



Managed Access Gateway (MAG) User Guide

December 2017





Managed Access Gateway (MAG)

ユーザガイド

2017年12月



Table of Contents

Purpose	3
Log-in to your MAG Account.....	4
Additional MAG Log-in Options	4
MAG Portal Navigation	5
Home Tab	5
Account Tab	6
Administration Tab	6
Registration Requests Tab	6
Credential Strength.....	6
Enterprise Access Gateway (EAG) Information	7
Forgotten User ID and Password	7
Forgotten User ID for an Active Account.....	8
Forgotten Password for an Active Account	8
Expired Password for an Active Account	10
Forgotten Security Questions/Answers.....	11
Application Management	12
Application Status Information.....	13
Request Access	13
Requesting Access to an Application Group.....	14
Requesting access to FIS.....	15
In-Person Proofing	17
Acceptance of Terms & Conditions	18
Account Management.....	19
Edit Profile.....	20
Update Enterprise Access Gateway (EAG) Account Settings.....	21
Link Accounts	21
Lost EAG Cookie: Re-link Accounts.....	24
Password Reset and other actions for EAG users	24
View Organization Details.....	24
Change Email.....	25
Change Password	26



Change Security Questions	27
Manage OTP	28
Manage Certificates	28
Download Certificates – BasicLevel of Assurance (Identity).....	29
Download Certificates – Basic Level of Assurance (SecureEmail)	30
Download Certificates – Medium Level of Assurance (Software)	31
Download Certificates – MediumLevel of Assurance (Hardware).....	34
Hardware Token FIPS Mode Review	34
Hardware Token FIPS Mode Initialization	35
Downloading certificates to your token	38
View Certificates (MAG)	40
View Certificates (eToken – for MLOA hardware).....	40
Revoke Certificates	41
Recover Encryption Keys	42
Importing Recovered Encryption Keys	46
Renew Certificates	49
Reapply for Certificates	49
Connect Accounts	50
Account Disablement	50
Frequently Asked Questions (FAQs).....	51
What is the difference between a One-Time Password and a System Generated Password?	51
How do I know who the administrators are for my organization?.....	51
Why don't I see the Administration tab after I log-in?	51
What do I do if I don't have my passcode for certificate download?	51
Why do I receive the disabled account error when I try to log-in?	51
Why do I receive the Invalid Log-in ID or Password error when I try to log-in?	52
Why do I get the error “You are currently not logged in with your certificates” when I attempt to renew my certificates?	52
When attempting to renew my certificates, I get an error message stating that my certificate is not eligible for renewal?	53
Why do I get an error message when I attempt to log-in using my certificates, or when I attempt to upgrade my log-in credentials during certificate renewal?	53

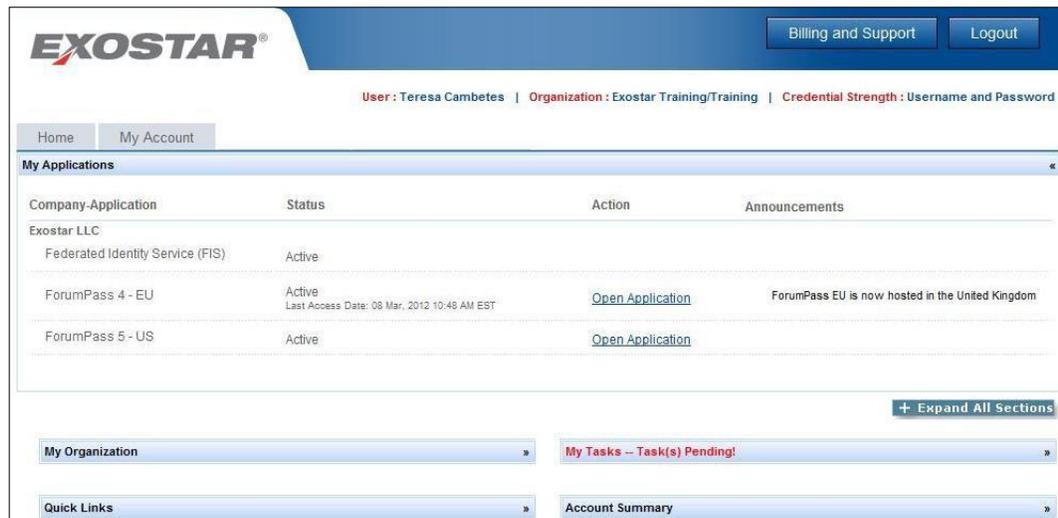
目次

目的.....	3
MAGアカウントにログインする	4
MAGにログインするその他のオプション	4
MAGポータルナビゲーション方法.....	5
Homeタブ	5
Accountタブ	6
Administrationタブ	6
Registration Requestsタブ	6
Credential Strength（クレデンシャルの強度）	6
Enterprise Access Gateway（EAG）に関する情報.....	7
ユーザIDとパスワードを忘れた場合	7
アクティブなアカウントのユーザIDを忘れた場合	8
アクティブなアカウントのパスワードを忘れた場合	8
アクティブなアカウントのパスワードの有効期限が切れた場合	10
セキュリティ質問／答えを忘れた場合	11
アプリケーションを管理する	12
アプリケーションのステータスに関する情報	13
アクセスを申請する.....	13
アプリケーション・グループへのアクセスを申請する	14
FISへのアクセスを申請する	15
対面検証.....	17
契約条件への合意.....	18
アカウントを管理する	19
プロフィールを編集する.....	20
Enterprise Access Gateway（EAG）アカウント設定を更新する.....	21
アカウントをリンクさせる	21
EAGクッキーを紛失した場合：アカウントを再リンクさせる	24
EAGユーザにおけるパスワードの再設定およびその他のアクション	24
組織情報を表示する.....	24
メールアドレスを変更する	25

パスワードを変更する.....	26
セキュリティ質問を変更する	27
OTPを管理する	28
証明書を管理する	28
証明書をダウンロードする — 基本保証レベル (Identity)	29
証明書をダウンロードする — 基本保証レベル (SecureEmail)	30
証明書をダウンロードする — 中保証レベル (Software)	31
証明書をダウンロードする — 中保証レベル (Hardware)	34
ハードウェアトークンのFIPS Modeを確認する.....	34
ハードウェアトークンのFIPS Modeを初期化する.....	35
トークンに証明書をダウンロードする	38
証明書を表示する (MAG)	40
証明書を表示する (eToken — MLOA ハードウェア)	40
証明書を失効させる	41
暗号鍵を復元する	42
復元した暗号鍵をインポートする	46
証明書を更新する	49
証明書を再申請する	49
アカウントを接続する.....	50
アカウントを無効化する.....	50
よくあるご質問 (FAQs)	51
「ワンタイムパスワード」と「システムが作成したパスワード」の違いは何ですか	51
組織の担当者が誰か、どうすれば分かりますか	51
ログイン後に「Administration」タブが表示されないのは何故ですか.....	51
証明書をダウンロードするためのパスコードを持っていない場合どうしたらいいですか	51
ログインしようとするすると無効なアカウントのエラーが表示されます	51
ログインしようとするすると無効なログインID又はパスワードのエラーが表示されます.....	52
証明書を更新しようとするすると「You are currently not logged in with your certificates (あなたの証明書で現在ログインしていません)」のエラーが表示されます	52
証明書を更新しようとするすると、証明書が更新対象外というエラーメッセージが表示されます	53
証明書を使用してログインしようとしたり、証明書更新時にログイン・クレデンシャルをアップグレードしようとするするとエラーメッセージが表示されます	53

Purpose

This guide was created for all **Managed Access Gateway (MAG)** users. This guide provides information on managing your user account, and provides information on your Exostar MAG account functionality. You can access MAG by logging on to: <https://portal.exostar.com>. When you log-in with your credentials, the system automatically identifies your designation, and presents your view of the dashboard. For most users, the following view is available:

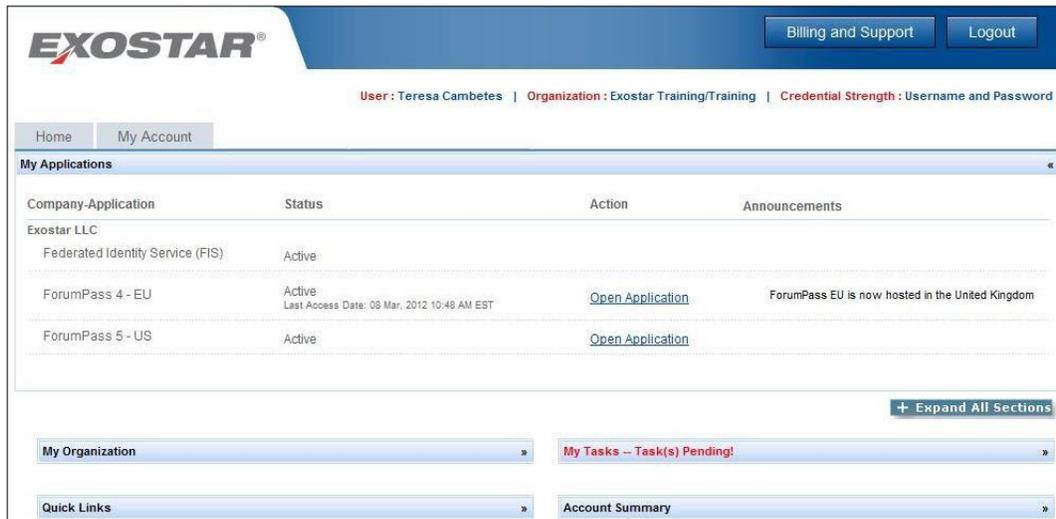


This guide provides information on the following:

- **Log-in Information**
 - ✓ Login
 - ✓ Your account
- **Forgotten User ID and Password**
 - ✓ Forgotten User ID
 - ✓ Forgotten Password
 - ✓ Expired Password
 - ✓ Application Management
- **View and Modify Account**
 - ✓ Edit Profile
 - ✓ View Organization Information
 - ✓ Change Email address
 - ✓ Change Password
 - ✓ Change Security Questions
- **Manage Certificates (For users with FIS subscription)**
 - ✓ Download Certificates
 - ✓ View Certificates
 - ✓ Revoke Certificates
 - ✓ Recover Encryption Keys
 - ✓ Import Recovered Encryption Keys
 - ✓ Reapply for Certificates

目的

本ガイドは**Managed Access Gateway (MAG)** のユーザ向けに作成されました。本ガイドでは、ユーザ・アカウントの管理に関する情報及びExostarのMAGアカウントの機能に関する情報を提供します。MAGには<https://portal.exostar.com>にログインしてアクセスすることができます。クレデンシャルを用いてログインすると、システムは自動でユーザの役割 (designation) を特定して各ユーザ用のダッシュボード画面を表示します。通常、以下の画面がご利用いただけます。



本ガイドでは以下の情報を提供します。

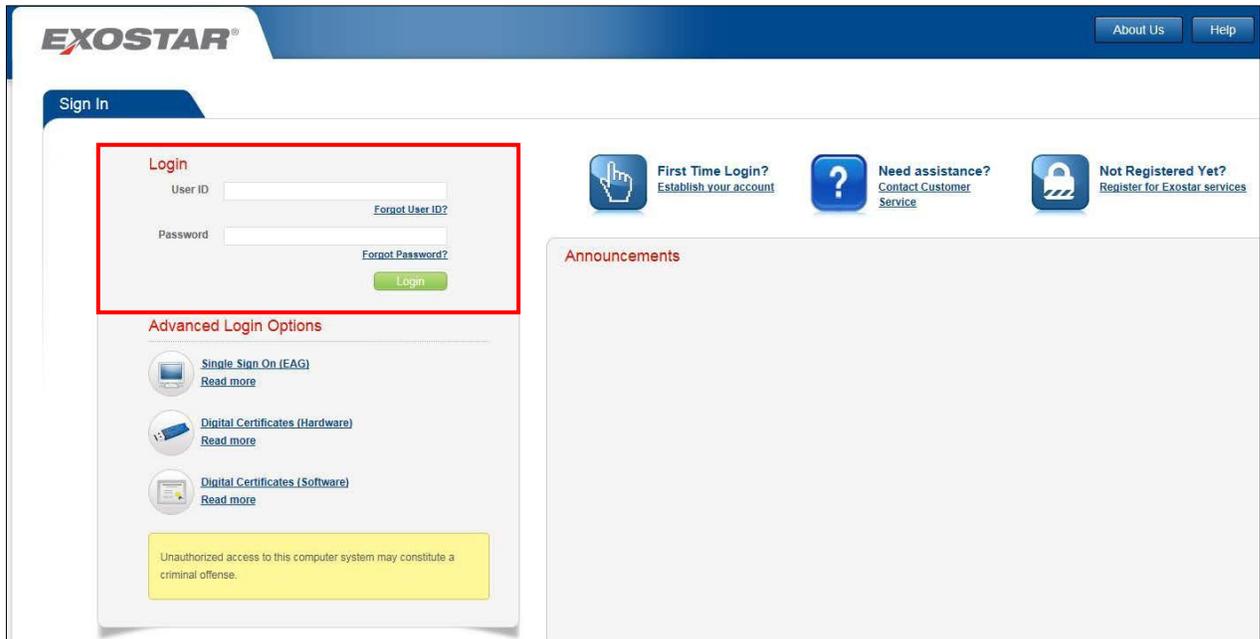
- ログイン情報
 - ✓ ログイン
 - ✓ アカウント
- ユーザIDとパスワードを忘れた場合
 - ✓ ユーザIDを忘れた場合
 - ✓ パスワードを忘れた場合
 - ✓ パスワードの有効期限切れ
 - ✓ アプリケーションの管理
- アカウントの表示・変更
 - ✓ プロフィールの編集
 - ✓ 組織情報の表示
 - ✓ Emailアドレスの変更
 - ✓ パスワードの変更
 - ✓ セキュリティ質問の変更
- 証明書の管理 (FIS会員のユーザ)
 - ✓ 証明書のダウンロード
 - ✓ 証明書の表示
 - ✓ 証明書の失効
 - ✓ 暗号鍵の復元
 - ✓ 復元した暗号鍵のインポート
 - ✓ 証明書の再申請

[Log-in to your MAG Account](#)

If you are a new user, you will receive an email with First Time Login information and instructions upon creation and approval of your account. The email will include your User ID and a system generated password. Please refer to the [First Time Login Guide](#) for more information.

Users who have completed the first time login will follow the steps below for all subsequent access to MAG.

1. Go to <https://portal.exostar.com>. The following screen is presented:



2. Enter your **User ID** and **password**, and click **Login**. Upon successful login, the MAG application page is presented.

[Additional MAG Log-in Options](#)

MAG allows you to log-in to your account using digital certificates, or via federation for additional security. Additional login options may include:

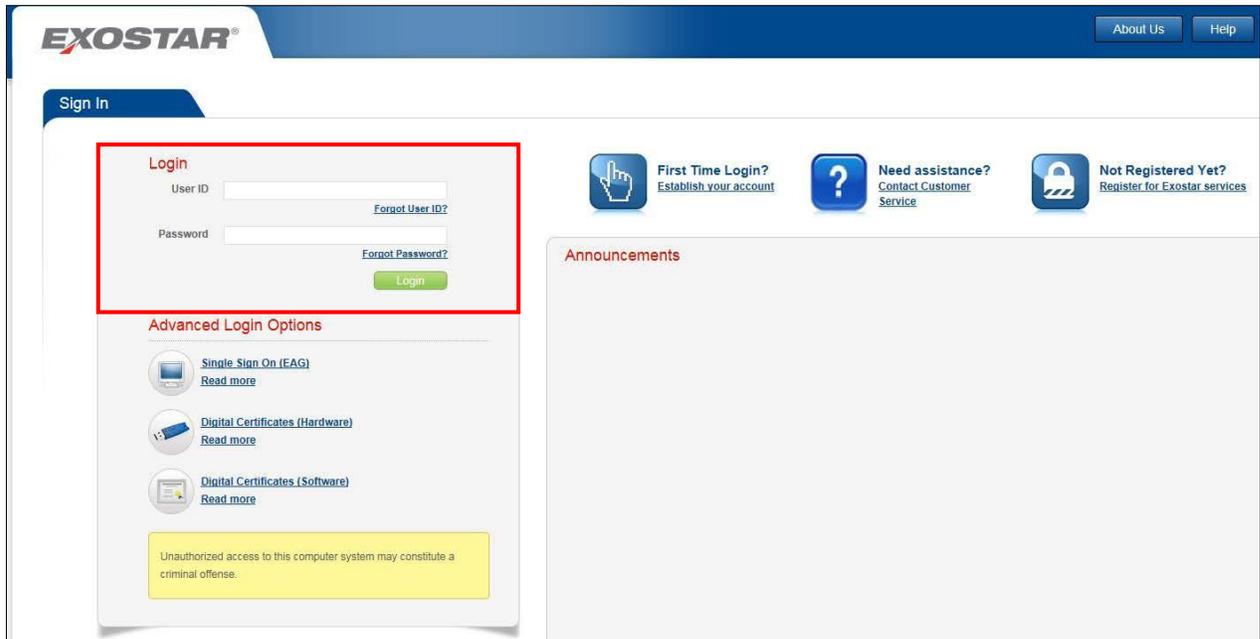
- **Exostar's Federated Identity Service (FIS) Certificates:** Allows you to invoke FIS certificates, in addition to your User ID and Password, to enable you to access all your applications, without being prompted to select the certificates when you access an application.
- **DOD Common Access Card (CAC):** Allows you to log-in to MAG, without your User ID and Password. For more information, refer to the [DOD CAC guide](#).
- **NGC OneBadge:** Allows you to use your NGC OneBadge to log-in to MAG without your User ID and Password.
- **Enterprise Access Gateway (EAG):** Allows you to log-in to MAG without your User ID and Password. Refer to **EAG section** for additional details.
- **One-Time Password Hardware Token:** In addition to your User ID and Password, you are required to enter the one-time password generated via a hardware token, purchased from Exostar. Refer to the [OTP Hardware Token User Guide](#) for additional details.

MAGアカウントにログインする

新しいユーザはアカウント作成後、承認されると初回ログイン(First Time Login)情報と手順を含んだメールを受け取ります。メールにはユーザID及びシステムが作成したパスワードが含まれます。詳細は[初回ログインガイド](#)を参照ください。

初回ログイン完了後は、以下の手順に沿ってMAGにアクセスしてください。

1. <https://portal.exostar.com>へ移動する。次の画面が表示される。



2. ユーザIDとパスワードを入力し、「Login」をクリックする。ログインできるとMAGアプリケーションのページが表示される。

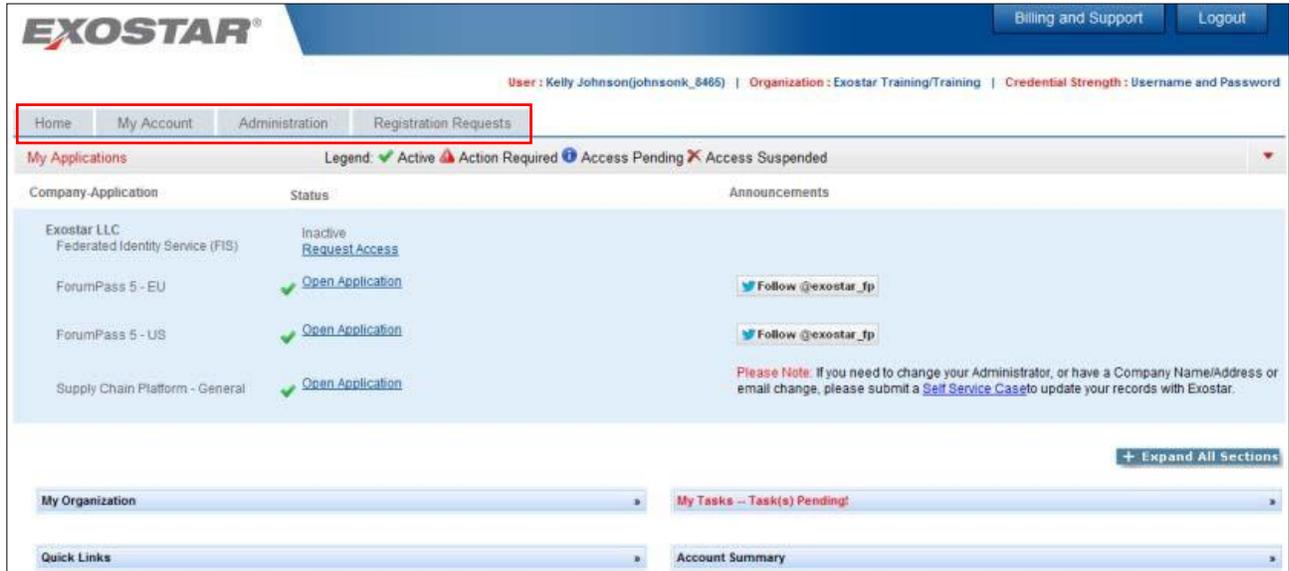
MAGにログインするその他のオプション

MAGでは、デジタル証明書を使用して、又は追加のセキュリティの連携によってアカウントにログインすることができます。その他のログインオプションには以下が含まれます。

- **Exostarのアイデンティティ連携サービス (FIS : Federated Identity Service) 証明書** : アプリケーションへのアクセス時に証明書の選択を求められることなく、ユーザIDとパスワード及びFIS証明書を呼び出し、すべてのアプリケーションにアクセスすることができます。
- **DODのコモンアクセスカード (CAC : Common Access Card)** : ユーザIDとパスワードなしでMAGにログインできます。詳細は[DOD CACガイド](#)を参照ください。
- **NGCのOneBadge** : NGCのOneBadgeを使用し、ユーザIDとパスワードなしでMAGにログインできます。
- **Enterprise Access Gateway (EAG)** : ユーザIDとパスワードなしでMAGにログインできます。詳細は[EAGセクション](#)を参照ください。
- **ワンタイムパスワード・ハードウェアトークン** : ユーザIDとパスワードのほかに、Exostarから購入したハードウェアトークンによって生成されるワンタイムパスワードを入力する必要があります。詳細は[OTP ハードウェアトークン・ユーザガイド](#)を参照ください。

MAG Portal Navigation

When you log-in to MAG, you are presented with the **Account Management Home** page. This may include two or more of the following four tabs (depending upon your role):



Note: click the **+Expand All Sections** button to expand all sections, or by clicking on the expander icon for the section

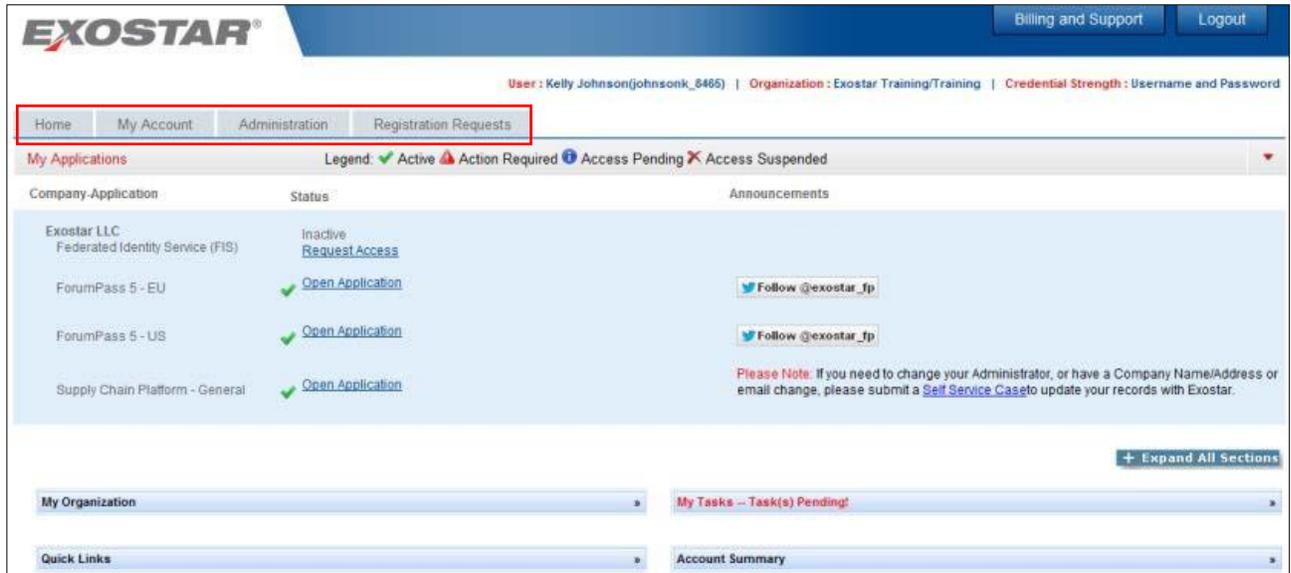
Home Tab

This tab has a number of components, which allow you to have a dashboard view of your MAG account. It contains information on your roles and responsibilities. Here is a brief introduction to the components of the Home tab:

- **My Applications:** The applications listed in the **My Applications** section are based on your subscriptions. Applications are grouped based on the **Service Provider** for easy view. The status of each application, and available actions, are provided next to the application name. If there are any special announcements for the application, the **Announcements** column provides the information.
- **My Organization:** Depending on your MAG roles, this section provides information regarding your organization account, along with the available subscriptions. The view presented below is for a user with the **Organization Administrator** role.
- **My Tasks:** You are able to view this section by clicking the **+Expand All Sections** button to expand all sections, or by clicking the expander icon for the section. Depending on your roles, you may view all requests pending approval by you.
- **Account Summary:** You are able to view this section by clicking the **+Expand All Sections** button to expand all sections, or by clicking the expander icon for the section. This section provides information on your account, and roles for your MAG account.
- **Quick Links:** You are able to view this section by clicking the **+Expand All Sections** button to expand all sections, or by clicking the expander icon for the section. This section provides links to various training demos, and additional support links for quick reference.

MAGポータルナビゲーション方法

MAGにログインすると、「**Account Management Home**（アカウント管理ホーム）」のページが表示されます。このページには次の4つのタブのうちの2つ以上が（ユーザの役割に応じて）含まれます。



注：すべてのセクションを展開するには「**+Expand All Sections**」ボタンをクリックしてください。各セクションを展開するには、該当セクションの展開アイコンをクリックしてください。

Homeタブ

このタブは多数の要素を含み、MAGアカウントのダッシュボード画面を表示します。ユーザ各自の役割及び責任に関する情報が含まれます。Homeタブの要素を以下に簡単に紹介します。

- My Applications**：「**My Applications**」セクションにはユーザの加入サービスに基づきアプリケーションが一覧で表示されます。アプリケーションは見やすいように「**Service Provider**」毎に表示されます。各アプリケーションのステータスや可能なアクションがアプリケーション名の横に示され、アプリケーションに関して特別なお知らせがある場合には「**Announcements**」に情報が表示されます。
- My Organization**：このセクションでは、MAGにおけるユーザ各自の役割に応じた利用可能な加入サービスの情報とともに組織アカウントに関する情報を提供します。以下に示す画面は、組織管理者（**Organization Administrator**）の役割を持つユーザ用の画面です。
- My Tasks**：このセクションを表示するには、「**+Expand All Sections**」ボタンをクリックしてセクションをすべて展開するか、又はこのセクションの展開アイコンをクリックしてください。役割に応じた、ユーザ本人からの承認待ちリクエストをすべて見ることができます。
- Account Summary**：このセクションを表示するには、「**+Expand All Sections**」ボタンをクリックしてセクションをすべて展開するか、又はこのセクションの展開アイコンをクリックしてください。このセクションではアカウント情報及びMAGアカウントにおける役割が提供されます。
- Quick Links**：このセクションを表示するには、「**+Expand All Sections**」ボタンをクリックしてセクションをすべて展開するか、又はこのセクションの展開アイコンをクリックしてください。このセクションでは様々なトレーニングデモへのリンクや参考用の追加のサポートリンクが提供されます。

Account Tab

This tab provides information regarding your account. You can also find information on your Organization, including Administrator information, and manage your Digital Certificates and/or Tokens. You can make modifications to your account by selecting appropriate actions.

Administration Tab: Users with administration privileges for your organization have access to this tab. Administrators can view information on all users linked to your organization, and can manage user accounts and access.

Registration Requests Tab

Users with administration privileges for your organization have access to this tab. Administrators can approve users who have self-registered, complete application approvals and authorization tasks, and approve OTP Hardware Tokens under this tab.

Note: For further information on the administration tasks, refer to [MAG Administration Guides](#).

Credential Strength

In addition to the available tabs, you are also provided information on the credential strength of your log-in. This information is provided in the upper right-hand corner of the screen.



The following information may be presented under **Credential Strength** depending on how you logged-in:

- **Username & Password:** If you logged-in to MAG using only your user ID and password
- **Basic Software Certificate:** If you logged-in to MAG using your FIS Basic Level of Assurance (BLOA) certificates
- **MLOA Software:** If you logged-in to MAG using FIS Medium Level of Assurance (MLOA) software certificates
- **MLOA Hardware:** If you logged-in to MAG using FIS Medium Level of Assurance (MLOA) hardware, or any eligible third party LOA three certificates, such as DOD Common Access Card (CAC)
- **OTP Hardware Token:** If you logged-in to MAG using an OTP Hardware Token

Accountタブ

このタブはユーザ・アカウントに関する情報を提供します。管理者 (Administrator)情報を含め、組織 (Organization)に関する情報を見ることができ、デジタル証明書及び/又はトークンを管理することもできます。該当するアクションを選択してアカウントの修正も行えます。

Administrationタブ

組織の管理権限を持つユーザはこのタブにアクセスすることができます。管理者 (Administrators)は、組織にリンクされたユーザすべての情報を見ることができ、ユーザのアカウント及びアクセス権を管理することができます。

Registration Requestsタブ

組織の管理権限を持つユーザはこのタブにアクセスすることができます。管理者 (Administrators)はこのタブで、セルフ登録したユーザの承認、申請承認・権限付与タスクの完了、及びOTPハードウェアトークンの承認を行うことができます。

注：管理タスクに関するさらなる詳細は、[MAG 管理ガイド](#)を参照ください。

Credential Strength (クレデンシャルの強度)

利用可能なタブのほかに、ログイン・クレデンシャルの強度に関する情報も提供されます。この情報は、画面右上の角に表示されます。

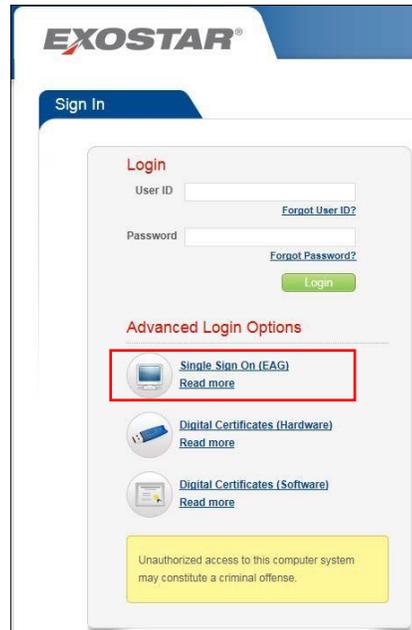


ログイン方法に応じて、次の情報が「**Credential Strength**」に表示されます。

- **Username & Password** : ユーザIDとパスワードのみでMAGにログインした場合
- **Basic Software Certificate** : FISの基本保証レベル (BLOA : Basic Level of Assurance) 証明書でMAGにログインした場合
- **MLOA Software** : FISの中保証レベル (MLOA : Medium Level of Assurance) ソフトウェア証明書でMAGにログインした場合
- **MLOA Hardware** : FISの中保証レベル (MLOA : Medium Level of Assurance) ハードウェア、又はDODのコモンアクセスカード (CAC : Common Access Card) 等の、適当な第三者のLOA 3証明書でMAGにログインした場合
- **OTP Hardware Token** : OTPハードウェアトークンでMAGにログインした場合

[Enterprise Access Gateway \(EAG\) Information](#)

For users using the **Enterprise Access Gateway (EAG)** functionality, you are able to link your account by following the link highlighted below:



For users with linked accounts: If you would like to access MAG outside of your company's network you may contact your Organization Administrator for delinking of your account.

[Forgotten User ID and Password](#)

You can change your password for the following three scenarios:

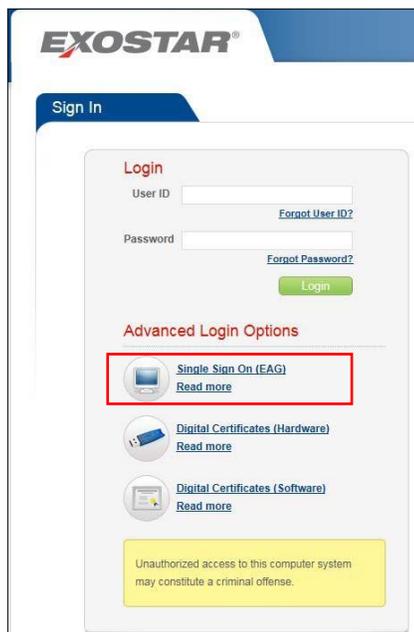
- Forgotten user ID for an active account
- Forgotten password for an active account
- Password has expired

Note: These options are not available if your MAG account is linked to your corporate network log-in via EAG. If you have issues accessing your account, refer to the [EAG User Guide](#) for quick reference, or contact [Exostar Customer Support](#) for additional information.

If you forgot your credentials for the **First Time Login**, refer to the [First Time Login Guide](#).

[Enterprise Access Gateway \(EAG\) に関する情報](#)

Enterprise Access Gateway (EAG) 機能を使用しているユーザは、以下の印がつけられたリンクからアカウントをリンクすることができます。



リンクしたアカウントを持つユーザ様へ：社内ネットワークの外でMAGにアクセスする場合は、アカウントのリンクを解除するため組織管理者（Organization Administrator）にご連絡ください。

[ユーザIDとパスワードを忘れた場合](#)

パスワードは次の3つの状況において変更することができます。

- アクティブなアカウントのユーザIDを忘れた場合
- アクティブなアカウントのパスワードを忘れた場合
- パスワードの有効期限が切れた場合

注：上記のオプションは、MAGアカウントがEAGを介した社内ネットワーク・ログインとリンクしている場合には使用できません。アカウントへのアクセスに問題がある場合、[EAGユーザガイド](#)を参照いただくか、追加の情報は[Exostarカスタマーサポート](#)までお問い合わせください。

初回ログイン（First Time Login）用のクレデンシャルを忘れた場合は、[初回ログインガイド](#)を参照ください。

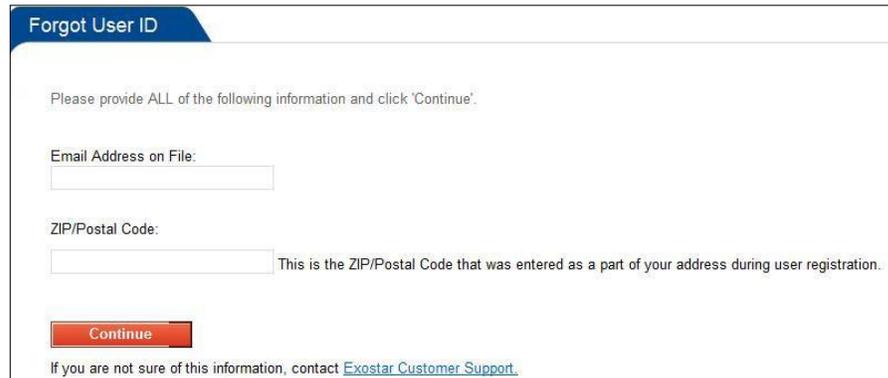
Forgotten User ID for an Active Account

1. Access the MAG log-in page at <https://portal.exostar.com>, and click the **Forgot User ID?** link.



The screenshot shows the 'Sign In' page with a 'Login' form. The form has two input fields: 'User ID' and 'Password'. A red box highlights the 'Forgot User ID?' link located to the right of the 'User ID' field. Below the 'Password' field is a 'Forgot Password?' link and a green 'Login' button.

2. Enter your **Email Address** and **Zip/Postal Code** for your MAG account, and click **Continue**.



The screenshot shows the 'Forgot User ID' page. It contains the following text: 'Please provide ALL of the following information and click 'Continue''. Below this are two input fields: 'Email Address on File:' and 'ZIP/Postal Code:'. A note next to the ZIP/Postal Code field states: 'This is the ZIP/Postal Code that was entered as a part of your address during user registration.' At the bottom, there is a red 'Continue' button and a link: 'If you are not sure of this information, contact [Exostar Customer Support](#).'

3. You will receive a confirmation page, and an email is sent to your email address with a password. You can now log-in to your MAG account using the new password.

If you receive an error stating multiple user IDs were found for this email address, contact [Exostar Customer Support](#) for further help.

Forgotten Password for an Active Account

1. Access the MAG login page at <https://portal.exostar.com>, and select the **Forgot Password?** link.



The screenshot shows the 'Sign In' page with a 'Login' form. The form has two input fields: 'User ID' and 'Password'. A red box highlights the 'Forgot Password?' link located to the right of the 'Password' field. Above the 'User ID' field is a 'Forgot User ID?' link and a green 'Login' button.

2. Enter your **User ID** and click **Continue**.



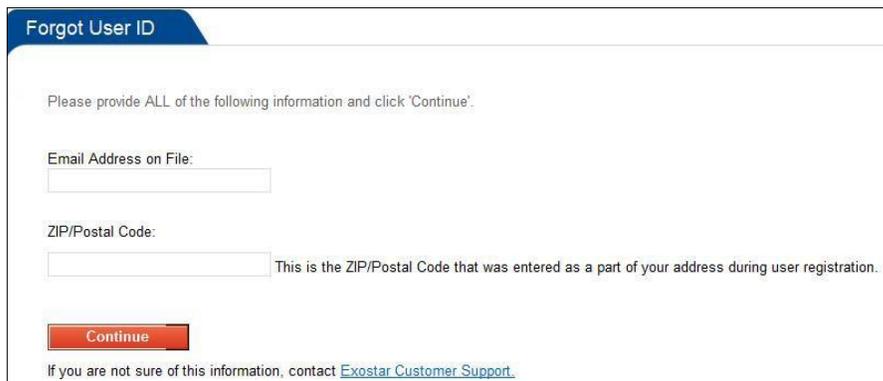
The screenshot shows the 'Forgot/Reset Password' page. It contains a single input field labeled 'User ID:' and a red 'Continue' button below it.

アクティブなアカウントのユーザIDを忘れた場合

1. <https://portal.exostar.com>でMAGログインページにアクセスし、「**Forgot User ID?**」のリンクをクリックする。



2. MAGアカウントの「**Email Address**」と「**Zip/Postal Code**」を入力後、「**Continue**」をクリックする。

A screenshot of the 'Forgot User ID' page. The page has a blue header with 'Forgot User ID'. Below it is a form with the instruction 'Please provide ALL of the following information and click 'Continue''. There are two input fields: 'Email Address on File:' and 'ZIP/Postal Code:'. Below the ZIP/Postal Code field is a note: 'This is the ZIP/Postal Code that was entered as a part of your address during user registration.' At the bottom, there is a red 'Continue' button. Below the button is a link: 'If you are not sure of this information, contact [Exostar Customer Support](#).'

3. 確認ページが表示され、メールアドレスにパスワードを含んだメールが届く。新しいパスワードを使用してMAGアカウントにログインできるようになる。

メールアドレスに対して複数のユーザIDが該当するというエラーが表示された場合は、[Exostarカスタマーサポート](#)までお問い合わせください。

アクティブなアカウントのパスワードを忘れた場合

1. <https://portal.exostar.com>でMAGログインページにアクセスし、「**Forgot User ID?**」のリンクをクリックする。



2. 「**User ID**」を入力後、「**Continue**」をクリックする。

A screenshot of the 'Forgot/Reset Password' page. The page has a blue header with 'Forgot/Reset Password'. Below it is a form with a 'User ID:' label and an input field. At the bottom, there is a red 'Continue' button.

3. The **Answer Security Questions** screen is displayed. Enter answers for two (2) questions, and click **Continue**.

Note: You will be prompted with the four questions that you previously selected during your initial account setup. The answers to the security questions are case sensitive. If you have forgotten the answers to your security questions, refer to the *Security Questions* section.

4. The **Create New Password** screen is displayed. Enter your new password twice and click **Continue**.

5. You will receive a confirmation message indicating your password has been successfully changed.

here'."/>

3. 「**Answer Security Questions**」画面が表示される。2つの質問の答えを入力して「**Continue**」をクリックする。

注：アカウントの初期設定時に選択した4つの質問が尋ねられます。セキュリティ質問の答えは大文字と小文字が区別されます。セキュリティ質問の答えをお忘れの場合、「セキュリティ質問」のセクションを参照ください。

4. 「**Create New Password**」画面が表示される。新しいパスワードを2回入力して「**Continue**」をクリックする。

5. パスワードが変更されたことを示す確認メッセージが届く。

here'."/>

Expired Password for an Active Account

If you attempt to log in and your password has expired you will receive the following message.



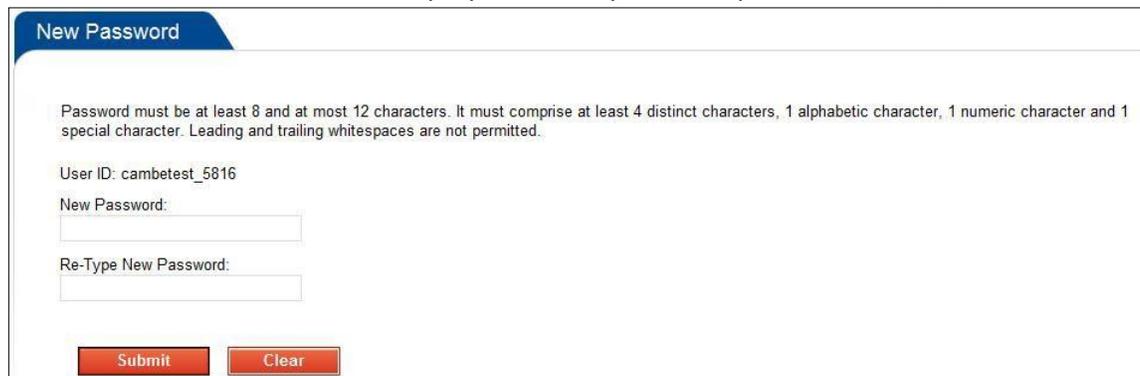
Follow the steps below to reset your password:

1. Click the **Reset Password** button (shown above).
2. The **Answer Security Questions** screen is displayed. Enter answers for two questions, and click **Continue**.



Note: You will be prompted with the four questions that you previously selected during your initial account setup. The answers to the security questions are case sensitive. If you have forgotten the answers to your security questions, refer to the *Security Questions* section.

3. The **Create New Password** screen is displayed. Enter your new password twice, and click **Submit**.



4. A confirmation message is presented indicating your password has been successfully changed.

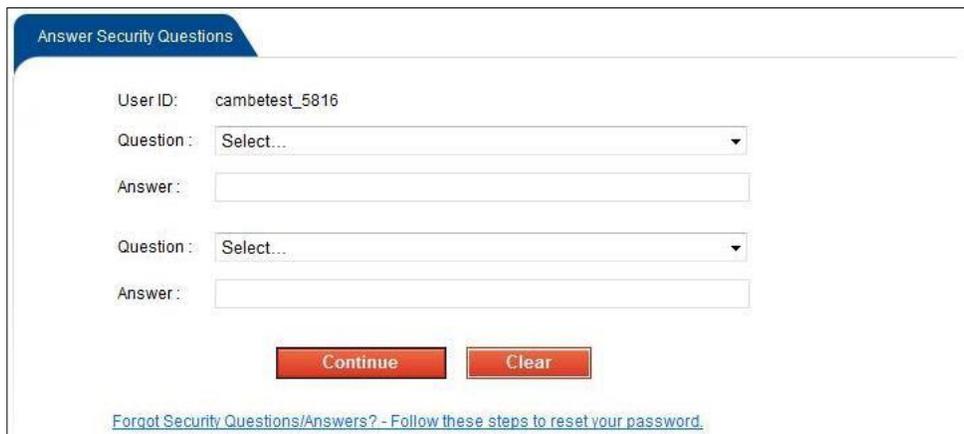
アクティブなアカウントのパスワードの有効期限が切れた場合



ログイン時にパスワードの有効期限が切れている場合、次のメッセージが表示されます。

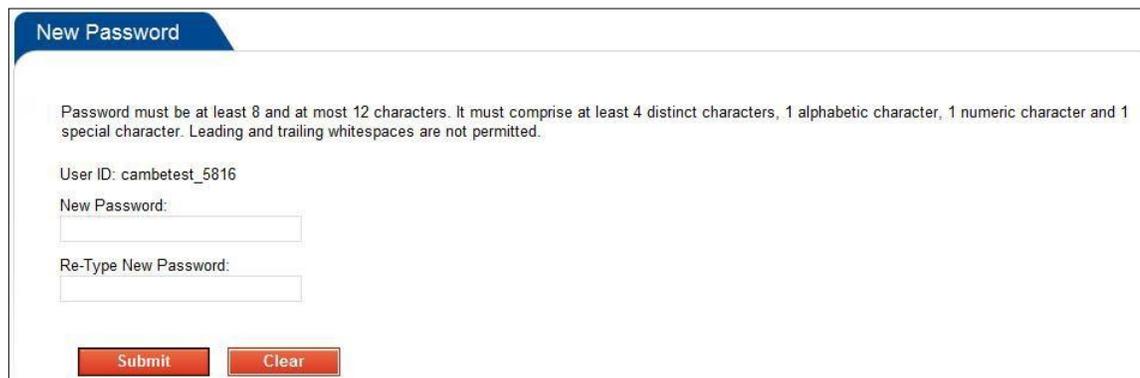
以下の手順に沿ってパスワードをリセットしてください。

1. 「**Reset Password**」 ボタンをクリックする（上記参照）。
2. 「**Answer Security Questions**」 画面が表示される。2つの質問の答えを入力して「**Continue**」をクリックする。



注：アカウントの初期設定時に選択した4つの質問が尋ねられます。セキュリティ質問の答えは大文字と小文字が区別されます。セキュリティ質問の答えをお忘れの場合、「**セキュリティ質問**」のセクションを参照ください。

3. 「**Create New Password**」 の画面が表示される。新しいパスワードを2回入力して「**Continue**」をクリックする。



4. パスワードが変更されたことを示す確認メッセージが届く。

Forgotten Security Questions/Answers

In the event that you have forgotten the answers to your security questions, follow the steps below to proceed:

1. Click on the **Forgot Security Questions/Answers?** link.



2. Enter the **Email Address** and the **ZIP/Postal Code** associated to this account, and click **Continue**.

Exostar Customer Support.' At the bottom of the form is a red button labeled 'Continue'." data-bbox="180 443 912 649"/>

3. You will receive an email containing a temporary **system-generated password**.
4. Return to the main MAG log-in page at <https://portal.exostar.com>. Log-in using your:
 - User ID
 - Temporary system-generated password

セキュリティ質問／答えを忘れた場合

セキュリティ質問の答えを忘れた場合、以下の手順に沿って進んでください。

1. 「**Forgot Security Questions/Answers?**」のリンクをクリックする。

2. アカウントの「**Email Address**」及び「**Zip/Postal Code**」を入力後、「**Continue**」をクリックする。

3. システムが作成した仮パスワードを含んだメールが届く。
4. MAGのメインログインページ (<https://portal.exostar.com>) に戻り、次の情報を使用してログインする。
 - ユーザID
 - システムが作成した仮パスワード

- The **Create New Password** screen is displayed. Enter your new password twice, and click **Submit**.

- You will receive a confirmation message indicating your password was successfully changed.

Note: This feature is not available if your MAG account is linked to your corporate network log-in via EAG. If you have issues accessing your account, refer to the [EAG User Guide](#) for quick reference, or contact [Exostar Customer Support](#) for additional information.

Application Management

The MAG **Applications** page displays all of applications for which your organization has a subscription. The Applications page also includes information on the status of these applications for your account, and all available actions. If your organization is subscribed to an application group, it is listed under the **Application Groups** section.

The page also displays any messages or announcements from Exostar or the application owner. When you log-in to <https://portal.exostar.com> with your credentials, the system automatically identifies your designation and presents your view of the dashboard. For most users, the following view is available:

- 「**Create New Password**」画面が表示される。新しいパスワードを2回入力して「**Continue**」をクリックする。

- パスワードが変更されたことを示す確認メッセージが届く。

注：この機能は、MAGアカウントがEAGを介した社内ネットワーク・ログインとリンクしている場合には使用できません。アカウントへのアクセスに問題がある場合、[EAGユーザガイド](#)を参照いただくか、追加の情報は[Exostarカスタマーサポート](#)までお問い合わせください。

アプリケーションを管理する

MAGの「**Applications**」ページでは、ユーザの組織が加入しているすべてのアプリケーションが表示されます。「**Applications**」ページには、ユーザのアカウントにおけるアプリケーションのステータス及び可能なアクションも含まれます。組織が・に加入している場合は「**Application Groups**」セクションに表示されます。

Exostarやアプリケーション・オーナーからのメッセージやお知らせもこのページに表示されます。クレデンシャルを使用して<https://portal.exostar.com>にログインすると、システムが自動でユーザの役割（**designation**）を特定して各ユーザ用のダッシュボード画面を表示します。通常、以下の画面がご利用いただけます。

Application Status Information

#	Status	Status Description	User Action
1.	Active	Subscription is approved to access the application	Click Open Application to launch the application in a separate browser window
2.	Organization Registration Approval Pending	The organization's request for subscription to the application has not yet been approved. No user can request access to the application	None
3.	Pending Account Creation by the Application	The application has not yet been provisioned by the Service Provider (SP).	None
4.	Pending Approval by the Application Owner	Request is pending approval by the SP Administrator	None
5.	Pending Application Administrator Approval	Application administrator (App Admin) has not approved the subscription request	Contact the App Admin for the application.
6.	Pending Activation	SCP App Admin has not yet activated your SCP application subscription	Contact the App Admin for the SCP application
7.	Pending Acceptance of Terms & Conditions	Organization Administrator (Org Admin) has not yet accepted the Terms & Conditions for access to the application	Contact the Org Admin for information.
8.	Inactive	You are not subscribed to the application, but the organization is subscribed to the application. The Org Admin & EPA can also request application subscriptions on your behalf.	If you need access to the application, click the Request Access button next to the inactive status. Your request is then in Pending Application Administrator Approval status.
9.	Suspended	Your application access has been suspended.	None
10.	Pending Exostar Approval	Specific to FIS Medium Level of assurance request, your request is pending approval by the Exostar Portal Administrator.	Contact Exostar Customer Support for information on delay in approval
11.	Pending Proofing	Specific to FIS Medium Level of assurance request, you need to complete in-person proofing process	Contact Exostar Customer Support for information if in-person proofing has been completed
12.	Pending Application Administrator Approval	You have an active FIS subscription, and have reapplied to get new certs.	None

Request Access

To request access to an application, click the **Request Access** link from the **Status** column. Depending on the selected application, you are presented with application specific registration upgrade screens. Refer to the sections below for application-specific information.

Requesting access to all single applications (other than FIS)

1. Click the **Request Access** button under the **Status** column.



NOTE: An Exostar Administrator, your Organization Administrator, or the organization who invited you to access the application *may* provide a sponsor code. This is **NOT** a required field, so if you do not have

アプリケーションのステータスに関する情報

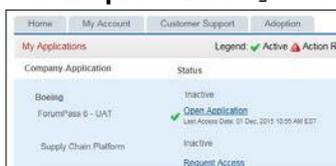
#	ステータス	ステータスの説明	ユーザによるアクション
1.	Active	アプリケーションにアクセスするための加入登録承認済み	新しいウィンドウでアプリケーションを起動するには「 Open Application 」をクリックする
2.	Organization Registration Approval Pending	組織がアプリケーションに加入するためのリクエストが未承認。ユーザからのアプリケーションへのアクセス申請は不可。	なし
3.	Pending Account Creation by the Application	アプリケーションがサービスプロバイダ (SP) にプロビジョニングされていない。	なし
4.	Pending Approval by the Application Owner	リクエストはSP管理者からの承認待ち	なし
5.	Pending Application Administrator Approval	加入リクエストはアプリケーション管理者(App Admin)から未承認。	アプリケーションのアプリケーション管理者に問い合わせる
6.	Pending Activation	アプリケーションへの加入はSCPのApp Adminによってまだ有効化されていない。	SCPアプリケーションのアプリケーション管理者に問い合わせる
7.	Pending Acceptance of Terms & Conditions	アプリケーションへアクセスするための契約条件は組織管理者(Org Admin)からの同意待ち。	組織管理者に問い合わせる
8.	Inactive	ユーザはアプリケーションに加入していないが、組織はアプリケーションに加入している。組織管理者及びEPAがユーザに代わりアプリケーションへの加入をリクエストできる。	アプリケーションへのアクセス権が必要な場合、非アクティブのステータスの横にある「Request Access」ボタンをクリックする。リクエストは「Pending Application Administrator Approval」のステータスになる。
9.	Suspended	アプリケーションへのアクセスが停止されている。	なし
10.	Pending Exostar Approval	FIS中保障レベルのリクエストに関して、Exostarの「ポータル管理者」からの承認待ち	承認の遅れに関して Exostarカスタマーサポート に問い合わせる
11.	Pending Proofing	FIS中保障レベルのリクエストにおいて、ユーザは対面検証を完了しなければならない。	対面検証が完了している場合、 Exostarカスタマーサポート に問い合わせる。
12.	Pending Application Administrator Approval	ユーザはアクティブなFIS会員であり、新しい証明書を取得するために再申請している。	なし

アクセスを申請する

アプリケーションへのアクセスを申請するには、「**Status**」の「**Request Access**」リンクをクリックしてください。選択したアプリケーションに応じて、アプリケーションに固有の登録アップグレード画面が表示されます。アプリケーション固有の情報に関しては以下を参照ください。

個々のアプリケーションへのアクセスを申請する (FISを除く)

1. 「**Status**」欄の「**Request Access**」ボタンをクリックする。



this information, click **Next**. If you have questions regarding the sponsor code, contact the sponsor or contact [Exostar Customer Support](#)

Home My Account

Request Access

ForumPass 5

This is an optional field. If available, enter comma-separated sponsor code(s). For help on Sponsor Codes, [view more information](#).

Cancel Next >>

2. Click **Next** to complete the application access request. You will be presented with a confirmation page.

Home My Account

Submission Confirmation

Thank you for submitting your registration. Once your registration has been processed, you will be contacted by Exostar Customer Service within the next 24-72 hours, after which you can access products and services that you have selected.
You may close your browser at any time or click <http://www.exostar.com> for more information about Exostar.
If you need to contact Exostar for any questions, visit our support site: <http://www.myexostar.com/contactSupport.aspx>. Our Customer Service Team is available Monday through Friday 3 a.m. to 9 p.m. EST.
Please use reference number SIG_1366642050888 when you contact Exostar Customer Service.

What Happens Next?

- The **Application Administrator** for the application needs to approve your request for access.
- If the **Application Administrator** approves the request, the **Application Owner** receives a notification to approve your access to the application.
- Once the **Application Owner** approves the access, you will receive a notification indicating your access to the application has been approved.

Requesting Access to an Application Group

1. Click the **Request Access** link under the **Status** column.

My Application Groups	
Group Name	Status
Rolls-Royce eTools Federated Identity Service (FIS) SourcePass Rolls-Royce Enterprise Supply Chain Platform Rolls-Royce Global Supplier Portal	Inactive Request Access

注：Exostar管理者（Exostar Administrator）、組織管理者（Organization Administrator）またはアプリケーションにアクセスするようユーザを招待した組織が、スポンサーコードを提供する場合があります。スポンサーコードは必須フィールドではないため、この情報がない場合は「Next」をクリックしてください。スポンサーコードに関する質問は、スポンサーまたは[Exostarカスタマーサポート](#)までお問い合わせください。

2. 「Next」をクリックし、アプリケーションへのアクセス申請を完了する。確認ページが表示される。

この後の流れ

- アクセス申請は、アプリケーションのアプリケーション管理者から承認されなければなりません。
- アプリケーション管理者が申請を承認すると、ユーザのアプリケーションへのアクセスを承認するようにアプリケーション・オーナーに通知が送信されます。
- アプリケーション・オーナーがアクセスを承認すると、アプリケーションへのアクセスが承認されたという通知がユーザに送信されます。

アプリケーション・グループへのアクセスを申請する

1. 「Status」欄の「Request Access」リンクをクリックする。

Group Name	Status
Rolls-Royce eTools Federated Identity Service (FIS) SourcePass	Inactive Request Access
Rolls-Royce Enterprise Supply Chain Platform	Inactive Request Access
Rolls-Royce Global Supplier Portal	Inactive Request Access

- Review all information, and click **Next** to complete the application access request. You are presented with a confirmation page.

Request Access

Please complete and submit the following information regarding this application group. Fields marked with asterisks(*) are required.

User Information

First Name: Teresa	Street Address 1: Selma Lane
Middle Name:	Street Address 2:
Last Name: Cambetes	City: Leesburg
Email: teresa.cambetes@exostar.com	State: VA
Phone: 703-431-8676	Zip/Postal Code: 20175
Fax:	Country: US

FIS Certificate Information

Partner/Application: * Select the partner or application for which you are requesting FIS certificates

Certificate Assurance Level: * Not sure of what to choose for any of these fields? - [View more information on Certificate Assurance Level, Type, and Usage.](#)

Certificate Usage: *

Certificate Type: *

Certificate Validity Period: *

Request Reason: *

Next >>

What Happens Next?

- The administrator for the application needs to approve your request for access to the application group.
- If the administrator approves the request, you receive an email advising of your access.
- If the application group includes FIS, and you are approved for a basic level of assurance certificate, you will receive an approval email with a passcode to download your certificates. Refer to the **Manage Certificates** section for information on downloading your certificate.

Requesting access to FIS

- Click the **Request Access** link under the **Action** column for the **FIS application**.
- Enter the **FIS Certificate Information**:

Home | My Account | Administration | Registration Requests

Request Access

FIS Certificate Information

Please complete and submit the following information regarding FIS certificates. Fields marked with asterisks (*) are required.

FIS Sponsor Code(s): This is an optional field. If you have multiple sponsor codes, enter each separated by a comma(,) - [View more information on sponsor codes.](#)

* Partner/Application: Select the partner or application for which you are requesting FIS certificates

* Certificate Assurance Level: Not sure of what to choose for any of these fields? - [View more information on Certificate Assurance Level, Type, and Usage.](#)

* Certificate Usage:

* Certificate Type:

* Certificate Validity Period:

* Request Reason:

2. 情報を確認後「Next」をクリックし、アプリケーションへのアクセス申請を完了する。確認ページが表示される。

Request Access

Please complete and submit the following information regarding this application group. Fields marked with asterisks(*) are required.

User Information

First Name: Teresa	Street Address 1: Selma Lane
Middle Name:	Street Address 2:
Last Name: Cambetes	City: Leesburg
Email: teresa.cambetes@exostar.com	State: VA
Phone: 703-431-8676	Zip/Postal Code: 20175
Fax:	Country: US

FIS Certificate Information

* Partner/Application: <input type="text" value="Rolls-Royce GSP"/>	Select the partner or application for which you are requesting FIS certificates
* Certificate Assurance Level: <input type="text" value="Basic"/>	Not sure of what to choose for any of these fields? - View more information on Certificate Assurance Level, Type, and Usage.
* Certificate Usage: <input type="text" value="Identity"/>	
* Certificate Type: <input type="text" value="Software"/>	
* Certificate Validity Period: <input type="text" value="1 Year"/>	
* Request Reason: <input type="text" value="Access Application"/>	

この後の流れ

- アプリケーション・グループへのアクセス申請は、アプリケーションの管理者から承認されなければなりません。
- 管理者が申請を承認すると、アクセスが承認されたというメール通知が届きます。
- アプリケーション・グループにFISが含まれ、基本保証レベルの証明書を承認されると、証明書をダウンロードするためのパスコードを含んだ承認メールが届きます。証明書のダウンロード方法については、「[証明書を管理する](#)」のセクションを参照ください。

FISへのアクセスを申請する

1. FISアプリケーションの「Action」欄の「Request Access」リンクをクリックする。
2. 「FIS Certificate Information (FIS証明書情報)」を入力する。

Request Access

FIS Certificate Information

Please complete and submit the following information regarding FIS certificates. Fields marked with asterisks (*) are required.

FIS Sponsor Code(s): <input type="text"/>	This is an optional field. If you have multiple sponsor codes, enter each separated by a comma(,) - View more information on sponsor codes.
* Partner/Application: <input type="text" value="Select..."/>	Select the partner or application for which you are requesting FIS certificates
* Certificate Assurance Level: <input type="text" value="Select..."/>	Not sure of what to choose for any of these fields? - View more information on Certificate Assurance Level, Type, and Usage.
* Certificate Usage: <input type="text" value="Select..."/>	
* Certificate Type: <input type="text" value="Select..."/>	
* Certificate Validity Period: <input type="text" value="Select..."/>	
* Request Reason: <input type="text" value="Select..."/>	

- **Sponsor Code:** An **Exostar Administrator**, your **Organization Administrator**, or the **organization who invited you** for access to the application may provide a sponsor code. This is **NOT** a required field.
Note: If you have questions regarding the sponsor code, contact the sponsor, and refer to the [information](#) on our customer site, or contact [Exostar Customer Support](#) for additional information.
- **Partner/Application:** Click this field to display the drop-down list of **Partners/Applications**, who may require you to have FIS certificates. This helps the FIS Administrator in approving your request with the appropriate information. You may select the **Other/Unspecified** option if you don't have this information.
- **Certificate Assurance Level:** You have the option to select **Basic** (for Basic Level of Assurance), **Medium** (for Medium Level of Assurance), or **Unknown**. Please note if you select **Unknown**, your FIS Administrator may take additional time to approve your request to ensure they approve you for the correct certificate option.
- **Certificate Usage:** This option is only available when you select **Basic Level of Assurance**. The available options are:
 - Identity
 - Secure Email
 - Unknown**Note:** If you request FIS certificates to access ForumPass-US or ForumPass-EU applications, you **MUST** select **Identity** as the option for this field.
- **Certificate Type:** Depending on the assurance level selected, as well as the FIS subscription level of your organization's account, you may have all or some of the following options:
 - Software
 - Hardware
 - Unknown
- **Certificate Validity Period:** If you select **Basic**, you have only one option – 1 year. If you select **Medium** assurance, you are able to select from:
 - 1 year
 - 3 years
 - Unknown
- **Request Reason:** This allows you to provide information to the FIS Administrator on why you need the certificates.

Note: If you have any questions regarding the information selected for these fields, refer to the [detailed information](#) available on our customer site specific to **FIS Request** options.

3. **User Information:** Review the information in this section including your address and email address. If you are requesting Medium level of assurance certificates, it is important that the address

- 「**Sponsor Code (スポンサーコード)**」 : **Exostar管理者 (Exostar Administrator)**、**組織管理者 (Organization Administrator)** またはアプリケーションにアクセスするようユーザーを招待した組織が、スポンサーコードを提供する場合があります。スポンサーコードは必須フィールドではありません。
注 : スポンサーコードに関する質問は、スポンサーまたは[Exostarカスタマーサポート](#)までお問い合わせください。またはExostarカスタマーサポートサイトの[インフォメーション](#)を参照ください。
- 「**Partner/Application (パートナー/アプリケーション)**」 : このフィールドをクリックすると、ユーザーにFIS証明書の所持を求める「**Partners/Applications**」のドロップダウンリストが表示されます。この情報は、FIS管理者 (FIS Administrator) が適切な情報でユーザーの申請を承認する際に役立ちます。この情報がない場合は「**Other/Unspecified**」を選択してください。
- 「**Certificate Assurance Level (証明書の保証レベル)**」 : 「**Basic**」 (基本保証レベル)、 「**Medium**」 (中保証レベル) 又は「**Unknown**」 (不明) から選択してください。「**Unknown**」を選択した場合、正しい証明書を承認するために、FIS管理者 (FIS Administrator) がユーザーの申請を承認するまで通常より時間を要する場合があります。
- 「**Certificate Usage (証明書の利用)**」 : この選択肢は「**Basic**」 (基本保証レベル) を選択した場合のみ有効です。以下から選択してください。
 - 「**Identity (アイデンティティ)**」
 - 「**Secure Email (セキュアメール)**」
 - 「**Unknown (不明)**」注 : ForumPass-US又はForumPass-EUのアプリケーションにアクセスするためのFIS証明書を申請している場合、このフィールドで「**Identity**」を選択してください。
- 「**Certificate Type (証明書の種類)**」 : 選択した保証レベル及び組織のアカウントのFIS加入レベルに応じて、以下の選択肢すべて又は幾つかが提供されます。
 - 「**Software (ソフトウェア)**」
 - 「**Hardware (ハードウェア)**」
 - 「**Unknown (不明)**」
- 「**Certificate Validity Period (証明書の有効期間)**」 : 「**Basic**」を選択した場合、「**1 year**」のみを選択できます。「**Medium**」を選択した場合、以下の選択肢から選ぶことができます。
 - 「**1 year (1年)**」
 - 「**3 years (3年)**」
 - 「**Unknown (不明)**」
- 「**Request Reason (申請の理由)**」 : このフィールドでは、証明書が必要な理由をFIS管理者 (FIS Administrator) に提供することができます。

注 : これらのフィールドで選択する情報に関してご質問がある場合は、**FISの申請**に関するExostarカスタマーサイトの[詳細情報](#)を参照ください。

3. 「**User Information (ユーザー情報)**」セクションの、住所およびメールアドレスなどの情報を確認する。「**Medium**」保証レベルの証明書を申請している場合、対面検証のために記入された住所に信頼される代理人が派遣されるため、この情報が正しいことが重要である。

information is correct as this is the address where a trusted agent will be dispatched to complete in-person proofing.

User Information

Verify your user information with special attention to the email address. If you need to change your email address, you must change it before submitting your certificate request.

*First Name: Kelly
Middle Name:
*Last Name: Johnson
Email: kelly.johnson@exostar.com [Change Email](#)
*Phone: 703-444-1234
Fax:
*Street Address 1: 13530 Dulles Technology
Street Address 2:
*City: Herndon
*State: VA
*Zip/Postal Code: 20171
*Country: United States

Cancel Next >>

Note: If you click to modify your email information, you need to go through the email change process first, and once the email change process is complete, you need to restart the FIS request process.

4. Click **Next** to complete the application access request. Your request is now complete, and a confirmation page is presented.

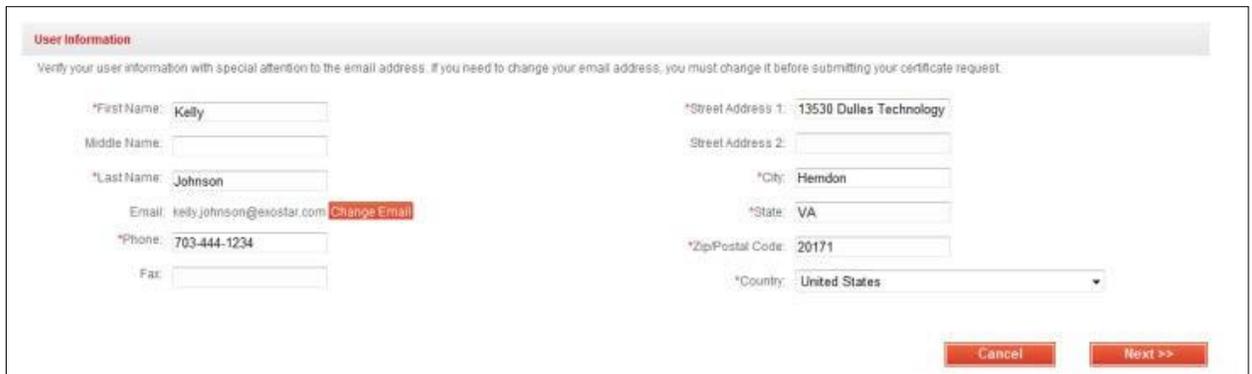
What Happens Next?

- The **FIS Administrator** receives a request to approve your FIS subscription. The FIS Administrator has the ability to modify your request.
- If your **FIS Application Administrator** approves you for **basic** level of assurance, you will receive an approval email with a passcode to download your certificates. Refer to the **Manage Certificates** section for information on the download process.
- If your **FIS Application Administrator** approves you for **medium** level of assurance, your request will be approved by **Exostar** (after purchase research), for an in-person proofing session with a trusted agent. More information on this proofing session is available [here](#). After a successful proofing session, the trusted agent provides a 16-digit passcode, which is needed to successfully download your certificates, after you receive an approval email from Exostar. Refer to the **Manage Certificates** section for information on downloading your certificates.

In-Person Proofing

Users who require **MLOA Software** or **MLOA Hardware** certificates are required to go through in-person proofing with a trusted agent. A trusted agent will contact you to set-up a proofing appointment at your convenience. Make sure you review the [proofing requirements](#) prior to your appointment, and take all required documentation to your appointment.

Note: If you fail to bring all required documents to the proofing appointment, you are invoiced additional charges for all subsequent appointments with the trusted agent or notary.



注：メールアドレスの変更をクリックした場合、まずメールアドレス変更手続きを行わなければなりません。メールアドレス変更手続き完了後、FISの申請手続きを再度開始してください。

4. 「Next」をクリックし、アプリケーションへのアクセス申請を完了する。申請手続きが完了し、確認ページが表示される。

この後の流れ

- **FIS管理者**は、FIS加入への承認申請を受け取ります。FIS管理者は申請内容を変更することができます。
- **FISアプリケーション管理者**により基本保証レベルが承認されると、証明書をダウンロードするためのパスコードを含んだ承認メールが届きます。証明書のダウンロード方法については、「[証明書を管理する](#)」のセクションを参照ください。
- **FISアプリケーション管理者**により中保証レベルが承認されると、この申請は、信頼される代理人との対面検証のためExostarから承認を受けます（購買リサーチ後）。対面検証に関する詳しい情報は[こちら](#)から。

信頼される代理人は対面検証終了後に16桁のパスコードを提供します。このパスコードは、Exostarから承認メールを受信した後に証明書をダウンロードする際に必要となります。証明書のダウンロードに関しては「[証明書を管理する](#)」セクションを参照ください。

対面検証

MLOAソフトウェア又は**MLOAハードウェア**証明書には、信頼される代理人との対面検証が必要となります。信頼される代理人から連絡がありますので、ご都合に合わせて対面検証を予約ください。予約日より前に[検証要件事項](#)をご確認いただき、当日は必要な書類をお持ちください。

注：対面検証時に必要書類をすべてお持ちでない場合、信頼される代理人又は公証人との次回以降の予約に追加料金がかかります。

Acceptance of Terms & Conditions

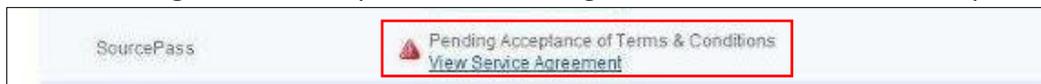
If you are the **Organization Administrator**, you will see a **View Service Agreement** link next to each application. Select this link to accept the terms and conditions.

The screenshot shows a web interface with a navigation bar at the top containing 'Home', 'My Account', 'Administration', and 'Registration Requests'. Below the navigation bar is a section titled 'My Applications' with a legend: Active (green checkmark), Action Required (red triangle), Access Pending (blue circle), and Access Suspended (red X). The main content area is divided into two tables. The first table, 'My Applications', has columns for 'Company-Application', 'Status', and 'Announcements'. It lists four applications: 'Exostar Rolls-Royce Enterprise Supply Chain Platform', 'Exostar LLC Federated Identity Service (FIS)', 'SourcePass', and 'Rolls-Royce Rolls-Royce Global Supplier Portal'. Each application has a status of 'Pending Acceptance of Terms & Conditions' and a 'View Service Agreement' link. The second table, 'My Application Groups', has columns for 'Group Name', 'Status', and 'Announcements'. It lists a group named 'Rolls-Royce eTools' which includes 'Federated Identity Service (FIS)', 'SourcePass', 'Rolls-Royce Enterprise Supply Chain Platform', and 'Rolls-Royce Global Supplier Portal'. This group also has a status of 'Pending Acceptance of Terms & Conditions' and a 'View Service Agreement' link.

NOTE: Users within your organization are not able to access the application until the **Organization Administrator** accepts the **Service Agreement** for the application.

To enable access to the application, complete the **Service Agreement** acceptance by following the steps below:

1. Click on **View Service Agreement** to open the Service Agreement for review and acceptance.



契約条件への同意

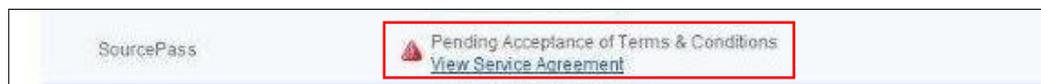
組織管理者（**Organization Administrator**）には、各アプリケーションの横に「**View Service Agreement**（サービス契約書を表示する）」のリンクが表示されます。このリンクを選択して契約条件に同意してください。

Home My Account Administration Registration Requests		
My Applications Legend: ✔ Active ⚠ Action Required ⏸ Access Pending ✖ Access Suspended		
Company-Application	Status	Announcements
Exostar Rolls-Royce Enterprise Supply Chain Platform	⚠ Pending Acceptance of Terms & Conditions View Service Agreement	
Exostar LLC Federated Identity Service (FIS)	⚠ Pending Acceptance of Terms & Conditions View Service Agreement	
SourcePass	⚠ Pending Acceptance of Terms & Conditions View Service Agreement	
Rolls-Royce Rolls-Royce Global Supplier Portal	⚠ Pending Acceptance of Terms & Conditions View Service Agreement	
My Application Groups		
Group Name	Status	Announcements
Rolls-Royce eTools Federated Identity Service (FIS) SourcePass Rolls-Royce Enterprise Supply Chain Platform Rolls-Royce Global Supplier Portal	⚠ Pending Acceptance of Terms & Conditions View Service Agreement	

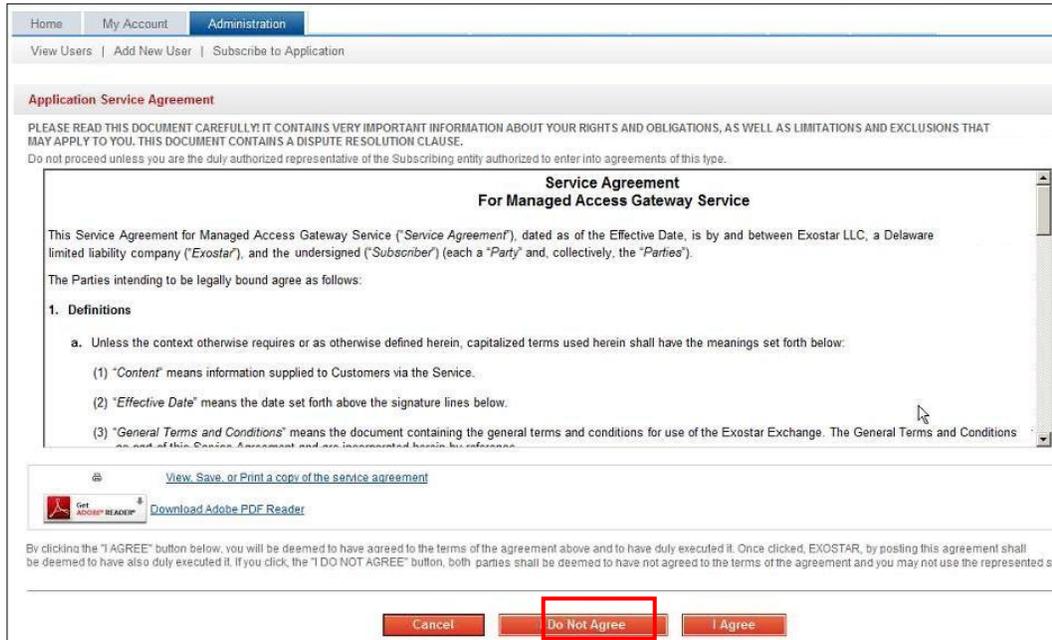
注：組織管理者（**Organization Administrator**）がアプリケーションのサービス契約書に同意するまで、組織内のユーザはアプリケーションにアクセスすることができません。

アプリケーションへのアクセスを有効にするには、以下の手順に沿ってサービス契約書に同意してください。

1. 「**View Service Agreement**（サービス契約書を表示する）」をクリックし、確認及び同意のためにサービス契約書を開く。



2. After reviewing the agreement, click the **I Agree** button to accept the agreement. The following screen is presented.



3. Complete this step for all subscribed applications.

What happens after accepting the Service Agreement?

- You can subscribe a user to the application. For information on how to add a user/subscribe a user to an application, refer to the [User Management Guide](#).
- A user within your organization may request access to the application themselves.

What happens if you do not accept the Service Agreement?

- If you select **Cancel**, you are taken back to the **Applications** page.
- If you select **I Do not Agree**, your application subscription will remain pending, and the **View Service Agreement** button is made available again.
- Users within your organization cannot access this application.

Email Confirmations

When the **Organization Administrator** accepts the **Service Agreement** for an application an email confirmation is sent out by **Exostar**.

[Account Management](#)

If you would like to change information regarding your account, you can do so by accessing the **My Account** tab after login. You have the following options:

- Update **Enterprise Access Gateway (EAG) Settings**
Note: This option is only available to those users who belong to an organizations subscribed to the EAG service
- View Organization Details

2. 契約内容を確認後、同意するには「I Agree」ボタンをクリックする。以下の画面が表示される。

3. 加入しているすべてのアプリケーションに対してこの手続きを行う。

サービス契約書に同意した後

- ユーザをアプリケーションに加入させることができます。ユーザをアプリケーションに追加／加入させる方法は、[ユーザ管理ガイド](#)を参照ください。
- 組織内のユーザは各自でアプリケーションへのアクセスを申請することができます。

サービス契約書に同意しない場合

- 「Cancel」を選択すると「Applications」ページに戻ります。
- 「I Do not Agree」を選択するとアプリケーションへの加入は保留され、「View Service Agreement」ボタンが再度表示されます。
- 組織内のユーザはアプリケーションにアクセスすることができません。

確認メール

組織管理者（Organization Administrator）がサービス契約書に同意すると、Exostarから確認メールが送信されます。

[アカウントを管理する](#)

アカウントの情報を変更したい場合は、ログイン後「My Account」タブにアクセスしてください。以下にオプションを紹介します。

- 「Update Enterprise Access Gateway (EAG) Settings（EAG設定を更新する）」
注：このオプションは、EAGサービスに加入している組織に属するユーザにのみ利用可能です。
- 「View Organization Details（組織情報を表示する）」

- Change Email
- Change Password
- Change Security Questions
- Manager Certificates (Note: This options is only available if you are approved for access to FIS)
- Manage OTP
- Connect Accounts

Edit Profile

- The **Edit Profile** page allows you to change your name and address information.
- Click on the **My Account** tab to view the **Edit Profile** page.
- You can update the available fields.
- Click the **Submit** button to complete the changes.

The screenshot displays the 'Edit Profile' page within the Exostar system. The navigation menu includes 'Home', 'My Account', 'Administration', and 'Registration Requests'. The 'My Account' section contains several options, with 'Edit Profile' highlighted by a red rectangle. The main content area is titled 'User Profile' and contains the following fields and information:

- User ID: cambetest_5816
- Email: tcambetes@aol.com
- Role: Org Admin, App Admin
- Organization Name: Exostar Training/Training
- Organization ID: EXO106099514
- Title: Select Title (dropdown)
- *First Name: Teresa
- Middle Name: (empty)
- *Last Name: Cambetes
- Job Title: (empty)
- *Phone: 703-555-1234
- Fax: (empty)
- *Street Address 1: 13530 Dulles Technology
- Street Address 2: (empty)
- *City: Herndon
- *State: VA
- *Zip/Postal Code: 20176
- *Country: UNITED STATES (dropdown)
- Time Zone: America/New_York (dropdown)
- Restricted Access: Off
- Created Date: N/A
- Suspended Date(From MAG): N/A
- Last MAG Access Date: 22 Apr, 2013 10:51 AM EDT

A red 'Submit' button is located at the bottom center of the form.

You are presented with a confirmation page, and an email is sent to the email address on record.

Notes:

- If your account has been linked to your corporate network account via Enterprise Access Gateway (EAG), your screen may look different. Refer to the section **Update Enterprise Access Gateway (EAG) Account Settings** for additional information.
- Not all profile information you update in the portal will propagate across all of your Exostar-enabled applications. You will have to update application-specific profiles within the respective application.
- **Restricted Access:** ON/OFF setting is one of the factors that determines whether you can access **Restricted Profile** sites in **ForumPass**. If you have any questions regarding this setting, please contact your **Organization Administrator**. If you are not using ForumPass, this setting is of no relevance to you.

- 「Change Email（メールアドレスを変更する）」
- 「Change Password（パスワードを変更する）」
- 「Change Security Questions（セキュリティ質問を変更する）」
- 「Manager Certificates（証明書を管理する）」（注：このオプションはユーザがFISへのアクセスを承認されている場合にのみ利用可能です。）
- 「Manage OTP（OTPを管理する）」
- 「Connect Accounts（アカウントを接続する）」

プロフィールを編集する

- 「**Edit Profile**」 ページで氏名および住所を変更することができます。
- 「**My Account**」 タブをクリックし、「**Edit Profile**」 ページを表示してください。
- 有効なフィールドを更新できます。
- 「**Submit**」 ボタンをクリックして変更を完了します。

確認ページが表示され、登録されたメールアドレスにメールが送信されます。

注：

- アカウントがEAGを介して社内ネットワーク・アカウントとリンクしている場合、画面が異なる場合があります。更なる情報に関しては、「**Enterprise Access Gateway (EAG) アカウント設定を更新する**」のセクションを参照ください。
- ポータルで更新したプロフィール情報のすべてが、Exostar対応のほかのアプリケーションに反映されるわけではありません。アプリケーション固有のプロフィール情報は各アプリケーションで更新する必要があります。
- 「**Restricted Access**」：ON/OFFの設定は、ユーザが**ForumPass**の「**制限付きプロフィール (Restricted Profile)**」サイトにアクセスできるかを決定する一要因です。この設定に関する質問は**組織管理者 (Organization Administrator)** にお問い合わせ下さい。ForumPassを使用していない場合、この設定は該当しません。

Update Enterprise Access Gateway (EAG) Account Settings

The option to update the **EAG Account Settings** is available to users who belong to organizations which are subscribed to the EAG service. This option allows users to access all MAG applications via their corporate network log-in credentials. As a user belonging to an organization subscribed to EAG, your **Edit Profile** page will have an additional section to link your account to your network log-in credentials as highlighted below:

The screenshot shows a user profile page with a navigation bar at the top containing 'Home', 'My Account', 'Customer Support', and 'Adoption'. Below the navigation bar are links for 'Edit Profile', 'View Organization Details', 'Change Email', 'Change Password', 'Change Security Questions', 'Manage Certificates', and 'Manage OTP'. The main content area is titled 'User Profile' and contains the following information:

- User ID: cambetest_3601
- Email: teresa.cambetes@exostar.com
- Role: Customer Support
- Organization Name: Exostar2
- Organization ID: EXOs029448149
- Title: Select Title (dropdown)
- *First Name: Teresa
- Middle Name: (empty)
- *Last Name: Cambetes
- Job Title: Training
- *Phone: 703-555-1212
- Fax: (empty)
- *Street Address 1: Unknown
- Street Address 2: (empty)
- *City: Unknown
- *State: VA
- *Zip/Postal Code: Unknown
- *Country: UNITED STATES (dropdown)
- Time Zone: America/New_York (dropdown)
- Restricted Access: Off
- Created Date: N/A
- Suspended Date (From MAG): N/A
- Last MAG Access Date: 22 Apr, 2013 12:55 PM EDT

At the bottom of the page, there is a section titled 'Enterprise Access Gateway (EAG) Account Settings' which is highlighted with a red box. This section contains the following information:

- Remote Identity Provider (R-IDP): ExostarUAT1
- Link Accounts button (highlighted with a red box) with the text: Click here to begin a multi-step process to link your MAG account to your Remote Identity Provider account.
- Submit button

Link Accounts

To link your corporate login credentials with your MAG account, log-in to your MAG user account, and access the **Edit Profile** tab. Scroll down to the **EAG Account Settings** section at the bottom of the page, and follow the steps below to complete account-linking:

1. Click the **Link Accounts** button located under the **Enterprise Access Gateway Account Settings** section.

This is a close-up screenshot of the 'Enterprise Access Gateway (EAG) Account Settings' section. It shows the 'Remote Identity Provider (R-IDP): ExostarUAT1' text. Below this text is a red box highlighting the 'Link Accounts' button. To the right of the button is the text: 'Click here to begin a multi-step process to link your MAG account to your Remote Identity Provider account.' Below the button is a 'Submit' button.

Enterprise Access Gateway (EAG) アカウント設定を更新する

「**EAG Account Settings**」を更新するオプションは、EAGサービスに加入している組織に属するユーザのみ利用可能です。このオプションによって、ユーザは社内ネットワーク用ログイン・クレデンシャルでMAGのすべてのアプリケーションにアクセスすることができます。EAGサービスに加入している組織に属するユーザの「**Edit Profile**」ページには、以下で印がつけられているように、ネットワーク・ログイン・クレデンシャルとアカウントをリンクさせる追加のセクションが表示されます。

アカウントをリンクさせる

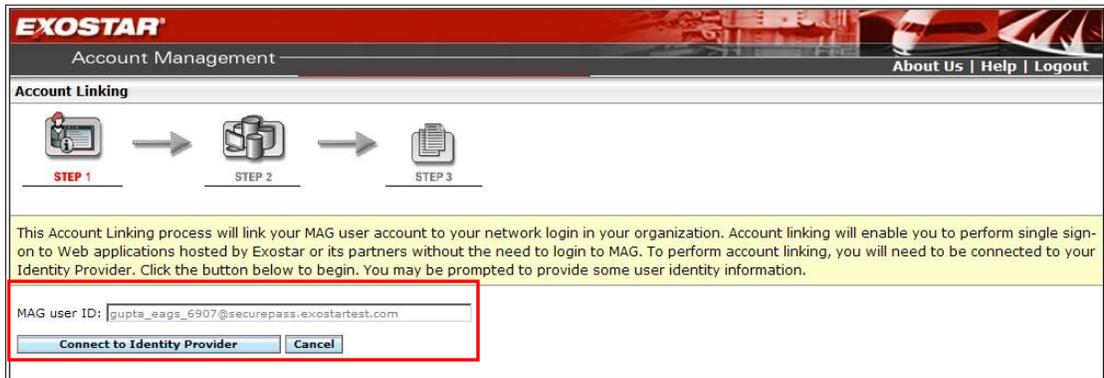
社内ネットワーク用ログイン・クレデンシャルとMAGアカウントをリンクさせるには、MAGのユーザ・アカウントにログインし、「**Edit Profile**」タブにアクセスしてください。ページ最下部の「**EAG Account Settings**」までスクロールし、以下の手順に沿ってアカウントをリンクさせてください。

1. 「**Enterprise Access Gateway Account Settings**」セクションの「**Link Accounts**」ボタンをクリックする。

- You are prompted to save any changes you made to the **Edit Profile** page. Click **OK** if you want to save any changes, otherwise click the **Cancel** button to start the account linking process.



- Step 1 of the **Account Linking** activities is presented. As shown below, your **MAG Login ID** is displayed, along with the **Connect to Identity Provider** and **Cancel** buttons. Click on **Connect to Identity Provider**.



IMPORTANT:

- If you are logged in with your FIS certificates, you are prompted to select the certificate. Select the certificate and click **OK**.
- If you do not have FIS certificates, but have a pending FIS request, you may also be prompted for a certificate. Click **Cancel**.

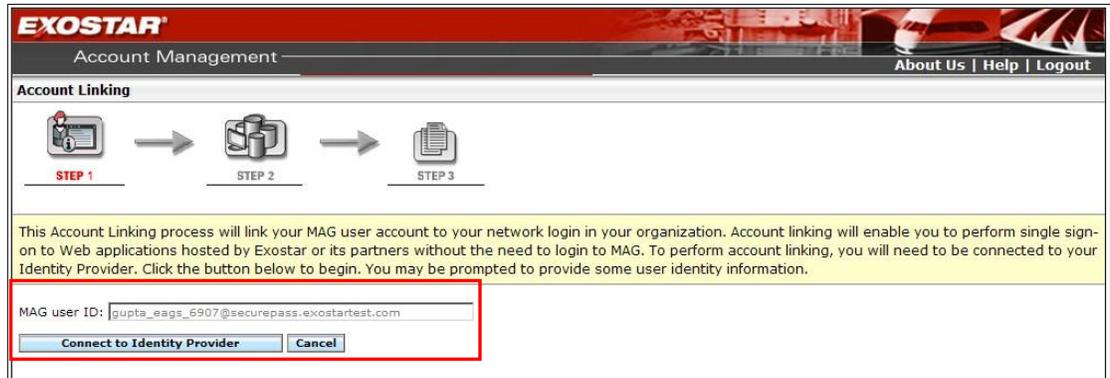


- If you are already logged in to your corporate network, you will go directly to step 5 below. If you are not logged in, you are prompted to provide your network log-in credentials in the next screen. Please note this screen is specific to your organization.

- 「Edit Profile」ページへの変更を保存するように求められるので、変更を保存したければ「OK」を、そうでなければ「Cancel」をクリックしてアカウントのリンクを開始する。



- 「Account Linking」操作のSTEP 1が表示される。以下のように、「MAG user ID」とともに「Connect to Identity Provider」および「Cancel」ボタンが表示される。「Connect to Identity Provider」をクリックする。



重要：

- FIS証明書でログインしている場合、証明書を選択するように求められます。証明書を選択し、「OK」をクリックしてください
- FIS証明書は持っていないがFIS申請の承認待ちの場合も証明書を求められることがあります。「Cancel」をクリックしてください。



- すでに社内ネットワークにログインしている場合、以下の手順5に進む。ログインしていない場合、次の画面で社内ネットワーク用ログイン・クレデンシャルを求められる。この画面はユーザの組織により異なる。

5. Step 2 of the **Account Linking** process is presented. Notice your corporate network user ID is populated. Click on the **Link accounts** button.

Account Linking

STEP 1 → **STEP 2** → STEP 3

Click the button below to link your Remote Identity Provider user account with your MAG user account.

MAG user ID:

BAE Systems user ID:

Link accounts

Note: The above screenshot displays your **MAG Login ID** and your **Corporate Login ID**. In this example, you see the Corporate User ID is defined as BAE Systems User ID. This is only for the example. You will see the name of your organization instead.

6. Step 3 of the **Account Linking** process is displayed. Click **Logout and Close Browser** to complete the account linking process.

Account Linking

STEP 1 → STEP 2 → **STEP 3**

You have successfully linked your MAG account to your Identity Provider account and a cookie has been written into your browser. Clicking the button below will complete the linking process and close all MAG sessions including this window. To access an application available via MAG, launch a new browser session and login to MAG using your linked account. Alternatively, if you have already bookmarked MAG application(s), select the bookmark and directly access the application.

MAG user ID:

BAE Systems user ID:

Logout & Close Browser

What Happens Next?

- When you click on the **Logout and Close Browser** button, you are logged out of your MAG session.
- A **persistent cookie** is saved on your machine to ensure you are not required to authenticate again to MAG.
- To access MAG again, you need to open a new browser, and access the [MAG login page](#). You are taken directly to the **MAG Applications** page, or the application you accessed.
- If you are not logged in to your corporate network, you may receive a prompt to log-in.
- If you would like to access MAG outside of your company's network you may contact your Organization Administrator for delinking of your account.

For FAQs related to EAG, refer to the [EAG User Guide](#).

5. 「Account Linking」のSTEP 2が表示される。社内ネットワーク用ユーザIDが挿入されていることを確認する。「Link accounts」ボタンをクリックする。

注：上のスクリーンショットでは「MAG user ID」と企業ログインIDが表示されています。この例では企業ログインIDは「BAE Systems user ID」となっていますが、これは単に例であり、実際はユーザの組織名が代わりに表示されます。

6. 「Account Linking」のStep 3が表示される。「Logout and Close Browser」をクリックし、アカウントのリンク手続きを終了する。

この後の流れ

- 「Logout and Close Browser」をクリックすると、MAGのセッションからログアウトします。
- パーシステントクッキーがユーザのパソコンに保存されるため、MAGへの認証を再度行う必要はありません。
- MAGに再ログインする際は、新しいブラウザを開いて[MAGログインページ](#)にアクセスしてください。「MAG Applications」ページ又はアクセスしたアプリケーションに直接移動されます。
- 社内ネットワークにログインしていない場合、ログインを促すメッセージが表示される場合があります。
- 社内ネットワークの外でMAGにアクセスしたい場合は、アカウントのリンクを解除するために組織管理者（Organization Administrator）に連絡してください。

EAGに関するよくあるご質問は、[EAGユーザガイド](#)をご参照ください。

Lost EAG Cookie: Re-link Accounts

As mentioned above, a **persistent cookie** is stored on your computer when you complete the account-linking process. If the cookie is lost, follow the steps below to re-link your accounts.

1. To re-link your corporate login credentials with your MAG account, access the MAG [login](#) page.



2. Click **Single Sign On (EAG)**, and you are prompted for an FIS certificate. Select the certificate you use to access your applications, and click **OK** or **Cancel** (if you don't have a certificate).
3. If you are not logged-in to your corporate network, you are presented with the log-in screen. Enter your corporate login credentials.
If you are already logged-in, you are taken directly to the next step.
4. You are presented with the **MAG Applications** page. A new **persistent cookie** is automatically set-up to ensure you are not prompted for MAG credentials again.

Password Reset and other actions for EAG users

If you're an EAG user, you are not required to reset your password or remember your security questions. The following options under **My Account** tab may not be available:

- Change Password
- Change Security Questions

View Organization Details

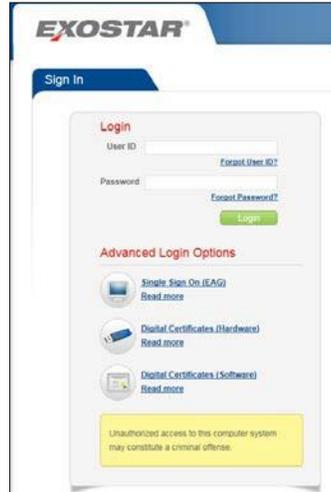
Access the **My Account** tab, and select **View Organization Details**. This tab provides information regarding the following:

- Organization name and address details
- Exostar Organization ID to reference when calling Customer Support
- Subscribed applications
- Organization Administrator contact information
- Application Administrator contact information per application

EAGクッキーを紛失した場合：アカウントを再リンクさせる

上で説明したように、アカウントのリンク手続きが終了するとパーシステントクッキーがユーザのパソコンに保存されます。クッキーを紛失した場合、以下の手順に沿ってアカウントを再リンクしてください。

1. 社内ネットワーク用ログイン・クレデンシャルとMAGアカウントを再リンクさせるため、[MAGログインページ](#)にアクセスする。



2. 「**Single Sign On (EAG)**」をクリックする。FIS証明書を求められるので、アプリケーションにアクセスする際使用する証明書を選択し、「**OK**」又は「**Cancel**」（証明書を持っていない場合）をクリックする。
3. 社内ネットワークにログインしていない場合、ログイン画面が表示される。企業ログイン・クレデンシャルを入力する。
すでにログインしている場合、次の手順に移動される。
4. 「**MAG Applications**」ページが表示される。新しいパーシステントクッキーが自動で設定され、MAGクレデンシャルは今後求められなくなる。

EAGユーザによるパスワードの再設定とその他のアクション

EAGユーザは、パスワードの再設定やセキュリティ質問を覚える必要はありません。「**My Account**」タブの次のオプションはご利用いただけないことがあります。

- 「**Change Password**（パスワードを変更する）」
- 「**Change Security Questions**（セキュリティ質問を変更する）」

組織情報を表示する

「**My Account**」タブにアクセスし、「**View Organization Details**」を選択してください。このタブでは以下の情報が提供されます。

- 組織名称・所在地
- カスタマーサポートに電話する際にExostarが参照する組織ID（Organization ID）
- 加入アプリケーション
- 組織管理者（Organization Administrator）の連絡先
- 各アプリケーションのアプリケーション管理者（Application Administrator）の連絡先

Home	My Account																				
Edit Profile View Organization Details Change Email Change Password Change Security Questions Manage Certificates Manage OTP																					
Need to change your organization's name, address, or organization administrator? Complete the organization information change request form and follow the instructions for submitting it to Exostar's Customer Service.																					
Organization Details																					
Organization Name: Exostar LLC Organization ID/Exostar ID: exostar / 97679 Business Unit: MPID: ae9da2ea-7835-1000-8cc0-ac160d880001 Organization's HQ/Country of Incorporation: US DUNS #: Do not allow users of my Organization to use Exostar No provided OTP tokens: Do not allow users of my Organization to be invited to No applications:	Address 1: 13241 Woodland Park Road Address 2: Ste 400 City: Herndon *State/Province: VA Zip/Postal Code: 20171 Country: US Created Date: N/A Suspended Date: N/A Do not allow users of my Organization to use Exostar provided Phone Based OTP: No																				
Organization Contact																					
<table border="1"> <thead> <tr> <th>First Name</th> <th>Last Name</th> <th>Email</th> <th>Phone</th> </tr> </thead> <tbody> <tr> <td>Ben</td> <td>Maphis</td> <td>ben.maphis@exostar.com</td> <td>703-793-7781</td> </tr> </tbody> </table>		First Name	Last Name	Email	Phone	Ben	Maphis	ben.maphis@exostar.com	703-793-7781												
First Name	Last Name	Email	Phone																		
Ben	Maphis	ben.maphis@exostar.com	703-793-7781																		
Organization Administrators																					
<table border="1"> <thead> <tr> <th>First Name</th> <th>Last Name</th> <th>Email</th> <th>Phone</th> <th>Able to Approve OTP HW Token Activations</th> </tr> </thead> <tbody> <tr> <td>Rose</td> <td>Brown</td> <td>rose.brown@exostar.com</td> <td>703 793 7747</td> <td>Yes</td> </tr> <tr> <td>Adrienne</td> <td>Evans</td> <td>adrienne.evans@exostar.com</td> <td>7037937767</td> <td>Yes</td> </tr> </tbody> </table>		First Name	Last Name	Email	Phone	Able to Approve OTP HW Token Activations	Rose	Brown	rose.brown@exostar.com	703 793 7747	Yes	Adrienne	Evans	adrienne.evans@exostar.com	7037937767	Yes					
First Name	Last Name	Email	Phone	Able to Approve OTP HW Token Activations																	
Rose	Brown	rose.brown@exostar.com	703 793 7747	Yes																	
Adrienne	Evans	adrienne.evans@exostar.com	7037937767	Yes																	
Application Administrators																					
<table border="1"> <thead> <tr> <th>First Name</th> <th>Last Name</th> <th>Email</th> <th>Phone</th> <th>Application</th> </tr> </thead> <tbody> <tr> <td>Rose</td> <td>Brown</td> <td>rose.brown@exostar.com</td> <td>703 793 7747</td> <td>Supply Chain Platform - General</td> </tr> <tr> <td>Adrienne</td> <td>Evans</td> <td>adrienne.evans@exostar.com</td> <td>7037937767</td> <td>Supply Chain Platform - General</td> </tr> <tr> <td>Nathan</td> <td>Cassedy</td> <td>nathan.cassedy@exostar.com</td> <td>866-238-6782</td> <td>Supply Chain Platform - General</td> </tr> </tbody> </table>		First Name	Last Name	Email	Phone	Application	Rose	Brown	rose.brown@exostar.com	703 793 7747	Supply Chain Platform - General	Adrienne	Evans	adrienne.evans@exostar.com	7037937767	Supply Chain Platform - General	Nathan	Cassedy	nathan.cassedy@exostar.com	866-238-6782	Supply Chain Platform - General
First Name	Last Name	Email	Phone	Application																	
Rose	Brown	rose.brown@exostar.com	703 793 7747	Supply Chain Platform - General																	
Adrienne	Evans	adrienne.evans@exostar.com	7037937767	Supply Chain Platform - General																	
Nathan	Cassedy	nathan.cassedy@exostar.com	866-238-6782	Supply Chain Platform - General																	
Proofoers																					
<table border="1"> <thead> <tr> <th>First Name</th> <th>Last Name</th> <th>Phone</th> <th>Email</th> </tr> </thead> <tbody> <tr> <td>Adrienne</td> <td>Evans</td> <td>7037937767</td> <td>adrienne.evans@exostar.com</td> </tr> </tbody> </table>		First Name	Last Name	Phone	Email	Adrienne	Evans	7037937767	adrienne.evans@exostar.com												
First Name	Last Name	Phone	Email																		
Adrienne	Evans	7037937767	adrienne.evans@exostar.com																		
Application Settings																					
Application Access:	<table border="1"> <thead> <tr> <th>Provider</th> <th>Application</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Information Manager Hll</td> <td>Information Manager Hll</td> <td>Active</td> </tr> <tr> <td>Exostar LLC</td> <td>Supply Chain Platform - General</td> <td>Active</td> </tr> <tr> <td>Exostar LLC</td> <td>ForumPass 4 - EU</td> <td>Active</td> </tr> <tr> <td>Exostar LLC</td> <td>Federated Identity Service (FIS)</td> <td>Active</td> </tr> </tbody> </table>	Provider	Application	Status	Information Manager Hll	Information Manager Hll	Active	Exostar LLC	Supply Chain Platform - General	Active	Exostar LLC	ForumPass 4 - EU	Active	Exostar LLC	Federated Identity Service (FIS)	Active					
Provider	Application	Status																			
Information Manager Hll	Information Manager Hll	Active																			
Exostar LLC	Supply Chain Platform - General	Active																			
Exostar LLC	ForumPass 4 - EU	Active																			
Exostar LLC	Federated Identity Service (FIS)	Active																			

注：組織がEAGにリンクしている場合にのみ「Enterprise Access Gateway Account Settings」は表示されます。

メールアドレスを変更する

「My Account」タブにアクセスし、「Change Email」を選択してください。以下の手順に沿ってメールアドレスを変更することができます。

1. 「My Account」タブにアクセスし、「Change Email」を選択する。
2. 新しいメールアドレスを入力し、「Continue」をクリックする。新しいメールアドレスにアクティベーション・コードが届く。
3. メールに記載されたアクティベーション・コードを入力し、「Activate」をクリックする。システムで新しいメールアドレスが有効になる。

Home | **My Account** | Administration | Registration Requests

Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | Manage OTP | Connect Accounts

Important Note:
If you have FIS certificates, you will not be able to proceed from here. To change your email address, contact [Exostar Customer Support](#).
Step 1: Enter new email address and click **Continue**. You will receive an activation code by email.

Modify Email

Current Email Address: kelly.johnson@exostar.com

*New Email Address:

Clear Continue

Step 2: To activate your new email address, enter activation code from email.

Activate Email

*Activation Code:

Activate

IMPORTANT:

- If you have valid FIS certificates, you need to revoke your certificates, and then change your email address. This requires a new purchase.
- If you have been approved for FIS certificates, but have not yet downloaded your certificates, and do not also have any other valid FIS certificates, you can modify your email address.
- You **MUST** notify all project partners of your email address change to ensure you can continue to access the applications.
- If your account is linked to your corporate network account via EAG, you are not able to access the **Change Email** tab.

Change Password

1. Access the **My Account** tab, and click **Change Password**.
2. Enter your current password, your new password, and then confirm your new password.

Home | **My Account** | Administration | Registration Requests

Edit Profile | View Organization Details | Change Email | **Change Password** | Change Security Questions | Manage OTP | Connect Accounts

Change Password

Old Password:

*New Password:

*Confirm New Password:

Submit Clear

Password Strength Policy

- Password must be at least 8 and at most 12 characters. It must comprise at least 4 distinct characters, 1 alphabetic character, 1 numeric character and 1 space. Whitespaces are not permitted.

重要：

- 有効なFIS証明書を持っている場合、証明書を失効させてからメールアドレスを変更する必要があります。この場合、新たに証明書を購入する必要があります。
- FIS証明書の承認後、まだ証明書をダウンロードしておらず、且つほかに有効なFIS証明書を持っていない場合、メールアドレスを変更することができます。
- アプリケーションに引き続きアクセスできるように、すべてのプロジェクト・パートナーにメールアドレスの変更を通知しなければなりません。
- アカウントがEAGを介して社内ネットワーク・アカウントとリンクしている場合、「**Change Email**」タブにアクセスすることはできません。

パスワードを変更する

1. 「**My Account**」タブにアクセスし、「**Change Password**」をクリックする。
2. 現在のパスワードと新しいパスワードを入力し、新しいパスワードを確認する。

Make sure your new password complies with the **Password Strength Policy**:

- Must contain a minimum of eight characters, and a maximum of 12 characters.
- Must contain at least four distinct characters:
 - One alphabetic character
 - One numeric character
 - One special character such as !,@,#,\$,% etc.
- Leading and trailing spaces are not permitted.

3. Click **Submit**.

Note: If your account is linked to your corporate network account via EAG, you are not able to access the **Change Password** tab.

Change Security Questions

1. Access the **My Account** tab, and click **Change Security Questions**. If you wish to change a question/answer combination, click on the **Change** check box. This makes the field editable.
2. Make any modifications, and then click the **Submit** button at the bottom of the page.

The screenshot displays the 'Change Security Questions' page. At the top, there is a navigation bar with tabs for 'Home', 'My Account', 'Administration', and 'Registration Requests'. Below this, a secondary navigation bar contains links: 'Edit Profile', 'View Organization Details', 'Change Email', 'Change Password', 'Change Security Questions' (highlighted with a red box), 'Manage OTP', and 'Connect Accounts'. The main content area is titled 'Change Security Questions' and includes a sub-header: 'Update your existing security questions and answers by clicking the change box, entering the new answer for that question, and clicking Submit.' Below this, there are four question entries, each with a dropdown menu for the question and a text input field for the answer. Each entry has a 'Change' checkbox to its right. The questions are: 'Question 1: What is your favorite color?', 'Question 2: What is your favorite sport?', 'Question 3: What is your favorite book?', and 'Question 4: What is your favorite food?'. At the bottom of the form is a red 'Submit' button.

Please note the following regarding your **Security Questions**:

- Security questions are used when you have forgotten your password, or when you need to change your password.
- The system only requires you to remember two of the four questions when resetting your password.
- You must make each of your question and answer combinations unique.
- The answers to the security questions are case-sensitive.
- You cannot select the same question twice.

新しいパスワードが「**Password Strength Policy**（パスワード強度ポリシー）」に対応していることを確認する。

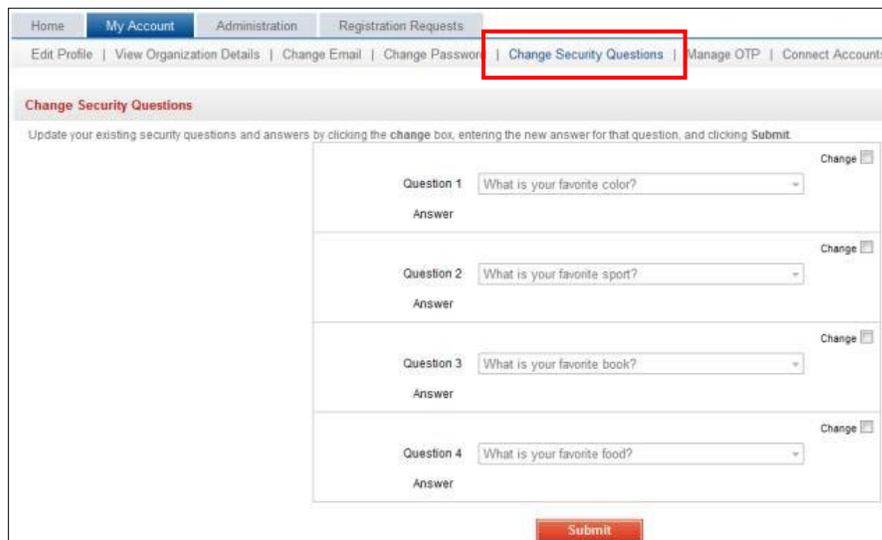
- 8文字以上12文字以内であること
- 少なくとも4つの異なる文字を含むこと
 - 英字1文字
 - 数字1文字
 - 特殊文字1文字（!、@、#、\$、%等）
- 先頭と末尾にスペースは使用不可

3. 「**Submit**」をクリックする。

注：アカウントがEAGを介して社内ネットワーク・アカウントとリンクしている場合、「**Change Email**」タブにアクセスすることはできません。

セキュリティ質問を変更する

1. 「**My Account**」タブにアクセスし、「**Change Security Questions**」をクリックする。変更したい質問と答えの組み合わせの「**Change**」のチェックボックスにチェックを入れる。これにより、フィールドが編集可能となる。
2. 変更後、ページ最下部の「**Submit**」ボタンをクリックする。



セキュリティ質問に関して、以下の点にご注意ください。

- セキュリティ質問は、パスワードを忘れてしまった場合、又はパスワードを変更する際に使用されます。
- パスワードをリセットする際は、4つの質問のうち2つに回答することが求められます。
- 質問と答えの各組み合わせは別のものである必要があります。
- セキュリティ質問の答えは大文字と小文字が区別されます。
- 同じ質問を2回選ぶことはできません。

Note: If your account is linked to your corporate network account via EAG, you are not able to access the **Change Security Questions** tab.

Manage OTP

From the **Manage OTP** tab, you can order, activate, and manage **One-Time Password Hardware Tokens**. These tokens are used with your MAG account for authentication purposes. For more information, refer to the [OTP Hardware Token User Guide](#).

The screenshot shows the 'Manage OTP Credentials' page. At the top, there are navigation tabs for 'Home' and 'My Account'. Below this is a menu with options: 'Edit Profile', 'View Organization Details', 'Change Email', 'Change Password', 'Change Security Questions', 'Manage Certificates', and 'Manage OTP'. The main content area is titled 'Manage OTP Credentials' and contains a table with the following data:

OTP Credential Type What's this ?	Status	Actions
OTP Hardware Token	Inactive	Purchase/Register
Phone Based OTP	Inactive	Purchase/Register

A red arrow points from the 'Purchase/Register' button for 'OTP Hardware Token' to a separate section below. This section contains the text: 'If you are interested in purchasing an OTP Hardware Token, visit our website by clicking the Order Token button.' followed by an 'Order Token' button. Below this is an 'Important' note: 'After you have purchased and received your OTP Hardware Token, approval for activating the token is required. If you need help, [view these frequently asked questions](#) about OTP Hardware Tokens.' This is followed by a sub-section titled 'Activate OTP Hardware Token' with an 'Activate' button. A note at the bottom says: 'To activate your OTP hardware token, click the Activate button.'

Manage Certificates

If you are approved for FIS access, you are able to view the **Manage Certificates** tab under the **My Account** tab.

The screenshot shows the 'Manage Certificates' page. At the top, there are navigation tabs for 'Home' and 'My Account'. Below this is a menu with options: 'Edit Profile', 'View Organization Details', 'Change Email', 'Change Password', 'Change Security Questions', 'Manage Certificates', and 'Manage OTP'. The main content area is titled 'Download Certificates' and contains a sub-menu with options: 'Download Certificates', 'View Certificates', 'Recover Encryption Keys', 'Revoke Certificates', and 'Renew Certificates'. Below this is a form with a '*Passcode:' label and an input field. There are 'Submit' and 'Reset' buttons. Below the form is a 'Helpful Tips:' section with the following list:

- Make sure your system meets the [requirements for downloading certificates](#).
- Enter your entire 16 digit Passcode including hyphens (-). Avoid extra spaces.
- If you are installing your certificates on a token, you MUST [run the system check](#) to ensure there is enough room on your token to download additional certificates.
- Need additional help? Refer [Online Help for FIS](#).
- See an error on this page? [Find out more](#).
- If your Passcode is lost or compromised, you must [reapply for FIS Certificates](#)

At the bottom, there is a note: 'Note: Once you reapply, your request will go through the approval process and you will receive an email notification regarding next steps.'

注：アカウントがEAGを介して社内ネットワーク・アカウントとリンクしている場合、「Change Security Questions」タブにアクセスすることはできません。

OTPを管理する

「Manage OTP」タブでは、「One-Time Password Hardware Token（ワンタイムパスワード用ハードウェアトークン）」の注文、有効化、および管理をすることができます。これらのトークンは、認証のためにMAGアカウントで使用されます。詳細は、[OTPハードウェアトークンのユーザガイド](#)を参照ください。

Home | My Account

Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | Manage Certificates | Manage OTP

Manage OTP Credentials

OTP Credential Type What's this ?	Status	Actions
OTP Hardware Token	Inactive	Purchase/Register
Phone Based OTP	Inactive	Purchase/Register

If you are interested in purchasing an OTP Hardware Token, visit our website by clicking the Order Token button. [Order Token](#)

Important: After you have purchased and received your OTP Hardware Token, approval for activating the token is required. If you need help, [view these frequently asked questions](#) about OTP Hardware Tokens.

Activate OTP Hardware Token

To activate your OTP hardware token, click the Activate button. [Activate](#)

証明書を管理する

FISへのアクセスが承認されると、「My Account」のタブで「Manage Certificates」のタブを見ることができます。

Home | My Account

Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | Manage Certificates | Manage OTP

[Download Certificates](#) | [View Certificates](#) | [Recover Encryption Keys](#) | [Revoke Certificates](#) | [Renew Certificates](#)

Download Certificates

*Passcode:

[Submit](#) [Reset](#)

Helpful Tips:

- Make sure your system meets the [requirements for downloading certificates](#).
- Enter your entire 16 digit Passcode including hyphens (-). Avoid extra spaces.
- If you are installing your certificates on a token, you MUST [run the system check](#) to ensure there is enough room on your token to download additional certificates.
- Need additional help? Refer [Online Help for FIS](#).
- See an error on this page? [Find out more](#).
- If your Passcode is lost or compromised, you must [reapply for FIS Certificates](#)

Note: Once you reapply, your request will go through the approval process and you will receive an email notification regarding next steps.

In certain situations, the FIS user may not obtain some or all of the permissions needed to download and install the Exostar **ActiveX XEnrollPlus** control via a web browser. To handle these situations, system administrators can use a Microsoft installer-based package (MSI), to install the Exostar ActiveX control. There are three versions of the installer currently available:

1. One for Windows 2000 platforms
2. One for Windows XP
3. One for Windows Vista.

In addition, Exostar has a system check functionality, which allows you to review the issues with the certificate download process. Complete [a system check](#) prior to downloading your certificates.

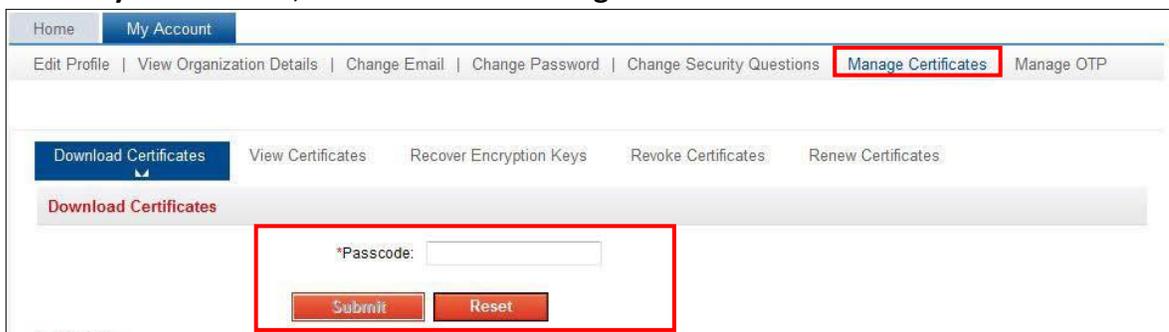
Download Certificates – Basic Level of Assurance (Identity)

Pre-requisites for downloading the certificates:

- Received 16-digit passcode from Exostar via email
- Reviewed the system and certificate download requirements document

To download the certificates you are approved for:

1. Go to the **My Account** tab, and click on the **Manage Certificates** tab.



The screenshot shows the 'My Account' section of the Exostar web interface. The 'Manage Certificates' tab is selected and highlighted with a red box. Below it, the 'Download Certificates' sub-tab is active. A form for entering a passcode is visible, with the label '*Passcode:' and an input field. The 'Submit' and 'Reset' buttons are also highlighted with a red box.

2. Enter the passcode you received via email from Exostar, and click **Submit**.

Note: The passcode is a 16-digit number separated by hyphens; for example: **1234-5678-1234-5678**. You **must** enter all the characters, including hyphens (or leave the hyphens out completely). The passcode is **NOT** the same as your MAG log-in password.

3. Download your certificates. If your passcode is correct, you will see the certificate listed with a status. The system will automatically select the certificate to download.

Note: You are only able to see the **Download Certificates** sub-tab under **Manage Certificates**, when you have an approved FIS request pending certificate download. If no certificates are available for download, you cannot view this sub-tab.

4. After the certificate is successfully downloaded, you will see a confirmation message on your screen.

Note: Refer to the **FAQ section for Federated Identity Service** on www.myexostar.com for information on any errors encountered while downloading the certificates.

特定の状況において、FISユーザはウェブブラウザでExostarの**ActiveX XEnrollPlus**コントロールをダウンロード、インストールするために必要な許可のいくつか又は全てを持っていない場合があります。このような状況に対処するため、システム管理者はMicrosoftインストーラ・ベース・パッケージ (MSI) を使用してExostar ActiveXコントロールをインストールすることができます。現在、3つのバージョンのインストーラが利用可能です。

1. Windows 2000プラットフォーム
2. Windows XP
3. Windows Vista.

また、Exostarにはシステムチェック機能があるため、ユーザは証明書ダウンロード手続きにおける問題を確認することができます。証明書をダウンロードする前に[システムチェック](#)を行ってください。

証明書をダウンロードする – 基本保証レベル (Identity)

証明書ダウンロードの条件

- Exostarからメールで16桁のパスコードを受け取っていること
- システム要件および証明書ダウンロード要件のドキュメントを確認済みであること

承認された証明書をダウンロードするには、以下の手順に従ってください。

1. 「**My Account**」タブから「**Manage Certificates**」タブをクリックする。



The screenshot shows a web application interface. At the top, there are navigation tabs: 'Home' and 'My Account'. Below 'My Account', there are several links: 'Edit Profile', 'View Organization Details', 'Change Email', 'Change Password', 'Change Security Questions', 'Manage Certificates' (highlighted with a red box), and 'Manage OTP'. Below these links, there are several buttons: 'Download Certificates' (highlighted with a blue box), 'View Certificates', 'Recover Encryption Keys', 'Revoke Certificates', and 'Renew Certificates'. Below the 'Download Certificates' button, there is a section titled 'Download Certificates' which contains a text input field labeled '*Passcode:' and two buttons: 'Submit' and 'Reset' (both highlighted with red boxes).

2. Exostarからメールで受け取ったパスコードを入力し、「**Submit**」をクリックする。

注：パスコードはハイフンで区切られた16桁の数字です（例：**1234-5678-1234-5678**）。ハイフンを含めたすべての数字を**必ず**入力してください（もしくは、ハイフンを完全に抜かしてください）。パスコードはMAGログイン用パスワードとは**異なります**。

3. 証明書をダウンロードする。パスコードが正しければ、証明書とステータスのリストが表示される。ダウンロードされる証明書が、システムによって自動で選択される。

注：「**Manage Certificates**」タブの「**Download Certificates**」サブタブは、FIS申請が承認され、未ダウンロードの証明書がある場合にのみ表示されます。ダウンロード可能な証明書がない場合、このサブタブは表示されません。

4. 証明書のダウンロード後、画面に確認メッセージが表示される。

注：証明書ダウンロード時に発生するエラーに関しては、www.myexostar.comで「**Federated Identity Service**」の「**FAQ**」セクションを参照ください。

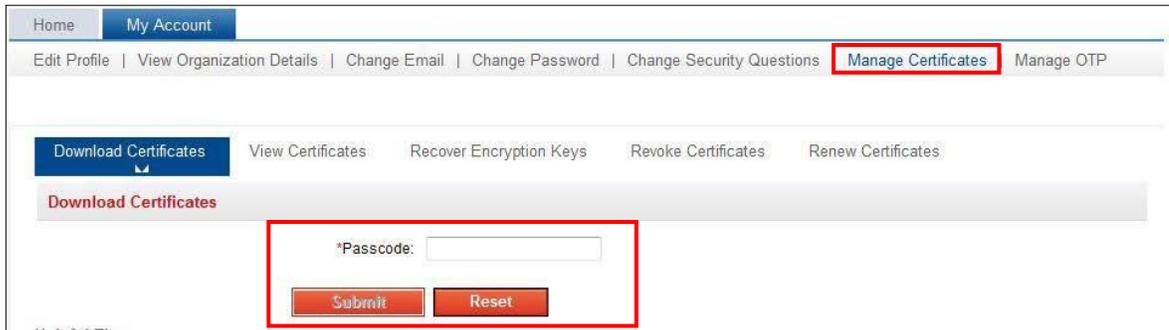
Download Certificates – Basic Level of Assurance (SecureEmail)

Pre-requisites for downloading the certificates:

- Received 16-digit passcode from Exostar via email
- Reviewed the system and certificate download requirements document

To download your certificates:

1. Go to the **My Account** tab, and click the **Manage Certificates** tab.



2. Enter the passcode you received via email from Exostar, and click **Submit**.

Note: The passcode is a 16-digit number separated by hyphens; for example: **1234-5678-1234-5678**. You **must** enter all the characters, including hyphens (or leave the hyphens out completely). The passcode is **NOT** the same as your MAG log-in password.

3. Download your certificates. If your passcode is correct, you will see the list of certificates you can download. The system will automatically select all of them for download.



4. Click the **OK** button to archive your encryption key and enable key recovery.



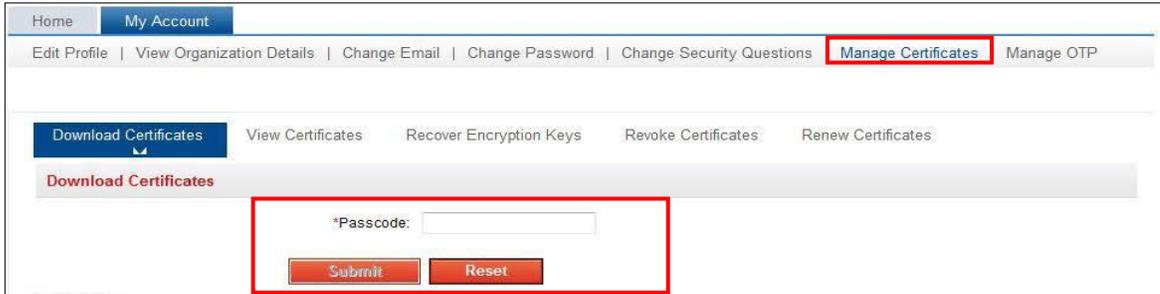
証明書をダウンロードする — 基本保証レベル (SecureEmail)

証明書ダウンロードの条件

- Exostarからメールで16桁のパスコードを受け取っていること
- システム要件および証明書ダウンロード要件のドキュメントを確認済みであること

証明書をダウンロードするには、以下の手順に従ってください。

1. 「My Account」タブから「Manage Certificates」タブをクリックする。



2. Exostarからメールで受け取ったパスコードを入力し、「Submit」をクリックする。

注：パスコードはハイフンで区切られた16桁の数字です（例：**1234-5678-1234-5678**）。ハイフンを含めたすべての数字を必ず入力してください（もしくは、ハイフンを完全に抜かしてください）。パスコードはMAGログイン用パスワードとは異なります。

3. 証明書をダウンロードする。パスコードが正しければ、ダウンロード可能な証明書のリストが表示される。すべての証明書をダウンロードするように自動で選択される。

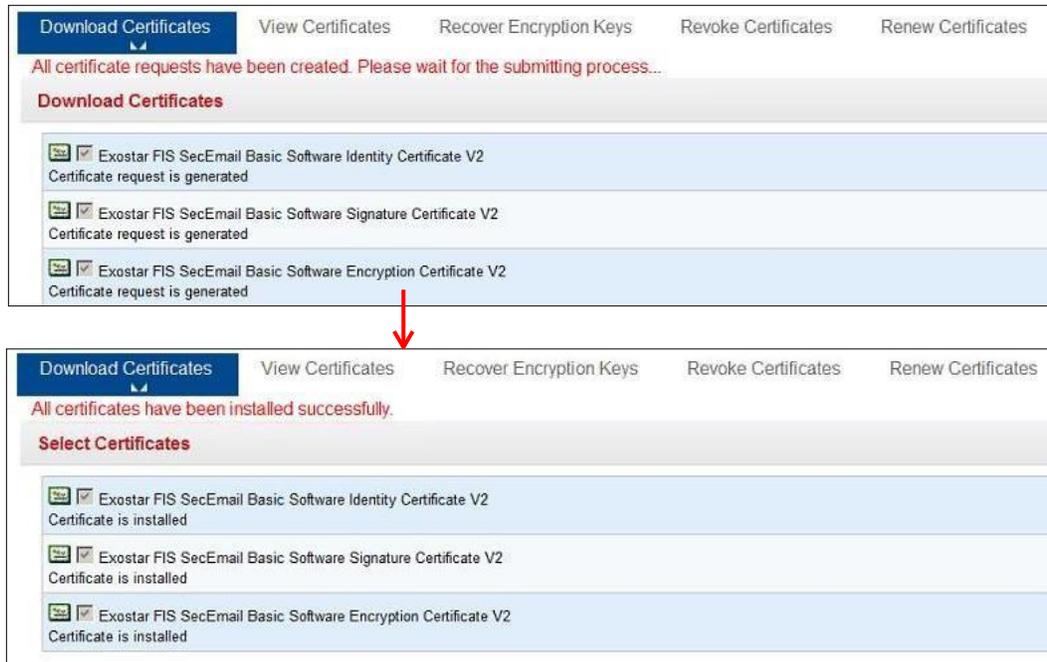


4. 「OK」ボタンをクリックし、暗号鍵をアーカイブして鍵の復元を有効にする。



Note: This activity allows Exostar to archive the encryption key for recovery at a later time. Refer to the **Recover Encryption Keys** section for details.

5. Complete the certificate download. The system presents the download status at each step.



6. Once the download is complete, you will receive the following message screen:

Note: Refer to the **FAQ section for Federated Identity Service** on <http://www.myexostar.com/fis.aspx> for information on any errors encountered while downloading.

Download Certificates – Medium Level of Assurance (Software)

Pre-requisites for downloading the certificates:

- Completed in-person proofing. For more information click [here](#).
- Received 16-digit passcode from the proofer. If you lose this passcode, you are required to complete a [reproofing purchase](#), and go through the in-person proofing process again.
- Reviewed the system and certificate download requirements document.

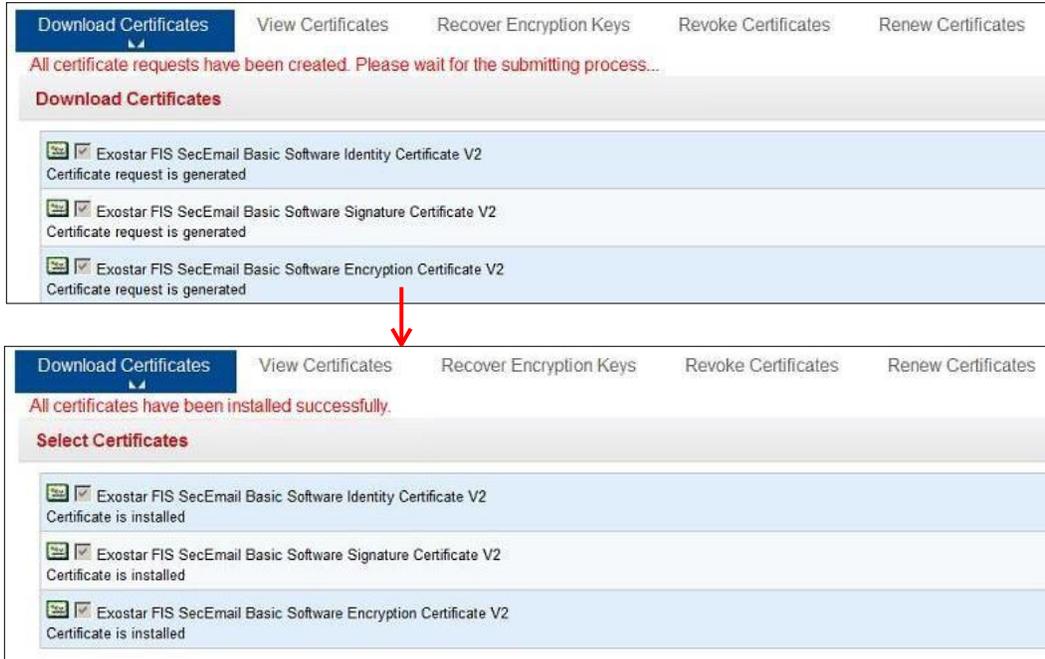
To download the certificates you are approved for:

1. Go to the **My Account** tab, and click the **Manage Certificates** tab.



注：この操作によって、Exostarは暗号鍵をアーカイブし、後に復元することができるようになります。詳細は、「[暗号鍵を復元する](#)」セクションを参照ください。

5. 証明書のダウンロードを完了する。ダウンロード状況の段階が表示される。



6. ダウンロードが完了すると、メッセージ画面が表示される。

注：ダウンロード時に発生するエラーに関しては、<http://www.myexostar.com/fis.aspx>で「**Federated Identity Service**」の「**FAQ**」セクションを参照ください。

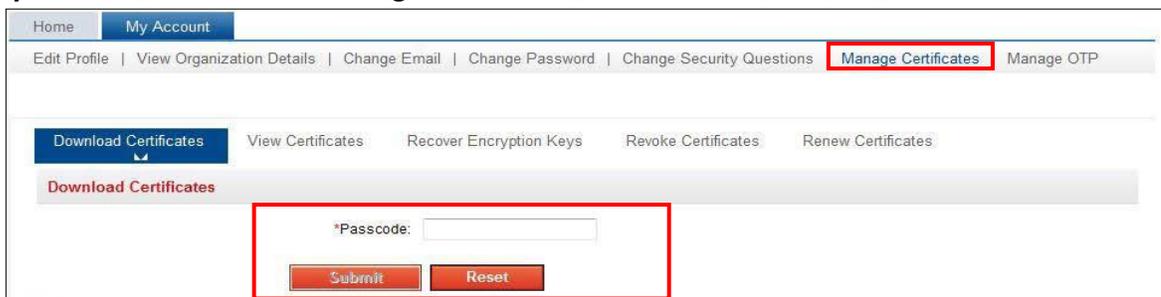
証明書をダウンロードする — 中保証レベル (Software)

証明書ダウンロードの条件

- 対面検証が完了していること。詳細は[こちら](#)をクリックしてください。
- 検証人（プルーフアー）から16桁のパスコードを受け取っていること。パスコードを紛失した場合、[再検証オプション](#)を購入し、再度対面検証を受ける必要があります。
- システム要件および証明書ダウンロード要件のドキュメントを確認済みであること

承認された証明書をダウンロードするには、以下の手順に従ってください。

1. 「**My Account**」タブから「**Manage Certificates**」タブをクリックする。



2. Enter the passcode provided to you by your proofing agent during your in-person proofing appointment. This passcode is only valid after you receive an FIS approval email from Exostar.

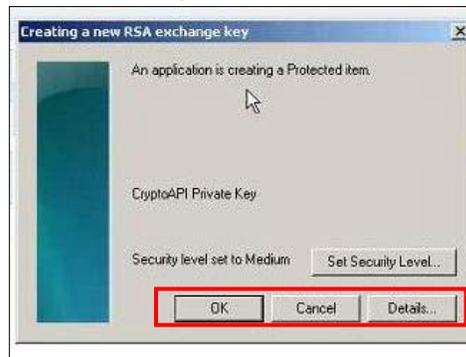
Note: The passcode is a 16-digit number separated by hyphens; for example: **1234-5678-1234-5678**. You **must** enter all the characters, including hyphens (or leave the hyphens out completely). The passcode is **NOT** the same as your MAG log-in password.

3. Archive the **encryption key**. If your passcode is correct, you will see the list of certificates you can download. The system will automatically select all of them for download. Click the **OK** button to archive your encryption key, and enable key recovery.



Note: This activity allows Exostar to archive the encryption key for recovery at a later time. Refer to the **Recover Encryption Keys** section for details.

4. Enable **Strong Protection**. Click on **Set Security Level**, and then set the security level to **High**.



Note: Exostar strongly recommends you enable strong protection for your MLOA certificates, unless there are corporate policies against doing so.

5. By default, the **Medium** option is already selected. Change this to **High** and click **Next**.



2. 対面検証時に検証人（プルーフアー）から提供されたパスコードを入力する。このパスコードは、ExostarからFIS承認メールを受信した後から有効になる。

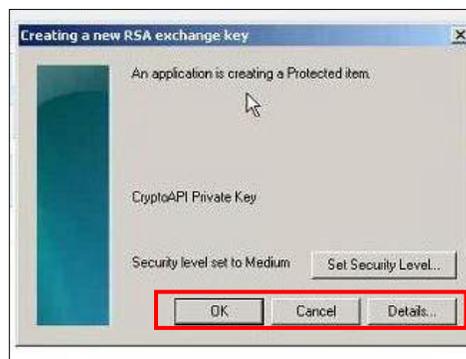
注：パスコードはハイフンで区切られた16桁の数字です（例：**1234-5678-1234-5678**）。ハイフンを含めたすべての数字を**必ず**入力してください（もしくは、ハイフンを完全に抜かしてください）。パスコードはMAGログイン用パスワードとは**異なります**。

3. **暗号鍵**をアーカイブする。パスコードが正しければ、ダウンロード可能な証明書のリストが表示される。すべての証明書をダウンロードするように自動で選択される。「**OK**」ボタンをクリックし、暗号鍵をアーカイブして鍵の復元を有効にする。



注：この操作によって、Exostarは暗号鍵をアーカイブし、後に復元することができるようになります。詳細は、「**暗号鍵を復元する**」セクションを参照ください。

4. **強力な保護**を有効にする。「**Set Security Level**」をクリックし、セキュリティレベルを「**High**」に設定する。



注：Exostarは、MLOA証明書に対して強力な保護の有効化を強く推奨しています。ただし、企業ポリシーに反している場合はこの限りではありません。

5. デフォルト設定では「**Medium**」オプションが選択されているので「**High**」に変更し、「**Next**」をクリックする。



6. Provide a password for this certificate. Please note you will need to provide this password each time you use your certificate.



7. The system now displays the new security level. Click **OK**.



8. Download the certificates. The system will prompt you for the password set in step 6, to download the certificates. Once you enter the password and click **OK**.



9. Once the download is complete, you will receive the following message screen:



6. この証明書のパスワードを設定する。証明書を使用する度にこのパスワードの入力が求められる。



7. 新しいセキュリティレベルが表示される。「OK」をクリックする。



8. 証明書をダウンロードする。証明書のダウンロードには、手順6で設定したパスワードが求められる。パスワードを入力し、「OK」をクリックする。



9. ダウンロードが完了すると、以下のメッセージ画面が表示される。



Note: Refer to the **FAQ section for Federated Identity Service** on <http://www.myexostar.com/fis.aspx> for information on any errors encountered during the download process.

Download Certificates – Medium Level of Assurance (Hardware)

To download the MLOA hardware certificates, you should complete the following tasks:

- Acquire the appropriate token. Exostar ships your token via FedEx once you have scheduled your in-person proofing appointment. If you haven't received your token, reach out to Customer Support.
- Install the token PKI Client middleware on your machine. Contact your token vendor for appropriate information, or your IT Support for organization specific information.
- Complete a system check to ensure you are able to download the certificates:
<http://www.myexostar.com/systemcheck>
- Initialize the token in FIPS 140-2 mode. For more information on how to check for FIPS mode, refer to the **Hardware Token FIPS Mode Review** section for details.
- Ensure you have been provided the initial token password to enable you to complete token installation. Contact your vendor to receive the initial password. You are required to enter a password for this token during the certificate download process.
- Complete the in-person proofing process. For more information, click [here](#).
- Receive the 16-digit passcode from the proofing agent at the end of your in-person proofing appointment. Note if you lose this passcode, you are required to complete a [reproofing purchase](#), and go through the in-person proofing process again.

Hardware Token FIPS Mode Review

Exostar's Medium Level of Assurance Hardware (MLOA) digital certificates are 2048 FIPS 140-2 compliant. To ensure the tokens also comply with the FIPS 140-2 compliance, review the token information.

Note: You must review this information **BEFORE** downloading the digital certificates.

1. If you completed the initial password change process for your token, plug the token into your USB drive. The following screen is presented to you for the Aladdin eToken PRO (72K) Java.



注：ダウンロード時に発生するエラーに関しては、<http://www.myexostar.com/fis.aspx>で「Federated Identity Service」の「FAQ」セクションを参照ください。

証明書をダウンロードする – 中保証レベル (Hardware)

MLOAハードウェア証明書をダウンロードするには、以下のタスクを完了している必要があります。

- 適切なトークンを取得する。対面検証が予約されると、ExostarはFedExでトークンを郵送します。トークンを受け取っていない場合、カスタマーサポートまでお問い合わせください。
- コンピュータにトークンPKI Clientミドルウェアをインストールする。問い合わせはトークンベンダーに、組織固有の情報に関してはITサポートにお問い合わせください。
- 証明書をダウンロードできるか確認するためにシステムチェックを行う。
<http://www.myexostar.com/systemcheck>
- FIPS 140-2モードでトークンを初期化する。FIPSモードを確認する方法に関しては「ハードウェアトークンのFIPS Modeを確認する」セクションを参照ください。
- トークンのインストールを完了するためのトークン初期パスワードを受け取る。ベンダーに連絡し、初期パスワードを受け取ってください。証明書ダウンロード時にこのトークンのパスワードを入力するよう求められます。
- 対面検証を完了する。詳細は[こちら](#)をクリックしてください。
- 対面検証の終了時に信頼される代理人から16桁のパスコードを受け取る。パスコードを紛失した場合、[再検証オプション](#)を購入し、再度対面検証を受ける必要があります。

ハードウェアトークンのFIPS Modeを確認する

Exostarの中保証レベル (MLOA : Medium Level of Assurance Hardware) デジタル証明書は2048 FIPS 140-2に準拠しています。トークンも同様にFIPS 140-2に準拠していることを確認するために、トークンの情報を確認してください。

注：この情報は、デジタル証明書をダウンロードするより前に確認してください。

1. トークンの初期パスワードを変更後、USBドライバにトークンを挿入する。Aladdin eToken PRO (72K) Javaでは、以下の画面が表示される。

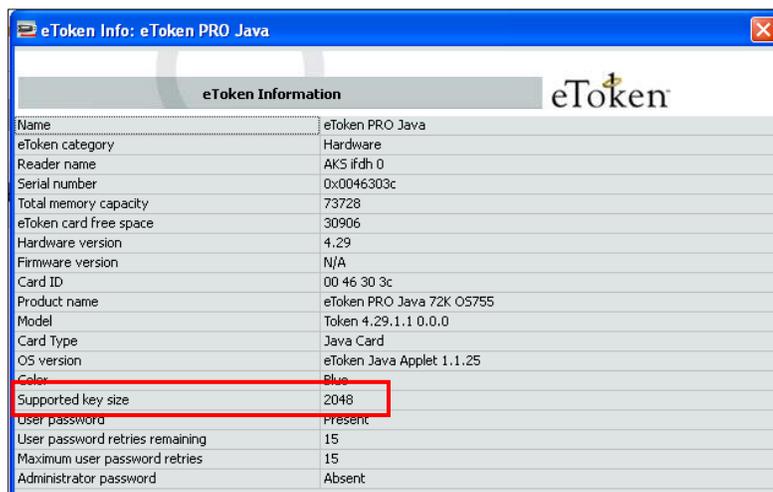


Note: Your view of the screenshots may differ from this guide. This is due to the token settings specific to your organization.

2. Click on **View eToken Info** to display the token details.



3. Scroll through the list, and search for **FIPS Mode** and **Supported Key Size** under the **Name** column. In the screenshot below, the token does not display information on FIPS Mode. At this time, you must follow the steps below to initialize your token in the FIPS Mode.

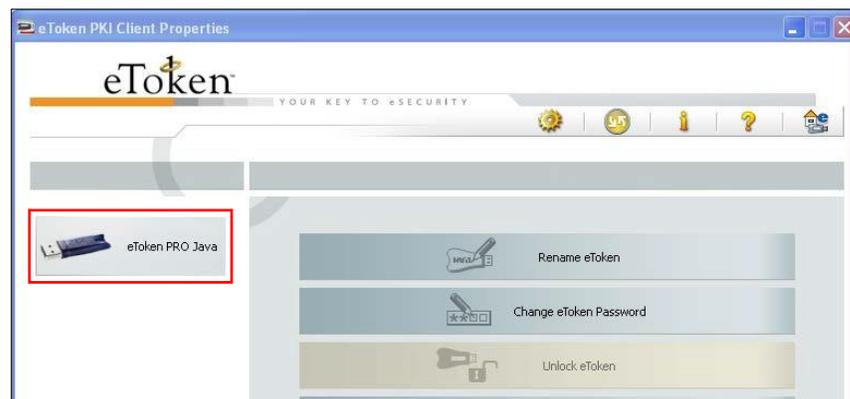


Note: Make sure the Supported Key size is 2048 (shown above).

Note: Any certificates on the token are invalid for FIPS 14-compliance. If you already have certificates installed on the tokens, you will need to re-initialize the token.

Hardware Token FIPS Mode Initialization

1. Click **eToken Pro Java**.

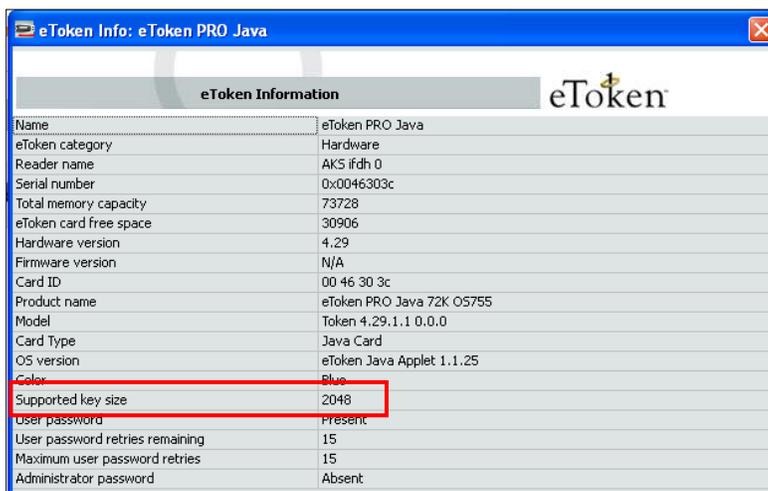


注：トークンの設定は各組織に固有なものであるため、実際のスクリーンショット画面は本ガイドと異なる場合があります。

2. トークンの詳細を表示するため「View eToken Info」をクリックする。



3. リストをスクロールして「Name」欄で「FIPS Mode」と「Supported Key Size」を見つける。以下のスクリーンショットでは、トークンの「FIPS Mode」に関する情報が表示されていない。この場合、以下の手順に沿ってトークンを「FIPSMODE」で初期化する。



注：「Supported Key size」が2048であることを確認してください（上記参照）。

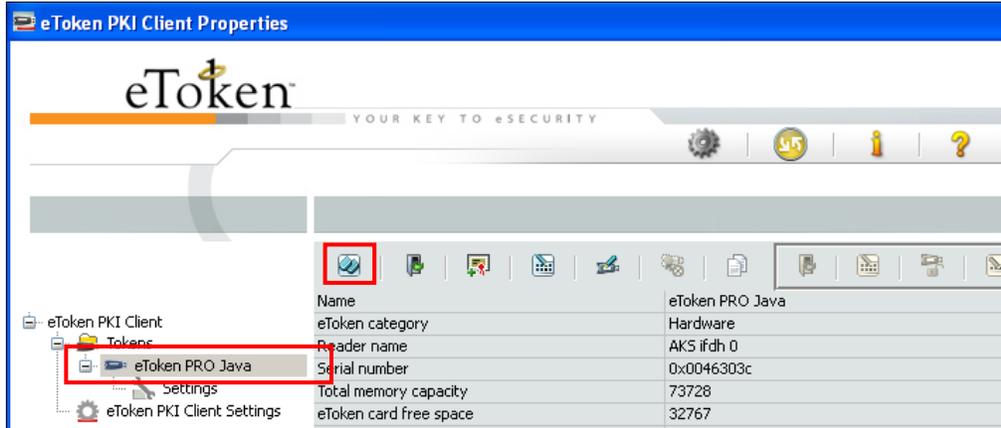
注：FIPS 14に準拠するにあたって、トークンに格納された証明書は無効です。すでに証明書がトークンにインストールされている場合、トークンを再初期化してください。

ハードウェアトークンのFIPSモードを初期化する

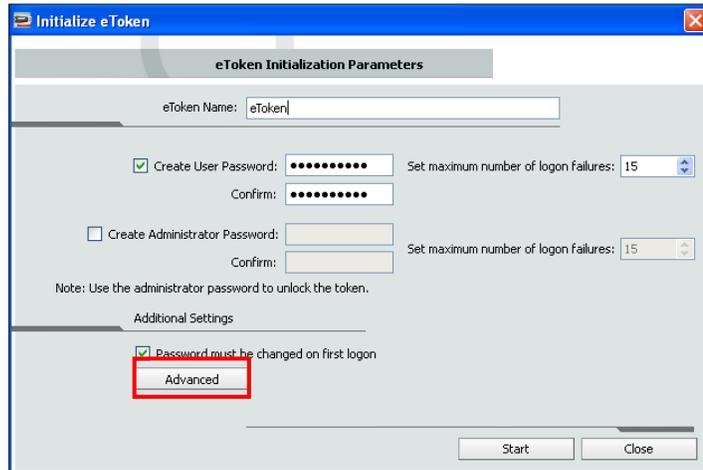
1. 「eToken Pro Java」をクリックする。



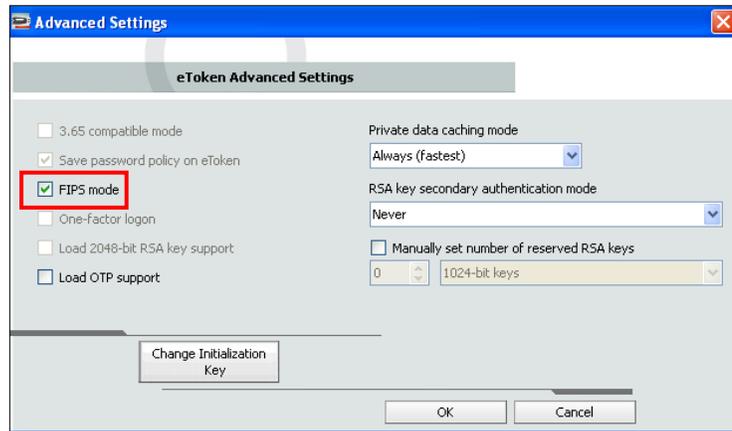
2. Select the Initialize eToken icon to display the initialize screen.



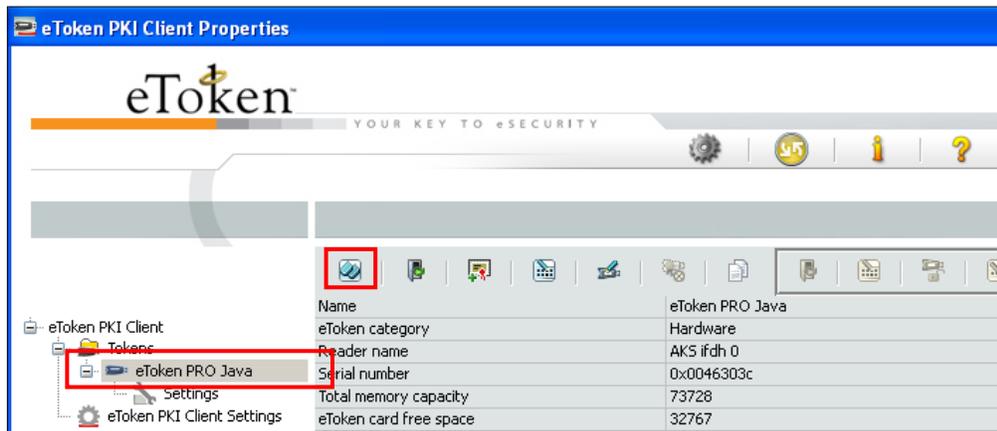
3. Click the **Advance View** icon on the **PKI Client**. . If this button is unavailable, contact your **IT Administrator** or **FISA** for additional information on how to set-up the token in the FIPS mode.



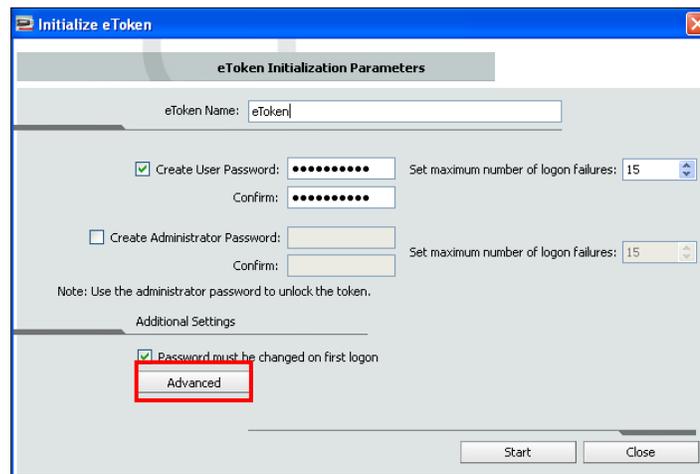
4. Check the box for **FIPS mode**, to set-up the FIS mode for the token. Click **OK** to complete the change.



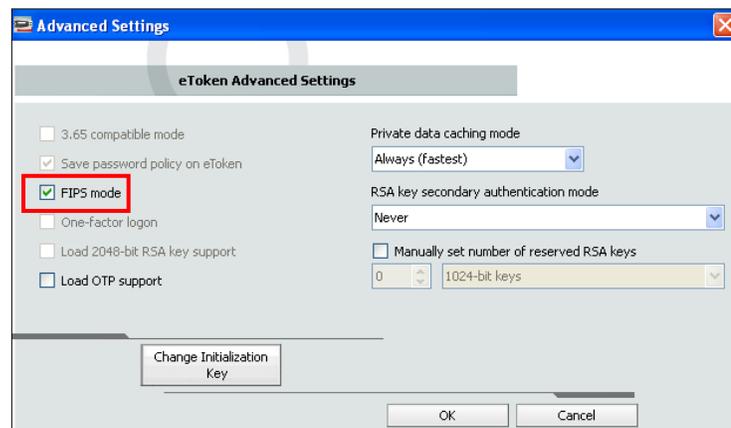
- 「Initialize eToken」アイコンを選択し、初期化画面を表示する。



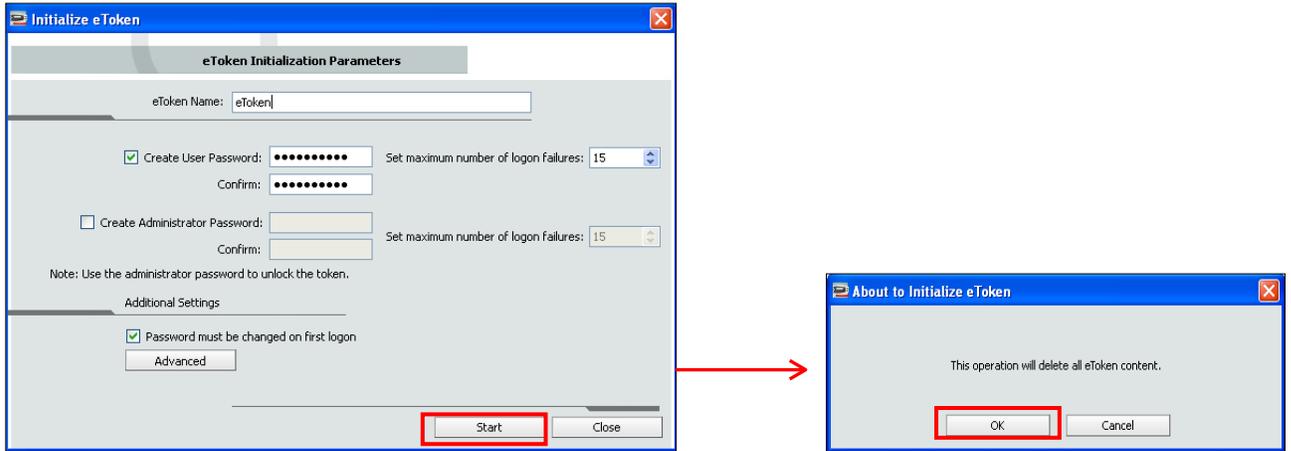
- PKIクライアントで「Advance View」アイコンをクリックする。このボタンが使用できない場合、トークンのFIPSモード設定方法に関する情報をIT管理者またはFISAに問い合わせる。



- 「FIPS mode」のボックスにチェックを入れ、トークンのFIPSモードを設定する。「OK」をクリックし、変更する。



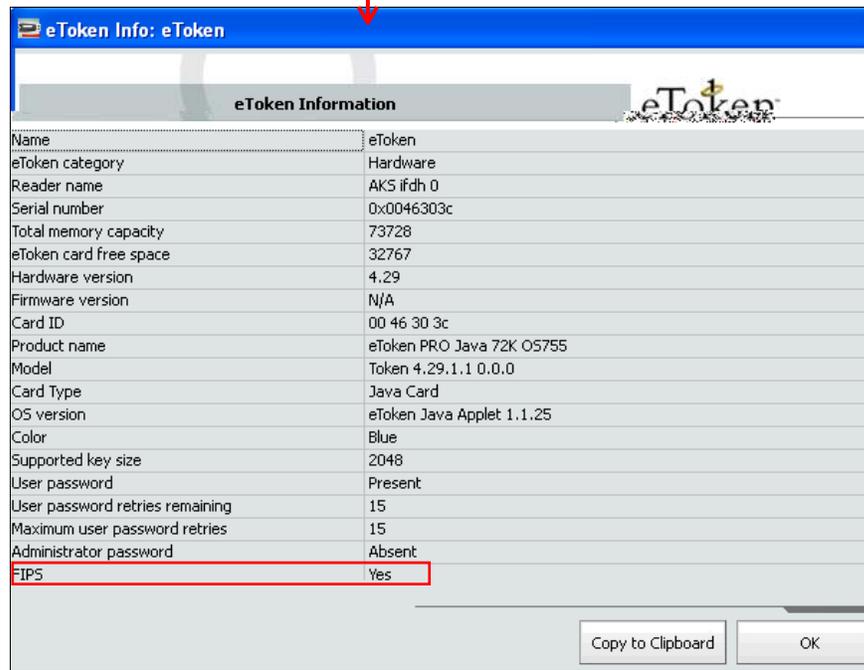
- On the **Initialize eToken** screen, click **Start**. The following screen is presented. Select **OK** to start token initialization.



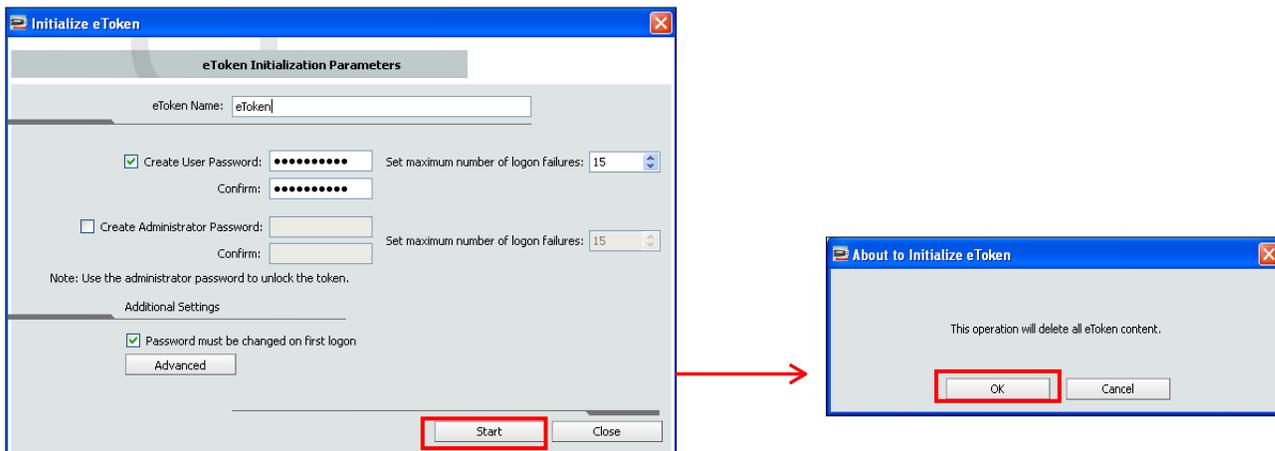
- Once you have successfully initialized your token, you will receive the following message:



- Click **OK**, and go back to the **PKI Client** main screen. Select **View eToken Info**. The FIPS Mode will appear as shown below.



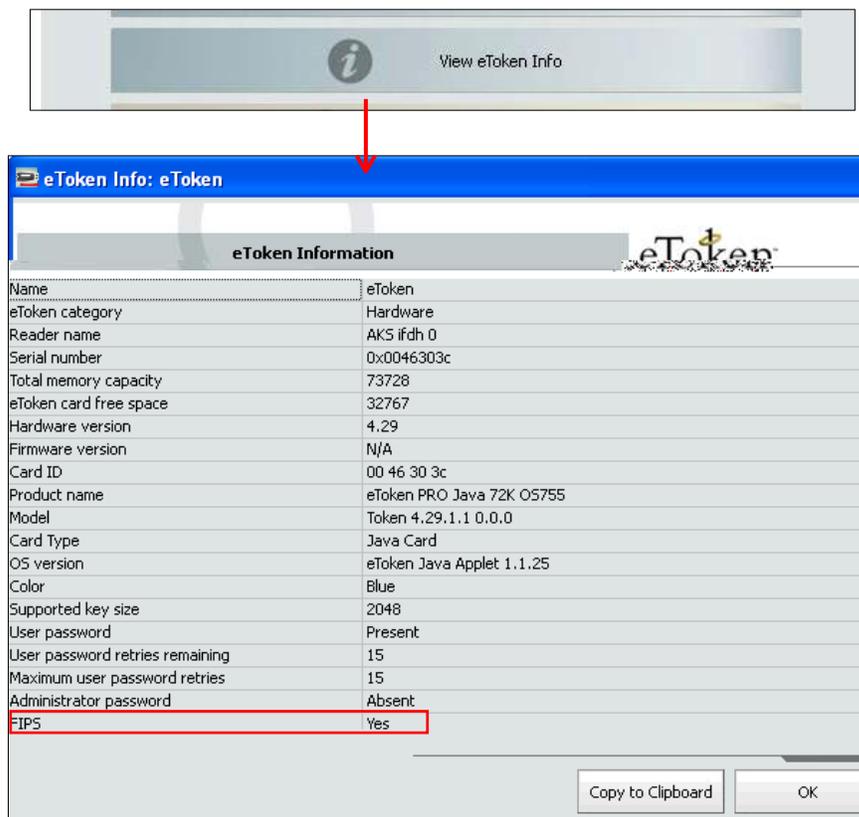
- 「Initialize eToken」画面で「Start」をクリックする。以下の画面が表示されるので、「OK」を選択し、トークンの初期化を開始する。



- トークンの初期化が完了すると、以下のメッセージが表示される。



- 「OK」をクリックし、PKIクライアントのメイン画面に戻る。「View eToken Info」を選択する。FIPSモードは以下のように示される。



Downloading certificates to your token

Before you begin downloading your certificates, you should install the **PKI Client** on your computer, as well as change the initial password of your token. Once you have completed this, please follow the steps below:

1. Plug the token into your USB drive, and make sure you are logged into your MAG user account.
2. To download the certificates you were approved for, go to the **My Account** tab and then click the **Manage Certificates** tab.



Note: You will only see the **Download Certificates** sub-tab under the **Manage Certificates** tab, when you have an approved FIS request pending certificate download. If no certificates are available for download, this sub-tab will not appear.

3. Enter your 16-digit passcode. At the time of in-person proofing appointment, the proofer provided you a passcode. This passcode is only valid after you receive a packet approval email from Exostar.

Note: The passcode is a 16-digit number separated by hyphens, for example: **1234-5678-1234-5678**. You **must** enter all characters, including the hyphens, OR leave the hyphens out completely. The passcode is **NOT** the same as your MAG log-in password.



4. If your passcode is correct, you will see a list of certificates to download. The system will automatically select all of them for download. Once selected, you are prompted to enter the hardware token password.

Enter the token password and click **OK**.

トークンに証明書をダウンロードする

証明書のダウンロードを開始する前に、コンピュータにPKIクライアントをインストールするとともに、トークンの初期パスワードを変更してください。終了後、以下の手順に従ってください。

1. トークンをUSBドライバに挿入し、MAGのユーザ・アカウントにログインする。
2. 承認された証明書をダウンロードするには、「My Account」タブから「Manage Certificates」タブをクリックする。



注：「Manage Certificates」タブの「Download Certificates」サブタブは、FIS申請が承認され、未ダウンロードの証明書がある場合にのみ表示されます。ダウンロード可能な証明書がない場合、このサブタブは表示されません。

3. 16桁のパスコードを入力する。パスコードは対面検証時に検証人（ブルーファーマー）から提供される。このパスコードは、Exostarからパケット承認メールを受信した後から有効になる。

注：パスコードはハイフンで区切られた16桁の数字です（例：1234-5678-1234-5678）。ハイフンを含めたすべての数字を必ず入力してください（もしくは、ハイフンを完全に抜かしてください）。パスコードはMAGログイン用パスワードとは異なります。



4. パスコードが正しければ、ダウンロード可能な証明書のリストが表示される。すべての証明書をダウンロードするよう自動で選択される。選択後、ハードウェアトークンのパスワードを入力するように求められる。

トークンのパスワードを入力し、「OK」をクリックする。



5. Click **OK**. Certificates are created and archived.



Note: This activity allows Exostar to archive the encryption key for recovery at a later time. Refer to the **Recover Encryption Keys** section for details.

6. Once the archiving process is complete, click **OK** to complete the installation process.



7. You are prompted again for your token password. Enter your password, and click **OK** to import the certificates to your token.





5. 「OK」をクリックする。証明書が作成・アーカイブされる。



注：この操作によって、Exostarは暗号鍵をアーカイブし、後に復元することができるようになります。詳細は、「暗号鍵を復元する」セクションを参照ください。

6. アーカイブ処理が終了したら、「OK」をクリックしてインストール処理を完了する。



7. トークンのパスワードを入力するように再度求められる。証明書をトークンにインポートするため、パスワードを入力し、「OK」をクリックする。



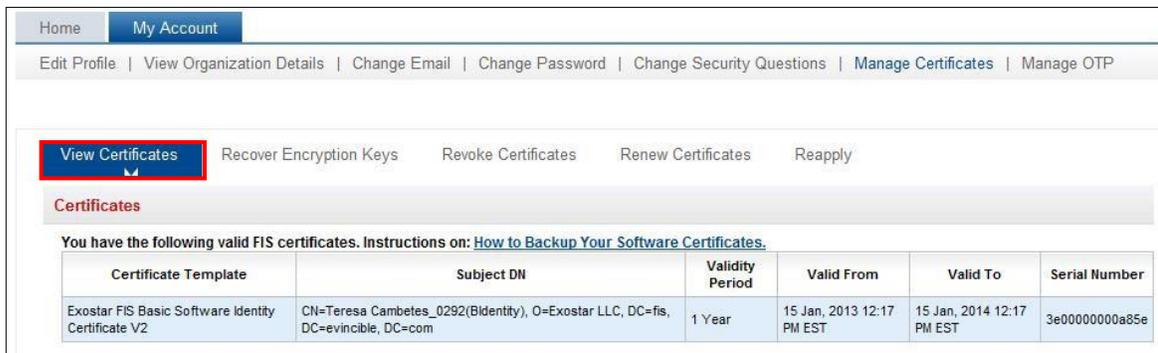
8. Click **OK** to complete the process.



Note: Refer to the **FAQ section for Federated Identity Service** on <http://www.myexostar.com/fis.aspx> for information on any download errors.

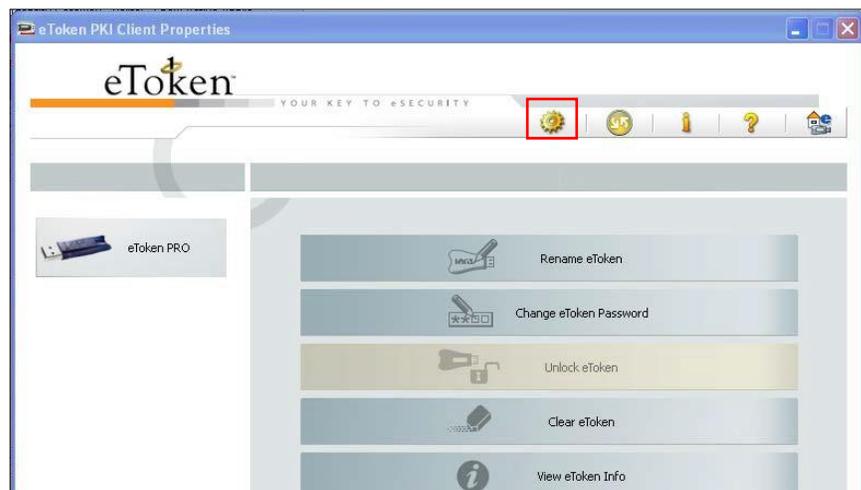
View Certificates (MAG)

After you successfully download your FIS certificates, you are able to view the certificates, and their details, under the **View Certificates** sub-tab.



View Certificates (eToken – for MLOA hardware)

1. After installing the certificates, open the token client. The following screenshots depict the information specific to **Aladdin eToken Pro 72 K** token.
2. Click on the advanced view (highlighted above).



- 「OK」をクリックし、処理を完了する。



注：ダウンロード時のエラーに関しては、<http://www.myexostar.com/fis.aspx>で「Federated Identity Service」の「FAQ」セクションを参照ください。

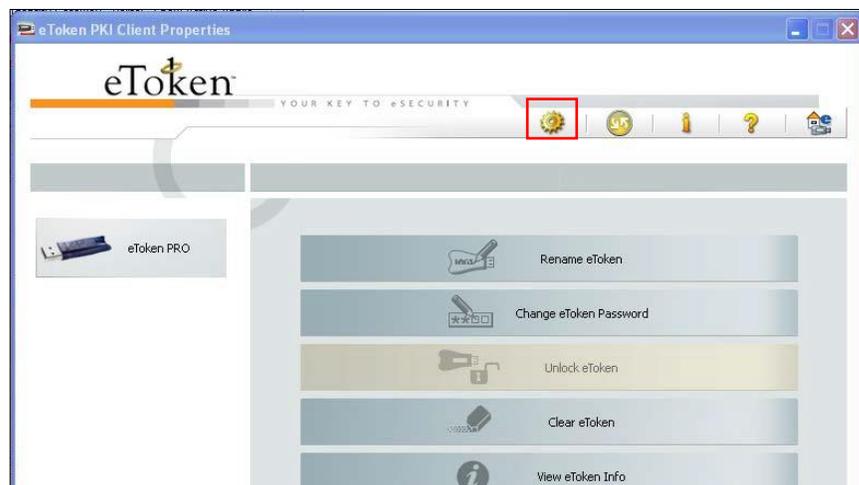
証明書を表示する (MAG)

FIS証明書のダウンロード後、証明書とその詳細を「View Certificates」サブタブで見ることができます。

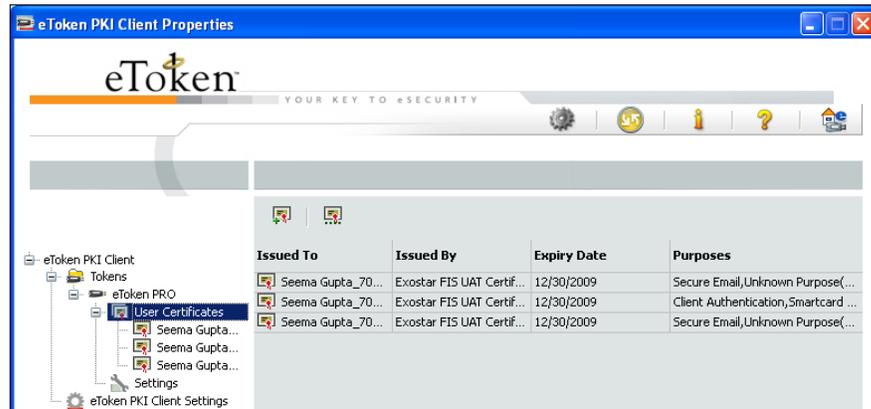


証明書を表示する (eToken – MLOA hardware)

- 証明書のインストール後、トークンクライアントを開ける。以下のスクリーンショットは、「Aladdin eToken Pro 72 K」トークンに関する情報を示している。
- 詳細表示をクリックする（以下で印が付けられたアイコン）。



3. Expand the **User Certificates** by clicking on plus sign (+). You should view the list of all installed certificates. Click on each certificate to view details.



Revoke Certificates

If you suspect one of the following, you should revoke your certificates:

- Loss, compromise or theft of your private key
- Fraud

There are four ways to revoke your certificates:

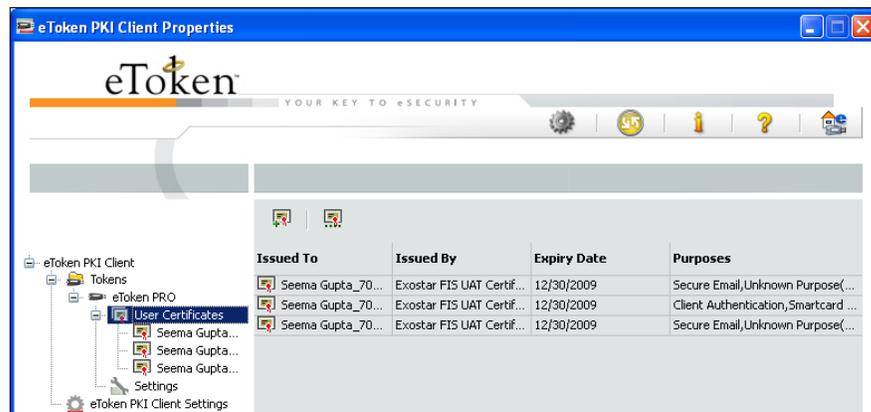
1. **Yourself:** Log-in to your MAG account using your user ID and password, and follow the steps provided below.
2. **Organization Administrator:** Your Organization Admin can revoke your certificates at any time.
3. **FIS Administrator:** Your organization's designated FIS Admin can revoke your certificates on your behalf.
4. **Exostar Customer Support:** If your certificates have been compromised, you can contact Exostar Customer Support and request certificate revocation.

To revoke your certificates, please follow the steps below:

1. Go to the **My Account** tab, click the **Manage Certificates** tab, and then click the **Revoke Certificates** tab.

Note: You cannot selectively revoke certificates. This activity will revoke all of your downloaded certificates.

3. プラス記号 (+) をクリックし、「**User Certificates**」を展開する。インストールしたすべての証明書が表示される。詳細を表示するには、各証明書ををクリックする。



証明書を失効させる

以下の疑いがある場合、証明書を失効させる必要があります。

- 秘密鍵の紛失・危殆化・盗難
- 詐欺・詐称

証明書を失効させるには以下の4つの方法があります。

1. **ユーザ自身**：ユーザIDとパスワードでMAGアカウントにログインし、以下の手順に従ってください。
2. **組織管理者**：証明書を随時失効させることができます。
3. **FIS管理者**：ユーザの組織が指定したFIS管理者は、ユーザに代わって証明書を失効させることができます。
4. **Exostarカスタマーサポート**：証明書の危殆化が生じた場合、Exostarカスタマーサポートに連絡し、証明書の失効を要求することができます。

証明書を失効させるには、以下の手順に従ってください。

1. 「**My Account**」タブから「**Manage Certificates**」タブ、「**Revoke Certificates**」タブの順にクリックする。

注：証明書を選択して失効することはできません。この操作によりダウンロードしたすべての証明書が失効されます。

Home | My Account

Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | **Manage Certificates** | Manage OTP

View Certificates | Recover Encryption Keys | **Revoke Certificates** | Renew Certificates | Reapply

Certificates

You should revoke your digital certificates immediately if you suspect that any of these conditions has occurred:

- Loss of your private key (For example, you lost your laptop containing your certificates)
- Compromise or theft of your private key
- Fraud

All your FIS certificates will be revoked when you click on "Revoke" below

Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number
Exostar FIS Basic Software Identity Certificate V2	CN=Teresa Cambetes_7221(BIdentity), O=Highline Technology Services, DC=securepass, DC=exostartest, DC=com	1 Year	22 Apr, 2013 02:26 PM EDT	22 Apr, 2014 02:26 PM EDT	3e000100000521

*Revocation Reason: Certificate Compromised

Comments (Maximum 300 characters):

Revoke

2. Click the **Revoke** button to revoke **ALL** of your FIS certificates. The following screen is presented:



3. Select **OK** to revoke all certificates. The **Certificate Revocation Confirmation** is presented.

Home | My Account

Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | **Manage Certificates** | Manage OTP

View Certificates | Recover Encryption Keys | **Revoke Certificates** | Renew Certificates | Reapply

Certificates

The following certificates have been revoked:

Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number
Exostar FIS Basic Software Identity Certificate V2	CN=Teresa Cambetes_7221(BIdentity), O=Highline Technology Services, DC=securepass, DC=exostartest, DC=com	1 Year	22 Apr, 2013 02:26 PM EDT	22 Apr, 2014 02:26 PM EDT	3e000100000521

Recover Encryption Keys

This section is only pertinent to users with **BLOA SecureEmail**, **MLOA Software** and **MLOA Hardware** certificates.

Home | My Account

Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | **Manage Certificates** | Manage OTP

View Certificates | Recover Encryption Keys | **Revoke Certificates** | Renew Certificates | Reapply

Certificates

You should revoke your digital certificates immediately if you suspect that any of these conditions has occurred:

- Loss of your private key (For example, you lost your laptop containing your certificates)
- Compromise or theft of your private key
- Fraud

All your FIS certificates will be revoked when you click on "Revoke" below

Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number
Exostar FIS Basic Software Identity Certificate V2	CN=Teresa Cambetes_7221(BIdentity), O=Highline Technology Services, DC=securepass, DC=exostartest, DC=com	1 Year	22 Apr, 2013 02:26 PM EDT	22 Apr, 2014 02:26 PM EDT	3e000100000521

*Revocation Reason: Certificate Compromised

Comments (Maximum 300 characters):

Revoke

2. 「**Revoke**」 ボタンをクリックしてすべてのFIS証明書を実効させる。以下の画面が表示される。



3. 「**OK**」 をクリックし、すべての証明書を失効させる。証明書失効の確認が表示される。

Home | My Account

Edit Profile | View Organization Details | Change Email | Change Password | Change Security Questions | Manage Certificates | Manage OTP

View Certificates | Recover Encryption Keys | **Revoke Certificates** | Renew Certificates | Reapply

Certificates

The following certificates have been revoked:

Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number
Exostar FIS Basic Software Identity Certificate V2	CN=Teresa Cambetes_7221(BIdentity), O=Highline Technology Services, DC=securepass, DC=exostartest, DC=com	1 Year	22 Apr, 2013 02:26 PM EDT	22 Apr, 2014 02:26 PM EDT	3e000100000521

暗号鍵を復元する

このセクションは、「**BLOA SecureEmail**」 「**MLOA Software**」 および 「**MLOA Hardware**」 のクレデンシャルを持っているユーザのみに関係します。

A user receives three certificates for FIS BLOA SecureEmail, MLOA Software, and Hardware:

1. Identity
2. Authentication
3. Encryption

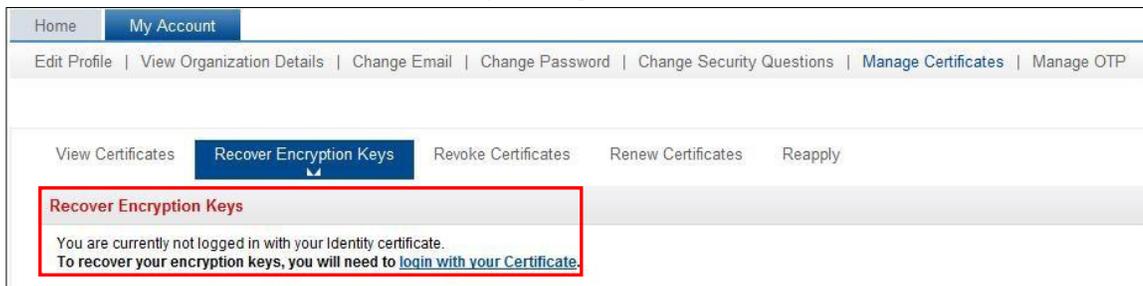
Once a user revokes or loses their MLOA certificates, they need to re-apply for certificates, and go through the in-person proofing process again. This may also require an additional purchase. To enable the users to access data encrypted using the revoked/lost certificates, Exostar offers the self-key recovery functionality.

IMPORTANT:

- If you are approved for and have downloaded FIS **BLOA SecureEmail** certificates, you can recover encryption keys for all active, revoked, or expired certificates.
- If you are approved for and have downloaded FIS **MLOA Software** certificates, you can recover both BLOA SecureEmail and MLOA Software encryption keys for all active, revoked or expired certificates.
- If you are approved for and have downloaded FIS **MLOA Hardware** certificates, you can recover encryption keys for all certificates – BLOA SecureEmail, MLOA Software, and MLOA Hardware. However, for hardware certificates, you can only recover expired or revoked encryption keys. Current keys cannot be recovered.
- If you are recovering hardware encryption keys, you need to log-in using your hardware token.
- You can use the keys only to access the data which was encrypted using the revoked or lost certificates.

To recover the keys, follow the steps below:

1. [Log-in](#) to your MAG account using your new MLOA certificates. If you have not reapplied for certificates, complete all the activities related to requesting access, in-person proofing, and downloading your certificates, prior to attempting to recover encryption keys. Refer to the **Reapply for Certificates** section for information on reapplying for certificates.
2. The following screen is presented if you have not logged-in using your new certificates. Click on the link to select the certificate associated with your log-in credentials.



3. Click the **Recover Encryption Keys** tab under the **Manage Certificates** tab.

ユーザは、FISの「BLOA SecureEmail」「MLOA Software」および「MLOA Hardware」において、3つの証明を受け取ります。

1. 「Identity (アイデンティティ情報)」
2. 「Authentication (認証)」
3. 「Encryption (暗号化)」

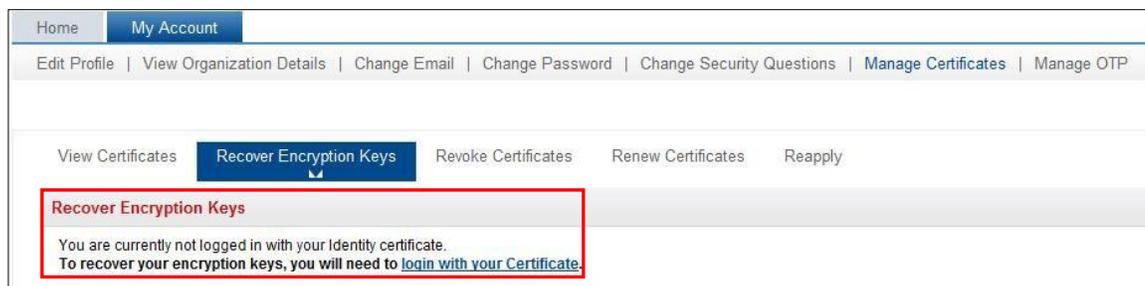
MLOA証明書が失効または無くなった場合、ユーザは証明書を再申請し対面検証を再度受ける必要があります。これには追加の購入を伴う場合もあります。ユーザが失効または紛失した証明書を使用して暗号化されたデータにアクセスできるように、Exostarでは鍵を自己復元できる機能を提供しています。

重要：

- FISの「**BLOA SecureEmail**」証明書を承認され、すでにダウンロードしている場合、アクティブ・失効・有効期限切れのすべての証明書の暗号鍵を復元することができます。
- FISの「**MLOA Software**」証明書を承認され、すでにダウンロードしている場合、「BLOA SecureEmail」と「MLOA Software」のアクティブ・失効・有効期限切れのすべての証明書の暗号鍵を復元することができます。
- FISの「**MLOA Hardware**」証明書を承認され、すでにダウンロードしている場合、「BLOA SecureEmail」、「MLOA Software」および「MLOA Hardware」のすべての証明書の暗号鍵を復元することができます。ただし、ハードウェア証明書に関しては、有効期限切れ又は失効した暗号鍵のみを復元することができます。現在の鍵を復元することはできません。
- ハードウェア暗号鍵を復元する場合、ハードウェアトークンを使用してログインする必要があります。
- 失効又は紛失した証明書を使用して暗号化されたデータにアクセスする時のみ、鍵を使用することができます。

鍵を復元するには、以下の手順に従ってください。

1. 新しいMLOA証明書を使用してMAGアカウントに[ログイン](#)する。証明書の再申請を行っていない場合、暗号鍵を復元する前に、アクセス申請、対面検証および証明書ダウンロードのためのすべての操作を行う。証明書の再申請に関する情報は、「[証明書を再申請する](#)」のセクションを参照ください。
2. 新しい証明書を使用してログインしたことがない場合、以下の画面が表示される。ログイン・クレデンシャルに関連した証明書を選択するためにリンクをクリックする。



3. 「**Manage Certificates**」タブで「**Recover Encryption Keys**」タブをクリックする。

View Certificates **Recover Encryption Keys** Revoke Certificates Renew Certificates Reapply

Recover Encryption Keys

Key Recovery Process - Important Information
 This page allows you to recover the encryption keys for your encryption certificate(s) only. This is commonly needed when you have previously encrypted information (e.g., email) using an encryption certificate that you no longer have and thereby can no longer decrypt the information.
 During the recovery process, you may be prompted to login again using your identity certificate.
 After a successful recovery, you will be prompted to download a P12 file to your computer.
 You will also receive an email (to your current email address on file), which contains a one-time use password that you'll need to unlock the file.
 After download, open the file and follow the steps to import that certificate into your computer or onto your token to make it available for use by your applications.
 Need additional Help? Refer [MAG User Guide](#).
You will be able to recover the keys for the following certificates:

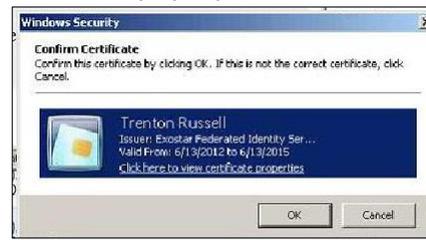
Select	Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number
<input type="radio"/>	Exostar FIS Medium Hardware Encryption Certificate V2	CN=Trent_Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostatetest, DC=com	3 Years	11 Dec, 2012 11:20 AM EST	11 Dec, 2015 11:20 AM EST	3e000100000438
<input type="radio"/>	Exostar FIS Medium Software Encryption Certificate V2	CN=Trent_Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostatetest, DC=com	1 Year	29 Apr, 2013 12:28 PM EDT	29 Apr, 2014 12:28 PM EDT	3e00010000052e
<input type="radio"/>	Exostar FIS Medium Software Encryption Certificate V2	CN=Trent_Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostatetest, DC=com	1 Year	11 Dec, 2012 09:50 AM EST	11 Dec, 2013 09:50 AM EST	3e000100000435
<input type="radio"/>	Exostar FIS SecEmail Basic Software Encryption Certificate V2	CN=Trent_Russell_3831(BEncryption), O=Seema Test Company, DC=securepass, DC=exostatetest, DC=com	1 Year	29 Apr, 2013 12:05 PM EDT	29 Apr, 2014 12:05 PM EDT	3e00010000052b
<input type="radio"/>	Exostar FIS Medium Hardware Encryption Certificate V2	CN=Trent_Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostatetest, DC=com	3 Years	11 Dec, 2012 01:30 PM EST	11 Dec, 2015 01:30 PM EST	3e00010000043d
<input type="radio"/>	Exostar FIS Medium Hardware Encryption Certificate V2	CN=Trent_Russell_3831(Encryption), O=Seema Test Company, DC=securepass, DC=exostatetest, DC=com	3 Years	11 Dec, 2012 08:44 AM EST	11 Dec, 2015 08:44 AM EST	3e00010000042f

Recover Key

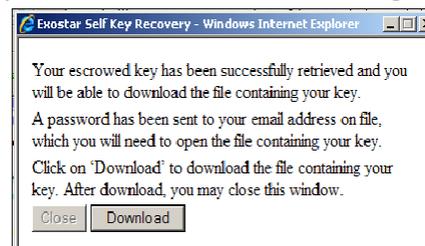
- Select the certificate for which you need to recover the encryption key. If multiple certificates are available, you will need to repeat the process to recover each key. The following screen is presented:

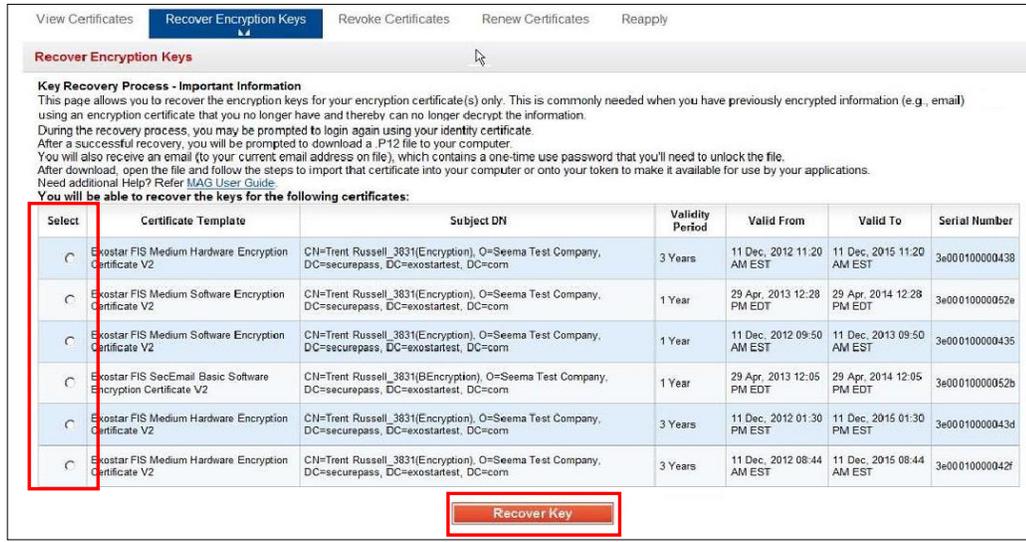


- Click **OK**. On the **Choose a digital certificate** pop-up screen, select the certificate you used to log-in.



- You may be prompted to log-in again using your MLOA certificate. Complete the log-in with the MLOA certificate used to log-in in step 1, and click **OK**. The following screen is presented. Click **Download**.

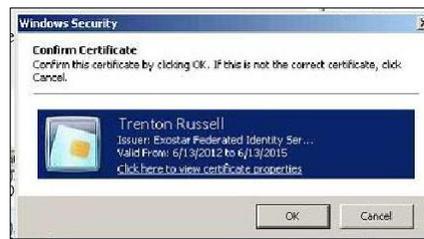




4. 暗号鍵を復元する証明書を選択する。複数の証明書が該当する場合、各鍵に対してこの処理を繰り返す。以下の画面が表示される。



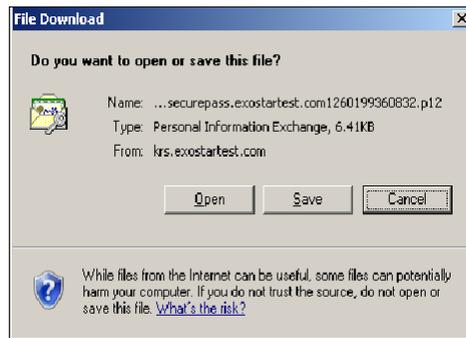
5. 「OK」をクリックする。「Choose a digital certificate」のポップアップ画面で、ログインに使用した証明書を選択する。



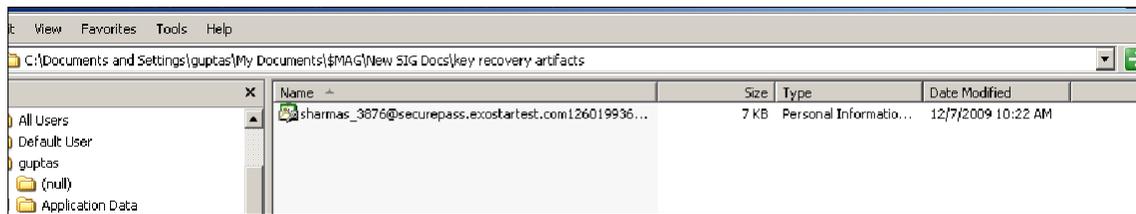
6. MLOA証明書を使用して再度ログインするように求められる場合がある。手順1でログインした際に使用したMLOA証明書でログインし、「OK」をクリックする。以下の画面が表示される。「Download」をクリックする。



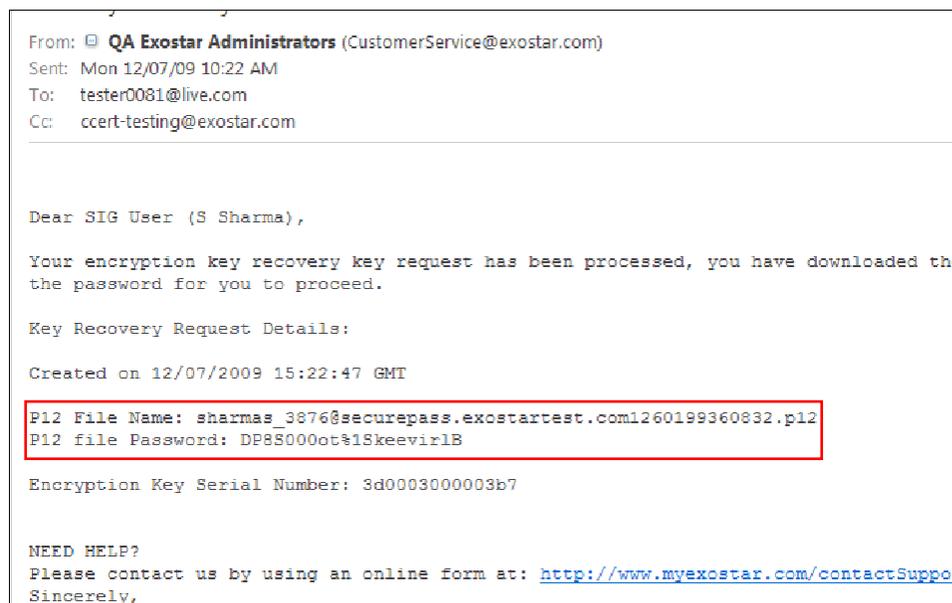
7. You will be prompted to either **open** or **save** the file. Click the **Save** button.



8. Save the certificate file (.p12 format) at a location of your choice. Click **Close** on the **Exostar Self Key Recovery** screen.



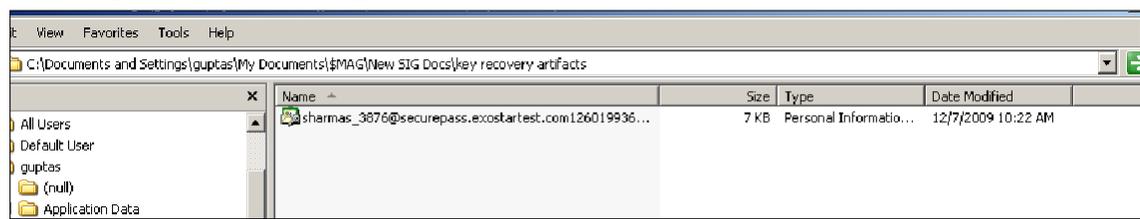
9. You will receive an email with a one-time password, which is required to unlock the file you have just downloaded. Follow the instructions under the **Importing Recovered Encryption Keys** section for the next steps.



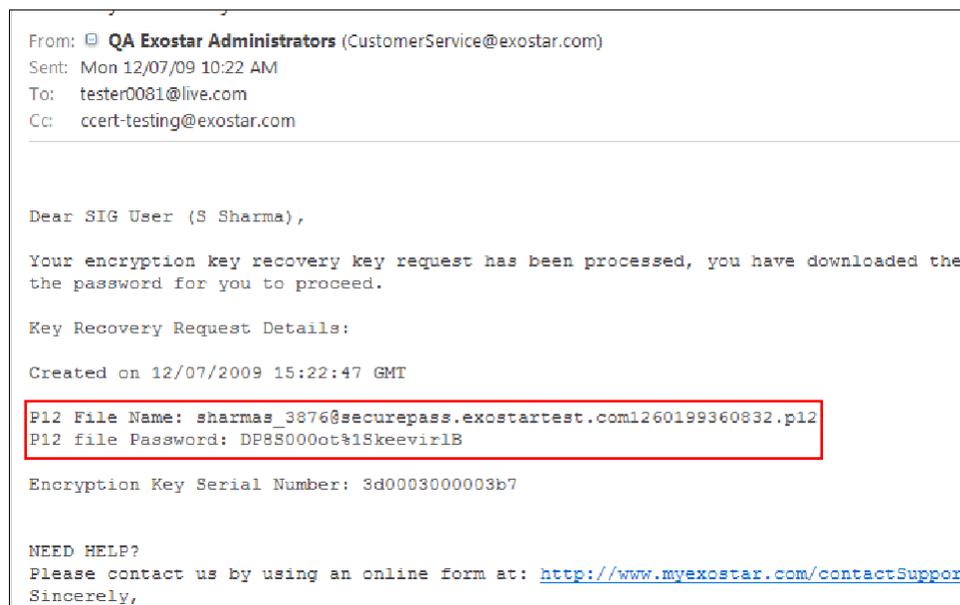
7. ファイルを「Open (開く)」か「Save (保存する)」か確認される。「Save」ボタンをクリックする。



8. 選択した場所に証明書のファイル (.p12フォーマット) を保存する。「Exostar Self Key Recovery」画面で「Close」をクリックする。



9. ダウンロードしたファイルのアンロックに必要なワンタイムパスワードがメールで届く。この後の手順は、「復元した暗号鍵をインポートする」のセクションの指示に従う。



Importing Recovered Encryption Keys

To import the encryption keys recovered in the section **Recover Encryption Keys**, you need the following:

- Access to the location where you saved the .p12 file.
- Email with the one-time password, to unlock the key for importing.

Follow the steps below to import your encryption key:

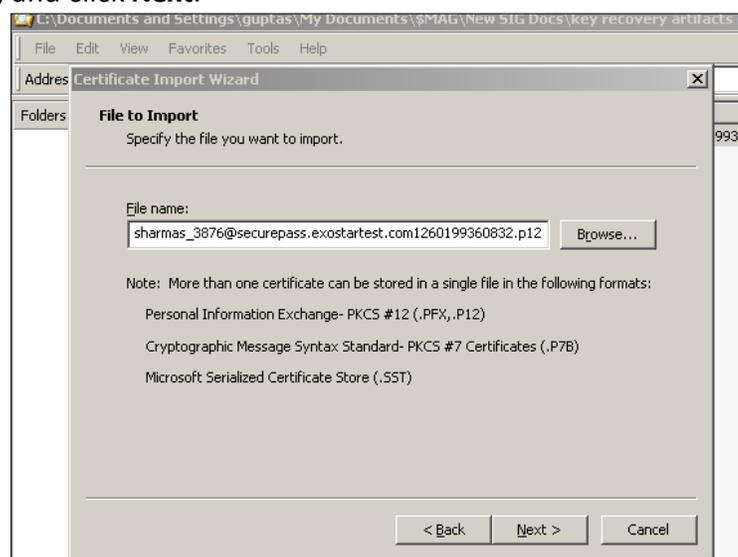
1. Double click on the saved .p12 file.



2. You are presented with the **Certificate Import Wizard**. Click **Next**.



3. Confirm the filename, and click **Next**.



復元した暗号鍵をインポートする

「暗号鍵を復元する」セクションで復元した暗号鍵をインポートするには、以下が必要となります。

- .p12ファイルの保存場所へのアクセス
- インポートのために鍵を解除するワンタイムパスワードが含まれたメール

暗号鍵をインポートするには、以下の手順に従ってください。

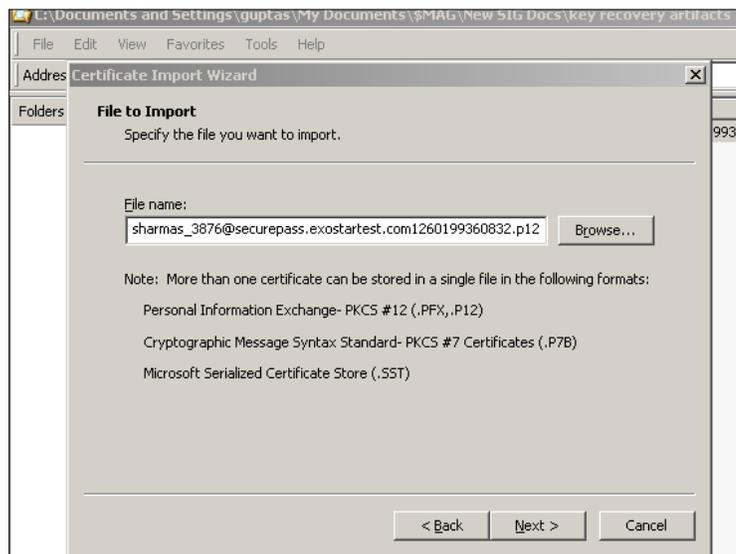
1. 保存した.p12ファイルをダブルクリックする。



2. 「Certificate Import Wizard」が表示されるので、「Next」をクリックする。



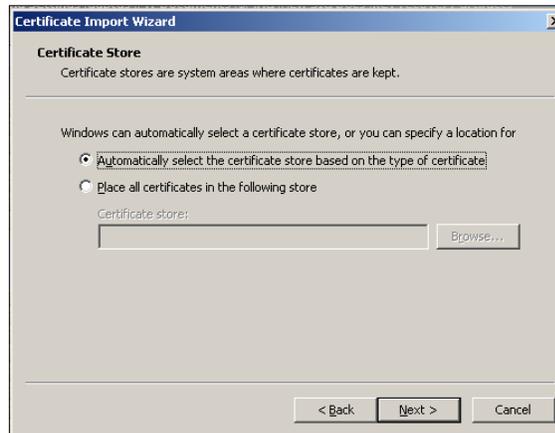
3. ファイル名を確認し、「Next」をクリックする。



- Copy or enter the one-time password from the email you received, make sure no trailing spaces are entered. In addition, it is strongly suggested you enable **strong key protection**, and set-up a password to access the encryption key. To enable further export of the key, you may also select **Mark this key as exportable** option.



- Click **Next**. You will be prompted to select a location to store the certificate. Click **Next**.



- Click **Next** again to complete the import process, then click **Finish**.



- 受信したメールに含まれているワンタイムパスワードをコピー又は入力する。この時、末尾にスペースが入力されていないか確認する。「**Enable strong key protection (鍵の強力な保護を有効にする)**」を設定し、暗号鍵にアクセスするためのパスワードを設定することが強く推奨される。さらに、鍵のエクスポートを可能にするには、「**Mark this key as exportable (この鍵をエクスポート可能にする)**」のオプションを選択する。



- 「**Next**」をクリックする。証明書を保存する場所を選択するように求められる。「**Next**」をクリックする。



- 「**Next**」を再度クリックし、インポート処理を完了する。「**Finish**」をクリックする。



7. If you selected to **Enable strong protection** in step four, you are presented with the below screen. Click **Set Security Level** to set a password for the encryption key.



8. Select **High** to ensure you are prompted for a password each time, and then click **Next**.



9. Enter a password and click **Finish**.



7. 手順4で「**Enable strong key protection (鍵の強力な保護を有効)**」を選択した場合、以下の画面が表示される。「**Set Security Level (セキュリティレベルを設定する)**」をクリックし、暗号鍵のパスワードを設定する。



8. 毎回パスワードを求められるようにするため「**High**」を選択し、「**Next**」をクリックする。



9. パスワードを入力し、「**Finish**」をクリックする。



10. Click **OK**, and the following screen is presented:



Note: When you attempt to open an encrypted document or email, which was encrypted using this key, you will be automatically prompted for the key password you set-up. Enter the password to access your document or email.

Renew Certificates

You may renew your certificates 90 days prior to expiration. If you have expiring certificates, you **must not** reapply for certificates, unless you are attempting to upgrade the certificate assurance level.

Note: For **FIS MLOA Software** and **Hardware** certificates, you must download your renewed certificates using your existing unexpired certificates.

Follow the instructions provided to you in the renewal email to complete the certificate download. For detailed information on renewing your certificates, refer to the [FIS Certificate Renewal/Reapply Guide](#).

Reapply for Certificates

You can reapply for certificates for any of the following reasons:

- Your certificates have been revoked.
- Your certificates have expired (you must complete a new purchase in this case).
- You want to upgrade the certificate assurance level, in which case, a new purchase must be made.
- Your Organization Administrator has instructed you to reapply for FIS certificates.

There are three ways to reapply for your certificates:

1. **Yourself:** Log-in to your MAG account using your user ID and password, and follow the steps provided below.
2. **Organization Administrator:** Your Organization Admin can reapply for certificates on your behalf.
3. **Exostar Customer Support:** If you are unable to request certificates yourself, or the Organization Administrator is unable to request them on your behalf, contact [Exostar Customer Support](#).

10. 「OK」をクリックする。以下の画面が表示される。



注：この鍵を使用して暗号化されたドキュメント又はメールを開こうとすると、設定した鍵のパスワードが求められます。ドキュメント又はメールにアクセスするには、パスワードを入力してください。

証明書を更新する

証明書は有効期限の90日前から更新することができます。有効期限が切れる証明書を持っている場合、証明書の保証レベルをアップグレードする場合以外は、証明書を再申請しないでください。

注：「FIS MLOA Software」および「FIS MLOA Hardware」証明書の場合は、有効期限内の現在の証明書を使用して更新した証明書をダウンロードしてください。

証明書のダウンロードは、更新通知メールに含まれる手順に従って行ってください。証明書の更新に関する詳細は、[FIS証明書更新／再申請ガイド](#)を参照ください。

証明書を再申請する

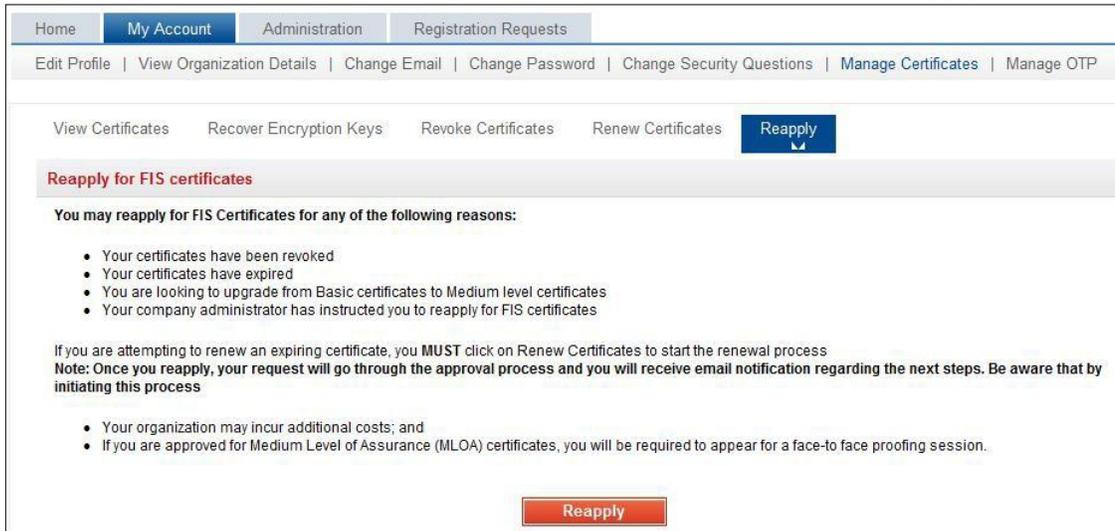
以下の理由に該当する場合、証明書を再申請することができます。

- 証明書が失効させられた場合
- 証明書の有効期限が切れた場合（この場合、新たに証明書の購入が必要です）
- 証明書の保証レベルをアップグレードしたい場合（この場合、新たに証明書の購入が必要です）
- 組織管理者（Organization Administrator）からFIS証明書の再申請を指示された場合

証明書を再申請するには以下の3つの方法があります。

1. **ユーザ自身**：ユーザIDとパスワードでMAGアカウントにログインし、以下の手順に従ってください。
2. **組織管理者**：ユーザに代わって証明書の再申請を行うことができます。
3. **Exostarカスタマーサポート**：ユーザ自身またはユーザに代わって組織管理者（Organization Admin）が証明書の申請を行うことができない場合、[Exostarカスタマーサポート](#)までお問い合わせください。

1. Go to the **My Account** tab, then the **Manage Certificates** tab, and then the **Reapply** tab.



2. Click on the **Reapply** button, and follow the instructions on the screen.

Note: For detailed information on renewing your certificates, refer to the [FIS Certificate Renewal/Reapply Guide](#).

[Connect Accounts](#)

Connecting Accounts allows you to use a single Exostar account to access multiple Exostar accounts you own. In order to enable this:

- You must designate a **Parent** account. This is the account you use to log into Exostar to access all your connected accounts.
- Your **Parent** account should be the account with any additional credentials, such as:
 - OTP Hardware Token
 - Phone Based OTP
 - FIS Certificates
 - 3rd party certificates
 - EAG (linked corporate credentials)

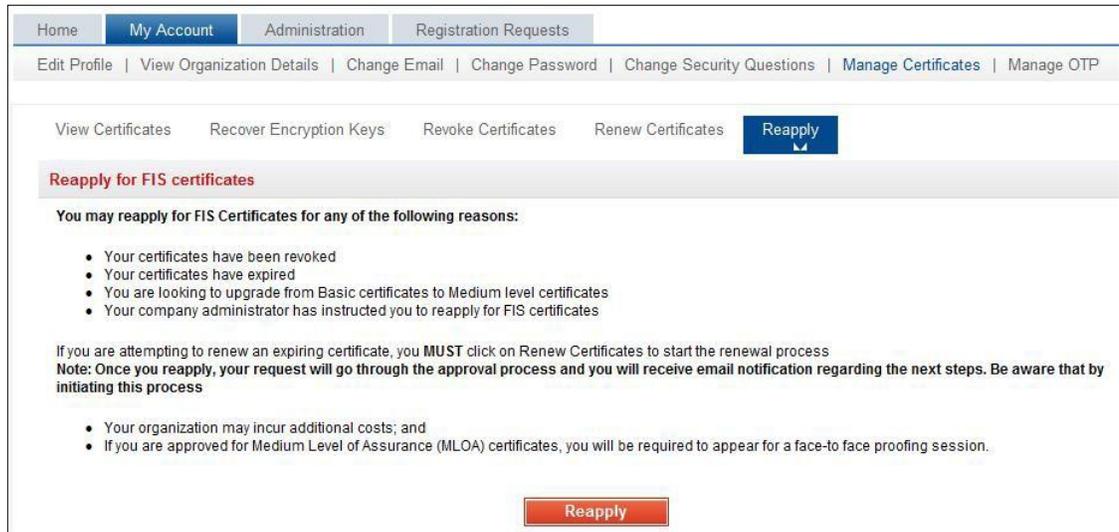
If you need additional assistance, refer to [MAG Account Connections](#).

[Account Disablement](#)

If your account is in a state of inactivity, it may get suspended or deleted. Here are reasons why your account may get **deleted** or **suspended**:

- **First Time Login not completed for more than 180 days:** If you have not completed **First-Time Login** (account activation) for your MAG account, your account will be deleted. You will be notified **30 days** prior to the deletion date, with instructions on how to complete the first-time log-in.
- **Application access suspension:** Each application can set parameters for the number of days of inactivity, which will lead to access suspension. If your application access is due for suspension in 30 days or less, each time you log-in to your MAG account, you are presented with a flash screen to

1. 「My Account」タブから「Manage Certificates」タブ、「Reply」タブの順に移動する。



2. 「Reply」ボタンをクリックし、画面の指示に従う。

注：証明書の更新に関する詳細は、[FIS証明書更新／再申請ガイド](#)をご参照ください。

アカウントを接続する

アカウントの接続によりExostarの1つのアカウントを使用して、所有するExostarの複数のアカウントにアクセスすることができます。

- 「Parent (親)」アカウントを指定してください。このアカウントは、接続したすべてのアカウントにアクセスするためにExostarにログインする際使用するアカウントです。
- 「Parent (親)」アカウントは、次のような追加のクレデンシャルを持つアカウントであるべきです。
 - OTPハードウェアトークン
 - 電話ベースOTP
 - FIS証明書
 - 第三者証明書
 - EAG (リンクした企業クレデンシャル)

さらにサポートが必要な場合、[MAGアカウントの接続](#)を参照ください。

アカウントの無効化

アカウントがアクティブでない場合、停止又は削除される場合があります。以下のような理由でアカウントは停止又は削除されます。

- 初回ログインが180日間以内にされていない：MAGアカウントへの初回ログイン（アカウントの有効化）が完了していない場合、アカウントは削除されます。アカウントが削除される30日前に、初回ログイン方法の手順とともに通知が送られます。
- アプリケーションへのアクセス停止：各アプリケーションで、アクセス停止をもたらす非アクティブ日数のパラメータを設定することができます。アプリケーションへのアクセスが30日以内に停止

remind you to access the application, and the number of days to suspension. To ensure you do not lose access to the applications you need, it is good practice to log-in to your MAG account regularly, and access available applications.

- **Application access deletion:** If your application access has been suspended for **X** number of days, as specified by the application owner, your access to the application will be deleted. You will be notified regarding this deletion **30 days in advance**.
- **Active account deletion:** If the last active application subscription is suspended, your MAG account will be suspended **30 days after the application suspension**. You will be notified regarding this suspension 30 days in advance. Contact [Exostar Customer Support](#) for information on how to re-establish application access.

[Frequently Asked Questions \(FAQs\)](#)

Listed below are some FAQs related to MAG:

Q: [What is the difference between a One-Time Password and a System Generated Password?](#)

A: **One-Time Password** is a manually-created password provided by your Org Admin. This must be used when you log-in for the first time. One-Time Passwords are used as an additional security measure to verify your account during **First-Time Log-in**. This password is different from the passwords generated from a One-Time Password Hardware Token.

System-Generated Password is the password sent via email when your account was created. This must be used during the **First-Time Login**.

Note: All the above passwords can only be used once.

Q: [How do I know who the administrators are for my organization?](#)

A: There may be multiple administrators for your organization. Refer to the **View Organization Details** section for more information.

Q: [Why don't I see the Administration tab after I log-in?](#)

A: If you have not been designated as an **administrator** within MAG, you will not see the **Administration** tab.

For further information on becoming an **Organization Administrator** or an **Application Administrator**, please contact your current Org Admin.

Q: [What do I do if I don't have my passcode for certificate download?](#)

A: Immediately contact [Exostar Customer Support](#).

Q: [Why do I receive the disabled account error when I try to log-in?](#)



する場合、MAGアカウントにログインする度に、アプリケーションへのアクセスを促すリマインダと停止までの日数がフラッシュスクリーンに表示されます。必要なアプリケーションへのアクセス権を失わないように、定期的にMAGアカウントにログインし、使用可能なアプリケーションにアクセスしてください。

- **アプリケーションへのアクセス削除**：アプリケーションへのアクセスが、アプリケーション・オーナーが指定したX日間停止している場合、アプリケーションへのアクセスは削除されます。この削除に関しては、**30日前**に通知がされます。
- **有効なアカウントの削除**：加入している有効な最後のアプリケーションが停止されると、アプリケーションの停止から**30日後**にMAGアカウントが停止されます。この停止に関しては、**30日前**に通知がされます。アプリケーションへのアクセスを再設定する方法に関しては、[Exostarカスタマーサポート](#)までお問い合わせください

よくあるご質問 (FAQ)

MAGに関するよくある質問をご案内します。

Q：「ワンタイムパスワード」と「システムが作成したパスワード」の違いは何ですか。

A：ワンタイムパスワードは手動で作成され組織管理者 (Org Admin) によって提供されます。このパスワードは初めてログインする際に使用します。ワンタイムパスワードは初回ログイン時にユーザ・アカウントを検証する追加のセキュリティ手段として使用されます。このパスワードは、ワンタイムパスワード・ハードウェアトークンが生成するパスワードとは異なります。

「システムが作成したパスワード」は、ユーザ・アカウントが作成された際にメールで送信されるパスワードです。このパスワードは初回ログイン時に使用します。

注：上記のパスワードはすべて1回のみ使用可能です。

Q：組織の担当者が誰か、どうすれば分かりますか。

A：組織の担当者は複数いる場合があります。詳細は「[組織情報を表示する](#)」セクションを参照ください。

Q：ログイン後に「Administration」タブが表示されないのは何故ですか。

A：MAGにおいて**管理者**として指定されていない場合、「Administration」タブは表示されません。

組織管理者 (Organization Administrator) 又はアプリケーション管理者 (Application Administrator) になるには、現在の組織管理者にお問い合わせください。

Q：証明書をダウンロードするためのパスコードを持っていない場合どうしたらいいですか。

A：[Exostarカスタマーサポート](#)までご連絡ください。

Q：ログインしようとする時無効なアカウントのエラーが表示されます。



A: You will receive the above message when the org admin or Exostar has disabled your account. You will not receive any notification when your account is disabled. Please reach out to your org admin for details.

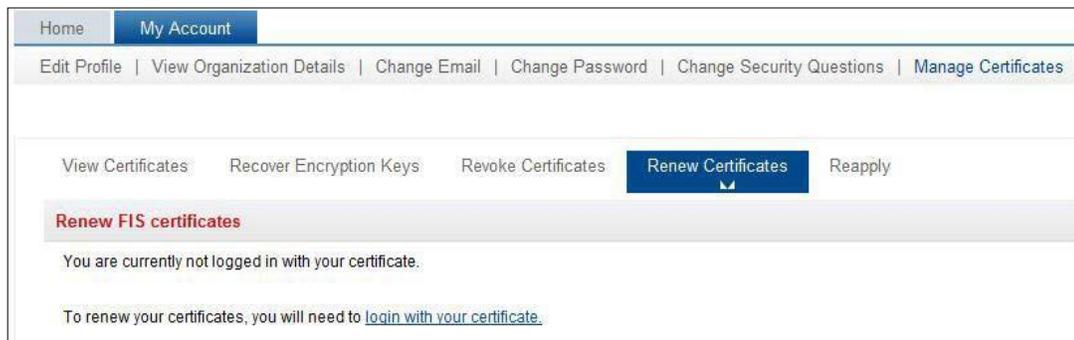
Q: Why do I receive the Invalid Log-in ID or Password error when I try to log-in?



A: You receive this error in two scenarios:

1. **You have entered your log-in credentials incorrectly:** Try again using your correct user name and password. If you forgot your password, follow the instructions provided in the **Forgotten Password** section for details on requesting a new password.
2. **Your account has been deleted:** If your account has been deleted by the org admin of your organization, your log-in credentials have been disabled. Please reach out to your org admin for details. If you need to have a valid account, you will need to complete the **User Registration** process again.

Q: Why do I get the error “You are currently not logged in with your certificates” when I attempt to renew my certificates?



A: This error message is presented when the user is attempting to renew certificates, but is not logged in with the expiring certificates. Click on the link highlighted in blue in the error message, and you will be presented with the certificate selection list (if your IE is set to present the certificates to choose), or the system will automatically pick-up a valid certificate, and complete the log-in process. You should then see the renew button if your certificate is eligible for renewal.

A：組織管理者又はExostarによってアカウントが無効化された場合に上記のメッセージが表示されます。アカウントが無効化された際に通知は送信されません。詳細は組織管理者にお問い合わせください。

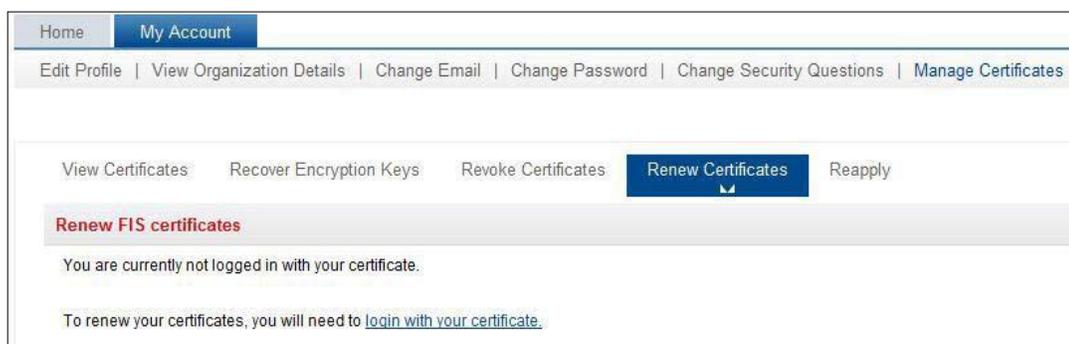
Q：ログインしようとするが無効なログインID又はパスワードのエラーが表示されます。



A：このエラーは以下の2つの状況で表示されます。

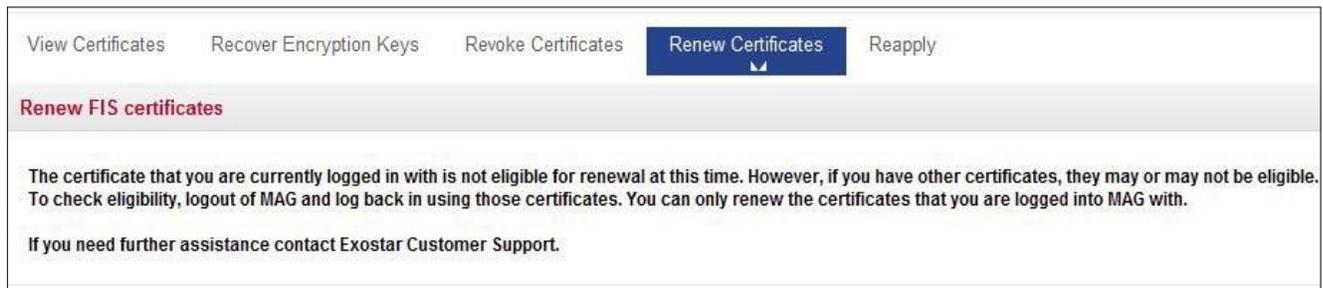
1. **誤ったログイン・クレデンシャルを入力しています**：正しいユーザ名とパスワードを使用して再度ログインしてください。パスワードを忘れてしまった場合、「パスワードを忘れた場合」セクションの手順に沿って新しいパスワードを取得してください。
2. **アカウントが削除されています**：組織管理者によってアカウントが削除された場合、ログイン・クレデンシャルは無効となります。詳細は組織管理者にお問い合わせください。有効なアカウントが必要な場合、**ユーザ登録**を再度行う必要があります。

Q：証明書を更新しようとする「**You are currently not logged in with your certificates**（あなたの証明書で現在ログインしていません）」のエラーが表示されます。



A：このエラーメッセージは、証明書を更新しようとする際に有効期限が切れる証明書でログインしていない場合に表示されます。エラーメッセージ内の青文字で記されたリンクをクリックしてください。証明書の選択リストが表示される(IEの設定が証明書の選択を表示するようになっている場合)か、またはシステムが自動で有効な証明書を選択してログイン・プロセスを完了します。証明書が更新対象である場合は更新ボタンが表示されます。

Q: When attempting to renew my certificates, I get an error message stating that my certificate is not eligible for renewal?



A: This message is presented if your certificate is not eligible for renewal. A certificate can be renewed any time from 90 days prior to the expiration date to the date of expiry.

Q: Why do I get an error message when I attempt to log-in using my certificates, or when I attempt to upgrade my log-in credentials during certificate renewal?



A: Follow the link provided in the error message for detailed information on how to resolve this error.

Q : 証明書を更新しようとする、証明書が更新対象外とのエラーメッセージが表示されます。



A : このメッセージは、証明書が更新対象外の場合に表示されます。証明書は、有効期限の90日前から有効期限日までの期間であれば更新することができます。

Q : 証明書を使用してログインしようとしたり、証明書更新中にログイン・クレデンシャルをアップグレードしようとする、エラーメッセージが表示されます。



A : エラーを解決するための方法をご覧になるには、エラーメッセージ内のリンクにアクセスしてください。