Enterprise Vault.cloud™ アーカイブ管理ヘルプ

VERITAS™

Enterprise Vault.cloud: Archive Administration ヘルプ

最終更新日: 2018-07-19。

法的通知と登録商標

Veritas、Veritas のロゴ、および Enterprise Vault.cloud は、Veritas Technologies LLC またはその関連会社の米国およびその他の国における商標または登録商標です。その他の名称はそれぞれの所有者の登録商標です。

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

目次

1

Archive Administration スタートガイド

この章では以下の項目について説明しています。

Enterprise Vault.cloud Archive Administration について

Veritas Enterprise Vault.cloud™ はクラウドベースのアーカイブサービスで、所属する組織で電子メールメッセージやその他のビジネスの重要な情報を保管、管理、検出することを可能にします。組織でサービスを有効化すると、組織内で送受信されたすべてのメッセージのコピーを Enterprise Vault.cloud にジャーナリングできるようになります。

Archive Administration は、Web でホストされるインターフェースで、管理者がこれを使用すると Enterprise Vault.cloud の設定および管理を行えます。

Archive Administration で、管理者は次のタスクを実行できます。

- Enterprise Vault.cloud アーカイブアカウントのプロビジョニングと管理。
- コンテンツソースのアーカイブの設定と管理。
- ユーザーの役割の割り当てと管理。
- アーカイブオプションとポリシーの管理。

- 保持ポリシーとタグの管理。
- 有効化された分類ポリシーを満たす電子メールに対する分類の設定。
- Email Continuity オプションの管理。
- 使用状況レポートの生成。

Archive Administration の最新の更新

Archive Administration の最新の更新には、次の機能強化が含まれています。

- Veritas Information Classifier との統合
  Enterprise Vault.cloud に格納された電子メールを分類するために、Enterprise Vault.cloud が Veritas Information Classifier と統合されました。Veritas Information Classifier は、電子メールを分類するための基準となる多くの規制や企業の規格に対応した、一連の分類ポリシーを提供します。各ポリシーは、電子メールに関連する 1 つ以上の分類タグを割り当てるために満たす必要がある条件を指定します。新しい［classification administrator］の役割を持つ管理者は、Administration Console から Veritas Information Classifier に直接アクセスして、必要な分類ポリシーを有効化できます。分類処理によって、有効化されたポリシーに一致する Enterprise Vault.cloud の受信電子メールにタグを付けます。Discovery.cloud ユーザーは、eDiscovery の一環として、分類タグが付けられた電子メールを検索できます。
  p.80 の「分類について」を参照してください。
- 請求用使用状況の通知
  使用のコミットが一定の割合を超過したときに、選択した個人に通知電子メールを送信します。
- 電子メール添付ファイルサイズ上限の増加
  電子メールに最大 200 MB のファイルを添付できます。

Archive Administration の以前のリリースに含まれていた更新に関する情報は、このヘルプの別の場所で提供されます。

p.120 の「以前のリリースの更新について」を参照してください。

Enterprise Vault.cloud サービススイートの各リリースの更新すべてについて詳しくは、Enterprise Vault.cloud リリースノートを参照してください。Veritasサポート Web サイトに掲載されている次の記事から、リリースノートを取得できます。

http://www.veritas.com/docs/000100485

Archive Administration の前提条件

Archive Administration を使うには、次の前提条件が必要です。

- Archive Administration URL。
- Enterprise Vault.cloud ユーザー名。

- Enterprise Vault.cloud パスワード。
- Archive Administration を使用するためのアクセス権限。

メモ: この情報がないか、Archive Administration へのアクセス権限が必要な場合は、管理者に問い合わせてください。

Archive Administration の Web ブラウザのサポート

Archive Administration は、Enterprise Vault.cloud 互換性リストに記載されているブラウザをサポートします。Veritasサポート Web サイトに掲載されている次の記事から、互換性リストを取得できます。

http://www.veritas.com/docs/000016792

Archive Administration へのログイン

Archive Administration にアクセスする前に、Enterprise Vault.cloud クレデンシャルを使ってログインする必要があります。

Archive Administration にログインするには

1 サポート対象のブラウザで、Archive Administration URL に移動します。

メモ: Archive Administration URL がわからない場合、または Archive Administration へのアクセス権限が必要な場合は、管理者に問い合わせてください。

2 [Login]ページで、セキュリティオプションを選択します。

詳しくは次の表を参照してください。

This is a public or shared computer	[Login]ページにアクセスすると毎回 Archive Administration によってクレデンシャルを求めるメッセージが表示され、20 分間何も操作が行われないと自動的にログアウトされます。 このオプションは選択済みのデフォルトのオプションです。
This is a private computer	Archive Administration では、正常にログインした後 1 年間クレデンシャルをキャッシュに保存し、[Login]ページをバイパスできるようになります。 キャッシュからクレデンシャルを消去するには、Archive Administration からログアウトします。

3 Enterprise Vault.cloud のユーザー名とパスワードを入力します。

4 [Log In]をクリックします。

パスワードの変更

[Change Password]ページから、Archive Administration にアクセスするために使うパスワードを変更できます。組織がデフォルトのパスワードポリシーを使用している場合、新しいパスワードは少なくとも 6 文字以上である必要があります。さらに、次の文字の種類のうち 2 つをパスワードに含める必要があります。

- 0 から 9 までの数字
- 小文字
- 大文字
- 英数字以外の文字

組織が高度なパスワードポリシーを使用している場合、新しいパスワードは、そのポリシーの必要条件を満たす必要があります。

p.77 の「高度なパスワードポリシーの設定」を参照してください。

メモ: Archive Administration のパスワードを変更すると、他の Enterprise Vault.cloud 製品のパスワードも変更されます。

パスワードを変更するには

1 左側のナビゲーションウィンドウ枠で、[Change Password]をクリックします。

2 [Change Password]ページの[Old Password]フィールドに、現在のパスワードを入力します。

3 [New Password]フィールドに、新しいパスワードを入力します。

4 [Re-Type New Password]フィールドに、新しいパスワードを再入力します。

5 [Save]をクリックします。

2

アーカイブの概要

この章では以下の項目について説明しています。

アーカイブの概要について

[Archive Overview]ページは、Archive Administration にログインすると自動的に表示されます。このページには、Enterprise Vault.cloud の一般的な情報と使用状況の統計が表示されます。[Archive Overview]から利用可能な情報には、次のものが含まれます。

- 会社が購入したサービスと、現在請求されている使用状況。
- アカウントに割り当てられている委任された役割。
- 会社のアーカイブの使用状況のスナップショットを示す、一連の表とグラフ。アーカイブの使用状況スナップショットには、次の情報が含まれます。
  - 10 日間ローリングメールボリューム
  - 7 日間ローリング添付ファイルの概要
  - 上位 10 個の非プロビジョニングアカウント

完全なアーカイブ使用状況レポートの表示

[Archive Overview]から利用可能な情報の他に、Enterprise Vault.cloud の完全なアーカイブ使用状況レポートにアクセスできます。完全なアーカイブ使用状況レポートから利用可能な情報には、次のものが含まれます。

- 10 日間ローリングメールボリュームのレポート。
- 10 週間ローリングメールボリュームのレポート。

- 5 カ月間ローリングメールボリュームのレポート。
- 7 日間ローリング添付ファイルの概要。
- 7 日間ローリングユーザー別レポート。
- 合計 MTD メール使用状況アカウントのレポート。
- 7 日間ローリング非プロビジョニングアカウントのレポート。
- アクセス IP レポート。
- 週単位のユーザーアクティビティの概要レポート。
- 7 日間ユーザーアクティビティの詳細レポート。

メモ: 7 日間ローリングユーザー別アクティビティレポートの外部ユーザーは、組織内の受信者にメッセージを送信する組織外の送信者を表します。認識されないユーザーは、組織内で Admin または Unassigned のユーザー名を持つ受信者を表します。これらのユーザー名は、Enterprise Vault.cloud のデフォルトの管理者と、割り当てられていないレガシーアカウントを表します。

完全なアーカイブ使用状況レポートを表示するには

1. 左側のナビゲーションウィンドウ枠で、[Archive Overview]をクリックします。
2. [Archive Overview]ページで、[View Full Archive Usage Report]をクリックします。

3

My Config

この章では以下の項目について説明しています。

［My Config］ページについて

［My Config］ページで、管理者は、管理の設定とプロビジョニングプロセス設定します。ページには次のものが表示されます。

- 会社で利用可能な Enterprise Vault.cloud サービスのリスト。
- 設定の状態 (設定を完了するのに必要なすべての手順に関する情報を含む)。

メモ: 表示されている設定手順は、[User Management]ページで選択したアカウントプロビジョニングオプションを反映します。

サービスについて

[My Config]の[Services]ページでは、会社にプロビジョニングされている Enterprise Vault.cloud サービスに関する詳細情報を表示できます。[Services]ページの情報には、次のものが含まれます。

- アーカイブの設定
- アーカイブの統計情報
- 有効なサービス
- アクティブなドメイン
- アーカイブのジャーナリングアドレス

このページの情報は、読み取り専用です。この情報を変更する必要がある場合は、Veritas のサービスとサポートにお問い合わせください。

ユーザー管理オプションの選択

[My Config]の[User Management]ページでは、Enterprise Vault.cloud アーカイブアカウントのプロビジョニングや管理に使用するオプションを選択できます。Archive Administration から手動でプロビジョニングと管理を実行したり、リモートプロビジョニングを使用したりできます。リモートプロビジョニングでは、組織内の新しいユーザーごとに Archive Administration で新しいアーカイブアカウントを手動で作成する必要がありません。リモートプロビジョニングを設定した場合、リモートオプションが新しいユーザーを同期すると、新しいアーカイブアカウントが自動的に Archive Administration に表示されます。

リモートプロビジョニングのオプションは次のとおりです。

- CloudLink。このオプションでは、個別にインストール可能な ArchiveTools CloudLink ツールを使用して、Microsoft Active Directory と IBM Lotus Domino ディレクトリのアカウントのプロビジョニングを管理できます。
- Office 365 Sync。このオプションでは、Microsoft Office 365 アカウント用の自動プロビジョニングを提供します。

ユーザーアカウントは、Office 365 Sync か CloudLink のいずれかを使用して同期できます。2 つの異なるユーザーのグループを管理するために、両方のリモートプロビジョニングオプションを使用することもできます。2 つのリモートオプションから同期されるユー

ザーは独立したままになるため、1 つのグループに存在しているアーカイブアカウントは、それらが別のグループ内に存在しない場合も削除されません。

ユーザー管理オプションを選択するには

1. 左側のナビゲーションウィンドウ枠の［My Config］で、［User Management］をクリックします。
2. ［User Management］ページで、次のプロビジョニングオプションのいずれかを選択します。
   - Manage account provisioning using the console application
   - Manage account provisioning remotely
3. アカウントプロビジョニングをリモートから管理するオプションを選択した場合は、［Using on-premise CloudLink tool］または［Using Microsoft Office 365］を選択するか、その両方を選択します。
4. ［Save］をクリックします。
5. ［Go To Next Step］をクリックします。

   Archive Administration の［My Configuration］ページに戻り、選択したプロビジョニングオプションで必要な設定手順を実行するための説明が表示されます。

Office 365 Sync の設定

［User Management］ページで、Microsoft Office 365 を使用してアカウントプロビジョニングを管理するオプションを選択した場合は、Office 365 Sync を設定する必要があります。

Office 365 Sync を設定するには、最初にこのセクションで説明する Office 365 の設定手順を完了する必要があります。次に、［Provisioning］ページに移動して、プロビジョニングオプションを設定する必要があります。その後、［Office 365 Config］ページに戻って、Office 365 Sync のスケジューラを設定できます。

Office 365 Sync を設定するときに、Microsoft Office 365 アカウントのクレデンシャルを指定する必要があります。このアカウントで、Office 365 Sync は以下を実行できます。

- Office 365 の PowerShell コマンドを実行して Office 365 アカウントを同期する
- Office 365 Exchange Web サービスを実行して Personal.cloud Web フォルダを配備する

これらの機能の両方で同じアカウントを使用することをお勧めします。Microsoft Office 365 のグローバル管理者アカウントか、Office 365 の必要な権限を持つアカウントのクレデンシャルを指定できます。必要な権限を付与する Office 365 のカスタムの役割グループを作成する方法については、別途説明します。

p.19 の「Office 365 Sync アカウント用カスタムの役割グループの作成」を参照してください。

メモ: その他の作業で、Windows PowerShell へのログオンに使用するアカウントを指定しないようにします。指定した場合、Microsoft Office 365 の調整ポリシーで接続エラーが発生する可能性があります。

Office 365 Sync を設定するには

1 左側のナビゲーションウィンドウ枠で、[My Config]の[Office 365 Config]をクリックします。

メモ: [Office 365 Config]ページは、[User Management]ページでプロビジョニングオプションとして Microsoft Office 365 を選択した場合にのみ利用可能です。

2 [Configuration]で、Office 365 共有メールボックスを同期するかどうかを選択します。

デフォルトでは、[Synchronize Shared Mailboxes]チェックボックスのチェックマークははずされています。[Synchronize Shared Mailboxes]オプションに関して、次に注意してください。

- このオプションを選択すると、すべての Microsoft Office 365 ドメインに含まれる各共有メールボックスが同期のターゲットになります。共有メールボックスは、ユーザーのメールボックスと同様に同期および課金されます。
- プロビジョニング対象のすべての Enterprise Vault.cloud サービスは、共有メールボックスのアーカイブアカウントに対してデフォルトで有効になります。いずれかのサービスを無効にする場合は、アーカイブアカウントを編集し、サービスを手動で無効にする必要があります。
- Personal.cloud のようこそメッセージを送信するように Office 365 Sync を設定すると、共有メールボックスにようこそメッセージが送信されます。
- フルアクセス権を持つ共有メールボックスのメンバーは、共有メールボックスにアクセスして、ようこそメッセージを表示できます。メンバーは、ようこそメッセージに含まれるクレデンシャルを使用して、共有メールボックスの Personal.cloud アーカイブにアクセスできます。
- ユーザーは、レビュー担当者の役割など、アカウントにアクセスするための必要な権限がある場合にのみ、自分の Personal.cloud アーカイブから共有メールボックスのアーカイブアカウントにアクセスできます。

  p.72 の「アーカイブアカウントへのレビュー担当者の役割の割り当て」を参照してください。

3 ［Mailbox Delegation Permissions］で、Office 365 のメールボックスに適用された委任権限で実施する処理を選択します。これらの設定に加えられた変更は、次回の Office 365 同期イベントから反映されます。

p.21 の「Office 365 メールボックスの委任権限の同期について」を参照してください。

必要なオプションを選択します。

Do not synchronize delegation permissions	メールボックスの委任権限の同期を実行しません。メールボックスの委任権限がすでに同期されている場合、これらは変更されないままになります。
Synchronize delegation permissions	ターゲットのメールボックスに適用される委任権限を同期します。その後、ユーザーは Personal.cloud で、委任アクセス権が付与された各メールボックスのアーカイブ済みコンテンツにアクセスできます。
Remove synchronized delegation permissions	Office 365 の同期済み委任権限を削除します。Office 365 アーカイブへのすべての委任されたアクセス権が削除されます。

4 ［Office 365 Config］ページで以前に Office 365 アカウントクレデンシャルを設定しており、それを変更しない場合には、手順 7 に進みます。

5 ［PowerShell Credentials］には、アカウント同期のために Office 365 Sync で PowerShell コマンドを実行できる Office 365 アカウントのクレデンシャルを指定する必要があります。

User Name	必要な権限がある Office 365 アカウントの電子メールアドレスを入力します。
Password	Office 365 アカウントのパスワードを入力します。

6 [Exchange Web Services Credentials]には、Office 365 Sync で Web フォルダを配備するときに、Exchange Web サービスを実行できる Office 365 アカウントの詳細を指定する必要があります。

Use the same credentials as Powershell	PowerShell コマンドを実行するために指定したアカウントと同じアカウントを使用するには、このチェックボックスにチェックマークを付けることをお勧めします。異なるアカウントを使用する必要がない限り、ここにチェックマークが付いていることを確認して次の手順に進みます。 Web フォルダの配備に別の Office 365 アカウントを使用するには、このチェックマークをはずして、アカウントのユーザー名とパスワードを入力します。
User Name	PowerShell クレデンシャルを使用しないように選択した場合は、必要な権限を持った別の Office 365 アカウントの電子メールアドレスを入力します。
Password	PowerShell クレデンシャルを使用しないように選択した場合は、別の Office 365 アカウントのパスワードを入力します。

7 必要な場合は、[Test]をクリックして、Archive Administration が Office 365 に接続できることと、指定したアカウントが必要な権限を持っていることを調べます。

テスト接続が成功するまで続行しないでください。

8 [Save]をクリックします。

9 Office 365 アカウントクレデンシャルを入力または変更した場合は、[Provisioning]ページで設定を保存する必要があります。次のように、適切な手順を実行します。

- [My Config]でプロビジョニングを設定していない場合は、[Next]をクリックしてリンクをたどり[Provisioning]ページに移動します。そのページで設定オプションを指定して保存します。
  p.24 の「プロビジョニングについて」を参照してください。
- [Provisioning]ページを以前に設定済みの場合は、[Provisioning]ページに移動して、[Save]または[Save and Set Journaling]をクリックします。

Office 365 Sync アカウント用カスタムの役割グループの作成

Office 365 の同期を実行する Microsoft Office 365 アカウントには、特定の管理者権限が割り当てられている必要があります。Office 365 のグローバル管理者アカウントを指定できますが、必要な権限のみを持ったアカウントを使用することもできます。次の手順では、必要な権限を持った Office 365 カスタム役割グループを作成する方法について説

明します。このカスタムの役割グループに割り当てられたすべてのアカウントは、[Office 365 Config]ページで指定するアカウントとして使用できます。

Office 365 Sync アカウント用カスタムの役割グループを作成するには

1. グローバル管理者として、Microsoft Office 365 にサインインします。
2. [Admin]アプリをクリックして、Office 365 管理センターを開きます。
3. カスタムの役割グループに割り当てる新しいユーザーアカウントを作成する場合は、次の手順を実行します。
   - [ユーザー]、[アクティブ ユーザー]の下で[+]アイコンをクリックします。
   - [新しいユーザーアカウントの作成]ダイアログボックスの設定を完了します。

   メモ: Office 365 が Exchange 管理センターで新しいアカウントを利用可能にするのに、時間がかかる場合があります。
4. Office 365 管理センターの左側のメニューバーで、[管理センター](以前の管理センターの[管理]) を展開し、[Exchange]を選択します。
5. Exchange 管理センターの左側のナビゲーションウィンドウ枠で、[アクセス許可]をクリックします。
6. [管理者の役割]ページで、[+]アイコンをクリックして、新しい役割グループを追加します。
7. [役割グループの新規作成]ウィンドウの上部にある[名前]フィールドに、役割のグループ名を入力します。
8. [役割グループの新規作成]ウィンドウの[役割]セクションで、[+]アイコンをクリックして必要な役割を追加します。
9. [役割を選択]ウィンドウで、次の役割をすべて選択して[追加]をクリックします。
   - ApplicationImpersonation
   - 配布グループ
   - メール受信者
10. [OK]をクリックして[役割を選択]ウィンドウを閉じて、[役割グループの新規作成]ウィンドウに戻ります。
11. [役割グループの新規作成]ウィンドウの[メンバー]セクションで、[+]アイコンをクリックして役割グループにアカウントを追加します。
12. [メンバーの選択]ウィンドウで、役割グループのメンバーにするアカウントを選択して[追加]をクリックします。

13 [OK]をクリックして[メンバーの選択]ウィンドウを閉じて、[役割グループの新規作成]ウィンドウに戻ります。

14 [保存]をクリックして、新しい役割グループを保存します。

メモ: 新しい役割グループが、[管理者の役割]ページの管理者の役割グループのリストに表示されます。新しい役割グループが表示されない場合は、数分間待機してページを更新します。Office 365 Sync のこの役割グループのメンバーである、任意のアカウントのクレデンシャルを使用できます。

Office 365 メールボックスの委任権限の同期について

Office 365 Sync には、メールボックスの委任権限を同期するためのオプションが含まれています。このオプションを使用すると、メールボックスに対して[Full Access]の委任権限を持つ Personal.cloud ユーザーは、Personal.cloud からメールボックスのアーカイブにアクセスできます。

通常、Office 365 の管理者が、メールボックスの委任権限を設定します。これらの権限は、Office 365 管理センターから、または PowerShell を使用して設定できます。Office 365 Sync では、ユーザーが Outlook または Outlook Web App から付与できる委任アクセス権は同期されません。

[Office 365 Config]ページのオプションは、メールボックスの委任権限が同期されているかどうかを制御します。また、以前に同期されたメールボックスの委任権限を削除するためのオプションも提供されています。

p.16 の「Office 365 Sync の設定」を参照してください。

[Account Management]でアーカイブアカウントの詳細を表示すると、[Delegate Access]ウィンドウ枠に、アーカイブへの委任アクセス権を持つユーザーや、メールが有効なセキュリティグループが一覧表示されます。

p.47 の「[Account Details]ページについて」を参照してください。

委任権限の同期の必要条件

メールボックスに設定された委任権限を同期するために、Office 365 Sync で次の条件を満たす必要があります。

- Office 365 Sync のターゲットは、メールボックスにする必要があります。
- メールボックスに、少なくとも 1 つの[Full Access]の委任権限を設定する必要があります。そうでない場合、メールボックスの委任権限は同期されません。
- 同期する委任権限について、委任されたユーザーのアーカイブアカウントがすでに存在する必要があります。

メールボックスの同期済み委任権限の影響

メールボックスの同期済み委任権限の影響は、権限が、ユーザーに付与されるか、メールが有効なセキュリティグループに付与されるかによって異なります。

表 3-1 は、権限がユーザーに付与された場合の影響について説明します。

表 3-1　同期済み委任権限がユーザーに付与された場合の影響

メールボックスの委任権限	Personal.cloud での同期済み権限の影響
フルアクセス	ユーザーは、アカウントのアーカイブ済み項目を、Personal.cloud で読み取ることができます。 **メモ:** ユーザーが、同期済みの[フルアクセスの拒否]の権限を持つグループに属している場合、このアクセス権は付与されません。
フルアクセスの拒否 *	ユーザーは、アカウントのアーカイブ済み項目を Personal.cloud で読み取ることができません。
差出人	このリリースに影響はありません。
代理人として送信する	このリリースに影響はありません。

* [フルアクセスの拒否]の権限は、PowerShell からのみ設定できます。

表 3-2 は、メールが有効なセキュリティグループに権限が付与された場合の影響について説明します。

表 3-2　メールが有効なセキュリティグループに同期済み委任権限が付与された場合の影響

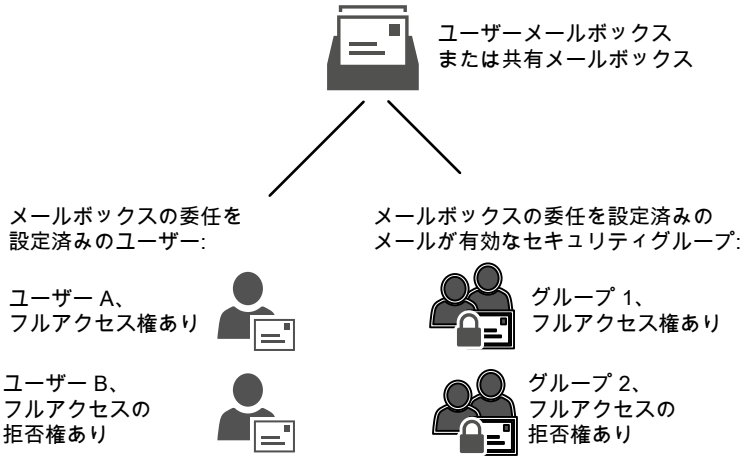
メールボックスの委任権限	Personal.cloud での同期済み権限の影響
フルアクセス	グループのメンバーであるユーザーは、アカウントのアーカイブ済み項目を、Personal.cloud で読み取ることができます。 **メモ:** ユーザーに同期済みの[フルアクセスの拒否]の権限がある場合、このアクセス権は付与されません。
フルアクセスの拒否 *	グループのメンバーであるユーザーは、アカウントのアーカイブ済み項目を、Personal.cloud で読み取ることができません。
差出人	このリリースに影響はありません。
代理人として送信する	このリリースに影響はありません。

* [フルアクセスの拒否]の権限は、PowerShell からのみ設定できます。

Enterprise Vault.cloud が競合する委任権限を同期する場合、拒否権が優先されます。この動作は、メールボックスへのアクセスに関して、Microsoft 社の競合する委任権限の扱いと一致します。

次に、Office 365 の管理者が多数の委任権限をメールボックスに割り当てるシナリオ例を検討します。

図 3-1 例: ユーザーとメールが有効なセキュリティグループに対する委任権限が設定された Office 365 メールボックス



この例で、Office 365 の管理者は、メールボックスに次の委任アクセス権を付与しました。

- ユーザー A とグループ 1 のメンバーには、[フルアクセス]の権限が指定されています。
- ユーザー B とグループ 2 のメンバーには、[フルアクセスの拒否]の権限が指定されています。

Office 365 Sync がこれらすべての委任権限を同期し、ユーザー A とグループ 1 のメンバーは、メールボックスのアーカイブにアクセスできると想定します。

このアクセス権は、委任拒否権の優先度に影響されます。たとえば、ユーザー A がグループ 2 のメンバーである場合、グループ 2 の[アクセス拒否]の委任権限がユーザー A の[フルアクセス]の権限を上書きするため、ユーザー A はメールボックスのアーカイブにアクセスできません。

アーカイブアカウントのすべての委任アクセス権が削除される要因となる条件

いくつかの状況で、Enterprise Vault.cloud は、不正アクセスのリスクを回避するために、Office 365 メールボックスのアーカイブアカウントへの委任アクセス権をすべて削除します。

Enterprise Vault.cloud は、次の状況のいずれかが発生した場合に、メールボックスへのすべての委任アクセス権を削除します。

- Office 365 Sync のプロビジョニング設定を変更した場合など、Office 365 Sync でメールボックスがターゲットではなくなった場合。
- または、ユーザーがメールボックスに対してアクセス拒否の委任権限を持っていて、そのユーザーに、まだアーカイブアカウントがない場合。

スケジュール設定された同期による委任権限の同期について

スケジュール設定された同期の初回実行の後、Office 365 Sync は通常、Active Directory のプロパティが変更されたターゲットユーザーのみの同期を考慮します。ただし、Office 365 の委任権限を同期する場合、Office 365 Sync は、委任されたメールボックスを持つすべてのターゲットユーザーを考慮します。このため、メールボックスの委任が変更されたユーザーは、ユーザーの Active Directory のプロパティが変更されたかどうかに関係なく同期される場合があります。この動作により、メールボックスの委任権限が確実に最新の状態になります。

プロビジョニングについて

アカウントプロビジョニングの管理に、コンソールアプリケーションまたは Microsoft Office 365 を使用することを選択した場合、[My Config]の[Provisioning]ページで設定を構成する必要があります。

メモ: CloudLink を使用してアカウントプロビジョニングの管理を行うことを選択した場合は、CloudLink を使用して独自のプロビジョニング設定を構成する必要があります。詳しくは、CloudLink のマニュアルを参照してください。

[Provisioning]ページに表示される設定オプションは、[User Management]ページで選択したオプションによって異なります。次のように、必要なオプションを入力します。

表 3-3 Office 365 Sync を使用したアカウント管理のプロビジョニング手順

プロビジョニング手順	詳細情報の参照先
次を設定する ■ アーカイブ元となる Office 365 ドメイン ■ プロビジョニング対象の Office 365 ユーザー ■ Office 365 Sync へのジャーナリング	p.25 の「Office 365 Sync のプロビジョニングオプションの設定」を参照してください。
Personal.cloud 配備オプションを設定する	p.29 の「Personal.cloud の配備オプションの設定」を参照してください。
管理者の通知オプションを設定する	p.32 の「管理者の通知オプションの設定」を参照してください。

表 3-4 コンソールアプリケーションを使用したアカウント管理のプロビジョニング手順

プロビジョニング手順	詳細情報の参照先
Personal.cloud 配備オプションを設定する	p.29 の「Personal.cloud の配備オプションの設定」を参照してください。
管理者の通知オプションを設定する	p.32 の「管理者の通知オプションの設定」を参照してください。

Office 365 Sync のプロビジョニングオプションの設定

[User Management]ページで、Microsoft Office 365 を使用してアカウントプロビジョニングを管理するように選択した場合は、[Provisioning]ページで Office 365 Sync のプロビジョニングオプションを設定する必要があります。

Office 365 Sync のプロビジョニングオプションを設定するには

1. Archive Administration の左側のナビゲーションウィンドウ枠で、[My Config]の[Provisioning]をクリックします。
2. [Domains to Provision]の下で、次のオプションのいずれかを選択します。

Provision specific domains	アーカイブアカウントをプロビジョニングするMicrosoft Office 365ドメインを選択するには、このオプションを選択します。次に、[Specify Domains]をクリックし、リストから目的のドメインを選択します。[Select Domains]ボックスに、設定済みの Microsoft Office 365 アカウントに関連付けられているすべてのドメインが一覧表示されます。 プライマリドメインを設定するには、必要なドメインで[Set as Primary]を選択します。 ドメインを選択したら、[Update]をクリックして、選択したオプションを保存します。
Provision all domains	設定済みの Microsoft Office 365 アカウントに関連付けられているすべての Microsoft Office 365 ドメインのアーカイブアカウントをプロビジョニングするには、このオプションを選択します。

3 [Archive Provisioning]の下で、次のオプションのいずれかを選択します。

Provision Distribution Lists	会社の特定の Office 365 配布リストに関連付けられているユーザーのアーカイブアカウントを作成するには、このオプションを選択します。次に、[Specify Lists]をクリックし、目的の配布リストを選択します。 **メモ:** 動的配布グループは[Specify Lists]の表に表示されません。現在 Enterprise Vault.cloud では、Office 365 の動的配布グループのプロビジョニングはサポートされていません。 配布リストを選択したら、[Update]をクリックして、選択したオプションを保存します。
Provision all users	以前の手順で指定したドメインのすべてのユーザーに対してアーカイブアカウントをプロビジョニングするには、このオプションを選択します。

メモ: [Provision Distribution Lists]オプションが利用できない場合は、[Office 365 Config]ページに移動し、[Run Now]をクリックして配布リストを取得します。

p.34 の「Office 365 同期イベントの実行およびスケジュール設定」を参照してください。

4 ［SMTP Journaling］で、Office 365 Sync 向けにジャーナリングのプロビジョニングを手動または自動のどちらで行うかを選択します。

Manually provision journaling in Office 365	Microsoft Office 365 インターフェースから手動で Office 365 ジャーナリングを設定するには、このオプションを選択します。 このオプションを選択した場合は、同期の実行を試行する前に、適切なジャーナリングルールを Office 365 に手動で設定する必要があります。 指定した配布グループにジャーナリングする場合など、特定のジャーナリングルールを設定する場合は、手動プロビジョニングを選択します。それ以外の場合は、自動プロビジョニングを選択できます。 Office 365 Sync のジャーナリングを手動で設定する方法について詳しくは、『Enterprise Vault.cloud ジャーナリングガイド』の「Office 365 のジャーナリングの設定」を参照してください。 **メモ:** Office 365 のジャーナリングを手動で設定した場合に入力する必要があるジャーナリングアドレスは、［Automatically provision journaling in Office 365］オプションの［Journal address］ボックスに表示されます。
Automatically provision journaling in Office 365	Archive Administration が Office 365 でジャーナリングルールを自動的に設定することを許可するには、このオプションを選択します。この手順の最後で［Save and Set Journaling］をクリックしたときに、Archive Administration はジャーナリングルールの作成を試行します。このルールによって、すべての項目が、割り当てられている Office 365 ジャーナリングアドレスにジャーナリングされます。 Enterprise Vault.cloud で会社に割り当てた Office 365 のジャーナリングアドレスが、Archive Administration の［Journal address］ボックスに事前に入力されています。 **メモ:** Office 365 の送信コネクタも設定する必要があります。『Enterprise Vault.cloud ジャーナリングガイド』の「Office 365 のジャーナリングの設定」を参照してください。

メモ: Microsoft の Azure RMS (Rights Management Services) で暗号化された Office 365 メッセージをアーカイブする場合は、ジャーナルレポートを復号するように Office 365 を設定する必要があります。『Enterprise Vault.cloud ジャーナリングガイド』の「Office 365 の RMS 暗号化メッセージのアーカイブに関する追加の前提条件」を参照してください。

5 [Save]または[Save and Set Journaling]をクリックします。

6 プロビジョニングプロセスを完了するために、[Provisioning]ページの追加オプションを使用して、設定をさらにカスタマイズします。

- Personal Archive Deployment Options
  p.29 の「Personal.cloud の配備オプションの設定」を参照してください。
- Notification Options
  p.32 の「管理者の通知オプションの設定」を参照してください。

Personal.cloud の配備オプションの設定

[User Management]ページで、コンソールアプリケーションまたは Microsoft Office 365 を使用してアカウントプロビジョニングを管理するように選択した場合は、[Provisioning]ページで Personal.cloud の配備オプションを指定できます。

Personal.cloud の配備プロビジョニングオプションを設定するには

1 Archive Administration の左側のナビゲーションウィンドウ枠で、[My Config]の[Provisioning]をクリックします。

2 ページの下部にある[Personal Archive Deployment Options]を展開します。

3 Microsoft Office 365 でアカウントをプロビジョニングしないことを選択した場合は、手順 5 に進みます。

4 [Web Folder Configuration]で、Office 365 Outlook に配備できる Personal.cloud Web フォルダの詳細を指定できます。Personal.cloud Web フォルダにより、ユーザーは Outlook 内から直接 Personal.cloud アーカイブにアクセスできます。

メモ: Office 365 OWA (Outlook Web App) からは、Personal.cloud Web フォルダにアクセスできません。現在 Microsoft 社は、Office 365 OWA のフォルダにデフォルトでホームページを表示する Outlook 機能をサポートしていません。

Personal.cloud Web フォルダの必要なオプションを設定します。

Deploy Web Folder to Office 365	アーカイブアカウントをプロビジョニングするときに、Office 365 Sync で Personal.cloud Web フォルダを配備する場合に、このオプションを選択します。 **メモ:** Office 365 Sync がすでに同期されているアカウントに Personal.cloud Web フォルダを配備する場合は、[Run Now]で同期を実行する必要があります。または、Personal.cloud Web フォルダを[Account Management]から手動で配備することもできます。 p.52 の「ユーザーの配備」を参照してください。
Archive Folder Name	Personal.cloud Web フォルダに使用する名前を入力します (「Personal Archive」など)。
Archive Folder URL	Personal.cloud のアクセス URL を入力します。

5 [Personal Archive Access]で、Enterprise Vault.cloud が Personal.cloud へのアクセスを自動的に有効にして、各ユーザーにようこそメッセージの電子メールを送信するかどうかを設定します。

メモ: 表示されるオプションは、Enterprise Vault.cloud で会社にシングルサインオン認証が設定されているかどうかによって異なります。これは、シングルサインオン認証を使用するユーザーにとって、ようこそメッセージが重要でないことを反映した結果です。

Enterprise Vault.cloud で会社にシングルサインオン認証が設定されていない場合、オプションは次のようになります。

Enable Personal Archive access and send Welcome Message

プロビジョニング対象の各アカウントに Personal.cloud へのアクセスを許可し、プロビジョニング対象ユーザーにようこそメッセージが送信されるようにするには、このオプションを選択します。

デフォルトでは、このオプションは選択されていません。

このオプションを選択する場合は、次のいずれかのサブオプションを選択する必要があります。

- Don't send Welcome Message if already sent

  プロビジョニング対象ユーザーに 1 回だけようこそメッセージを送信するには、このオプションを選択します。これはデフォルトのオプションです。

- Send Welcome Message anyway

  以前にようこそメッセージが送信された場合でも、Office 365 Sync でアカウントが同期されるたびにようこそメッセージを送信するには、このオプションを選択します。

Enterprise Vault.cloud で会社にシングルサインオン認証が設定されている場合、オプションは次のようになります。

Enable Personal Archive access

プロビジョニング対象の各アカウントに Personal.cloud へのアクセスを許可するには、このオプションを選択します。

デフォルトでは、このオプションは選択されていません。

このオプションを選択すると、Enterprise Vault.cloud がプロビジョニング対象ユーザーにようこそメッセージを送信するかどうかを選択できます。

- Send Welcome Message

  プロビジョニング対象ユーザーにようこそメッセージが送信されるようにするには、このオプションを選択します。

  新規設定の場合、デフォルトではこのオプションは選択されていません。

  このオプションを選択する場合は、次のいずれかのサブオプションを選択する必要があります。

- Don't send Welcome Message if already sent

  プロビジョニング対象ユーザーに 1 回だけようこそメッセージを送信するには、このオプションを選択します。これはデフォルトのオプションです。

- Send Welcome Message anyway

  以前にようこそメッセージが送信された場合でも、Office 365 Sync でアカウントが同期されるたびにようこそメッセージを送信するには、このオプションを選択します。

6 [Welcome Message Template]で、次のメッセージのテンプレートの詳細を設定します。

- プロビジョニング対象ユーザーに送信するようこそメッセージ。
- Enterprise Vault.cloud が新しいアーカイブアカウントをプロビジョニングしたときに、選択した管理者の役割に送信される通知メッセージ。

Select Template	プロビジョニング対象ユーザー向けにようこそメッセージのテンプレートを設定するには、[Account]を選択します。 管理者の通知メッセージを設定するには、[Administrator]を選択します。
From	メッセージ送信者の電子メールアドレスを入力します。
Subject	電子メールメッセージの件名として保存する情報を入力します。
Body	メッセージの本文テキストを編集します。 Enterprise Vault.cloud がアーカイブ情報に基づいて関連する情報で置き換える、次のマクロを使用できます。 ■ {username}: ユーザーのログインユーザー名が自動的に入力されます。 ■ {password}: ユーザーのログインパスワードが自動的に入力されます。 ■ {accountlist}: 新しく作成された電子メールアカウントのリストが自動的に入力されます。管理者テンプレートのみで使用します。

7 [Save]をクリックします。

管理者の通知オプションの設定

[User Management]ページで、コンソールアプリケーションまたは Microsoft Office 365 を使用してアカウントプロビジョニングを管理するように選択した場合は、[Provisioning]ページで管理者の通知オプションを指定できます。

管理者の通知オプションを設定するには

1 Archive Administration の左側のナビゲーションウィンドウ枠で、[My Config]の[Provisioning]をクリックします。

2 ページの下部にある[Notification Options]を展開します。

3 [Administration Roles to Notify]で、Enterprise Vault.cloud がアーカイブアカウントを作成したときに管理者の通知を受信する、Enterprise Vault.cloud の管理者の役割を選択します。

メモ: 役割に割り当てられている管理者のリストを表示するには、その役割をクリックします。

4 [Save]をクリックします。

Office 365 の同期について

[Office 365 Config]ページおよび[Provisioning]ページの設定オプションの指定が完了したら、[Office 365 Config]ページに戻って、Office 365 ユーザーの同期を管理および監視できます。

プロビジョニング対象の Office 365 アカウントに関して、次の動作に注意してください。

- Microsoft Office 365 でアカウントを削除したり、ライセンスを無効にしたりした場合、Office 365 Sync は、次回の同期中に Personal.cloud アクセス権を無効化し、アカウントのアーカイブを一時停止します。そのアカウントの新しい電子メールはアーカイブされませんが、既存の電子メールは、引き続き eDiscovery で利用できます。Office 365 Sync は、アーカイブアカウントの電子メールアドレスに `Disabled_on_date` を追加します。ここで、*date* は、アーカイブが一時停止された日時です。その後、Office 365 でアカウントを復元したり、ライセンスを再度有効化したりすると、Office 365 Sync は、次回の同期中に Personal.cloud アクセス権を再度有効化して、アーカイブを再開します。
- アカウントのサインイン状態を、Office 365 で[ブロック]に設定した場合、Office 365 Sync は、次回の同期中にアカウントの Personal.cloud アクセス権を無効化します。そのアカウントへの新しい電子メールは、引き続きアーカイブされます。その後、サインイン状態を[許可]に戻すと、Office 365 Sync は、次回の同期中に Personal.cloud アクセス権を再度有効化します。
- Office 365 Sync で、[Provision Distribution Lists]オプションを使用してユーザーをプロビジョニングし、その後アカウントが Office 365 の配布リストから削除されると、その後の同期でアーカイブアカウントは無効化されません。アーカイブを停止する場合は、Office 365 でアカウントを削除するか、ライセンスを無効化する必要があります。

[Office 365 Config]ページは、Office 365 ユーザーの同期を管理および監視するための、次のオプションを提供します。

表 3-5 Office 365 Sync のオプション

Office 365 Sync のオプション	目的	参照先
Run Now	オンデマンドの Office 365 同期を実行できます。	p.34 の「Office 365 同期イベントの実行およびスケジュール設定」を参照してください。
Sync Scheduler	Office 365 アカウントの同期をスケジュール設定できます。	p.34 の「Office 365 同期イベントの実行およびスケジュール設定」を参照してください。
Report	Office 365 Sync が実行した同期の概要情報と詳細レポートを表示できます。	p.35 の「Office 365 Sync の概要とレポートの表示」を参照してください。

Office 365 同期イベントの実行およびスケジュール設定

Office 365 の同期をオンデマンドで実行したり、同期スケジュール設定したりできます。

メモ: 同期イベントを実行またはスケジュール設定する前に、[Office 365 Config]ページと[Provisioning]ページで、必要な設定オプションの指定を完了する必要があります。

Office 365 の同期をオンデマンドで実行するには

1 Archive Administration の左側のナビゲーションウィンドウ枠で、[My Config]の[Office 365 Config]をクリックします。

メモ: [Office 365 Config]ページは、[User Management]ページでプロビジョニングオプションとして Microsoft Office 365 を選択した場合にのみ表示されます。

2 [Run Now]をクリックします。

メモ: このオプションは、以前のイベントで同期されたユーザーを含む、すべてのユーザーを同期します。このオプションは、通常の同期イベントよりも時間がかかります。また、このオプションは、保存されている同期スケジュールをリセットします。完全な同期イベントが完了した後で、同期スケジュールを再設定することをお勧めします。

Office 365 同期イベントをスケジュール設定するには

1 Archive Administration の左側のナビゲーションウィンドウ枠で、[My Config]の[Office 365 Config]をクリックします。

メモ: [Office 365 Config]ページは、[User Management]ページでプロビジョニングオプションとして Microsoft Office 365 を選択した場合にのみ表示されます。

2 [Sync Scheduler]セクションで[On]を選択して、スケジューラを有効化します。

3 [Start]フィールドで、同期スケジュールの開始日時を選択します。

4 [Repeat]フィールドで、同期イベントの頻度を選択します。

5 [Save]をクリックして、スケジュールを保存します。

メモ: 最初の同期イベントが発生するまで、または、変更が適用されるまで、最大で 12 時間かかることがあります。

Office 365 Sync の概要とレポートの表示

[Office 365 Config]ページで、Office 365 同期イベントの概要テーブルを表示またはエクスポートできます。また、概要テーブルで、個々の同期イベントの詳細が含まれるレポートを表示またはエクスポートすることもできます。

Office 365 Sync の概要テーブルを表示するには

1 Archive Administration の左側のナビゲーションウィンドウ枠で、[My Config]の[Office 365 Config]をクリックします。

メモ: [Office 365 Config]ページは、[User Management]ページでプロビジョニングオプションとして Microsoft Office 365 を選択した場合にのみ表示されます。

2 [Office 365 Config]ページの右側のウィンドウ枠に、Office 365 Sync 同期イベントの詳細を示す、概要テーブル[Report]が表示されます。

メモ: レポートテーブルは、Office 365 Sync の最初の同期が発生した後にのみ表示されます。

3 必要な場合は、[Export]をクリックして、概要の詳細を Microsoft Excel ファイルにエクスポートします。

4 レポートテーブルの内容を更新するには、右側のウィンドウ枠の左上で、[Report]または更新の記号をクリックします。

同期イベントのレポートを表示するには

1 Archive Administration の左側のナビゲーションウィンドウ枠で、[My Config]の[Office 365 Config]をクリックします。

メモ: [Office 365 Config]ページは、[User Management]ページでプロビジョニングオプションとして Microsoft Office 365 を選択した場合にのみ表示されます。

2 [Office 365 Config]ページの右側のウィンドウ枠に、Office 365 Sync 同期イベントの詳細を示す、概要テーブル[Report]が表示されます。

メモ: レポートテーブルは、Office 365 Sync の最初の同期が発生した後にのみ表示されます。

3 特定の同期イベントのレポートを表示するには、テーブルの該当する行の右端にある列[View]をクリックします。

新しい[Report]ウィンドウに、レポートが表示されます。

4 レポートに表示される情報をフィルタするには、[Report Type]と[Object Type]で必要なオプションを選択します。

5 必要な場合は、[Select a format]フィールドでエクスポート形式を選択し、[Export]をクリックしてレポートの詳細をファイルにエクスポートします。

管理対象タグについて

[Managed Tags]ページから、ユーザーに割り当てられるグローバルタグを作成できます。管理対象タグを作成して保持ポリシーを関連付けると、ユーザーは、アーカイブ済みメッセージにタグを適用して、保持期間を延長できます。保持ポリシーの保持期間によって、タグが付けられたメッセージが Enterprise Vault.cloud で保持される期間が決まります。

表 3-6 に、管理対象タグに関連する、実行可能なタスクを一覧表示します。

表 3-6　管理対象タグを使用するタスク

タスク	参照先
新しい管理対象タグを作成する。	p.37 の「管理対象タグの作成」を参照してください。
ユーザーに管理対象タグを割り当てる。	p.38 の「ユーザーへの管理対象タグの割り当て」を参照してください。
管理対象タグに関連付けられている保持ポリシーを変更する。	p.38 の「管理対象タグに関連付けられている保持ポリシーの変更」を参照してください。
管理対象タグを編集および削除する。	p.39 の「管理対象タグの削除」を参照してください。

メモ: 管理対象タグと分類タグを混同しないでください。Veritas Information Classifier は、有効になっている分類ポリシーに一致する電子メールに分類タグを割り当てます。分類タグを手動で追加または削除することはできません。分類タグは、Discovery.cloud で表示できます。

管理対象タグの作成

管理対象タグを作成し、必要に応じて、既存の保持ポリシーを割り当てることができます。

管理対象タグを作成するには

1. 左側のナビゲーションウィンドウ枠で、[Managed Tags]をクリックします。
2. [Managed Tags]ページの上部で、[Create New]をクリックします。
3. [Create Managed Tag]ページで、[Tag Name]フィールドに名前を入力します。
4. 必要な場合は、[Assign Policy]をクリックして、管理対象タグに保持ポリシーを関連付けます。

   メモ: 管理対象タグに保持ポリシーを関連付ける前に、保持ポリシーを作成する必要があります。

   p.100 の「保持ポリシーの作成」を参照してください。

5. [Retention Policies]ウィンドウで保持ポリシーを選択して、[Assign Retention Policy]をクリックします。
6. 必要な場合は、[Description]フィールドに、タグの説明を入力します。

7 必要な場合は、[Set Managed Tag Permissions]セクションの設定を構成します。

メモ: [Tagged Email Visibility]のオプションを選択すると、管理者、レビュー担当者、およびユーザーは、管理対象タグが適用された他のユーザーのメッセージを表示できるようになります。[Tagged Email Visibility and Remove Tag]のオプションを選択すると、管理者、レビュー担当者、およびユーザーは、他のユーザーに属しているメッセージから管理対象タグを削除できるようになります。

8 [Save]をクリックします。

ユーザーへの管理対象タグの割り当て

デフォルトでは、作成した管理対象タグは、組織内のすべてのユーザーが使用できるようにするために、すべてのユーザーに割り当てられます。必要に応じて、選択したユーザーにのみ管理対象タグを割り当てることができます。

メモ: 選択したユーザーに割り当てることができるのは既存の管理対象タグのみです。新規タグの作成中に、ユーザーを選択して管理対象タグを割り当てることはできません。

ユーザーに管理対象タグを割り当てるには

1 左側のナビゲーションウィンドウ枠で、[Managed Tags]をクリックします。

2 [Managed Tags]ページで、既存の管理対象タグを選択します。

3 [Users Assigned]セクションで、[Selected Users]をクリックします。

4 [Add Users]をクリックします。

5 [Add Users]ウィンドウで、ユーザーを選択します。

6 [Add]をクリックしてユーザーを追加して、[Add Users]ウィンドウを閉じます。

7 [Edit Managed Tag]ページの上部で、[Save]をクリックします。

管理対象タグに関連付けられている保持ポリシーの変更

必要な場合は、管理対象タグに関連付けられている保持ポリシーを変更できます。

管理対象タグに関連付けられている保持ポリシーを変更するには

1 左側のナビゲーションウィンドウ枠で、[Managed Tags]をクリックします。

2 [Managed Tags]ページで、既存の管理対象タグを選択します。

3 [Edit Managed Tag]セクションで、[Change Policy]をクリックします。

4 [Retention Policies]ウィンドウで、新しい保持ポリシーを選択して[Assign Retention Policy]をクリックします。

5 ページの上部で、[Save]をクリックします。

管理対象タグの削除

必要な場合は、不要になった管理対象タグを削除できます。

メモ: 保持ポリシーに関連付けられている管理対象タグは、削除できません。

管理対象タグを削除するには

1 左側のナビゲーションウィンドウ枠で、[Managed Tags]をクリックします。

2 [Managed Tags]ページで、削除するタグを選択します。

3 必要な場合は、[Remove Policy]をクリックして、管理対象タグから保持ポリシーの関連付けを解除します。

4 ページの上部で、[Save]をクリックし、次に[Edit]をクリックします。

5 [削除]をクリックします。

6 確認のウィンドウで、[OK]をクリックします。

アカウント管理について

[Account Management]ページから、Enterprise Vault.cloud のアーカイブアカウントを管理できます。

表 3-7 に、[Account Management]ページで実行できるタスクのリストと、詳細情報の場所を示します。

表 3-7 アカウント管理タスク

タスク	参照先
アーカイブアカウントを検索する	p.40 の「アーカイブアカウントの検索」を参照してください。
一覧表示されたアーカイブアカウントをフィルタする	p.42 の「検索フィルタの使用」を参照してください。
新しいアーカイブアカウントを作成する	p.43 の「アーカイブアカウントの作成」を参照してください。

タスク	参照先
アーカイブアカウントの詳細を表示する	p.46 の「アーカイブアカウントの詳細の表示」を参照してください。 p.47 の「[Account Details]ページについて」を参照してください。
アーカイブアカウントを編集する	p.51 の「アーカイブアカウントの編集」を参照してください。
アーカイブアカウントを削除する	p.52 の「アーカイブアカウントの削除」を参照してください。
ユーザーを配備する	p.52 の「ユーザーの配備」を参照してください。
ユーザーのアクセス権を削除する	p.53 の「ユーザーのアクセス権の削除」を参照してください。
既存のアーカイブアカウントのサービスを有効にする	p.53 の「既存のアーカイブアカウントのサービスの有効化」を参照してください。
既存のアーカイブアカウントの Mobile Web Access 権限を編集する	p.54 の「既存のアーカイブアカウントの Mobile Web Access 権限の編集」を参照してください。
アーカイブアカウントの情報をエクスポートする	p.56 の「アーカイブアカウントの情報のエクスポート」を参照してください。
アーカイブアカウントのロックを解除する	p.55 の「アーカイブアカウントのロック解除」を参照してください。

アーカイブアカウントの検索

[Account Management]ページには、組織のアーカイブアカウントが一覧表示されます。多数のアーカイブアカウントがある場合は、複数のページにアカウントが表示されます。メインのウィンドウ枠の下部にあるコントロールを使用して、ページをスクロールできます。

クイック検索と詳細な検索を使用して、特定のアーカイブアカウントを検索できます。詳細な検索では、アカウントに割り当てられている役割や、Enterprise Vault.cloud のその他のアクセスオプションに従って検索できます。

クイック検索を使うには

1. 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。
2. [Search]フィールドに、アーカイブアカウントに関連付けられているユーザー名または電子メールアドレスを入力します。
3. [Search]をクリックします。

詳細な検索を使うには

1. 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。
2. [Search]フィールドの右側にある[Expansion]アイコンをクリックして、詳細な検索の基準を表示します。

3 次のフィールドで検索基準を指定します。

Email Address or Alias	ユーザーの電子メールアドレスまたは関連付けられているエイリアス電子メールアドレスを入力します。
Last Name	ユーザーの姓を入力します。
First Name	ユーザーの名前を入力します。
Role	ユーザーに割り当てられている役割の種類を選択します。
Personal Archive Access	ユーザーに Personal.cloud のアクセス権が有効化されている場合に選択します。
Discovery Archive Access	ユーザーに Discovery.cloud のアクセス権が有効化されている場合に選択します。
Welcome Message Sent	ユーザーがようこそメッセージを受信した場合に選択します。
Account Status	ユーザーのアカウントの状態がアクティブか、削除された場合に選択します。
Archive	ユーザーのアーカイブが現在アクティブな場合に選択します。
Enterprise Vault.cloud Mobile	ユーザーが Mobile Web Access のアクセス権を持つ場合に選択します。
Account Locked	ユーザーが、アーカイブアカウントからロックアウトされている場合に選択します。
Blackberry Access and Collection	ユーザーが Blackberry のアクセス権を持ち、収集が有効化されている場合に選択します。
Office 365 PA Collection	ユーザーに Microsoft Office 365 Personal Archive の収集が有効化されている場合に選択します。 **メモ:** この機能は、Enterprise Vault.cloud ではサポート対象ではなくなりました。

4 ［Search］をクリックします。

検索フィルタの使用

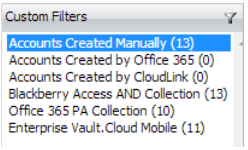
クイック検索または詳細な検索に加えて、検索フィルタを使用してアーカイブアカウントを検索できます。事前定義済みのカスタムフィルタのいずれかを使用するか、配布リストを基準にしてフィルタできます。

検索フィルタを使用するには

1 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。

2 検索フィルタのウィンドウ枠で、検索フィルタのグループの[Custom Filters]または[Distribution Lists]をクリックします。

3 選択したグループからフィルタを選択します。



4 [Filter]アイコンをクリックします。

これで、選択した検索フィルタに一致するアーカイブアカウントのみが、アカウントリストに含まれるようになりました。

5 検索フィルタを削除する場合は、[Remove Filter]アイコンをクリックします。

アーカイブアカウントの作成

[Account Management]ページから、ユーザーのアーカイブアカウントを手動で作成できます。

アーカイブアカウントを作成するには

1 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。

2 [Account Management]ページの上部で、[Archives]、[New Archive]の順にクリックします。

3 ［Accounts］ページの［Archive Detail］で、必要な詳細情報を次のように入力します。

Email Address	ユーザーのプライマリ電子メールアドレスを入力します。 **メモ:** 組織に複数のドメインがある場合は、ドロップダウンリストから適切なドメインを選択します。
First Name	ユーザーの名前を入力します。
Last Name	ユーザーの姓を入力します。
User Name	アカウントのユーザー名です。Archive Administration は、デフォルトで、ユーザー名として電子メールアドレスを使用しますが、必要に応じて変更できます。
Password	組織のパスワードポリシーの必要条件を満たす、ユーザーのパスワードを入力します。 p.77 の「高度なパスワードポリシーの設定」を参照してください。 **メモ:** ［Provisioning］、［Personal Archive Deployment Options］、［Personal Archive Access］の順に選択して［Enable Personal Archive Access and send Welcome Message］を選択した場合、このオプションは表示されません。その場合、Archive Administration は、パスワードを自動的に生成してユーザーに送信します。
Confirm Password	パスワードを入力したら、確認のためにパスワードを再度入力する必要があります。
Time Zone	ユーザーの適切なタイムゾーンを選択します。
Role	このアーカイブアカウントに対して現在設定されている役割を示します。

4 ［Status］で、ユーザーの状態のオプションを選択します。

Account	アカウントを有効な状態で作成するか、無効な状態で作成するかを選択します。
Login	Enterprise Vault.cloud アカウントのログインのロックを解除するか、ロックするかを選択します。
Archiving	アーカイブが有効か無効かを選択します。 ［Enabled］を選択した場合、アーカイブアカウントの作成後すぐに、ユーザーの電子メールメッセージの Enterprise Vault.cloud へのジャーナリングが開始されます。

Folder Sync	Folder Sync 機能が有効か無効かを示します。 **メモ:** この状態は、情報提供のみを目的としています。Folder Sync は、Archive Administration から有効化または無効化できません。Folder Sync は、Folder Sync アプリケーションからアカウントレベルで有効化または無効化します。
External Reviewer	ユーザーを外部のレビュー担当者にするかどうかを選択します。外部のレビュー担当者とは、組織には属していなくても、アーカイブ済みメッセージを Discovery.cloud の事案向けにレビューする必要があるユーザーです。 外部のレビュー担当者のアーカイブアカウントには、次の条件が該当します。 ■ アカウントの役割にのみ割り当てることができます。 ■ 標準のレビュー担当者の役割が割り当てられたユーザーと同様に、任意の事案に割り当てることができます。 ■ Discovery.cloud の[E-Discovery]タブにのみアクセスできます。 ■ 自身に割り当てられている事案にのみアクセスできます。 ■ 権限が付与されていれば、ラベル、レビューの状態、およびメモをメッセージに適用できます。 ■ 事案の期限が切れると、事案にアクセスできなくなります。 ■ 組織の設定に関係なく、メッセージの復元、転送、または返信はできません。 ■ メッセージにすでに割り当てられているラベルやレビューの状態は編集できません。 外部のレビュー担当者のアカウントでは、アーカイブが無効になっています。

5 ［Services］で、アーカイブアカウントに対して有効にするサービスを選択します。

Personal.cloud	ユーザーが Personal.cloud にアクセスできるようにします。
Personal.cloud Mobile	ユーザーが Mobile Web Access にアクセスできるようにします。 **メモ:** このサービスを有効にするには、［Archive Options］ページでも Mobile Web Access のオプションを有効にする必要があります。
Discovery.cloud	ユーザーが Discovery.cloud にアクセスできるようにします。
Chatter	ユーザーに対して Salesforce Chatter アーカイブを有効にします。 **メモ:** このオプションは、組織がサービスのサブスクリプションを利用している場合にのみ利用可能になります。
Office 365	ユーザーに対して Microsoft Office 365 Personal Archive の収集を有効にします。 **メモ:** この機能は、Enterprise Vault.cloud のサポート対象ではなくなったため、選択しないでください。
Blackberry	ユーザーに対して Personal Archive for BlackBerry を有効にします。

6 ［Archive Aliases］で、必要に応じて、アーカイブアカウントに関連付けるエイリアス電子メールアドレスを入力します。次に、［Add］をクリックします。必要に応じて、手順を繰り返して複数のエイリアスを追加します。

メモ: これらのエイリアス電子メールアドレスに送信されたメッセージは、プライマリ電子メールアドレスに自動的に転送されます。アーカイブアカウントにエイリアス電子メールアドレスを関連付けない場合、エイリアス電子メールアドレスに送信されたメッセージは、割り当てられていないレガシーアカウントに保存されます。

7 ［Save］をクリックして、入力した詳細を保存して、新しいユーザーを作成します。

アーカイブアカウントの詳細の表示

［Account Management］から、アーカイブアカウントの詳細を表示できます。

アーカイブアカウントの詳細を表示するには

1. 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。
2. アカウントリストで、詳細を表示するアーカイブアカウントをクリックします。

   アカウントの詳細が表示されます。

   p.47 の「[Account Details]ページについて」を参照してください。

   アカウントのリストに戻るには、表示されているブレッドクラムで[Account Management]をクリックできます。

[Account Details]ページについて

アーカイブアカウントの詳細を表示する場合、[Account Details]ページに、アカウントに関する情報を示すさまざまなパネルが表示されます。

[Archive Detail]パネル

[Archive Detail]パネルには、アーカイブアカウントに関する次のような詳細が含まれています。

Email Address	ユーザーのプライマリ電子メールアドレスです。
First Name	ユーザーの名前です。
Last Name	ユーザーの姓です。
User Name	Archive Administration は、デフォルトで、ユーザー名として電子メールアドレスを使用します。
Time Zone	Enterprise Vault.cloud がユーザーに対して使用するタイムゾーンです。
Role	このアーカイブアカウントに現在設定されている役割です。

[Status]、[Services]および[Archive Aliases]パネル

[Status]、[Services]および[Archive Aliases]のパネルは、アーカイブアカウントの現在の状態、そのアカウントに現在設定されている Enterprise Vault.cloud サービス、アカウントの電子メールエイリアスを表示します。

メモ: [Status]の見出しの隣にある、赤い[External]フラグは、アーカイブアカウントが外部のレビュー担当者であることを示します。

[Status]セクションは、アカウントの状態に関する次の情報を表示します。

Account	アカウントが有効な状態か無効な状態かを示します。

Login	アカウントの Enterprise Vault.cloud ログインが、ロック解除されているかロックされているかを示します。
Archiving	アーカイブが有効か無効かを示します。
Folder Sync	Folder Sync 機能が有効か無効かを示します。

[Services]セクションは、アカウントでどの Enterprise Vault.cloud サービスが有効になっているかを示します。

 アカウントに対してサービスが有効になっていることを示します。

[Archive Aliases]セクションには、アカウントのすべてのアーカイブエイリアス電子メールアドレスと、各エイリアスが作成された日付が一覧表示されます。

 この電子メールアドレスがプライマリ管理者アカウントであることを示します。

[Delegate Access]パネル

[Delegate Access]パネルは、1 人以上のユーザーまたはメールが有効な 1 つ以上のセキュリティグループに、アーカイブアカウントの同期済み委任アクセス権がある場合に表示されます。

次に注意してください。

- このリリースで、Enterprise Vault.cloud は、Exchange オンプレミスメールボックスと Office 365 メールボックスに設定されている委任権限を同期できます。通常、Exchange または Office 365 の管理者が、これらの権限を設定します。Enterprise Vault.cloud は、ユーザーが Outlook から設定できるメールボックスフォルダへの委任アクセス権は同期しません。
- Exchange オンプレミスメールボックスの委任権限の同期には、CloudLink バージョン 4.0 が必要です。詳しくは、『CloudLink 管理者ガイド』を参照してください。
- Office 365 メールボックスの委任権限の同期は、Archive Administration の[Office 365 Config]ページにある、[Mailbox Delegation Permissions]の設定を使用して制御します。
p.16 の「Office 365 Sync の設定」を参照してください。

[Delegate Access]パネルには、以下が表示されます。

- アーカイブアカウントに対する同期済み委任アクセス権を持つ、委任ユーザーとメールが有効なセキュリティグループ。
- 各委任について、Enterprise Vault.cloud でどの委任アクセス権が付与されているか。
次のアイコンは、委任アーカイブアクセス権が付与されているかどうかを示します。

- Enterprise Vault.cloud で権限が付与されていることを示します。
- Enterprise Vault.cloud で権限が付与されていないことを示します。

次の表は、委任アーカイブアクセス権と、Enterprise Vault.cloud でのそれぞれの影響を示します。

表 3-8 委任アーカイブアクセス権がユーザーに付与された場合の影響

委任アーカイブアクセス権	付与されたときの状況	付与された権限による **Personal.cloud** での影響
READ	ユーザーまたは所属するグループは、同期済みの[フルアクセス]の委任権限を持っています。	ユーザーは、委任されたアカウントのアーカイブ済み項目を、Personal.cloud で読み取ることができます。
SEND AS	ユーザーまたは所属するグループは、同期済みの[差出人]の委任権限を持っています。	このリリースの Personal.cloud には影響ありません。
ON BEHALF	ユーザーまたは所属するグループは、同期された[代理人として送信する]の委任権限を持っています。	このリリースの Personal.cloud には影響ありません。

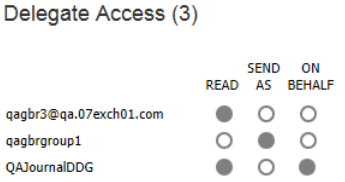
表 3-9 メールが有効なセキュリティグループに委任アーカイブアクセス権が付与された場合の影響

委任アーカイブアクセス権	付与されたときの状況	付与された権限による **Personal.cloud** での影響
READ	グループは、同期済みの[フルアクセス]の委任権限を持っています。	グループに属するユーザーは、委任されたアカウントのアーカイブ済み項目を、Personal.cloud で読み取ることができます。 **メモ:** ユーザーが同期済みの[フルアクセスの拒否]の委任権限を持っている場合は、拒否権が優先されて、このユーザーには読み取りアクセス権は付与されません。
SEND AS	グループは、同期済みの[差出人]の委任権限を持っています。	このリリースの Personal.cloud には影響ありません。

委任アーカイブアクセス権	付与されたときの状況	付与された権限による Personal.cloud での影響
ON BEHALF	グループは、同期済みの[代理人として送信する]の委任権限を持っています。	このリリースの Personal.cloud には影響ありません。

[Delegate Access]パネルのリストには、同期済みの委任拒否権は表示されませんが、Enterprise Vault.cloud では、委任されたアクセス権を許可するかどうかを判断するときに、これらの権限が考慮されます。競合する委任権限が同期される場合、Enterprise Vault.cloud は拒否権を優先します。たとえば、メールボックスに対する[フルアクセス]の委任権限がユーザーに付与されているとします。このユーザーが、同じメールボックスに対する[フルアクセスの拒否]の委任権限を持つ、メールが有効なセキュリティグループにも属していると想定します。Enterprise Vault.cloud がこれら両方の委任権限を同期する場合、ユーザーには、このメールボックスのアーカイブに対する読み取りアクセス権は付与されません。

次の図は、アーカイブアカウント例に対する[Delegate Access]パネルを示しています。



3 人のユーザーまたは 3 つのグループが、このアカウントに対して委任アーカイブアクセス権を持っていることが、このパネルに示されています。

- ユーザー qagbr3@qa.07exch01.com は、READ の権限を持っています。この権限は、qagbr3 が Personal.cloud にログインすると、アカウントのアーカイブ済み項目の読み取りが可能になることを意味します。
- グループ qagbrgroup1 は、SEND AS の権限を持っています。この SEND AS の権限は、このリリースの Enterprise Vault.cloud には影響しません。
- グループ QAJournalDDG は、READ 権限と ON BEHALF 権限の両方を持っています。READ のアクセス権により、このグループに属するユーザーは、Enterprise Vault.cloud から同期された[アクセス拒否]の委任権限を持っていない限り、アカウントのアーカイブ済み項目を Personal.cloud から参照できます。ON BEHALF の権限は、このリリースの Enterprise Vault.cloud には影響しません。

[History]パネル

[History]パネルには、アーカイブアカウントの設定に加えられた最新の変更の概要が含まれています。パネルには、[Account Details]ページに表示される詳細に関連する、次のような変更がすべて記録されます。

- アカウントの作成の詳細情報。この情報は、常に[History]パネルの上部に表示されます。
- 名前、姓、ユーザー名、プライマリ電子メールアドレス、タイムゾーン、または役割への変更。
- アカウントの有効化や、ログインの有効化など、アカウントの状態に対する変更。
- 有効なサービスに対する変更。
- アーカイブエイリアスに対する変更。

メモ: Folder Sync の状態の変更は、[History]パネルには記録されません。

[History]パネルには、最大で 30 個の変更が表示されます。

特定の変更の詳細を取得するには、[History]ウィンドウ枠の下部にある[View logs for more details]をクリックして、Enterprise Vault.cloud のログを確認します。リンクをクリックすると、左ウィンドウ枠の[Reporting]にある[Logs]ページに移動します。

p.110 の「Enterprise Vault.cloud のレポートとログについて」を参照してください。

アーカイブアカウントの編集

アーカイブアカウントを編集して、その状態や設定されたサービスなどを変更できます。

アーカイブアカウントを編集するには

1. 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。
2. アカウントリストでアーカイブアカウントをクリックして、そのアカウントの詳細を表示します。
3. 詳細を編集するには、[Account Details]ページの右下で、[Edit]をクリックします。
4. 必要に応じて、アカウントの詳細を更新します。

   CloudLink または Office 365 Sync を使用して、アカウントプロビジョニングをリモートから管理する場合、一部のアカウントの詳細は、Archive Administration 内からは更新できないことに注意してください。

   メモ: アーカイブアカウントを無効にすると、ユーザーは Personal.cloud にアクセスできなくなり、そのユーザーのメッセージは Enterprise Vault.cloud にジャーナリングされなくなります。

5. [Save]をクリックして、変更を保存します。

アーカイブアカウントの削除

必要な場合は、アーカイブアカウントを削除できます。

eDiscovery で事案に含まれているアーカイブアカウントは、削除できません。

メモ: アーカイブアカウントを削除した場合、ユーザーのアーカイブ済みメッセージは Enterprise Vault.cloud に残り、必要な権限を持ったレビュー担当者や管理者は引き続き検索の対象にできます。ユーザーに送信されるすべての新しい電子メールメッセージは、割り当てられていないレガシーアカウントにアーカイブされます。

アーカイブアカウントを削除するには

1. 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。
2. アカウントリストで、削除するアーカイブアカウントをクリックして、そのアカウントの詳細を表示します。
3. [Account Details]ページの下部で、[Edit]をクリックします。
4. アーカイブアカウントを削除するには、[Delete Archive]をクリックします。

ユーザーの配備

新しいアーカイブアカウントを作成したら、Personal.cloud と Discovery.cloud へのアクセス権を[Account Management]からユーザーに付与できます。また、Personal.cloud Web フォルダを配備して、ユーザーにようこそメッセージを送信することもできます。

ユーザーを配備するには

1. 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。
2. アカウントリストで、配備する各アーカイブアカウントにチェックマークを付けます。
3. [Account Management]ページの上部で、[Archives]、[Deploy User]の順にクリックします。
4. [Deploy Users]ウィンドウで、次の配備タスクを 1 つ以上選択します。
   - [Enable DA Access]: Discovery.cloud へのアクセスを提供します。
   - [Enable PA Access]: Personal.cloud へのアクセスを提供します。
   - [Deploy PA Web Folder]: Personal.cloud にアクセスするために、Microsoft Outlook Web フォルダを作成します。
   - [Send Welcome Message]: ログインクレデンシャルを使用してようこそメッセージを送信します。
5. [OK]をクリックします。

ユーザーのアクセス権の削除

[Account Management]ページから、選択したアーカイブアカウントの、Personal.cloud と Discovery.cloud へのユーザーアクセス権を削除できます。

メモ: 配備済みの Personal.cloud Web フォルダを削除する場合は、Veritasのサービスとサポートにお問い合わせください。

ユーザーのアクセス権を削除するには

1. 左側のナビゲーションウィンドウ枠の[My Config]で、[Account Management]をクリックします。
2. アカウントリストで、ユーザーアクセス権を削除する各アーカイブアカウントにチェックマークを付けます。
3. [Account Management]ページの上部で、[Archives]、[Remove User]の順にクリックします。
4. [Remove User]ウィンドウで、1 つ以上のオプションを選択します。
   - [Disable DA Access]: Discovery.cloud アクセス権を削除します。
   - [Disable PA Access]: Personal.cloud アクセス権を削除します。
5. [OK]をクリックします。

既存のアーカイブアカウントのサービスの有効化

新しいアーカイブアカウントを作成するときにサービスを有効化する以外にも、[Account Management]ページから、1 つ以上の既存のアーカイブアカウントに対してサービスを有効化できます。

既存のアーカイブアカウントに対してサービスを有効化するには

1. 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。
2. アカウントリストで、サービスを有効化するアーカイブアカウントにチェックマークを付けます。
3. [Account Management]ページの上部で、[Enable Services]をクリックします。
4. [Enable Services]ウィンドウで、次のオプションを 1 つ以上選択します。
   - [Office 365 PA Collection]: Microsoft Office 365 Personal Archive の収集を有効化します。

     メモ: この機能は、Enterprise Vault.cloud のサポート対象ではなくなったため、選択しないでください。

- ［Salesforce Chatter Collection］: Salesforce Chatter の収集を有効化します。

メモ: ［Blackberry Access and Collection］オプションは、ユーザーごとには設定できません。組織がこのサービスのサブスクリプションを利用している場合に、すべてのユーザーに対してサービスが自動的に有効化されます。

5 ［OK］をクリックします。

既存のアーカイブアカウントの Mobile Web Access 権限の編集

［Account Management］ページから、1 つ以上の既存のアーカイブアカウントに対する Mobile Web Access 権限を編集できます。

メモ: Mobile Web Access の機能を利用可能にするには、［Policy Management］、［Archive Options］の順に選択して、Mobile Web Access も有効にする必要があります。

p.74 の「アーカイブオプションの設定」を参照してください。

次の手順のいずれかを使用して、既存のアーカイブアカウントの Mobile Web Access 権限を必要に応じて設定します。

選択したまたはすべての既存のアカウントに対する Mobile Web Access 権限を編集するには

1 左側のナビゲーションウィンドウ枠の［My Config］で、［Account Management］をクリックします。

2 既存のアーカイブアカウントすべての権限を設定する場合は、次の手順に進みます。それ以外の場合は、アカウントリストで、権限を編集する各アカウントにチェックマークを付けます。

3 ［Account Management］ページの上部で、［Mobile Permissions］をクリックします。

4 ［Mobile Interface Account Permissions］ウィンドウで、次のオプションのいずれかを選択します。

- Permit Mobile Web Access for selected accounts
  このオプションは、選択したアカウントに Mobile Web Access 権限を付与します。
- Permit Mobile Web Access for all current accounts

メモ: 既存のすべてのアーカイブアカウントに Mobile Web Access 権限が付与されるため、このオプションを使用する場合は注意が必要です。

- Deny Mobile Web Access for selected accounts
  このオプションは、選択したアカウントの Mobile Web Access 権限を削除します。
- Deny Mobile Web Access for all current accounts

メモ: 既存のすべてのアーカイブアカウントの Mobile Web Access 権限が削除されるため、このオプションを使用する場合は注意が必要です。

5 [Save]をクリックします。

単一アカウントに対する Mobile Web Access 権限を編集するには

1 左側のナビゲーションウィンドウ枠の[My Config]で、[Account Management]をクリックします。

2 アーカイブアカウントのリストで、必要なアカウントの詳細を表示します。

[Account Details]ページの[Services]にある[Personal.cloud Mobile]の状態は、Mobile Web Access 権限が設定されているかどうかを示します。

3 Mobile Web Access 権限の設定を変更するには、[Edit]をクリックします。

4 [Services]で、必要に応じて[Personal.cloud Mobile]を選択またはクリアします。

5 [Save]をクリックして、変更を保存します。

アーカイブアカウントのロック解除

セキュリティ上の手段として、Enterprise Vault.cloud は、間違ったログインクレデンシャルを 1 時間に 5 回入力したユーザーを、アーカイブアカウントから一時的にロックアウトします。クレデンシャルを 3 回間違えると、ユーザーに、残りの試行回数は 2 回であることが通知されて、画像認証 (CAPTCHA) の検証コードの入力が求められます。間違ったクレデンシャルを 5 回入力すると、Enterprise Vault.cloud はアーカイブアカウントをロックします。アカウントがロックされた場合、管理者は Archive Administration からロックを解除できます。

アーカイブアカウントのロックを解除するには

1 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。

2 アカウントリストから、ロックされているアーカイブアカウントを選択します。

3 [Account Details]ページの[Services]セクションで、[Account Locked]をクリアします。

4 [Save]をクリックします。

アーカイブアカウントの情報のエクスポート

［Account Management］ページから、組織内のすべてのアーカイブアカウントのアカウント情報をエクスポートできます。パスワードの情報は、エクスポートファイルには含まれません。

メモ: 現在エクスポートできるのは、すべてのアーカイブアカウントのアカウント情報のみです。アカウント情報をエクスポートする前に、アカウントリストから個々のアカウントを選択した場合でも、エクスポートファイルには、すべてのアカウントの情報が含まれています。

アーカイブアカウントの情報をエクスポートするには

1. 左側のナビゲーションウィンドウ枠で、［Account Management］をクリックします。
2. ［Account Management］ページの上部で、［Export to Excel］をクリックします。

4

アーカイブコレクタ

この章では以下の項目について説明しています。

アーカイブコレクタについて

組織は Enterprise Vault.cloud を使用して、電子メールメッセージ以外のコンテンツソースの項目もアーカイブできます。現在、Enterprise Vault.cloud では、次の項目のアーカイブがサポートされています。

- Box
- Salesforce Chatter
- Microsoft Lync Server オンプレミス

[Archive Collectors]セクションから Archive Administration のページにアクセスして、Box や Salesforce Chatter のアーカイブサービスを設定および管理したり、[Lync On-Premises Archiving]機能を有効にしたりできます。

Box ファイルアーカイブについて

Box ファイルアーカイブサービスは、Enterprise Vault.cloud のアーカイブアカウントでプロビジョニングされている Box アカウントから、組織がファイルをアーカイブすることを可能にするアドオン機能です。

このサービスを設定すると、Box ユーザーアカウントと、対応する Enterprise Vault.cloud アーカイブアカウントのマッピングが開始されます。マッピングが成功するためには、アー

カイブアカウントのプライマリ電子メールアドレスが、Box ユーザーアカウントの電子メールアドレスと一致する必要があります。マッピングが成功した、アーカイブが有効な Box アカウントについて、アーカイブエージェントはファイルを収集し、それらをメッセージの添付ファイルとして Enterprise Vault.cloud に送信します。

表 4-1 に、Box ファイルアーカイブがデフォルトで収集するファイルの拡張子を一覧表示します。必要な場合は、追加のファイル拡張子を指定できます。

表 4-1 Box ファイルアーカイブがデフォルトで収集するファイルの拡張子

ファイルカテゴリ	Box ファイルアーカイブがデフォルトで収集するファイルの拡張子
Microsoft Word	doc、docx
Microsoft Excel	xls、xlsx
Microsoft PowerPoint	ppt、pptx、pps
Adobe Acrobat	pdf
圧縮ファイル	zip
画像	gif、jpg、bmp、png
テキスト	txt
ハイパーテキスト	htm、html
電子メールメッセージ	eml
Adobe Flash	swf

メモ: Box ファイルアーカイブのファイル収集で現在サポートされるファイルの最大サイズは、45 MB です。

Box ファイルアーカイブは、収集する各ファイルに電子メールメッセージを作成します。ファイルは、メッセージの添付ファイルとして提供されます。表 4-2 に、各メッセージの形式について説明します。

表 4-2 Box ファイルアーカイブのメッセージ形式

メッセージコンポーネント	情報
宛先フィールド	`file@box.com` **メモ:** Enterprise Vault.cloud に送信されるすべての Box ファイルで、このデフォルト値が使用されます。

メッセージコンポーネント	情報
差出人フィールド	ファイルの送信元である Box ユーザーの電子メールアドレスが使用されます。 **メモ:** 項目を正しくアーカイブするためには、対応する Box アカウントと Enterprise Vault.cloud アカウントで使用されるプライマリ電子メールアドレスが一致する必要があります。
件名フィールド	Box.com に続いて、ファイル名が記載されます。
メッセージの本文	ファイル名、元のファイルの作成日、最終更新日、ファイルのサイズを含むファイルの情報が記載されます。

メモ: Box ファイルアーカイブでは、ファイルがアーカイブされたときに Box が生成する、ファイルダウンロードの電子メール通知メッセージはすべて抑制されます。この機能に現在関連付けられているすべての制限事項について詳しくは、次の Enterprise Vault.cloud のサポート記事を参照してください。http://www.veritas.com/docs/000023852

Archive Administration から、次の Box ファイルアーカイブ向けタスクを実行できます。

- Box と Enterprise Vault.cloud 間のリンクの設定。
- 新しくマッピングされたアカウントに対するファイル収集の自動有効化。
- マッピングされていないユーザーの週単位レポート生成の有効化。
- Box からアーカイブするファイル拡張子のリストへの追加。
- 個々のユーザー向けのアーカイブのファイル拡張子の変更。
- マッピングされたユーザーに対する手動収集の有効化または無効化。
- Box ユーザーリストのダウンロード。

Box へのリンクの設定

Box ファイルアーカイブサービスがプロビジョニングされた Box アカウントからファイルをアーカイブする前に、Box と Enterprise Vault.cloud の間のリンクを設定する必要があります。

リンクを設定するには、Enterprise Vault.cloud が Box ユーザーのコンテンツを収集するために使用できる Box アカウントのクレデンシャルを指定する必要があります。クレデンシャルは、Box のプライマリ管理者または共同管理者のものである必要があります。プライマリ管理者のアカウントを指定することをお勧めします。共同管理者アカウントを指定すると、Enterprise Vault.cloud は管理者または他の共同管理者からファイルを収集できない場合があります。

指定する Box アカウントは、Box アカウントの電子メールアドレスと同じプライマリ電子メールアドレスを持つ Enterprise Vault.cloud アーカイブアカウントを持つ必要があります。Enterprise Vault.cloud アカウントは、Archive Administration にログインするのに使用する同じアカウントである必要はありません。

リンクを設定した直後に、Box ファイルアーカイブは、Box ユーザーアカウントと対応するアーカイブアカウントのマッピングを開始します。

Box へのリンクを設定するには

1. Archive Collections Manager の管理者の役割が割り当てられているアカウントを使用して、Archive Administration にログインします。

   p.69 の「組み込み管理プログラムの役割の編集」を参照してください。

2. 左側のナビゲーションウィンドウ枠で、[Box]をクリックします。
3. [設定]タブで[Box にログイン]をクリックします。
4. [ログインして Box へのアクセスを許可]ウィンドウで、Box アカウントの管理者のクレデンシャルを入力して[承認]をクリックします。

   メモ: [ログインして Box へのアクセスを許可]ウィンドウが新しいブラウザウィンドウで開きます。新しいウィンドウが表示されない場合は、ブラウザのポップアップブロックの設定を確認してください。

5. [次へ]ウィンドウで、[Box へのアクセスを許可]をクリックします。

   メモ: アクセスするときに確認メッセージが表示されます。Archive Administration への接続を失うことなく、確認メッセージを含むブラウザウィンドウを閉じることができます。

6. 元の Archive Administration Box ブラウザウィンドウで、[続行]をクリックします。Box ファイルアーカイブサービスは、プロビジョニングされた Box アカウントと対応するアーカイブアカウントのマッピングを自動的に開始します。

Box へのリンクの削除

必要な場合は、Box への Enterprise Vault.cloud リンクを削除できます。リンクを削除すると、すべての Box ユーザーに対するファイルアーカイブがすぐに停止されます。

メモ: Box へのリンクの削除を元に戻すことはできません。Box へのアクセスを削除する前に、Veritasのサービスとサポートに問い合わせることをお勧めします。

Box へのリンクを削除するには

1. 左側のナビゲーションウィンドウ枠で、[Box]をクリックします。
2. [Configuration]タブの[Archive Link Status]セクションで、[Edit]をクリックします。
3. [Deactivate Box Archiving]の警告ページで、[Deactivate]をクリックします。

サービスがアカウントをマッピングしたときのファイル収集の自動有効化

Box ファイルアーカイブサービスが Box アカウントを対応するアーカイブアカウントにマッピングしたときに、ファイル収集が自動的に有効化されるように選択できます。このオプションを選択した場合、新しくマッピングされた Box アカウントに対して、手動でアーカイブを有効化する必要はありません。

メモ: アカウントのマッピングが成功するためには、Box アカウントの電子メールアドレスに一致するプライマリ電子メールアドレスを持つアーカイブアカウントが存在する必要があります。

サービスがアカウントをマッピングしたときにファイル収集を自動的に有効化するには

1. 左側のナビゲーションウィンドウ枠で、[Box]をクリックします。
2. [Configuration]タブの[Map and Collect Users]セクションで、チェックマークを付けます。
3. [Save]をクリックします。

マッピングされていないユーザーのレポートの有効化

Box ファイルアーカイブサービスでは、リンクされている Box 管理者アカウントに関連付けられている電子メールアドレスに、マッピングされていないユーザーレポートを、必要な場合は毎週送信できます。マッピングされていないユーザーレポートには、アーカイブアカウントに割り当てられていない Box アカウントのリストが含まれています。

マッピングされていないユーザーとは、対応するアーカイブアカウントがない Box アカウントを表します。サービスがこれらのユーザーをマッピングするためには、Box アカウントの電子メールアドレスに一致するプライマリ電子メールアドレスを持つアーカイブアカウントを作成する必要があります。これらのアーカイブアカウントを作成すると、サービスは、Box アカウントを新しいアーカイブアカウントに自動的にマッピングします。

メモ: [Account Management]セクションの[Map]列には、一覧表示されたユーザーごとにマッピングの状態が表示されます。[Yes]の状態は、ユーザーアカウントが正常にマッピングされていることを示します。[No]の状態は、サービスがユーザーアカウントをマッピングできなかったことを示します。

マップされていないユーザーのレポートを有効化するには

1. 左側のナビゲーションウィンドウ枠で、[Box]をクリックします。
2. [Configuration]タブの[Unmapped User Report]セクションで、チェックマークを付けます。
3. [Save]をクリックします。

Box からアーカイブするファイル拡張子のリストへの追加

Box ファイルアーカイブは、デフォルトで、事前定義済みのファイル拡張子のリストに一致する拡張子が付いたファイルを収集します。

p.57 の「Box ファイルアーカイブについて」を参照してください。

必要な場合は、ファイル拡張子を追加できます。

Box からアーカイブされるファイル拡張子をリストに追加するには

1. 左側のナビゲーションウィンドウ枠で、[Box]をクリックします。
2. [設定]タブを選択します。
3. [Default File Types to Archive]に、Box ファイルアーカイブがデフォルトで収集するファイル拡張子のリストが示されます。

   ファイル拡張子のリストに追加するには、[Additional File Types]ボックスに 1 つ以上の追加のファイル拡張子を入力します。それぞれのファイルの拡張子は、スペース、カンマ、または改行で区切ります。

   メモ: 注意して追加のファイル拡張子を指定します。Box ファイルアーカイブは、入力された拡張子に対して、ファイル拡張子に含める文字として有効かどうかを調べる以外の検証はできません。

4. [Save]をクリックします。

個々のユーザー向けのアーカイブのファイル拡張子の変更

[Configuration]タブで設定するファイル拡張子を使用する代わりに、個々のユーザー向けに、アーカイブするファイルの拡張子を選択できます。

メモ: [Account Management]タブのユーザーリストの[File Types]列は、ユーザーごとに収集されるファイルの種類を示します。[Configured Types]のエントリは、[Configuration]タブで定義されているファイル拡張子を Box ファイルアーカイブが収集することを示します。

個々のユーザー向けにアーカイブのファイル拡張子を変更するには

1. 左側のナビゲーションウィンドウ枠で、[Box]をクリックします。
2. [Account Management]タブを選択します。
3. ユーザーリストからユーザーを選択し、[Pick File Types]をクリックします。
4. [Select File Types]ダイアログボックスで、次のいずれかの操作を行います。
   - [Configuration]タブで指定されているファイル拡張子をすべて収集するには、[Configured File Types]を選択します。
   - または、[Selected File Types]を選択して、収集するファイルの種類を選択します。
5. [Save]をクリックします。

マッピングされたユーザーに対する手動収集の有効化または無効化

マッピングされたユーザーをユーザーリストから選択して、Box ファイルの手動収集を有効化または無効化できます。

メモ: ユーザーリストから選択できるのは、マッピングされたユーザーのみです。

ユーザーのファイル収集を有効にしたら、次の収集イベントの間に、ユーザーの Box アカウントからのファイルアーカイブが開始されます。

マッピングされたユーザーに対する Box ファイルの手動収集を有効化または無効化するには

1. 左側のナビゲーションウィンドウ枠で、[Box]をクリックします。
2. [Account Management]タブを選択します。
3. ユーザーリストからユーザーを選択します。

   メモ: [Search]フィールドに、ユーザーの名、姓、またはユーザー名を入力して、ユーザーを検索します。

4. 次のいずれかを実行します。
   - Box ファイルの収集を有効化するには、[Enable Box Collection]をクリックします。
   - Box ファイルの収集を無効化するには、[Disable Box Collection]をクリックします。
5. [Confirm Action]ウィンドウで、[OK]をクリックします。

Box ユーザーリストのダウンロード

必要に応じて、現在の Box ユーザーのすべてに関する情報を含むリストをダウンロードできます。リストは CSV 形式で提供され、次の情報が含まれています。

- 名
- 姓
- ユーザー名
- アカウント登録日またはアカウントがマッピングされた日付

Box ユーザーリストをダウンロードするには

1. 左側のナビゲーションウィンドウ枠で、[Box]をクリックします。
2. [Account Management]タブを選択します。
3. [ユーザーリストのダウンロード]をクリックします。

Salesforce Chatter アーカイブについて

Salesforce Chatter アーカイブサービスは、組織が、プロビジョニング対象の Chatter アカウントの投稿をアーカイブすることを可能にするアドオン機能です。所属する組織でこのサービスを設定すると、アーカイブエージェントが Chatter の投稿を収集し、それらをメッセージの添付ファイルとして Enterprise Vault.cloud に送信します。アーカイブできる項目には、次のものが含まれます。

- Chatter の投稿の最初の 1,000 文字
- 他の Chatter の投稿への返信
- Chatter に投稿された URL
- ローカルコンピュータまたは Salesforce から Chatter にアップロードされたファイル
- プライベート Chatter メッセージ
- グループへの Chatter の投稿
- 他の Salesforce ユーザーへの直接の投稿

アーカイブプロセスの間、アーカイブエージェントは、アーカイブ済みの Chatter の投稿それぞれにメッセージを作成します。次の表に、アーカイブエージェントが各メッセージコンポーネントに使用する情報を示します。

表 4-3 アーカイブされる Chatter メッセージコンポーネント

メッセージコンポーネント	情報
宛先フィールド	chatterpost@salesforce.com **メモ:** Enterprise Vault.cloud に送信されるすべての Chatter の投稿で、このデフォルト値が使用されます。
差出人フィールド	投稿を作成した Chatter ユーザーの電子メールアドレス。 **メモ:** 項目を正しくアーカイブするためには、対応する Chatter アカウントと Enterprise Vault.cloud アカウントで使用されるプライマリ電子メールアドレスが一致する必要があります。
件名フィールド	Chatter の投稿のテキスト。
メッセージの本文	アーカイブする Chatter の投稿の種類に基づきます。また、Chatter に投稿された URL またはアップロードされたファイルの URL が含まれる場合があります。

Archive Administration から、Salesforce Chatter ファイルアーカイブサービスに関連する次のタスクを実行できます。

- Salesforce Chatter アーカイブサービスの設定。
- アーカイブの概要の表示。
- 個々のユーザーの Salesforce Chatter アーカイブの有効化または無効化。

Salesforce Chatter アーカイブの設定

Salesforce Chatter アーカイブサービスが、プロビジョニング対象の Chatter アカウントからの投稿をアーカイブする前に、Archive Administration でサービスを設定する必要があります。

Salesforce Chatter アーカイブを設定するには

1. Archive Collections Manager の管理者の役割が割り当てられているアカウントを使用して、Archive Administration にログインします。

   p.69 の「組み込み管理プログラムの役割の編集」を参照してください。

2. 左側のナビゲーションウィンドウ枠で、[Salesforce Chatter]をクリックします。
3. [Configuration]ページの[SF User Name]フィールドと[SF Password]フィールドに、Salesforce 管理者のクレデンシャルを入力します。
4. 必要な場合は、[Archive New]を選択して、新しいユーザーにサービスを自動的に有効化します。

5 必要な場合は、[Send Direct Email]を選択して、テスト環境でサービスをテストします。

6 [Save]をクリックします。

Salesforce Chatter アーカイブ概略の表示

Salesforce Chatter アーカイブサービスを設定すると、次の情報を含む概略を表示できます。

- サービスに設定されているアーカイブアカウントの数。
- サービスがアーカイブした更新の合計数。
- 最後にアーカイブされた更新のタイムスタンプ。

Salesforce Chatter アーカイブ概略を表示するには

1 左側のナビゲーションウィンドウ枠で、[Salesforce Chatter]をクリックします。

2 [概略情報]タブを選択します。

Salesforce Chatter アーカイブの有効化および無効化

必要な場合は、個々のアーカイブアカウントの Salesforce Chatter アーカイブを、[Account Management]ページから手動で有効化または無効化できます。そこから、サービスが有効化されているアーカイブアカウントを表示することもできます。サービスが有効化されているアーカイブアカウントには、[Account Management]ページの[Chatter]列に、値[Yes]が表示されます。

Salesforce Chatter アーカイブを有効化または無効化するには

1 左側のナビゲーションウィンドウ枠で、[Account Management]をクリックします。

2 アカウントリストで、1 つ以上のアーカイブアカウントにチェックマークを付けます。

3 [Enable Services]をクリックします。

4 [Enable Services]ウィンドウで、次のいずれかを行います。

- サービスを有効化するには、[Salesforce Chatter Collection]を選択します。
- サービスを無効化するには、[Salesforce Chatter Collection]のチェックマークをはずします。

メモ: [Salesforce Chatter Collection]チェックボックスは、組織がサービスのサブスクリプションを利用する場合にのみ使用できます。

---

5 [OK]をクリックします。

Lync オンプレミスアーカイブについて

個別にインストール可能な Enterprise Vault.cloud Lync Connector アプリケーションにより、オンプレミスの Microsoft Lync Server のインスタントメッセージのコンテンツを Enterprise Vault.cloud にアーカイブできます。アーカイブした Lync コンテンツは、eDiscovery 検索で使用でき、各参加者の Personal.cloud アーカイブ内からアクセスできます。各会話または会議が、レビュー時に完全なコンテキストを提供する、単一の項目としてアーカイブされます。

Lync Connector アプリケーションは、Lync Server 2010 および 2013 と、Skype for Business Server 2015 からのコンテンツアーカイブをサポートします。サポート対象バージョンの最新情報については、Enterprise Vault.cloud 互換性リストを参照してください。

Lync Connector では、現在、次の Lync Server コンテンツのアーカイブをサポートしています。

- ピアツーピアのインスタントメッセージの会話
- 配付資料、ホワイトボード、および投票などの添付ファイルを含む会議

Lync Connector は、現在、次の Lync コンテンツのアーカイブをサポートしていません。

- ピアツーピアのファイル転送
- オーディオおよびビデオ
- 常設チャット

Lync Connector についてと、オンプレミスの Lync Server からのアーカイブ方法について詳しくは、次の場所から入手可能な『Enterprise Vault.cloud Lync Connector 管理者ガイド』を参照してください。

http://www.veritas.com/docs/000025139

Lync Connector アプリケーションを設定する前に、Archive Administration で［Lync On-Premises Archiving］機能を有効にする必要があります。

p.67 の「Lync オンプレミスアーカイブ機能の有効化と無効化」を参照してください。

Lync オンプレミスアーカイブ機能の有効化と無効化

［Archive Collectors］セクションから、［Lync On-Premises Archiving］機能を有効化または無効化できます。この機能は、Enterprise Vault.cloud Lync Connector アプリケーションを設定する前に有効化する必要があります。

Lync オンプレミスアーカイブ機能を有効化または無効化するには

1. この機能を初めて有効化する場合は、必要な Enterprise Vault.cloud セカンダリサービスが会社で有効化されていることを調べます。
   - Archive Administration の左側のナビゲーションウィンドウ枠で、［My Config］の［Services］をクリックします。

- [Secondary Services]で、[Lync On-Premise Archiving]が有効化されているサービスとしてリストに表示されていることを確認します。Lync On-Premise Archiving が有効として表示されない場合は、Veritasのサービスとサポートにお問い合わせください。サービスが有効になるまで、続行することはできません。

2 [Configure Lync Archival]の権限を含む管理者の役割に割り当てられているアカウントで、Archive Administration にログオンします。

メモ: システム管理者に組み込まれている管理者の役割には、[Configure Lync Archival]の権限が含まれています。デフォルトでは、[Archive Collections Manager]に組み込まれている管理者の役割にも、この権限が含まれます。

---

3 左側のナビゲーションウィンドウ枠の[Archive Collectors]で、[Lync]をクリックします。

4 [Lync]ページに、Enterprise Vault.cloud の[Lync On-Premises Archiving]機能の状態と、会社に割り当てられている Lync オンプレミスジャーナリングアドレスのリストが表示されます。

[Lync On-Premises Archiving]機能を使用するには、[Journal Addresses]に少なくとも 1 つのジャーナリングアドレスが表示されている必要があります。

メモ: [Journal Addresses]のリストにジャーナリングアドレスが 1 つも表示されない場合は、Veritasのサービスとサポートにお問い合わせください。

---

5 [Lync]ページに、[Lync On-Premises Archiving]機能の現在の状態と、状態の最終更新日が表示されます。状態を変更するには、次のように行います。

- [編集]をクリックします。
- 次に、[Service Status]で[Enabled]コントロールをクリックして、設定を必要な値に変更します。
- [Save]をクリックして、変更を保存します。

メモ: Lync オンプレミスアーカイブを使用するには、Lync Connector アプリケーションも設定する必要があります。次の場所から入手可能な『Enterprise Vault.cloud Lync Connector 管理者ガイド』を参照してください。

http://www.veritas.com/docs/000025139

5

役割管理

この章では以下の項目について説明しています。

役割管理について

[Role Management]セクションから、組織のアーカイブ管理者の役割に対する権限をカスタマイズできます。また、組織内のアーカイブアカウントに、これらの役割を割り当てることもできます。

このセクションでは、次のタスクを実行できます。

- 組み込み管理プログラムの役割に対する権限の編集。
- カスタム管理者の役割に対する権限の作成および編集。
- アーカイブアカウントへの役割の割り当て。

さらに、[Role Management]のページから、現在使用されている組み込みおよびカスタムの管理者の役割を表示できます。各管理者の役割の横に表示される数字は、その役割が割り当てられているアーカイブアカウントの数を示します。

組み込み管理プログラムの役割の編集

Archive Administration には、アーカイブアカウントに割り当てる、組み込み管理プログラムの役割のセットが含まれます。デフォルトでは、それぞれの役割に、異なる権限のセッ

トが付与されています。各役割に付与されている権限をカスタマイズして、これらの役割を編集できます。

組み込み管理プログラムの役割には、次のものが含まれます。

- アカウントマネージャ: ユーザー、エイリアス、設定、およびパスワードを管理します。
- 役割マネージャ: アーカイブアカウントの管理者の役割と権限を設定します。
- ポリシーマネージャ: アーカイブのオプションと設定を指定します。
- 保持マネージャ: アーカイブの保持ポリシーと設定を指定します。
- 継続マネージャ: Email Continuity 機能 (組織が Email Continuity サービスのサブスクリプションを利用している場合にのみ利用可能) を管理します。
- Discovery 管理者: Enterprise Vault Discovery.cloud の使用状況を設定および管理します。
- システム管理者: すべての Personal.cloud アカウント (他の管理者を含む) を監督します。
- アーカイブコレクションマネージャ: サードパーティのコンテンツソースからのアーカイブを設定および管理します。
- 分類管理者: Veritas Information Classifier の分類ポリシーを編集および有効化します。

メモ: Discovery 管理者およびシステム管理者の役割に対する権限は、編集できません。

組み込み管理プログラムの役割を編集するには

1. 左側のナビゲーションウィンドウ枠で、[Administration Roles]をクリックします。
2. [Built-in Roles]セクションで、編集する役割をクリックします。

   メモ: アーカイブの概要の権限は削除できません。

3. 選択した役割に追加または削除する権限の隣で、チェックマークを付けるか、はずします。
4. [Save]をクリックします。

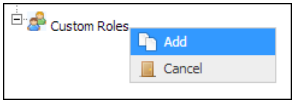
カスタム管理者の役割の作成

必要な場合は、カスタム管理者の役割を作成して、アーカイブアカウントに割り当てることもできます。カスタム管理者の役割を作成した後に、役割の権限を編集できます。

カスタム管理者の役割を作成するには

1 左側のナビゲーションウィンドウ枠で、[Administrator Roles]をクリックします。

2 [Custom Roles]を右クリックして、[Add]をクリックします。



3 空のテキストボックスに、カスタム管理者の役割の名前を入力します。

4 カスタムの役割に追加する権限の隣に、チェックマークを付けます。

5 [Save]をクリックします。

メモ: カスタム管理者の役割を編集または削除するには、役割の名前を右クリックして、[Edit]または[Delete]をクリックします。

アーカイブアカウントへの管理者の役割の割り当て

Archive Administration で作成したすべてのアーカイブアカウントには、デフォルトで、アカウントの役割が自動的に割り当てられます。必要な場合は、アーカイブアカウントに、組み込み管理プログラムの役割か、作成したカスタム管理者の役割を割り当てることができます。

アーカイブアカウントに管理者の役割を割り当てるには

1 次のいずれかを実行します。

- 左側のナビゲーションウィンドウ枠の[Role Management]で、[Assign Accounts]をクリックします。
- 左側のナビゲーションウィンドウ枠で[Role Management]をクリックし、次にページの下部にある[Manage your User Membership]をクリックします。

2 アカウントリストから、アーカイブアカウントを選択します。

3 [Role Change]セクションで、[Role]フィールドの[Administrator]を選択します。

4 必要な場合は、[Monitor All Accounts]を選択して、選択したアカウントが他のすべてのアーカイブアカウントのアーカイブ済みメッセージを表示できるようにします。

メモ: このオプションは、組織が Enterprise Vault Discovery.cloud のサブスクリプションを利用している場合にのみ利用可能になります。

---

5 [Group Privileges]セクションで、割り当てる組み込みまたはカスタムの役割にチェックマークを付けます。

メモ: アーカイブアカウントには、複数の役割を割り当てることができます。

6 [Save]をクリックします。

アーカイブアカウントへのレビュー担当者の役割の割り当て

組織が Enterprise Vault Discovery.cloud のサブスクリプションを利用している場合、レビュー担当者の役割をアーカイブアカウントに割り当てることができます。レビュー担当者は、組織のコミュニケーションポリシーに違反するものがないか、他の従業員の電子メールメッセージを監視します。

メモ: アカウントアーカイブにレビュー担当者の役割を割り当てることができるのは、組織が Discovery.cloud のサブスクリプションを利用している場合だけです。

アーカイブアカウントにレビュー担当者の役割を割り当てるには

1 次のいずれかを実行します。

- 左側のナビゲーションウィンドウ枠で、[Assign Accounts]をクリックします。
- 左側のナビゲーションウィンドウ枠で、[Administrator Roles]をクリックし、次に、ページの下部にある[Manage your User Membership]をクリックします。

2 アカウントリストから、アーカイブアカウントを選択します。

3 [Role Change]セクションで、[Role]フィールドの[Reviewer]を選択します。

4 必要な場合は、[Monitor All Accounts]を選択して、選択したアカウントが他のすべてのアーカイブアカウントのアーカイブ済みメッセージを表示できるようにします。

メモ: このオプションを選択する場合は、[Accounts to Monitor]セクションの手順を完了する必要はありません。

5 [Accounts to Monitor]セクションで、[Add/Remove Monitored Accounts]をクリックします。

6 [Add/Remove Monitored Accounts]ウィンドウで、レビュー担当者が監視するアーカイブアカウントを選択します。

7 ［Update］、［Close］の順にクリックして、［Add/Remove Monitored Accounts］ウィンドウを閉じます。

8 レビュー担当者の権限を期限切れにする場合は、必要に応じて、［Accounts to Monitor］リストで、［Never Expires］列のチェックマークをはずします。

次に、［Expiration］列で［Calendar］アイコンをクリックし、レビュー担当者の権限が期限切れになる日付を選択します。

6

ポリシー管理

この章では以下の項目について説明しています。

ポリシー管理について

[Policy Management]セクションから、次のタスクを実行できます。

- さまざまなオプションアーカイブの設定。
- 選択したアーカイブアカウントのアーカイブの無効化。
- パスワードの高度なポリシーの設定。
- Enterprise Vault.cloud アクセス用の信頼できるネットワークの設定。

メモ: 必要な権限を持つ管理者は、[Policy Management]セクションから Enterprise Vault.cloud の認証管理も設定できます。

p.86 の「Enterprise Vault.cloud 認証サービスの設定」を参照してください。

アーカイブオプションの設定

[Policy Management]ノードの[Archive Options]ページでは、Enterprise Vault.cloud 向けに次のオプションを設定できます。

- ［Email Direction］: Enterprise Vault.cloud でインバウンドメッセージ、アウトバウンドメッセージ、および内部メッセージをアーカイブするかどうかを決定します。
- ［Active Folder Synchronization］: Folder Sync サービスのサブスクリプションを利用している組織で、Outlook フォルダの同期を有効にするかどうかを決定します。
- ［Enterprise Vault.cloud Actions］: Personal.cloud ユーザーがメッセージを送信、返信、転送、印刷、または保存できるかどうかを決定します。
- ［Time Zone and Date Format］: Enterprise Vault.cloud のデフォルトのタイムゾーンと日付形式を設定します。
- ［Mobile Web Access］: Mobile Web Access を有効にするか無効にするかを決定し、関連する設定を制御します。

アーカイブオプションを設定するには

1. 左側のナビゲーションウィンドウ枠の［Policy Management］で、［Archive Options］をクリックします。
2. ［編集］をクリックします。
3. ［Email Direction］で次のメッセージの種類の 1 つ以上にチェックマークを付けます。
   - ［Inbound Emails］: ドメイン外からドメイン内の電子メールアドレスに送信される電子メールメッセージをアーカイブします。
   - ［Outbound Emails］: ドメイン内からドメイン外の電子メールアドレスに送信される電子メールメッセージをアーカイブします。
   - ［Internal Emails］: ドメイン内の電子メールアドレス間で送信される電子メールメッセージをアーカイブします。

   メモ: デフォルトでは、すべてのメッセージの種類が選択されています。
4. ［Active Folder Synchronization］で、フォルダ同期を［Enabled］または［Disabled］のどちらにするかを選択します。

   メモ: この機能は、Folder Sync アプリケーションを使用して、Microsoft Outlook フォルダを Enterprise Vault.cloud に同期します。このオプションは、組織がサービスのサブスクリプションを利用しており、Folder Sync アプリケーションを設定している場合にのみ利用可能になります。
5. ［Enterprise Vault.cloud Actions］で、Personal.cloud で有効にするアクションにチェックマークを付けます。

- [Send, Reply and Forward]: Personal.cloud でメッセージを送信、返信、転送するオプションを有効にします。
- [Save]: Personal.cloud からコンピュータにアーカイブ済みメッセージを保存するオプションを有効にします。
- [Print]: Personal.cloud からアーカイブ済みメッセージを印刷するオプションを有効にします。

6 [Time Zone and Date Format]で、次のオプションを設定します。

- [Personal Time Zone]: アーカイブアカウントのタイムゾーンです。
- [Default Company Time Zone]: 組織のデフォルトのタイムゾーンです。
- [Date Format]: 組織のデフォルトの日付形式です。

7 [Mobile Web Access]で、必要なオプションを選択します。

- [Enabled]または[Disabled]を選択して、Mobile Web Access 権限を持つすべてのアーカイブアカウントで、Mobile Web Access を有効にするか無効にするかを決定します。

  メモ: ユーザーがこの機能を使用するためには、アーカイブアカウントが Mobile Web Access 権限を持っている必要があります。

  p.54 の「既存のアーカイブアカウントの Mobile Web Access 権限の編集」を参照してください。

- Archive Administration で新しいアーカイブアカウントを手動で作成するときに、Enterprise Vault.cloud で Mobile Web Access 権限を付与する場合は、[Automatically grant Mobile Web Access permission for new accounts]を選択します。

  メモ: このオプションは、CloudLink または Office 365 Sync で作成されたアーカイブアカウントには適用されません。

- Mobile Web Access で[Send]、[Reply]、[Forward]の各オプションを有効にするには、[Send, Reply and Forward from Mobile Web Access]を選択します。

8 [Save]をクリックします。

アカウントのアーカイブの無効化

デフォルトでは、すべてのアーカイブアカウントのメッセージは、自動的に Enterprise Vault.cloud にジャーナリングされます。[Disabled Users]ページから、特定のアーカイブアカウントのアーカイブを無効化できます。

アカウントのアーカイブを無効化するには

1. 左側のナビゲーションウィンドウ枠の[Policy Management]で、[Disable Users]をクリックします。
2. [Disabled Users]セクションで、次のいずれかのアーカイブオプションを選択します。
   - [Archive emails for all users]: すべてのアーカイブアカウントの電子メールメッセージをアーカイブします。
   - [Archive emails for all users, except anyone listed below]: 選択した以外のすべてのアーカイブアカウントの電子メールメッセージをアーカイブします。
   - [Archive emails only for the users listed below]: 選択したアーカイブアカウントの電子メールメッセージのみをアーカイブします。
3. 必要な場合は、[Add/Remove Accounts]をクリックして、アーカイブで除外するまたは含めるアーカイブアカウントを選択します。
4. [Add/Remove Accounts]ウィンドウで、アーカイブで除外するまたは含めるアーカイブアカウントを選択します。
5. [Update]、[Close]の順にクリックして、[Add/Remove Accounts]ウィンドウを閉じます。
6. [Save]をクリックします。

高度なパスワードポリシーの設定

Enterprise Vault.cloud のデフォルトのパスワードポリシーでは、すべてのアカウントパスワードを少なくとも 6 文字以上にする必要があります。さらに、次の文字の種類のうち、少なくとも 2 つをすべてのパスワードに含める必要があります。

- 0 から 9 までの数字
- 小文字
- 大文字
- 英数字以外の文字

[Password Policy]ページで、すべてのアーカイブアカウントに対して、高度なパスワードポリシーを設定できます。

メモ: アカウント認証にシングルサインオンを設定している場合は、[Password Policy] ページを利用できません。

高度なパスワードポリシーを設定するには

1. 左側のナビゲーションウィンドウ枠の[Policy Management]で、[Password Policy] をクリックします。
2. [Password Policy]セクションの[Advanced Password Policy]で、パスワードポリシーに含める必要条件を選択します。

   詳しくは次の表を参照してください。

Enforce Password History	この必要条件を選択して、保存する過去のパスワードの数の値を入力します。ユーザーは、現在のパスワードを保存されているパスワードに変更できません。
Maximum Password Age	この必要条件を選択して、パスワードの変更が必要になる日数の値を入力します。
Minimum Password Age	この必要条件を選択して、パスワードの変更が必要になる最短日数の値を入力します。このオプションは、ユーザーがパスワードを変更できる頻度を制御します。
Minimum Password Length	この必要条件を選択して、パスワードの最も短い文字数の値を入力します。
Password Must Meet Complexity Requirements	この必要条件を選択して、次のパスワードの複雑さの必要条件を 3 つまで選択します。 ■ [Use base-10 digits characters in password]: 0 から 9 までの数字が 1 つ以上必要です。 ■ [Use lowercase characters in password]: 小文字が 1 つ以上必要です。 ■ [Use non-alphanumeric characters in password]: 記号が 1 つ以上必要です。 ■ [Use uppercase characters in password]: 大文字が 1 つ以上必要です。
Prevent Username in Passwords	ユーザーがパスワードに自分のユーザー名を使用できないようにするには、この必要条件を選択します。

3 次回ログイン時にパスワードを変更するようにすべてのユーザーに求める場合は、必要に応じて、[Enforce the password policies for all users]を選択します。

メモ: このオプションを選択すると、パスワードが指定した必要条件を満たす場合でも、すべてのユーザーが、次回ログイン時にパスワードを変更する必要があります。このオプションを選択しない場合、ユーザーは、パスワードが指定された必要条件を満たしていない場合でも、パスワードの期限が切れるまでパスワードを変更する必要はありません。

4 [Save]をクリックします。

Enterprise Vault.cloud アクセス用の信頼できるネットワークの設定

デフォルトでは、ユーザーは、任意のインターネットプロトコル (IP) アドレスから Enterprise Vault.cloud にアクセスできます。[Set Trusted Networks]ページから、特定のアドレス範囲へのアクセスを制限できます。

Enterprise Vault.cloud アクセス用に信頼できるネットワークを設定するには

1 左側のナビゲーションウィンドウ枠の[Policy Management]で、[Set Trusted Networks]をクリックします。

2 [Starting]フィールドに、アドレス範囲の開始 IP アドレスを入力します。

3 [Ending]フィールドに、アドレス範囲の終了 IP アドレスを入力します。

4 アクセスを制限する Enterprise Vault.cloud にチェックマークを付けます。

メモ: [Manage]を選択すると、Archive Administration へのアクセスが制限され、[Discovery/Personal]を選択すると、Discovery.cloud と Personal.cloud へのアクセスが制限されます。

5 アドレス範囲の制限を追加するには、[Add]をクリックします。

6 [Save]をクリックします。

メモ: アドレス範囲の制限を追加した後、[Edit]をクリックして変更を加えるか、[Delete]をクリックして制限を解除します。

7

分類

この章では以下の項目について説明しています。

分類について

構造化されていないデータがビジネス環境に累積すると、ビジネスまたは法的な価値のあるコンテンツをアーカイブするか削除するかの決断が難しくなります。分類ポリシーに基づいてデータを分類および整理すると、データ管理の意思決定を簡略化できます。

会社で Veritas Information Classifier サービスを有効にしている場合、Veritas Information Classifier で有効なポリシーに一致する Enterprise Vault.cloud の受信電子メールに、このサービスで分類タグを割り当てることができます。Discovery.cloud ユーザーは、調査や eDiscovery の間に、分類タグでタグ付けされた電子メールを検索できます。

[classification administrator]の役割を持つ管理者は、Archive Administration から Veritas Information Classifier にアクセスして、組織が使用するポリシーを有効化できます。各ポリシーは、関連する 1 つ以上の分類タグを電子メールに割り当てるために、電子メールが満たす必要がある条件を指定します。組み込みポリシーは、電子メールを分類するための基準となる、多くの規制上の必要条件や企業の規格に対応しています。

たとえば、個人識別情報を検出するポリシーを通じて、一般データ保護規則 (GDPR) などのプライバシー規制に対応できます。個人識別情報 (PII) ポリシーは、クレジットカード番号、電子メールアドレス、生年月日、パスポート番号、および運転免許証番号などのコンテンツで検索します。Enterprise Vault.cloud で受信する電子メールがポリシーの基準

に一致した場合、関連する PII 分類タグが電子メールヘッダーに割り当てられます。Discovery.cloud レビュー担当者は、割り当てられている PII タグを使用して電子メールを検索できます。このように、分類は、組織の規制要件を満たすという側面において、レビューする電子メールの数を削減するために役立ちます。

分類ポリシーと分類タグの設定方法について詳しくは、Veritas Information Classifier で提供されているヘルプを参照してください。

分類タグを含む電子メールの処理について詳しくは、『Discovery.cloud ユーザーガイド』を参照してください。

電子メールの分類方法

会社で Veritas Information Classifier サービスを有効にしている場合、Veritas Information Classifier で有効なポリシーに一致する Enterprise Vault.cloud の受信電子メールに、このサービスで分類タグを割り当てることができます。

Veritas Information Classifier でポリシーが有効になったら、Enterprise Vault.cloud が取り込む新しい電子メールに対して分類処理が実行されます。注意:

- ポリシーに関連付けられている分類タグは、ポリシーが有効化されたあとに Enterprise Vault.cloud に取り込まれた電子メールのうち、一致するものにのみ適用されます。以前にアーカイブされている電子メールには、タグは付けられません。
- システム管理者が分類ポリシーを変更したり無効にした場合、その変更は、それ以降 Enterprise Vault.cloud に取り込まれた電子メールに影響します。既存のアーカイブ済み電子メールには、変更は反映されません。たとえば、以前に有効にした分類ポリシーを無効にした場合、ポリシーに一致した結果としてタグ付けされたアーカイブ済みの電子メールは、Enterprise Vault.cloud でタグが付いたままになります。

メモ: 分類タグは、Veritas Information Classifier を介してのみ割り当てられます。他の種類のタグとは異なり、分類タグの割り当てや削除は手動で実行できません。

分類を設定する手順

表 7-1 は、Enterprise Vault.cloud に取り込まれた電子メールに対して、Veritas Information Classifier を使用して分類を設定する手順を示します。

表 7-1 分類を設定するプロセス

手順	説明	詳細情報
手順 1	Veritas Information Classifier サービスが、Enterprise Vault.cloud で会社向けに有効になっていることを確認します。	組織で分類を有効にするには、Veritasのサービスとサポートにお問い合わせください。

手順	説明	詳細情報
手順 2	Veritas Information Classifier への必要なアカウントアクセス権を設定します。	必要なアカウントに、[classification administrator]の役割を割り当てます。 p.69 の「役割管理について」を参照してください。
手順 3	Veritas Information Classifier にアクセスします。	Veritas Information Classifier には、Archive Administration から直接アクセスできます。 p.82 の「Veritas Information Classifier へのアクセス」を参照してください。
手順 4	必要な分類ポリシーを決定して、これらのポリシーを有効化します。 必要な場合は、カスタムポリシーを作成できます。	Veritas Information Classifier のヘルプを参照してください。 p.83 の「カスタム分類ポリシーで使用する Enterprise Vault.cloud 項目のプロパティ」を参照してください。

Veritas Information Classifier へのアクセス

[classification administrator]の役割を持つアカウントは、Archive Administration から Veritas Information Classifier にアクセスできます。

Veritas Information Classifier にアクセスするには

- Archive Administration の左ウィンドウ枠で、[Classification]ノードをクリックします。

メモ: [Classification]ノードは、[classification administrator]の役割が割り当てられているアカウントにのみ表示されます。.

Veritas Information Classifier が別のブラウザタブの[Policies]ページに表示されます。

Veritas Information Classifier が初めて表示されたときは、リストの最初の分類ポリシーが選択されています。この最初のポリシーを選択解除し、有効にするポリシーの検索を実行する必要がある場合があります。

分類ポリシーの有効化について詳しくは、Veritas Information Classifier のヘルプを参照してください。

メモ: [Veritas Information Classifier]タブが表示されている間に改めて[Classification]ノードをクリックすると、Enterprise Vault.cloud は、既存の[Veritas Information Classifier]タブをアクティブ化しようとします。ブラウザとその設定に応じて、タブを手動でアクティブ化する必要がある場合があります。情報が最新であることを保証するには、必要に応じてアクティブ化されたタブの内容を更新します。

カスタム分類ポリシーで使用する Enterprise Vault.cloud 項目のプロパティ

Enterprise Vault.cloud は、項目にインデックスを付けるときに、項目のメタデータプロパティに項目に関する情報を入力します。この情報の例には、メッセージ作成者の表示名と電子メールアドレス、アーカイブされた日付、項目のファイルサイズが含まれます。

インデックス付き項目には、多数のプロパティを設定できますが、分類の目的には 1 つのサブセットのみが対象となります。Enterprise Vault.cloud は、このプロパティのサブセットとそれに関連付けられた値を、分類のために Veritas Information Classifier に渡します。カスタムの Veritas Information Classifier ポリシーを作成する際には、ポリシーの条件を定義するときに、ユーザー設定の日付、カスタム番号、またはカスタム文字列の各フィールドで、これらのプロパティの名前を入力できます。

表 表 7-2 に、Enterprise Vault.cloud が Veritas Information Classifier に渡す項目のプロパティを示します。

表 7-2 Veritas Information Classifier に渡される項目のプロパティ

プロパティ	種類	説明
adat	日付	項目をアーカイブした日付。
audn	文字列	作成者の表示名と、該当する場合は項目が誰の代わりに送信されたかを示す表示名。
auea	文字列	作成者の電子メールアドレスと、該当する場合は項目が誰の代わりに送信されたかを示す電子メールアドレス。
date	日付	作成日、送信日、受信日、またはアーカイブ日。
natc	数値	添付ファイルの数。
nrcp	数値	受信者の数 (宛先、CC、BCC の受信者の合計)
rbdn	文字列	BCC 受信者の表示名。
rbea	文字列	BCC 受信者の電子メールアドレス。
rcdn	文字列	CC 受信者の表示名。
rcea	文字列	CC 受信者の電子メールアドレス。
rtdn	文字列	宛先受信者の表示名。
rtea	文字列	宛先受信者の電子メールアドレス。
size	数値	項目のサイズ (KB 単位)。
subj	文字列	件名またはタイトル。

表 表 7-3 に、Enterprise Vault.cloud が Veritas Information Classifier に渡すメッセージ添付ファイルのプロパティを示します。

表 7-3 Veritas Information Classifier に渡される添付ファイルのプロパティ

プロパティ	種類	説明
a_dat	日付	添付ファイルの作成日、送信日、受信日、またはアーカイブ日。
a_dtyp	文字列	添付ファイルのデータの種類。たとえば、DOCX、XSLX、MSG などがあります。

プロパティ	種類	説明
a_size	数値	添付ファイルのサイズ (KB 単位)。
a_subj	文字列	添付ファイルのファイル名、またはメッセージの場合は件名。

メモ: 分類機能は、添付ファイルをファイルとして処理します。このため、添付ファイルが電子メールメッセージの場合、その送信者情報と受信者情報を分類には使用できません。

カスタム分類ポリシーの作成について詳しくは、Veritas Information Classifier のヘルプを参照してください。

8

認証管理

この章では以下の項目について説明しています。

Enterprise Vault.cloud 認証サービスの設定

このセクションでは、Active Directory フェデレーションサービス (AD FS) 環境と連携するための、Enterprise Vault.cloud 認証サービスの設定方法について説明します。

Enterprise Vault.cloud では現在、AD FS のバージョン 2.0、2.1 および 3.0 をサポートしています。その他のバージョンの AD FS は、現在サポートされていません。

メモ: Enterprise Vault.cloud の互換性リストに、その他のシングルサインオンソリューションについてと、それらの設定についてサポートを受ける方法についての情報が提供されています。

Enterprise Vault.cloud 互換性リストを参照してください。

Enterprise Vault.cloud 認証サービスと AD FS 環境を設定すると、Enterprise Vault Personal.cloud ユーザーにシングルサインオンアクセスを提供できます。

メモ: ここに示す手順は、Personal.cloud ユーザーに対するシングルサインオンアクセスのプロビジョニングにのみ該当します。Discovery.cloud と Archive Administration に対するプロビジョニングについてサポートが必要な場合は、Veritasのサービスとサポートにお問い合わせください。

表 8-1 に、AD FS 環境と連携するための Enterprise Vault.cloud 認証サービスの設定手順をまとめます。

表 8-1 Enterprise Vault.cloud 認証サービスの設定

手順	処理	参照先
手順 1	Archive Administration で、[Policy Manager]の役割に対して、[Authentication Settings]の権限を有効にします。	p.87 の「ポリシーマネージャの役割に対する認証設定権限の有効化」を参照してください。
手順 2	[Authentication Settings]の権限が有効になった[Policy Manager]の役割を、管理者に割り当てます。	p.88 の「管理者へのポリシーマネージャの役割の割り当て」を参照してください。
手順 3	[Authentication Management]ページで、組織の認証方法として AD FS を選択します。	p.88 の「認証方法の選択」を参照してください。
手順 4	AD FS 環境から生成したトークン署名証明書をアップロードします。	p.89 の「トークン署名証明書のアップロード」を参照してください。
手順 5	組織の ID プロバイダの URL を検証します。	p.90 の「ID プロバイダの URL の検証」を参照してください。
手順 6	Personal.cloud ユーザーのシングルサインオンをアクティブ化します。	p.91 の「シングルサインオンのアクティブ化」を参照してください。

ポリシーマネージャの役割に対する認証設定権限の有効化

Archive Administration の[Authentication Management]ページでは、Enterprise Vault.cloud 認証サービスを設定できます。[Authentication Settings]の権限が有効になっている管理者のみが、[Authentication Management]ページにアクセスできます。デフォルトでは、[System Administrator]の役割のみに[Authentication Settings]の権限が有効になっています。必要な場合は、この権限を[Policy Manager]の役割に対して有効にし、この役割を、システム管理者以外の管理者に割り当てることができます。[Policy Manager]の役割には限定的な権限しかないため、管理者に完全なシステム管理者権限を提供する代わりに[Authentication Settings]の権限を付与できます。

ポリシーマネージャの役割に対して認証設定権限を有効化するには

1 左側のナビゲーションウィンドウ枠の[Role Management]で、[Administration Roles]をクリックします。

2 [Built-in Roles]セクションで、[Policy Manager]をクリックして[Authentication Settings]を選択します。

3 [Administration Roles]ページの上部で、[Save]をクリックします。

管理者へのポリシーマネージャの役割の割り当て

ポリシーマネージャの役割に対して認証設定権限を有効にした後、Enterprise Vault.cloud 認証サービスを管理する管理者に、この役割を割り当てることができます。

メモ: [Authentication Management]ページにアクセスするため、管理者は Archive Administration からログアウトし、再度ログインする必要がある場合があります。

管理者にポリシーマネージャの役割を割り当てるには

1 左側のナビゲーションウィンドウ枠で、[Assign Accounts]をクリックします。

2 ユーザーリストから、役割を割り当てる管理者を選択します。

3 [Role Change]ページで、[Policy Manager]を選択し、ページの上部の[Save]をクリックします。

認証方法の選択

Enterprise Vault.cloud 認証サービスを[Authentication Management]ページから設定できます。設定プロセスを開始するには、Personal.cloud ユーザーの認証に使用する認証方法として、AD FS を選択する必要があります。

メモ: 使用する認証方法として AD FS を選択すると、[Your Trust Information]セクションが表示されます。AD FS 環境を設定するときに、このセクションの[Entity ID]フィールドに提供されている値を使用する必要があります。エンティティ ID は、組織の場所によって異なります。組織のエンティティ ID を見つけることができない場合は、Veritasのサービスとサポートにお問い合わせください。

認証方法を選択するには

1 左側のナビゲーションウィンドウ枠の[Policy Management]ノードで、[Authentication Management]をクリックします。

2 [Setup Authentication]セクションの[Authentication Type]フィールドで、[Single Sign-On ADFS]を選択します。

メモ: AD FS 2.0、2.1 および 3.0 環境で、このオプションを選択できます。

---

3 Personal.cloud へのログインのために一意の ID プロバイダ (IdP) URL を設定した場合は、必要に応じて、[Unique OWA IdP]フィールドで[Yes]を選択します。

4 OWA IdP URL に一意のカスタマ ID (CID) を関連付ける必要がある場合は、必要に応じて、[Unique OWA CID]フィールドで[Yes]を選択します。

メモ: [Unique OWA CID]フィールドは、[Unique OWA IdP]フィールドで[Yes]を選択した場合にのみ表示されます。Veritasのサービスとサポートからの指示がない限り、[Unique OWA CID]フィールドで[Yes]を選択しないようにすることをお勧めします。このオプションに[Yes]を選択すると、Archive Administration は、シングルサインオンをアクティブ化したときに提供された値を、OWA IdP URL に自動的に追加します。

---

5 表示される指示を確認したら、[I have read the instructions for setting the provided Entity ID and created my public key for upload]を選択します。

6 [Save]をクリックして、次の手順に進みます。

トークン署名証明書のアップロード

組織の認証方法として AD FS を選択したら、AD FS 環境からトークン署名証明書をアップロードする必要があります。

p.92 の「Enterprise Vault.cloud と連携するための AD FS の設定」を参照してください。

[Authentication Management]ページの[Upload Your Public Key]セクションから、トークン署名証明書をアップロードできます。[Upload Your Public Key]セクションは、[Setup Authentication]セクションの完了後に表示されます。

トークン署名証明書をアップロードするには

1 [Upload Your Public Key]セクションで[Browse and Upload]をクリックします。

2 表示されたウィンドウで、生成したトークン署名証明書のファイルの場所に移動します。

メモ: アップロードするトークン署名証明書は、.cer のファイル拡張子である必要があります。

---

3 [Public Key Upload]の確認ウィンドウで、[Return to Setup]をクリックして次の手順に進みます。

ID プロバイダの URL の検証

トークン署名証明書をアップロードした後は、組織の ID プロバイダの URL を検証する必要があります。[Authentication Management]ページの[Validate Relying Trust]セクションから、必要に応じて、ID プロバイダの URL と OWA ID プロバイダの URL を検証できます。[Validate Relying Trust]セクションは、[Upload Your Public Key]セクションの完了後に表示されます。

ID プロバイダの URL を検証するには

1 [Validate Relying Trust]セクションの[Identity Provider URL]フィールドに、組織の ID プロバイダの URL を入力します。

メモ: ID プロバイダの URL では、通常、AD FS サーバーまたは AD FS プロキシの完全修飾ドメイン名の後に adfs/ls が続きます。たとえば、完全修飾ドメイン名が example.com の adfs という名前の AD FS サーバーの ID プロバイダの URL は、https://adfs.example.com/adfs/ls になります。Enterprise Vault.cloud 認証サービスは、現在、ダッシュを含む ID プロバイダの URL をサポートしません。ID プロバイダの URL にダッシュが含まれる場合には、Veritasのサービスとサポートにお問い合わせください。

---

2 必要な場合は、[OWA Identity Provider URL]フィールドに、組織の OWA ID プロバイダの URL を入力します。

メモ: [OWA Identity Provider URL]フィールドは、[Setup Authentication]セクションの[Unique OWA IdP]フィールドで[Yes]を選択した場合にのみ表示されます。

---

3 [Validate]をクリックします。

4 [Validation Successful]メッセージが表示されたら、[Save]をクリックして次の手順に進みます。

シングルサインオンのアクティブ化

ID プロバイダの URL を検証した後は、Personal.cloud ユーザーのシングルサインオンをアクティブ化する必要があります。[Authentication Management]ページの[Activate SSO]セクションで、シングルサインオンをアクティブ化できます。[Activate SSO]セクションは、[Validate Relying Trust]セクションの完了後に表示されます。

シングルサインオンをアクティブ化するには

1 [Activate SSO]セクションで、[Activate SSO]をクリックします。

2 [Activation Successful]のメッセージが表示されたら、[Application Login URL(s)]セクションにリストされる URL を Personal.cloud ユーザーに提供できます。

メモ: 認証サービスを設定してシングルサインオンをアクティブ化する前にユーザーに提供した Enterprise Vault.cloud クレデンシャルは、引き続き Personal.cloud へのログインに使用できます。

9

AD FS 設定ガイド

この章では以下の項目について説明しています。

Enterprise Vault.cloud と連携するための AD FS の設定

このセクションでは、Enterprise Vault.cloud 認証サービスと連携するための、Active Directory フェデレーションサービス (AD FS) 環境の設定方法について説明します。AD FS 環境と Enterprise Vault.cloud 認証サービスを設定すると、Enterprise Vault Personal.cloud ユーザーにシングルサインオンアクセスを提供できます。

Enterprise Vault.cloud は現在、AD FS 2.0、2.1 および 3.0 をサポートしています。その他のバージョンの AD FS は、現在サポートされていません。

メモ: ここに示す手順は、Personal.cloud ユーザーに対するシングルサインオンアクセスのプロビジョニングにのみ該当します。Discovery.cloud と Archive Administration に対するプロビジョニングについてサポートが必要な場合は、Veritasのサービスとサポートにお問い合わせください。

次の表は、Enterprise Vault.cloud 認証サービスと連携するために必要な AD FS の設定手順を示します。

表 9-1 Enterprise Vault.cloud 認証サービスと連携するための AD FS の設定手順

処理	参照先
AD FS の管理コンソールを使用して、Enterprise Vault.cloud に対する証明書利用者信頼を追加します。	p.93 の「Enterprise Vault.cloud に対する証明書利用者信頼の追加」を参照してください。
Archive Administration でのアップロード用に、トークン署名証明書を AD FS の管理コンソールから生成およびエクスポートします。	p.96 の「トークン署名証明書の生成」を参照してください。

ここに示す手順では、AD FS 環境の設定方法に関する情報は提供しません。AD FS 環境の設定に関する情報は、次の Microsoft 社のマニュアルを参照してください。

- AD FS 2.0 (Windows Server 2008 R2)
- AD FS 2.1 (Windows Server 2012)
- AD FS 3.0 (Windows Server 2012 R2)

SSO のネットワーククロック同期の必要条件

Enterprise Vault.cloud は、Secure Assertion の認証および権限の交換の間に提示される NotBefore と NotOnOrAfter の条件を受け入れます。

SAML 交換中に Enterprise Vault.cloud に提示される値を理解するために、SSO オーソリティや ID プロバイダの設定を確認することをお勧めします。NotBefore と NotOnOrAfter の値とドリフト値が、セキュリティを維持しつつ、誤って認証の問題が発生することがないように設定されていることを確認する必要があります。Enterprise Vault.cloud は、外部のいくつかの UTC 時間ソースと同期しますが、ネットワーク間のドリフトを最小限に抑えるため、同様の設定にすることをお勧めします。AD FS 環境でのこれらの値の設定方法については、Microsoft 社のマニュアルを参照してください。

時間の不一致が許可されるようにするための NotBeforeSkew 条件の設定方法について詳しくは、サポート Web サイトで次の記事を参照してください。

http://www.veritas.com/docs/000097921

Enterprise Vault.cloud に対する証明書利用者信頼の追加

AD FS 環境を設定する最初の手順は、Enterprise Vault.cloud に証明書利用者信頼を追加することです。

メモ: エンドポイントのインデックス値は、デフォルト値のまま変更しないことをお勧めします。エンドポイントのインデックス値を変更すると、Enterprise Vault.cloud 認証サービスが AD FS 環境で適切に動作しなくなる場合があります。

Enterprise Vault.cloud に証明書利用者信頼を追加するには

1. 次のいずれかの操作を行って、AD FS の管理コンソールにアクセスします。
   - AD FS 2.0 の場合、[スタート]をクリックして[管理ツール]を選択し、[AD FS 2.0 の管理]をクリックします。
   - AD FS 2.1 の場合、[スタート]をクリックし、[検索]フィールドに「AD FS の管理」と入力して、Enter キーを押します。
   - AD FS 3.0 の場合、[サーバー マネージャー]で[ツール]をクリックして、[AD FS の管理]を選択します。
2. AD FS の管理コンソールの左ウィンドウ枠で、[信頼関係]を展開し、[証明書利用者信頼]を右クリックして、[証明書利用者信頼の追加]をクリックします。
3. [証明書利用者信頼の追加ウィザード]の[ようこそ]パネルで、[スタート]をクリックします。
4. [データ ソースの選択]パネルで、[証明書利用者についてのデータを手動で入力する]を選択して、[次へ]をクリックします。
5. [表示名の指定]パネルの[表示名]フィールドに、「Cloud Archive」と入力し、[次へ]をクリックします。
6. [プロファイルの選択]パネルで、次のいずれかの操作を行います。
   - AD FS 2.0 の場合は、[AD FS 2.0 プロファイル]を選択して[次へ]をクリックします。
   - AD FS 2.1 の場合は、[AD FS プロファイル]を選択して[次へ]をクリックします。
   - AD FS 3.0 の場合は、[AD FS プロファイル]を選択して[次へ]をクリックします。
7. [証明書の構成]パネルで[次へ]をクリックして、このオプションの手順をスキップします。

   メモ: 証明書は設定しないことをお勧めします。証明書を設定すると、Enterprise Vault.cloud 認証サービスが AD FS 環境で適切に動作しなくなります。

8. [URL の構成]パネルの[SAML 2.0 WebSSO プロトコルのサポートを有効にする]を選択します。

9 [URL の構成]パネルの[証明書利用者 SAML 2.0 SSO サービスの URL]フィールドに、Archive Administration の[Authentication Management]ページにある[Your Trust Information]セクションのエンティティ ID を入力して、[次へ]をクリックします。

メモ: エンティティ ID は、組織の場所によって異なります。組織のエンティティ ID を見つけることができない場合は、Veritasのサービスとサポートにお問い合わせください。

---

10 [識別子の構成]パネルの[証明書利用者信頼の識別子]フィールドにエンティティ ID を再入力し、[追加]をクリックして識別子を追加して、[次へ]をクリックします。

11 AD FS 3.0 の場合にのみ、[今すぐ多要素認証を構成しますか?]パネルで、[現時点ではこの証明書利用者信頼に多要素認証を構成しない。]を選択して、[次へ]をクリックします。

12 [発行承認規則の選択]パネルで、[すべてのユーザーに対してこの証明書利用者へのアクセスを許可する]を選択し、[次へ]をクリックします。

13 [信頼の追加の準備完了]パネルで、構成済みの設定を確認して[次へ]をクリックします。

14 [終了]パネルで、[ウィザードの終了時にこの要求に証明書利用者信頼の [発行承認規則の編集] ダイアログを開く]を選択して、[閉じる]をクリックします。

15 [Cloud Archive の要求規則の編集]ウィンドウで、[規則の追加]をクリックします。

16 [変換要求規則の追加ウィザード]の[規則テンプレートの選択]パネルで、[要求規則テンプレート]フィールドの[LDAP 属性を要求として送信]を選択し、[次へ]をクリックします。

17 [規則の構成]パネルで、[要求規則名]セクションに「Cloud Archive への要求の送信」と入力します。

18 [規則の構成]パネルの[属性ストア]セクションで、[Active Directory]を選択します。

19 [規則の構成]パネルの[LDAP 属性の出力方向の要求の種類への関連付け]セクションで、LDAP 属性と出力方向の要求の種類のセットを次のように選択します。

LDAP 属性	出力方向の要求の種類
E-Mail-Addresses	電子メールアドレス
Given-Name	名
Surname	姓

20 [規則の構成]パネルで、[完了]をクリックして[変換要求規則の追加ウィザード]を閉じます。

21 [Cloud Archive の要求規則の編集]ウィンドウで、[OK]をクリックしてウィンドウを閉じます。

22 AD FS の管理コンソールの[証明書利用者信頼]ウィンドウ枠で、[Cloud Archive]を選択します。

23 [アクション]ウィンドウ枠の[Cloud Archive]セクションで、[プロパティ]をクリックします。

24 [Cloud Archive のプロパティ]ウィンドウで、[詳細]タブを選択します。

25 [セキュア ハッシュ アルゴリズム]フィールドで、次のアルゴリズムのいずれかを選択します。

- SHA-1
- SHA-256

メモ: SHA-1 アルゴリズムを選択することをお勧めします。

---

26 [OK]をクリックして、[Cloud Archive のプロパティ]ウィンドウを閉じます。

トークン署名証明書の生成

AD FS 環境を設定する 2 番目の手順は、Archive Administration の[Authentication Management]ページのアップロード用にトークン署名証明書を生成することです。

メモ: 証明書のデフォルトのキーサイズである 2,048 ビットを使用することをお勧めします。現在サポートされている証明書の最大キーサイズは、4,096 ビットです。

トークン署名証明書を生成するには

1 次のいずれかの操作を行って、AD FS の管理コンソールにアクセスします。

- AD FS 2.0 の場合、[スタート]をクリックして[管理ツール]を選択し、[AD FS 2.0 の管理]をクリックします。
- AD FS 2.1 の場合、[スタート]をクリックし、[検索]フィールドに「AD FS の管理」と入力して、Enter キーを押します。
- AD FS 3.0 の場合、[サーバー マネージャー]で[ツール]をクリックして、[AD FS の管理]を選択します。

2 AD FS の管理コンソールの左ウィンドウ枠で、[サービス]を展開して[証明書]を選択します。

3 [証明書]ウィンドウ枠で、トークン署名のセクションの下に表示されている証明書を選択します。

4 [アクション]ウィンドウ枠で、[証明書の表示]をクリックします。

5 [証明書]ウィンドウの[詳細]タブを選択し、次に[ファイルへコピー]をクリックします。

6 [証明書のエクスポート ウィザード]の[ようこそ]パネルで、[次へ]をクリックします。

7 [エクスポート ファイルの形式]パネルで、[Base 64 encoded X.509 (.CER)]を選択して[次へ]をクリックします。

8 [エクスポートするファイル]パネルの[ファイル名]フィールドにファイルのパスを入力して、[次へ]をクリックします。

9 [完了]パネルで、指定した情報を確認して[終了]をクリックします。

10 [OK]をクリックして、エクスポートの確認ダイアログボックスを閉じます。証明書は、以前に指定したファイルの場所にエクスポートされます。

10

保持管理

この章では以下の項目について説明しています。

保持管理について

[Retention Management]セクションでは、アーカイブ済みメッセージを Enterprise Vault.cloud に保持する期間を決定する設定やポリシーを管理できます。デフォルトでは、Enterprise Vault.cloud はアーカイブ済みメッセージを無制限に保持します。必要な場合は、アーカイブ済みメッセージを定義した期間保持した後で、Enterprise Vault.cloud が、これらのメッセージを削除のために収集するように設定できます。

デフォルトの保持期間とは、アーカイブ済みメッセージが削除のために収集されるまでに保持される期間を決定する、グローバル設定です。グローバルな保持期間を設定し、ストレージの有効期限の設定を有効化すると、アーカイブ済みメッセージを削除するための収集が開始されます。毎日の収集イベントで、デフォルトの保持期間より長く保持されているすべてのメッセージは、14 日後に削除されるようにスケジュール設定されます。保持

管理者は、14 日間の猶予期間中に、削除がスケジュール設定されているアーカイブ済みメッセージの数を知らせる通知電子メールを毎日受信します。

メモ: アーカイブ済みメッセージのうち、事案レベル、検索レベル、またはメッセージレベルの法定保持が Enterprise Vault Discovery.cloud で適用されているメッセージは削除されません。

次のポリシーターゲットに関連付ける保持ポリシーを作成することで、アーカイブ済みメッセージの保持期間は、グローバルな保持期間より長くできます。

- 管理対象タグ: 作成してユーザーを割り当てるグローバルタグです。管理対象タグを作成して保持ポリシーを関連付けると、ユーザーは、アーカイブ済みメッセージにタグを適用して、保持期間を延長できます。関連付けられた保持ポリシーの保持期間によって、タグが付けられたメッセージが Enterprise Vault.cloud で保持される期間が決まります。
- Active Directory の配布グループ: Active Directory から ArchiveTools CloudLink を使用して同期される配布グループです。配布グループに保持ポリシーを関連付けると、そのグループのメンバーすべてのアーカイブ済みメッセージの保持期間が延長されます。関連付けられた保持ポリシーの保持期間によって、配布グループのメンバーのメッセージが Enterprise Vault.cloud で保持される期間が決まります。

メモ: アーカイブ済みメッセージは、最も長い保持期間に応じて保持されるため、保持期間がデフォルトの保持期間よりも長い保持ポリシーを作成する必要があります。

メモ: 管理対象タグと分類タグを混同しないでください。Veritas Information Classifier は、有効になっている分類ポリシーに一致する電子メールに分類タグを割り当てます。分類タグは、Discovery.cloud で表示できます。

デフォルトの保持期間の設定

デフォルトの保持期間は、アーカイブ済みメッセージが Enterprise Vault.cloud に保持される期間を決定します。デフォルトの保持期間を設定して、ストレージの有効期限の設定を有効化すると、Enterprise Vault.cloud からメッセージを削除するプロセスを開始できます。

デフォルトの保持期間を設定するには

1. 左側のナビゲーションウィンドウ枠で、[Retention Policies]をクリックします。
2. [Default Retention Period]セクションで、[Edit]をクリックします。

3 [Days]フィールドに、保持期間を入力します。

4 [Save]をクリックします。

メモ: デフォルトの保持期間の初回設定後は、既存の期間の編集のみを行えます。アーカイブ済みメッセージを削除するため、Enterprise Vault.cloud から収集する必要がなくなったら、ストレージの有効期限の設定を無効化できます。

保持ポリシーの作成

ポリシーターゲットに関連付ける保持ポリシーを作成することで、アーカイブ済みメッセージの保持期間は、デフォルトの保持期間より長くできます。保持ポリシーに関連付けられるポリシーターゲットには、管理対象タグと Active Directory の配布グループが含まれます。

保持ポリシーを作成するには

1 左側のナビゲーションウィンドウ枠で、[Retention Policies]をクリックします。

2 [Retention Policies]セクションで、[Create New]をクリックします。

3 [Create Retention Policy]ページの[Policy Name]フィールドに、ポリシーの名前を入力します。

4 [Retention Period]フィールドに、ポリシーの保持期間を日単位で入力します。

5 作成した保持ポリシーを有効化する場合は、[Policy Status]を[Enabled]に設定します。

6 必要な場合は、[Description]フィールドに、保持ポリシーの説明を入力します。

7 [Save]をクリックします。

保持ポリシーの編集

必要な場合は、既存の保持ポリシーの詳細を編集できます。編集できる詳細には、ポリシー名、保持期間、ポリシーの状態、およびポリシーの説明が含まれます。

保持ポリシーを編集するには

1 左側のナビゲーションウィンドウ枠で、[Retention Policies]をクリックします。

2 保持ポリシーリストの[Policy Name]列で、編集する保持ポリシーの名前をクリックします。

3 [Retention Policy Summary]ページの上部で、[Edit]をクリックします。

4 保持ポリシーの詳細を編集します。

5 [Save]をクリックします。

保持ポリシーの削除

必要な場合は、不要になった保持ポリシーを削除できます。

メモ: ポリシーターゲットに関連付けられている保持ポリシーは、削除できません。

保持ポリシーを削除するには

1 左側のナビゲーションウィンドウ枠で、[Retention Policies]をクリックします。

2 保持ポリシーリストの[Delete Policy]列で、[X]アイコンをクリックします。

3 表示されるダイアログボックスで[OK]をクリックして、削除を確認します。

保持ポリシーとポリシーターゲットの関連付け

保持ポリシーを作成した後に、ポリシーターゲットに関連付けられます。保持ポリシーに関連付けられるポリシーターゲットには、管理対象タグと Active Directory の配布グループが含まれます。

メモ: 保持ポリシーは、複数のポリシーターゲットに関連付けられます。ただし、各ポリシーターゲットは、1 つの保持ポリシーにのみ関連付けることができます。

保持ポリシーとポリシーターゲットを関連付けるには

1 左側のナビゲーションウィンドウ枠で、[Retention Policies]をクリックします。

2 保持ポリシーリストの[Policy Name]列で、保持ポリシーの名前をクリックします。

3 [Retention Policy Summary]ページの[Targets]セクションで、[Add]をクリックします。

4 [Policy Targets]ウィンドウで、関連付けるターゲットにチェックマークを付けます。

メモ: ターゲットの種類でフィルタして、すべてのターゲット、管理対象タグのみ、または配布グループのみを表示できます。

5 [Policy Targets]ウィンドウの上部で、[Add Targets]をクリックします。

保持ポリシーとポリシーターゲットの関連付け解除

必要な場合は、保持ポリシーの関連付けをポリシーターゲットから解除できます。

保持ポリシーの関連付けをポリシーターゲットから解除するには

1. 左側のナビゲーションウィンドウ枠で、[Retention Policies]をクリックします。
2. 保持ポリシーリストの[Policy Name]列で、保持ポリシーの名前をクリックします。
3. ターゲットリストの[Remove]列で[X]アイコンをクリックします。
4. 表示されるダイアログボックスで[OK]をクリックして、削除を確認します。

ストレージの有効期限設定の有効化および無効化

デフォルトの保持期間を設定したら、アーカイブ済みメッセージを削除するための収集が開始される前に、ストレージの有効期限設定を有効化する必要があります。

次の条件の 1 つ以上に一致するアーカイブ済みメッセージは、Enterprise Vault.cloud から削除されません。

- 事案レベル、検索レベル、またはメッセージレベルの法定保持が Enterprise Vault Discovery.cloud で適用されているメッセージ。
- 保持期間がデフォルトの保持期間を超える保持ポリシーに関連付けられている管理対象タグが適用されたメッセージ。
- 保持期間がデフォルトの保持期間を超える保持ポリシーに関連付けられている Active Directory 配布グループのメンバーのメッセージ。

メモ: Enterprise Vault.cloud から削除されたアーカイブ済みメッセージは、削除が完了すると取得できません。

ストレージの有効期限設定を有効化または無効化するには

1. 左側のナビゲーションウィンドウ枠で、[Storage Expiry]をクリックします。
2. ページの上部で、[Edit]をクリックします。
3. [Storage Expiry]セクションで、次のいずれかを行います。
   - [Daily]を選択して、ストレージの有効期限設定を有効化します。
   - [Never]を選択して、ストレージの有効期限設定を無効化します。
4. [Save]をクリックします。

ストレージの有効期限の状態テーブルの表示

デフォルトの保持期間を設定し、ストレージの有効期限の設定を有効化すると、アーカイブ済みメッセージを削除するための収集が開始されます。[Storage Expiry]ページから、削除するメッセージの各バッチについて、次の情報が含まれた状態テーブルを表示できます。

Date	バッチが作成された日時を示します。
Number of Emails	バッチ内のアーカイブメッセージの数を示します。
Expiration Status	バッチの現在の状態を示します。 ■ [Completed]: メッセージのバッチは削除されました。 ■ [In progress]: メッセージのバッチは削除処理中です。 ■ [Not started]: メッセージのバッチは、削除のキューにあります。

ストレージの有効期限の状態テーブルを表示するには

1. 左側のナビゲーションウィンドウ枠で、[Storage Expiry]をクリックします。
2. 必要な場合は、[Expiration Status]フィールドで次のオプションのいずれかを選択して、テーブルをフィルタします。
   - [All]: 削除するメッセージのすべてのバッチの状態を表示する場合に選択します。
   - [Not Started]: 削除のキューにあるメッセージのバッチのみを表示する場合に選択します。
   - [In Progress]: 削除中のメッセージのバッチのみを表示する場合に選択します。
   - [Completed]: 削除されたメッセージのバッチのみを表示する場合に選択します。

11

継続性管理

この章では以下の項目について説明しています。

Email Continuity について

Email Continuity は、メールサーバーの停止中に、Personal.cloud ユーザーが電子メールメッセージを送受信することを可能にするアドオン機能です。

受信電子メールメッセージは、通常、電子メールのセキュリティプロバイダを経由してメールサーバーにルーティングされます。メールサーバーに到達したメッセージは、Enterprise Vault.cloud にジャーナリングされます。メールサーバーからの発信メッセージは、その受信者に到達する前に、通常 Enterprise Vault.cloud にジャーナリングされます。ただし、メールサーバーの停止中、メールサーバーは電子メールメッセージの受信、送信またはジャーナリングを行えません。

Email Continuity を使用すると、メールサーバーが使用できないときに、Enterprise Vault.cloud を電子メールのセカンダリゲートウェイとして使用するように、電子メールの

セキュリティプロバイダが設定されます。メールサーバーの停止中に、電子メールのセキュリティプロバイダは、メールを Enterprise Vault.cloud にルーティングし、ユーザーは Personal.cloud を通じて電子メールメッセージの送受信を行えます。メールサーバーの停止が終わると、Email Continuity サービスは、停止中にメールサーバーまたはリレーサーバーで送受信された電子メールメッセージすべてを、正常な配信のために自動的に消去します。

メモ: 停止中に、Email Continuity サービスは、最大 7 日間 5 分おきに、メールサーバーへのメッセージの消去を試みます。

Email Continuity の前提条件

Email Continuity を設定する前に、互換性のある電子メールセキュリティプラットフォームを使用していることを確認する必要があります。

Email Continuity がサポートする電子メールセキュリティプラットフォームについて詳しくは、Enterprise Vault.cloud 互換性リストを参照してください。

Email Continuity の設定

表 11-1 に、Email Continuity の設定に必要な手順を示します。

表 11-1 Email Continuity の設定手順

手順	処理	参照先
手順 1	メールサーバーへの Email Continuity サービスのプロビジョニングについて、Veritasのサービスとサポートに問い合わせます。	p.106 の「メールサーバーへの Email Continuity サービスのプロビジョニング」を参照してください。
手順 2	Email Continuity の IP の範囲を、必要に応じてファイアウォールとメールサーバーのホワイトリストに追加します。	p.107 の「Email Continuity の IP の範囲のファイアウォールとメールサーバーのホワイトリストへの追加」を参照してください。
手順 3	Email Continuity が電子メールのセカンダリルートとして使用されるように、電子メールのセキュリティプロバイダを設定します。	p.107 の「電子メールのセキュリティプロバイダのルーティング設定の更新」を参照してください。
手順 4	Email Continuity が正しく設定されていることを確認するために、新しい設定をテストします。	p.107 の「Email Continuity の設定のテスト」を参照してください。

メールサーバーへの Email Continuity サービスのプロビジョニング

Veritasのサービスとサポートに依頼して、会社に Email Continuity サービスをプロビジョニングし、Email Continuity の設定に必要な追加情報を受け取る必要があります。

メールサーバーに Email Continuity サービスをプロビジョニングするには

1. メールサーバーで使用するすべてのインバウンドドメインのリストを取得します。
2. Enterprise Vault.cloud Archive Administration にログインします。
3. [My Config]、[Services]の順に移動して、[Domains]セクションまでスクロールします。
4. [Domains]のリストに、メールサーバーの受信ドメインすべてが表示されるかどうかを調べます。

   表示されないドメインがある場合は、それらのドメインを書き留めます。
5. Veritasのサービスとサポートに問い合わせて、次のようにします。
   - 組織の Enterprise Vault.cloud サービスとして Email Continuity の追加を希望する旨を、Veritasのサービスとサポートに伝えます。
   - 手順 4 で、メールサーバーのインバウンドドメインのいずれかが Archive Administration に設定されていないことがわかった場合は、会社の Enterprise Vault.cloud の設定に必要なインバウンドドメインを追加するようにVeritasのサービスとサポートに依頼します。
   - Veritasのサービスとサポートに、Email Continuity を有効にする各メールサーバー名の IP アドレスとドメイン名を伝えます。これで、会社の Email Continuity サービスのプロビジョニングが可能になります。

     メモ: Email Continuity は、ドメインごとに 1 つのメールサーバーにのみ設定できます。
   - 後の手順で使用するために、Veritasのサービスとサポートから次の情報を入手します。
     - Enterprise Vault.cloud インスタンス用の Enterprise Vault.cloud Email Continuity の IP の範囲。
     - 地理的な地域用の Enterprise Vault.cloud Email Continuity メールサーバードメイン。

Email Continuity の IP の範囲のファイアウォールとメールサーバーのホワイトリストへの追加

Veritasのサービスとサポートから取得した Email Continuity の IP の範囲を、必要に応じて、ファイアウォールのホワイトリストとメールサーバーのホワイトリストに追加する必要があります。

Email Continuity の IP の範囲をファイアウォールとメールサーバーのホワイトリストに追加するには

1. ファイアウォールとメールサーバーのコントロールパネルにログオンします。
2. Enterprise Vault.cloud インスタンスの IP の範囲をポート 25 (SMTP) に追加します。
3. Email Continuity を、リレーサーバーではなくメールサーバーにメッセージを戻して消去する設定にする場合は、Exchange の受信コネクタまたは Domino の許可されたホストに、同じ IP アドレスの範囲を追加します。この手順により、メールサーバーが、戻されたメッセージをユーザーにリレーできるようになります。

電子メールのセキュリティプロバイダのルーティング設定の更新

電子メールのセキュリティプロバイダを設定して、ルーティングリスト内の最後のルートとして、Email Continuity に電子メールがルーティングされるようにする必要があります。電子メールのセキュリティプロバイダは、通常のメッセージルートが失敗したときに、Email Continuity サーバードメインにメールをルーティングする必要があります。

この手順には、Veritasのサービスとサポートから入手した、Enterprise Vault.cloud Email Continuity メールサーバーのドメインが必要です。

電子メールのセキュリティプロバイダのルーティング設定を更新するには

1. 電子メールのセキュリティプロバイダのコントロールパネルにログオンします。
2. Enterprise Vault.cloud Email Continuity のメールサーバードメインを、メールをルーティングするときに最後に使用するドメインとして追加します。

Email Continuity の設定のテスト

Email Continuity が正しく設定されており、メールサーバーでエラーが発生した時に正常に動作することを確認する必要があります。

Email Continuity の設定をテストするには

1. Veritasのサービスとサポートに問い合わせて、Email Continuity の接続性をテストし、消去して戻す機能が正しく設定されていることを確認します。
2. 通常業務時間外などの都合の良いときに、メールサーバーの SMTP レシーバを一時停止して、メールサーバーのエラーをシミュレートします。この処理によって、電子メールのセキュリティプロバイダから Email Continuity にフェールオーバーが行われます。その後、次の各処理を試行します。
   - Personal.cloud の自分のアカウントで、外部の電子メールアドレスから電子メールを受け取れることをテストします。
   - Personal.cloud から外部の電子メールアドレスに電子メールを送信できることをテストします。
   - Personal.cloud から内部の電子メールアドレスに電子メールを送信できることをテストします。
3. 電子メールサービスを再起動し、以前の手順で Personal.cloud で送受信したテスト電子メールが消去されてメールサーバーに戻されたことを確認します。

Email Continuity の管理

Archive Administration の［Continuity Management］ページで、Email Continuity の状態をユーザーに表示し、サービスの概要を参照するためのオプションを設定できます。

Email Continuity を管理するには

1. 左側のナビゲーションウィンドウ枠で、［Continuity Management］をクリックします。

   メモ: ［Continuity Management］ページは、組織が Email Continuity のサブスクリプションを利用している場合にのみ表示されます。

2. ［Email Continuity Settings］セクションで［Indicate EC Active］を選択して、メールサーバーの停止中にユーザーに通知が送られるようにします。
3. ［Email Continuity Summary］セクションで、停止中に Email Continuity サービスで処理された電子メールメッセージの数について提供される情報を確認します。

Email Continuity についてよく寄せられる質問

次のよく寄せられる質問は、Email Continuity について、詳細な情報を提供します。

- Email Continuity の設定時に、ファイアウォールまたはメールサーバーのホワイトリストにどの IP の範囲を追加する必要がありますか。

IP の範囲は、地域によって異なります。詳しくは、Veritasのサービスとサポートにお問い合わせください。

- メールサーバーの停止中にどのように Email Continuity を有効化できますか。
  Email Continuity は、停止時に自動的に有効になります。
- 停止後に、どのように電子メールメッセージをメールサーバーに戻して消去することができますか。
  停止の後、Email Continuity サービスは、停止中に送受信されたすべての電子メールメッセージを、メールサーバーに自動的に戻して消去します。
- メールサーバーに戻された電子メールメッセージは、Microsoft Outlook のどこに表示されますか。
  停止中に送受信されたすべての電子メールメッセージは、Outlook の受信トレイに表示されます。
- メールサーバーの停止後、電子メールメッセージがメールサーバーに戻されて消去された後に通知は送られますか。
  いいえ。Email Continuity サービスがメールサーバーに電子メールメッセージを戻して消去した後、通知は提供されません。
- Email Continuity サービスは配布リストを展開しますか。
  いいえ。Email Continuity サービスは配布リストを展開しません。ただし、配布リストは、停止の後にメールサーバーに戻された電子メールメッセージに対して展開されます。

12

レポートと通知

この章では以下の項目について説明しています。

Enterprise Vault.cloud のレポートとログについて

[Reports and notifications]セクションから、組織ごとの Enterprise Vault.cloud の使用状況に関する情報を提供するログとレポートにアクセスできます。さらに、ログとレポートをさまざまなファイル形式でエクスポートすることもできます。

アクティビティログの表示

アクティビティログには、ユーザーログイン、パスワードのリセット、ユーザーの役割の変更など、Enterprise Vault.cloud で発生するすべてのイベントが表示されます。[Activity

Log]ページから、完全なログを表示したり、日付範囲、ユーザー名、イベント、またはイベントの詳細を基準にしてログをフィルタしたりできます。

アクティビティログを表示するには

1. 左のナビゲーションペインの[Reports and Notifications]で[Logs]をクリックします。
2. [Activity Log]タブを選択します。
3. 必要な場合は、次の条件を使用してログをフィルタします。
   - [From Date/To Date]: 日付範囲を入力して、ログをフィルタします。
   - [Detail Substring]: 成功やエラーなど、イベント詳細のキーワードを入力して、ログをフィルタします。
   - [User]: ユーザー名または電子メールアドレスを入力して、ログをフィルタします。
   - [Event]: 特定のイベントの種類を選択して、ログをフィルタします。
4. [Search]をクリックします。

   結果のアクティビティログレポートが、メインウィンドウ枠に表示されます。

   メモ: Enterprise Vault.cloud サービスがログに記録したイベントのプライベート IP アドレスは、レポートには表示されません。代わりに、[IP Address]列に、[Internal Service]が表示されます。

5. 必要な場合は、[Export]をクリックしてログを CSV 形式にエクスポートします。

メッセージログの表示

メッセージログには、Enterprise Vault.cloud のアーカイブ済みメッセージに関する情報が表示されます。[Message Log]ページから、完全なログを表示したり、日付範囲、メッセージの送信者、メッセージの受信者、または件名を基準にしてログをフィルタしたりできます。

メッセージログを表示するには

1. 左のナビゲーションペインの[Reports and Notifications]で[Logs]をクリックします。
2. [Message Log]タブを選択します。
3. 必要な場合は、次の条件を使用してログをフィルタします。
   - [From Date/To Date]: 日付範囲を入力して、ログをフィルタします。

- ［Sender］: メッセージ送信者の電子メールアドレスを入力して、ログをフィルタします。
- ［Recipient］: メッセージ受信者の電子メールアドレスを入力して、ログをフィルタします。
- ［Subject］: メッセージの件名のキーワードを入力して、ログをフィルタします。
- ［Has Attachment］: 添付ファイル付きのメッセージの場合は［Yes］を選択し、添付ファイルの付いていないメッセージの場合は［No］を選択して、ログをフィルタします。

4 ［Search］をクリックします。

5 必要な場合は、ファイル形式を選択して［Export］をクリックして、ログをエクスポートします。

使用状況ログの表示

使用状況ログには、Enterprise Vault.cloud の使用状況に関する情報が表示されます。［Usage Log］ページから、次の情報を表示できます。

- アーカイブ済みメッセージの合計数。
- 過去 24 時間にアーカイブされた新しいメッセージの数。
- 1 日にアーカイブされたメッセージの平均数。
- アーカイブ済みメッセージの平均サイズ。
- メッセージのアーカイブに使用された合計ストレージ。

使用状況ログを表示するには

1 左のナビゲーションペインの［Reports and Notifications］で［Logs］をクリックします。

2 ［Usage Log］タブを選択します。

3 必要な場合は、ファイル形式を選択して［Export］をクリックして、ログをエクスポートします。

保持ログレポートの作成

保持ログレポートには、保持ポリシーの使用状況の情報が表示されます。［Retention Log］ページから、完全なログが含まれるレポートを作成できます。また、日付範囲、ユーザー名、処理の種類、またはポリシー名でログをフィルタすることもできます。

保持ログレポートを作成するには

1. 左のナビゲーションペインの［Reports and Notifications］で［Logs］をクリックします。
2. ［Retention Log］タブを選択します。
3. 必要な場合は、次の条件を使用してログをフィルタします。
   - ［From Date/To Date］: 日付範囲を入力して、ログをフィルタします。
   - ［User Name］: ユーザー名を入力して、ログをフィルタします。
   - ［Action Type］: 処理の特定の種類を選択して、ログをフィルタします。
   - ［Policy Name］: 保持ポリシーの名前を入力して、ログをフィルタします。
4. ［Run Report］をクリックします。
5. 必要な場合は、［Export］をクリックして、作成したレポートをエクスポートします。

モバイルブラウザログの表示

モバイルブラウザログには、Enterprise Vault.cloud Mobile Web Access の使用状況に関する情報が表示されます。［Mobile Browser Log］タブから、完全なログを表示したり、日付範囲でログをフィルタしたりできます。

モバイルブラウザログを表示するには

1. 左のナビゲーションペインの［Reports and Notifications］で［Logs］をクリックします。
2. ［Mobile Browser Log］タブを選択します。
3. 必要な場合は、［From Date］と［To Date］のフィールドを使用して、日付範囲を基準にしてログをフィルタします。
4. ［Search］をクリックします。
5. 必要な場合は、［Export］をクリックしてログを CSV 形式にエクスポートします。

Personal ブラウザログの表示

Personal ブラウザログには、Enterprise Vault Personal.cloud の使用状況に関する情報が表示されます。［Personal Browser Log］タブから、完全なログを表示したり、日付範囲でログをフィルタしたりできます。

Personal ブラウザログを表示するには

1. 左のナビゲーションペインの[Reports and Notifications]で[Logs]をクリックします。
2. [Personal Browser Log]タブを選択します。
3. 必要な場合は、[From Date]と[To Date]のフィールドを使用して、日付範囲を基準にしてログをフィルタします。
4. [Search]をクリックします。
5. 必要な場合は、[Export]をクリックしてログを CSV 形式にエクスポートします。

Discovery ブラウザログの表示

Discovery ブラウザログには、Enterprise Vault Discovery.cloud の使用状況に関する情報が表示されます。[Discovery Browser Log]タブで、完全なログを表示したり、日付範囲でログをフィルタしたりできます。

Discovery ブラウザログを表示するには

1. 左のナビゲーションペインの[Reports and Notifications]で[Logs]をクリックします。
2. [Discovery Browser Log]タブを選択します。
3. 必要な場合は、[From Date]と[To Date]のフィールドを使用して、日付範囲を基準にしてログをフィルタします。
4. [Search]をクリックします。
5. 必要な場合は、[Export]をクリックしてログを CSV 形式にエクスポートします。

メッセージレポートの作成

メッセージレポートには、次のパラメータに基づく Enterprise Vault.cloud の使用状況に関する情報が表示されます。

- ユーザーごとのアーカイブ済みメッセージの平均サイズ。
- 1 日にアーカイブされたメッセージのユーザーごとの平均数。
- メッセージの添付ファイルの平均サイズ。
- 組織内のユーザーによる検索の平均速度。
- インポートされたアーカイブ済みメッセージの合計数。

さらに、組織の Enterprise Vault.cloud の使用状況を、他の組織の使用状況と比較できます。

メッセージレポートを作成するには

1 左のナビゲーションペインの[Reports and Notifications]で[Reports]をクリックします。

2 [Messaging]タブを選択します。

3 [Select Report]セクションで、作成するレポートの種類のタブを選択します。

4 [Range]フィールドで、レポートの日付範囲を選択します。

5 必要な場合は、[Compare to All Companies]を選択して、使用状況を他の組織の使用状況と比較します。

6 [Apply]をクリックして、レポートを作成します。

7 必要な場合は、ファイルを選択して[Export]をクリックして、レポートをエクスポートします。

Personal Archive レポートの作成

Personal Archive レポートには、次のパラメータに基づく Personal.cloud の使用状況に関する情報が表示されます。

- Personal.cloud にログインしたユーザーの数。
- ユーザーごとの作成済み管理対象タグの数。
- ユーザーごとの適用済み管理対象タグの数。
- 実行された検索の数。
- 組織内のユーザーによる検索の平均速度。
- 使用された検索文字列のリスト。

さらに、組織の Personal.cloud の使用状況を、他の組織の使用状況と比較できます。

メモ: Personal Archive レポートでは、分類タグは報告されません。分類タグは、Personal.cloud でユーザーに表示されません。

Personal Archive レポートを作成するには

1 左のナビゲーションペインの[Reports and Notifications]で[Reports]をクリックします。

2 [Personal Archive]タブを選択します。

3 [Select Report]セクションで、作成するレポートの種類のタブを選択します。

4 検索文字列のレポートを選択した場合は、[Range]フィールドで日付範囲を選択します。

5 必要な場合は、[Compare to All Companies]を選択して、使用状況を他の組織の使用状況と比較します。

メモ: このオプションは、検索文字列のレポートでは利用できません。

6 [Apply]をクリックして、レポートを作成します。

7 必要な場合は、ファイルの種類を選択して[Export]をクリックして、レポートをエクスポートします。

Mobile Web Access レポートの作成

Mobile Web Access Mobile Web Access レポートには、次のパラメータに基づく使用状況に関する情報が表示されます。

- Mobile Web Access にログインしたユーザーの数。
- 実行された検索の数。
- 使用された検索文字列のリスト。

さらに、組織の Mobile Web Access の使用状況を、他の組織の使用状況と比較できます。

Mobile Web Access レポートを作成するには

1 左のナビゲーションペインの[Reports and Notifications]で[Reports]をクリックします。

2 [Mobile Web Access]タブを選択します。

3 [Select Report]セクションで、作成するレポートの種類のタブを選択します。

4 検索文字列のレポートを選択した場合は、[Range]フィールドで日付範囲を選択します。

5 必要な場合は、[Compare to All Companies]を選択して、使用状況を他の組織の使用状況と比較します。

6 [Apply]をクリックして、レポートを作成します。

7 必要な場合は、ファイルの種類を選択して[Export]をクリックして、レポートをエクスポートします。

13

IBM Notes 用の Personal.cloud の配備

この章では以下の項目について説明しています。

IBM Notes 用の Personal.cloud の配備

IBM Notes 内で、ユーザーは Notes ブラウザを使用するか、Internet Explorer と Notes を組み合わせて使用してインターネットにアクセスできます。この機能により、Notes ユーザーは、Notes アプリケーション内から Personal.cloud にアクセスできます。Microsoft Windows 環境の Active Directory グループポリシーを使用して、Personal.cloud へのアクセス URL をお気に入りとして Notes ユーザーに配備できます。

メモ: Personal.cloud のアクセス URL を配備するには、グループポリシーの管理など、Active Directory の基本概念に関する知識が必要です。すべてのユーザーにアクセス URL を配備する前に、テストユーザーのグループを対象に、配置をテストすることをお勧めします。

Personal.cloud のアクセス URL を配備するには

1. [グループ ポリシーの管理]コンソールで、[ユーザー構成]、[Internet Explorer のメンテナンス]の順に展開します。
2. [Internet Explorer のメンテナンス]で[URL]を選択します。
3. 右側のウィンドウ枠で、[お気に入りとリンク]をダブルクリックします。

4 [お気に入りとリンク]ウィンドウで、[URL の追加]をクリックします。

メモ: [お気に入りとリンクを一覧の先頭に指定した順序で配置する]は選択しないでください。

---

5 [詳細]ウィンドウの[名前]フィールドに「Personal.cloud」と入力し、Personal.cloud のアクセス URL を[URL]に入力します。

6 [OK]をクリックして[詳細]ウィンドウを閉じて、[お気に入りとリンク]ウィンドウを閉じます。

14

以前のリリースの Archive Administration の更新

この章では以下の項目について説明しています。

以前のリリースの更新について

このヘルプの概要には、Archive Administration の最新の更新に関する説明が含まれています。

p.8 の「Enterprise Vault.cloud Archive Administration について」を参照してください。

Archive Administration の以前のリリースで利用可能になった新機能や更新の説明については、次を参照してください。

- p.121 の「2017 年 3 月更新」を参照してください。
- p.122 の「2016 年 8 月更新」を参照してください。
- p.122 の「2016 年 5 月更新」を参照してください。
- p.123 の「2016 年 1 月更新」を参照してください。
- p.123 の「2015 年 12 月更新」を参照してください。
- p.124 の「2015 年 11 月更新」を参照してください。
- p.124 の「2015 年 8 月更新」を参照してください。
- p.124 の「2015 年 5 月更新」を参照してください。
- p.125 の「2015 年 2 月更新」を参照してください。
- p.126 の「2014 年 11 月更新」を参照してください。
- p.126 の「2014 年 8 月更新」を参照してください。
- p.127 の「2014 年 5 月更新」を参照してください。
- p.127 の「2013 年 11 月更新」を参照してください。
- p.127 の「2013 年 7 月更新」を参照してください。
- p.128 の「2013 年 5 月更新」を参照してください。
- p.128 の「2013 年 2 月/3 月更新」を参照してください。

- p.129 の「2012 年 11 月更新」を参照してください。
- p.131 の「2012 年 5 月更新」を参照してください。
- p.131 の「2012 年 3 月更新」を参照してください。
- p.131 の「2012 年 1 月/2 月更新」を参照してください。
- p.132 の「2012 年 1 月更新」を参照してください。

Enterprise Vault.cloud サービススイートの各リリースの更新すべてについて詳しくは、Enterprise Vault.cloud リリースノートを参照してください。Veritasサポート Web サイトに掲載されている次の記事からリリースノートを参照できます。

http://www.veritas.com/docs/000100485

2017 年 3 月更新

次の製品の更新は Archive Administration の 2017 年 3 月リリースの一部として利用可能になりました。

機能強化:

- Office 365 Config ノードの機能強化:
  [Office 365 Config]ノードの設定が更新されて、Office 365 Sync の設定が簡略化されました。[Powershell Credentials]と[Exchange Web Services Credentials]で、2 つの[URL]フィールドが削除されました。これらの固定 URL は、自動的に設定されるようになりました。また、[Exchange Web Services Credentials]の新しい[Use same credentials as Powershell]チェックボックスでは、同じクレデンシャルを再入力せずに使用できます。
  p.16 の「Office 365 Sync の設定」を参照してください。
- シングルサインオンが設定されている場合にようこそメッセージを送信しないオプション:
  Enterprise Vault.cloud で会社にシングルサインオン認証が設定されている場合、[Personal Archive Deployment Options]、[Personal Archive Access]の下にある[Provisioning]ノードのオプションが変更されました。Personal Archive のアクセスを有効化している場合、ようこそメッセージを送信するかどうかを選択できるようになりました。更新の前に Personal Archive のアクセス設定が構成されていた場合のシングルサインオン設定では、更新の後もデフォルトでようこそメッセージが引き続き送信されます。ようこそメッセージの送信を無効化するには、[Personal Archive Access]の新しいオプションを使用します。
  p.29 の「Personal.cloud の配備オプションの設定」を参照してください。

新機能:

- Google G Suite Enterprise Gmail のアーカイブのサポート。

Archive Administration から、Google G Suite Enterprise Gmail のアーカイブアカウントを管理できるようになりました。Enterprise Vault.cloud を Google G Suite Gmail のアーカイブ用に設定する方法について詳しくは、『Enterprise Vault.cloud ジャーナリングガイド』を参照してください。特定の要件についてのご相談は、Veritasのサービスとサポートにお問い合わせください。

2016 年 8 月更新

次の製品の更新は Archive Administration の 2016 年 8 月リリースの一部として利用可能になりました。

機能強化:

- シングルサインオンソリューションへの Microsoft Azure Active Directory の追加:
  Personal.cloud、Discovery.cloud、および Archive Administration のシングルサインオンソリューションに、AD FS 2.0、2.1 および 3.0 と、OneLogin、Okta および PingOne のほかに、Azure Active Directory が追加されました。Azure Active Directory でのシングルサインオンアクセスの設定についてサポートが必要な場合は、Veritasのサービスとサポートにお問い合わせください。

2016 年 5 月更新

次の製品の更新は Archive Administration の 2016 年 5 月リリースの一部として利用可能になりました。

新機能:

- Office 365 メールボックスの委任権限の同期:
  Office 365 Sync で、ユーザーメールボックスや共有メールボックスの委任権限を同期するためのオプションが提供されるようになりました。同期の後、Personal.cloud ユーザーは、[Full Access]の委任権限が付与された、Office 365 メールボックスのアーカイブ済みメッセージにアクセスできます。
  p.21 の「Office 365 メールボックスの委任権限の同期について」を参照してください。

機能強化:

- Personal.cloud の印刷と保存のオプションを非表示にする新しい設定:
  デザインが新しくなった[Archive Options]ページに 2 つの新しい設定が追加されて、Personal.cloud でユーザーにメッセージの印刷と保存のオプションが表示されないようにできます。
  p.74 の「アーカイブオプションの設定」を参照してください。

2016 年 1 月更新

次の製品の更新は Archive Administration の 2016 年 1 月リリースの一部として利用可能になりました。

新機能:

- Exchange の委任アクセス権の同期のサポート:
  このリリースでは、オンプレミスの Exchange ユーザーメールボックスと共有メールボックスに適用されている、委任権限の同期に対するサポートが導入されました。Enterprise Vault.cloud は、ユーザーとメールが有効なセキュリティグループに付与された委任権限を同期できます。この機能により、ユーザーは、[フルアクセス]の委任権限を持っている Exchange メールボックスのアーカイブ済みメッセージを、Personal.cloud で読み取ることができます。
  Archive Administration のアカウントの詳細に新しく追加された[Delegate Access]パネルは、同期済み委任アクセス権を持つ委任ユーザーまたはメールが有効なセキュリティグループと、アーカイブにどの権限が付与されているかを表示します。

  メモ: 委任権限の同期では、CloudLink バージョン 4.0 の新しい機能を使用する必要があります。

機能強化:

- アカウントの詳細の強化されたユーザーインターフェース:
  [Account Details]ページのデザインが新しくなり、パネルベースの見やすいレイアウトになりました。変更点の 1 つである新しい[History]パネルには、そのアーカイブアカウントの設定に過去 30 日間で加えられた変更の概要が表示されます。
  p.47 の「[Account Details]ページについて」を参照してください。

2015 年 12 月更新

次の製品の更新は Archive Administration の 2015 年 12 月リリースの一部として利用可能になりました。

機能強化:

- 商標変更されたインターフェース:
  Administration Console のユーザーインターフェースが、Veritas向けに商標変更されました。

2015 年 11 月更新

次の製品の更新は Archive Administration の 2015 年 11 月リリースの一部として利用可能になりました。

機能強化:

- シングルサインオン認証の変更:
  Enterprise Vault.cloud は、Secure Assertion の認証および権限の交換の間に提示される NotBefore と NotOnOrAfter の条件を受け入れるようになりました。SAML 交換中に Enterprise Vault.cloud に提示される値を理解するために、SSO オーソリティや ID プロバイダの設定を確認することをお勧めします。
  p.92 の「Enterprise Vault.cloud と連携するための AD FS の設定」を参照してください。

2015 年 8 月更新

次の製品の更新は Archive Administration の 2015 年 8 月リリースの一部として利用可能になりました。

機能強化:

- Box ファイルアーカイブのファイルのフィルタリング:
  Box ファイルアーカイブで、アーカイブ用に収集したファイルを、ファイルの拡張子に基づいてフィルタできるようになりました。ファイルフィルタリングを使用すると、eDiscovery 用にインデックス付けできるコンテンツを、より高速にアーカイブできます。アーカイブするファイル拡張子のデフォルトのリストに項目を追加して、個々のユーザー向けに、ファイルの種類の特定のセットを継続的に定義できます。p.57 の「Box ファイルアーカイブについて」を参照してください。
- Lync オンプレミスアーカイブによる Skype for Business へのサポートの追加:
  Lync Connector バージョン 1.0 アプリケーションを、Skype for Business Server 2015 からのアーカイブに使用できるようになりました。
- シングルサインオンソリューション拡張による、PingOne のサポート追加:
  Personal.cloud、Discovery.cloud、および Archive Administration でサポートされるシングルサインオンソリューションに、AD FS 2.0、2.1 および 3.0 と、OneLogin および Okta のほかに、PingOne が追加されました。PingOne でのシングルサインオンアクセスの設定についてサポートが必要な場合は、Veritasのサービスとサポートにお問い合わせください。

2015 年 5 月更新

次の製品の更新は Archive Administration の 2015 年 5 月リリースの一部として利用可能になりました。

新機能:

- Lync オンプレミスアーカイブのサポート:
  [Archive Collectors]セクションに、新しく[Lync]ページが追加されました。ここから、[Lync On-Premises Archiving]機能を有効化および無効化できます。Microsoft Lync Server のコンテンツをアーカイブするように Enterprise Vault.cloud Lync Connector アプリケーションを設定する前に、この機能を有効化する必要があります。
  新しい[Lync]ページにアクセスするには、新しい[Configure Lync Archival]の権限を含む管理者の役割に、アカウントが割り当てられている必要があります。
  Lync Connector アプリケーションは、Lync Server 2010 および 2013 のコンテンツアーカイブをサポートします。アプリケーションは、Archive Administration の 2015 年 5 月のリリース直後に利用可能になります。

機能強化:

- Office 365 Sync のユーザーインターフェースの更新:
  [Office 365 Config]と[Office 365 Sync]のページが、1 つのページに統合されました。Office 365 Sync に関連するすべてのタスクを、更新された[Office 365 Config]ページから実行できるようになりました。これらのタスクには、サービスの設定、同期のスケジュール設定、完全同期の実行、およびレポートの確認が含まれます。
- Discovery.cloud および Archive Administration に対するシングルサインオンサポート:
  Enterprise Vault.cloud 認証サービスを、Discovery.cloud と Archive Administration のユーザーにシングルサインオンアクセスを提供するように設定できるようになりました。Discovery.cloud と Archive Administration で現在サポートされるシングルサインオンソリューションには、現在、AD FS 2.0、2.1 および 3.0 と、OneLogin および Okta が含まれます。
  Discovery.cloud と Archive Administration に対するシングルサインオンアクセスの設定についてサポートが必要な場合は、Veritasのサービスとサポートにお問い合わせください。

2015 年 2 月更新

次の製品の更新は Archive Administration の 2015 年 2 月リリースの一部として利用可能になりました。

- Okta シングルサインオンソリューションのサポート: Okta が、Enterprise Vault.cloud 認証サービスのサポート対象になりました。2 月のリリースの後、Okta シングルサインオンソリューションを使用して、Personal.cloud ユーザーにシングルサインオンアクセスを提供するように、Enterprise Vault.cloud 認証サービスを設定できます。
  Okta シングルサインオンソリューションの設定についてサポートが必要な場合は、Veritasのサービスとサポートにお問い合わせください。

- OneLogin シングルサインオンソリューションのサポート: OneLogin が、Enterprise Vault.cloud 認証サービスのサポート対象になりました。2 月のリリースの後、OneLogin シングルサインオンソリューションを使用して、Personal.cloud ユーザーにシングルサインオンアクセスを提供するように、Enterprise Vault.cloud 認証サービスを設定できます。
  OneLogin シングルサインオンソリューションの設定についてサポートが必要な場合は、Veritasのサービスとサポートにお問い合わせください。
- Internet Explorer 11 の互換性: Archive Administration は Microsoft Internet Explorer 11 をサポートするようになりました。

2014 年 11 月更新

次の製品の更新は Archive Administration の 2014 年 11 月リリースの一部として利用可能になりました。

新機能:

- Office 365 共有メールボックスからのアーカイブのサポート: 新しいオプションを使用すると、Office 365 共有メールボックスと同期できます。このオプションを選択すると、すべての Microsoft Office 365 ドメインに含まれる各共有メールボックスが同期のターゲットになります。共有メールボックスは、ユーザーのメールボックスと同様に同期および課金されます。
  デフォルトでは、このオプションはオフになっています。
  この更新の一環として、Archive Administration の左側のナビゲーションウィンドウ枠の[My Config]ノード内で、2 つのページの名前が変更されました。
  - [Credentials]ページの名前は[Office 365 Config]になりました。
  - [Scheduler]ページの名前は[Office 365 Sync]になりました。

  Archive Administration ヘルプで、新しいオプションとその選択方法を説明します。p.16 の「Office 365 Sync の設定」を参照してください。

機能強化:

- アーカイブ済みファイルに対する Box ファイルダウンロード通知電子メールの抑制: Box ファイルアーカイブで、ファイルがアーカイブされたときに Box が生成する、ファイルダウンロードの電子メール通知メッセージがすべて抑制されるようになりました。
  この機能強化に現在関連付けられているすべての制限事項について詳しくは、次のサポート記事を参照してください。http://www.veritas.com/docs/000023852

2014 年 8 月更新

次の製品の機能強化は Archive Administration の 2014 年 8 月リリースの一部として利用可能になりました。

- Personal.cloud と Discovery.cloud のブラウザログ: Personal.cloud と Discovery.cloud の使用状況に関する情報を提供する新しいログが 2 つ利用できるようになりました。新しいログには、Archive Administration の[Reporting]セクションにある[Logs]ページからアクセスできます。
- AD FS 2.1 および 3.0 のサポート: Active Directory フェデレーションサービス (AD FS) バージョン 2.1 および 3.0 が、Enterprise Vault.cloud 認証サービスでサポートされるようになりました。8 月リリースの後、AD FS 2.1 または 3.0 を使用する組織の管理者は、Enterprise Vault.cloud 認証サービスを設定して、Personal.cloud ユーザーにシングルサインオンアクセスを提供できるようになりました。

2014 年 5 月更新

次の製品の機能強化は Archive Administration の 2014 年 5 月リリースの一部として利用可能になりました。

- Domino 9 ジャーナル互換性 - Enterprise Vault Personal.cloud は、IBM Domino 9 からジャーナルをサポートするようになりました。

2013 年 11 月更新

次の製品の機能強化は Archive Administration の 2013 年 11 月リリースの一部として利用可能になりました。

- Mobile Web Access プロビジョニングの追加: 管理者は、必要な権限を持ったユーザーに、Mobile Web Access を有効化できるようになりました。
p.74 の「アーカイブオプションの設定」を参照してください。
- アーカイブログとレポートの追加: 管理者は、[Reporting]セクションから、モバイルブラウザログと Mobile Web Access レポートにアクセスできるようになりました。

2013 年 7 月更新

次の製品の更新は Archive Administration の 2013 年 7 月リリースの一部として利用可能になりました。

機能強化:

- SHA-256 ハッシュアルゴリズムの互換性: Personal.cloud ユーザー向けにシングルサインオンが実装されている場合に、Active Directory フェデレーションサービスを設定するために SHA-256 ハッシュアルゴリズムが使用できるようになりました。

修正:

- アカウントエクスポートの問題の修正: ユーザーアカウントの検索後に[Accounts]ページからエクスポートを実行した場合に発生する問題は解決されました。このリリースの

前は、エクスポートされた Excel ファイルに、組織のすべてのユーザーアカウントが含まれていました。このリリースの後、エクスポートされる Excel ファイルには、ユーザーアカウントの検索から返されたユーザーアカウントのみが含まれます。

- Office 365 の検証の問題の修正: ダッシュやアンダースコアなどの特定の文字が含まれるユーザー名が、[Office 365 Credentials]ページで検証されない問題は解決されました。

2013 年 5 月更新

次の製品の機能拡張は Archive Administration の 2013 年 5 月リリースの一部として利用可能になりました。

- 管理タグ機能の更新 - 管理タグ機能が更新され、管理者が個々のユーザーに管理タグを割り当てられるようになりました。このリリース以後、管理者は、管理タグへのアクセスを特定のユーザーに制限できます。
- Office 365 アカウントの同期の改善 - 同期イベントが発生した後、Microsoft Office 365 で無効になっているユーザーが Personal.cloud と Discovery.cloud にアクセスできなくなりました。

2013 年 2 月/3 月更新

次の製品の更新は Archive Administration の 2013 年 2 月/3 月リリースの一部として利用可能になりました。

機能強化:

- Exchange 2013 ジャーナリングの互換性 - Enterprise Vault.cloud が Microsoft Exchange 2013 からのジャーナリングをサポートするようになりました。
- IM Security.cloud の互換性 - Enterprise Vault.cloud が IM Security.cloud からのメッセージのアーカイブをサポートするようになりました。
- Enterprise Vault Discovery.cloud のみのアカウントの追加 - Discovery.cloud にのみアクセスできる Enterprise Vault.cloud アカウントを作成するオプションを利用できるようになりました。

メモ: この機能拡張の結果として、Discovery.cloud に以前アクセスできたユーザーがアプリケーションにログインできなくなる可能性があります。このリリース後、レビュー担当者や管理者ではないのに問題に割り当てられたユーザーは、アプリケーションにログインできなくなります。問題に割り当てられてログインできないユーザーは、その問題の[問題の編集]ページに赤色で表示されます。これらのユーザーがアクセスできるようにするには、Archive Administration のレビュー担当者または管理者の役割に割り当てます。

p.69 の「役割管理について」を参照してください。

- Box ファイルアーカイブのユーザーインターフェースの更新 - Box ファイルアーカイブを管理するユーザーインターフェースが操作性を改善するため更新されました。

修正:

- メッセージサイズのレポートの更新 - ユーザー 1 人あたりのメッセージの平均サイズレポートが、ギガバイト単位ではなくメガバイト単位で平均メッセージサイズを表示するように更新されました。
- Office 365 機能に関する問題の修正 - [Office 365 配布リスト選択]ウィンドウの改ページと[すべてを選択]機能に関する問題に対応しました。

2012 年 11 月更新

次の製品の更新は Archive Administration の 2012 年 11 月リリースの一部として利用可能になりました。

新機能:

- 保持管理機能の更新: 保持管理機能が更新されて、管理者が複数の保持ポリシーを作成できるようになりました。これらの保持ポリシーは、ArchiveTools CloudLink を使用して同期された Active Directory グループか、管理対象タグに割り当てることができます。
  p.98 の「保持管理について」を参照してください。
- 新しい保持ログレポートの追加: 管理者は、[Reporting]セクションの[Logs]ページから、保持管理の変更をまとめたレポートを生成できるようになりました。
- Box と Salesforce Chatter のアーカイブ: Box のファイルや投稿、プライベートメッセージとパブリックメッセージ、および Salesforce Chatter からの添付ファイルのアーカイブはサポートされていません。これらのサービスのサブスクリプションを利用している組織の管理者は、[Archive Collectors]セクションからこれらのサービスを管理できます。
  p.57 の「アーカイブコレクタについて」を参照してください。

- SharePoint 2010 のアーカイブ: Enterprise Vault.cloud で、オンプレミス Microsoft SharePoint 2010 サーバーからのファイルのアーカイブがサポートされるようになりました。

ユーザーインターフェースの更新:

- 新しい[Storage Expiry]ページ: [Expiration Management]ページが更新されて操作性が向上し、[Storage Expiry]ページという名前になりました。
- 管理対象タグ: 保持タグは、管理対象タグと呼ばれるようになりました。これらのタグを管理者が作成し、保持ポリシーに関連付けることができる新しいページ[Managed Tags]が、[My Config]セクションに追加されました。

機能強化:

- Office 365 アカウントの同期の改善: ユーザーの電子メールアドレスの変更が、Microsoft Office 365 から自動的に同期されるようになりました。管理者がユーザーに新しいプライマリ電子メールアドレスを割り当てており、古いアドレスをエイリアスにした場合、これらの変更は自動的に Enterprise Vault.cloud に同期されます。
- アプリケーションパフォーマンスの向上: Archive Administration の全体的なパフォーマンスを向上する更新が実装されました。

修正:

- アクティビティログの問題の修正: アクティビティログに表示されるタイムスタンプの問題が解決されました。このリリースの前は、会社で選択したタイムゾーンに関係なく、タイムスタンプは太平洋標準時刻で表示されていました。このリリースの後は、会社に設定されたタイムゾーンによって、表示されるタイムスタンプが決定されます。
- ようこそメッセージに関する問題の修正: [Provisioning]ページの[Welcome Message Template]セクションに表示される、アーカイブアクセス URL の問題が解決されました。
- 無効なユーザーリストの問題の修正: 誤ったアカウントが表示される問題と、[Disabled Users]ページからアカウントが正しく削除されない問題が解決されました。
- パスワードのリセットの問題の修正: ユーザーがログインページでパスワードを忘れた場合の機能を使用するとエラーが表示される問題が解決されました。
- Office 365 Sync の問題の修正: Office 365 Sync のスケジューラが、[Recurrence]のチェックマークがはずれている場合でも、繰り返し実行される問題が解決されました。
- Office 365 Sync の問題の修正: 同期イベントの実行で、Office 365 Sync のスケジューラが[Enabled]の状態を保存しない問題が解決されました。
- ID プロバイダの URL の問題の解決: 認証ページに直接リンクする ID プロバイダの URL が検証されない問題は解決されました。

2012 年 5 月更新

次の製品の機能強化は Archive Administration の 2012 年 5 月リリースの一部として利用可能になりました。

- Domino ジャーナリングの更新 - Domino ジャーナリングの方式が更新されました。更新された方式では、メールジャーナリングテンプレートを使用する必要がなくなりました。
- Office 365 同期ページの更新 - Office 365 同期のページが機能を設定している組織に対してのみ表示されるようになりました。
- ID プロバイダの URL 検証の更新 - ID プロバイダの URL と Outlook Web Access の ID プロバイダの URL の検証プロセスが更新されました。プロセスによって接続が確実に確立したことが確認されるようになりました。

2012 年 3 月更新

次の製品の更新は Archive Administration の 2012 年 3 月リリースの一部として利用可能になりました。

機能強化:

- Microsoft Office 365 ドメイン同期 - 複数の Microsoft Office 365 ドメインを Archive Administration に自動的に同期できるようになりました。管理者は、[プロビジョニング]ページでプロビジョニングする特定の同期ドメインを選択することもできます。
- AD FS のシングルサインオン機能の更新 - Active Directory フェデレーションサービス (AD FS) を使用した Personal.cloud のシングルサインオンを完全に設定して、Archive Administration から配備できるようになりました。
- 保持タグ権限定義の変更 - より詳細な情報を提供するように保持タグの各権限の定義が更新されました。

修正:

- Office 365 の同期スケジュールの問題を修正 - Office 365 同期スケジューラ機能に関する問題に対応しました。終了日を指定せずに設定されているときに、同期スケジューラが正しく動作するようになりました。
- Office 365 同期スケジューラレポートの問題を修正 - 管理者が[レポートを表示するをクリックしたときに Office 365 同期スケジューラのレポートが表示されない問題に対応しました。

2012 年 1 月/2 月更新

次の製品の更新は Archive Administration の 2012 年 1 月/2 月リリースの一部として利用可能になりました。

機能強化:

- Office 365 Web フォルダのプッシュ - 管理者は、Windows PowerShell コマンドを使用する Office 365 Web フォルダのプッシュに偽装コマンドを設定する必要がなくなりました。

修正:

- AD FS の公開鍵アップロードの問題を修正 - [認証の管理]ページでアップロードされる公開鍵の検証に関する問題に対応しました。
- ID プロバイダの URL のテスト接続に関する問題を修正 - [認証の管理]ページに入力される ID プロバイダの URL の検証に関する問題に対応しました。

2012 年 1 月更新

次の製品の更新は Archive Administration の 1 月リリースの一部として利用可能になりました。

機能強化:

- AD FS シングルサインオン: Active Directory フェデレーションサービス (AD FS) を使用した、Personal.cloud のシングルサインオンが可能になりました。この機能の設定は、新しい[Authentication Management]ページで実行できます。

メモ: この機能を有効にする前に、Veritasのサービスとサポートにお問い合わせください。シングルサインオンを完全に設定するには、手動による追加手順を配備前に実施する必要があります。

修正:

- Office 365 Sync の問題の修正: さまざまな Microsoft Office 365 の同期の問題が解決されました。
- エイリアスの問題の修正: ユーザーエイリアスにアポストロフィーが含まれていると[Accounts]ページが正常に読み込まれない問題は解決されました。

15

Archive Administration の既知の問題

この章では以下の項目について説明しています。

Archive Administration の既知の問題

このドキュメントは Archive Administration に現在存在している既知の問題について情報を提供します。

一般的な問題

- 現在、Microsoft Office 365 ユーザー向けの Personal Archive Web フォルダの配備をスケジュール設定できません。
  回避策: Web フォルダを手動で配備します。
  p.52 の「ユーザーの配備」を参照してください。
- [My Config]セクションの特定のページで[Go to Next Step]をクリックした場合に、次のページではなく、[My Config]ページにリダイレクトされます。
- Microsoft Office 365 OWA (Outlook Web App) は、フォルダにデフォルトでホームページを表示する Outlook の機能をサポートしていません。そのため、Microsoft Office 365 から Personal Archive Web フォルダにアクセスできません。
- Archive Administration の検索機能は、現在、CJK (中国語、日本語、韓国語) 統合漢字の一部しかサポートしていません。
  詳しくは、Unicode 7.0 文字コード表の中日韓統一イデオグラフィックのセクションを参照してください。

[Archive Overview]ページ

- アーカイブの概要情報と、アーカイブの完全な使用状況レポートは、ファイルにエクスポートできません。

［Office 365 Config］ページ

- ［Office 365 PowerShell Credentials］セクションの［URL］フィールドで、現在、値は事前に入力されません。
  回避策: Microsoft Exchange Online にアクセスするため、このフィールドに「https://ps.outlook.com/powershell」と入力します。

［Provisioning］ページ

- ［Archive Provisioning］セクションで［Select Group Name］ウィンドウを閉じると、選択した配布リストの状態は保持されません。
- ［Personal Archive Deployment］オプションの［Personal Archive Access］セクションは、Microsoft Office 365 プロビジョニングオプションを選択した場合にのみ表示されます。

［Accounts］ページ

- アーカイブアカウントごとに、すべてのエイリアス電子メールアドレスを入力する必要があります。エイリアス電子メールアドレスを入力しない場合、その電子メールアドレスのアーカイブ済みメッセージは、割り当てられていないレガシーアカウントに移動します。必要な場合は、メッセージの再割り当ての要求を、割り当てられていないレガシーアカウントからデータ管理チームに送信できます。
- アーカイブアカウントを検索するときに、検索条件としてエイリアスフィールドを使用できません。
- 新しいアーカイブアカウントを作成するときに、エイリアスとして共通名を追加することをお勧めします。
- アーカイブアカウントを無効にすると、そのアカウントに送信された新しいメッセージは、そのアーカイブには保存されなくなります。アーカイブアカウントを無効にしても、アーカイブは削除されず、そのアカウントの設定は変更されません。
- アーカイブアカウントを削除した場合は、そのアカウントのアーカイブ済みメッセージも削除されます。

［Role Management］ページ

- ユーザーの役割や権限に加えられた変更を有効にするには、ユーザーはアーカイブアカウントからログアウトして、再度ログインする必要があります。

Box ファイルアーカイブ

- ユーザーの Box アカウントを削除しても、ユーザーリストでそのユーザーの［Mapped］の状態が［No］に変更されません。
  回避策: ユーザーの Box ファイルアーカイブを手動で無効にします。
  p.63 の「マッピングされたユーザーに対する手動収集の有効化または無効化」を参照してください。
- Box アカウントをリンクすると、［Map and Collect Users］オプションを無効にしても、新しい Box ユーザーが自動的にマッピングされます。Box ファイルアーカイブサービ

スは新しいユーザーを自動的にマッピングするため、マッピングを無効にすることはできません。
回避策: ユーザーの Box ファイルアーカイブを手動で無効にします。
p.63 の「マッピングされたユーザーに対する手動収集の有効化または無効化」を参照してください。

Salesforce Chatter アーカイブ

- [Account Details]ページで[Archive Active]をクリアしても、Salesforce Chatter アーカイブが自動的に無効になりません。
  回避策: ユーザーの Salesforce Chatter アーカイブを手動で無効にします。
  p.53 の「既存のアーカイブアカウントのサービスの有効化」を参照してください。
- Salesforce Chatter アーカイブのサブスクリプションを利用していない組織では、[Account Details]ページで Chatter を有効にするオプションが無効になっていません。
- Salesforce Chatter アーカイブの概要に表示される情報は、不正確な場合があります。
- 拡張 ASCII 文字は、現在、Chatter の投稿の件名フィールドに正しく表示されません。
  回避策: ユーザーは、Chatter の投稿のメッセージ本文でテキストを参照できます。ここでも、情報が提供されます。
- 新しい Salesforce Chatter グループが作成されたことを示す Chatter の投稿は、現在、正しくアーカイブされません。

メモ: 新しいグループへのそれ以降の Chatter の投稿は、正しくアーカイブされます。