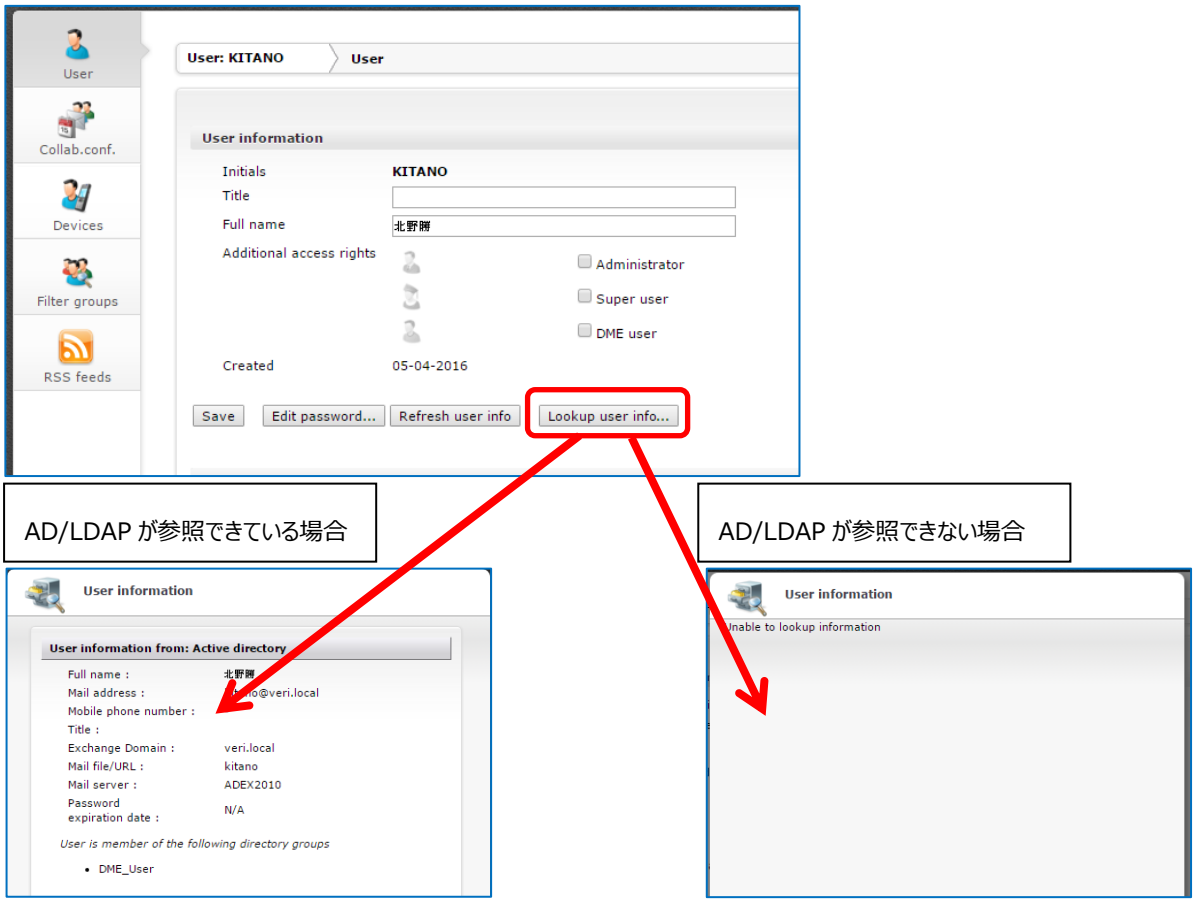
AD/LDAP と通信が可能な状態かどうかを確認する為、ユーザー情報の取得を行ってみます。

Web 管理画面にログインし、[Devices]タブを選択します。利用中のユーザーを選択し、画面左の[View user info]を選択します。



ユーザーインフォメーション画面で＜Lookup user info＞をクリックしてみます。

AD/LDAP が参照可能であればユーザーの情報が表示されますが、参照できない場合は何の情報も表示されません。



AD/LDAP が参照できない場合は弊社サポートまでご連絡ください。

改定履歴

日付	内容
2016/9/8	初版作成
2016/12/15	1.1 版作成（端末事前登録手順を修正）

Workspace Mobility

Workspace Mobility システム管理者ガイド

Ver.1.1　2016 年 12 月版

※Workspace Mobility　免責事項

・故意や正常な操作に関わらず、管理コンソールをご利用いただいたことにより生じる直接的また間接的な損失に対して当社および関連会社には一切責任を負うものはありません。

・・各種マニュアル（ユーザーマニュアル、管理コンソールマニュアル）に記載されている内容以外はサポート対象外となります。故意や正常な操作に関わらず各種マニュアルに掲載されていない設定操作を実施することによる不具合について、当社および関連会社にはデータ復旧や再設定のための作業等一切責任を負うものはありません。

・故意や正常な操作に関わらず、デバイスロックおよびリモートワイプを実行した結果、端末不具合および端末データが消えても当社および関連会社にはデータ復旧や再設定のための作業等一切責任を負うものはありません。

・本サービスの設定により、各端末との通信が増える事が想定されます。キャリアモデルの場合はパケット定額プランを推奨します。また設定により、定額プランの上限値を超えないか等の確認はお客様にて行ってください。

・当社は理由の如何に関わらず、情報の内容および変更により生じるお客様の直接的または関節的な損失に関しても、一切責任を負うものではありません