

MI·RA·Is/AZ

DDS 指紋認証環境構築手順

初めに読む資料

初版 2017年12月22日

目次

1. 概要.....	1
2. 制限事項.....	2
3. DDS 社指紋認証環境の構築.....	4
3-1. ハードウェア要件およびシステム要件.....	4
3-2. 指紋認証機能のインストール.....	4
3-3. EVE MA 管理用端末の環境構築.....	5
3-4. EVE MA 管理者用ドメインユーザーの作成.....	5
3-5. EVE MA 初期ユーザー作成と EVE MA 管理者権限付与.....	6
3-6. EVE MA 管理ツールにログオンする.....	9
4. ID Manager の設定.....	13
4-1. 認証セットの追加.....	13
4-2. 共通アプリケーションの設定.....	16
4-2-1. ID Manager アプリケーションを追加する.....	17
4-2-2. 詳細の設定.....	18
4-2-3. 対象アプリケーションを登録する.....	20
4-2-4. ID Manager アプリケーションの設定内容一覧.....	29
4-3. 認証セットの設定.....	34
4-4. ID Manager のリロード.....	36
5. クライアント端末の環境構築.....	37
5-1. クライアント端末のセットアップ.....	37
6. 指紋登録.....	37
6-1. ユーザーの作成.....	37
6-2. 指紋登録.....	37
7. 職員マスター (ComStaff) の設定.....	47
8. 関連設定ファイル.....	48
8-1. MIRAI.xml.....	48
8-2. KartePrint.xml.....	48
8-3. SeatOff.xml.....	49
8-4. OrderCheck.xml.....	49
8-5. MIRAIMSTMNT.xml.....	49

1. 概要

MIRAIs でユーザーID・パスワードの認証画面を有する機能において、DDS 社提供の指紋認証キット「UBF-neo」「UBF-Tri」を用いて認証を行う為の環境構築を目的とする。

2. 制限事項

No	制限事項	補足
1	「Windows Logon Lite」方式でログインを行う。	「仮想スマートカード」を利用した場合の検証は行っておりません。
2	「パスワード変更通知」を利用する。インストール先はドメインコントローラーサーバーとする。	
3	指紋の登録/更新/削除は管理用端末のみ可能とし、クライアント端末は Windows ログオン時の認証機能のみインストールする。	インストール機能 <管理用端末> <ul style="list-style-type: none"> ・ Windows ログオン時の認証機能 ・ EVE MA 管理ツールのインストール <クライアント端末> <ul style="list-style-type: none"> ・ Windows ログオン時の認証機能
4	MIRAIs を使用している全ての端末に「クライアント端末」の設定を行う。	クライアント環境構築には以下手順が必要です。 <ul style="list-style-type: none"> ・ 指紋認証ドライバーのインストール ・ ドメインに参加させる ・ install.ini の設定 ・ インストーラーの実行 ※install.ini は共通の設定となるため端末毎の設定は不要です。
5	EVE MA ユーティリティは使用しない。	環境構築時にインストールを行わない。
6	持ち出し機能は使用しない。	環境構築時にインストールを行わない。
7	Windows 起動時にログイン画面を表示する設定とする。	ログイン時に DDS 社指紋認証画面を表示する為、Windows 起動時にログイン画面を表示する設定とする。。
8	AD アクセス用ユーザーのパスワード変更は行わないこと。	AD アクセス用ユーザーのパスワード変更を行った場合、EVE MA サーバーが AD にアクセスできなくなり、パスワードの再設定、レジストリの再設定などが必要となるため、パスワードの変更は禁止します。
9	AD LDS アクセス用ユーザーのパスワード変更は行わないこと。	AD LDS アクセス用ユーザーのパスワード変更を行うと、EVE MA サーバーが AD LDS インスタンスにアクセスできなくなります。
10	各ドメインユーザーのユーザー名/パスワードの登録/変更を行った場合、変更内容を MIRAIs (職員マスター(ComStaff)) に登録/変更を行う。	Windows ログイン時のユーザー (ドメインユーザー) で MIRAIs ログインユーザーの判断をしています。 登録/変更内容を職員マスターに反映しなかった場合、そのユーザーは MIRAIs へログインを行えません。

No	制限事項	補足
11	職員マスター（ComStaff）へユーザー名を登録する際はすべて大文字に変換した状態で登録を行う。小文字を含めた状態で登録を行った場合、ログインできません。	<p><職員マスターへの登録例></p> <p>AD ユーザー名 : mirai</p> <p>職員マスター登録時 : MIRAI</p> <p>※ドメインユーザーのユーザー名を大文字にする必要はありません。</p> <p>※パスワードは大文字、小文字を判断するため、大文字、小文字の区別をして登録する。</p>
12	パスワードは最大 10 文字までとする。	職員マスター（ComStaff）では 11 文字以上のパスワードが登録可能となりますが、11 文字以上で登録した場合 MIRAIs へのログインは行えません。
13	各ドメインユーザーのユーザー名/パスワードの登録/変更を行った場合、変更内容を EVE MA サーバーに登録/変更を行う。	<p>以下の条件が整っている場合 EVE MA サーバーへの変更内容の更新は不要です。</p> <ul style="list-style-type: none"> ドメインサーバーにパスワード変更通知がインストールされていること。 EVE MA サーバー設定時に maconfig.ini - [Server¥50008_winlogonlite]セクション- [CreateEntry]で「1」を指定していること。 <p>※手順書通り設定を行った場合、上記設定となる為、各ドメインユーザーのユーザー名/パスワードの登録/変更を行った際の EVE MA サーバーへの変更内容の更新作業は不要となります。</p>
14	「認証画面をロックする方法」では「ウィンドウをロック」以外の設定にしないこと。 ※「4-2-3-1.詳細画面の設定」を参照	「ウィンドウをロック」以外の設定にした場合、DDS 社指紋認証画面が正常に起動しません。
15	MIRAIs にログインしているユーザーの変更を行う場合、1 度 Windows をログアウトして、ユーザーを変え再度 Windows のログインを行う。	
16	DDS 社以外の指紋認証機能と DDS 社の指紋認証が混在しないように DDS 社指紋認証以外の機能を無効にする。	MIRAIs[SIMON]PIDSW=0
17	MIRAIs メイン画面の職員パスワードは使用不可とします。	MIRAIsMain[MENU]MENUDISPxx=パスワード変更^0^0
18	パスワード変更督促機能は使用不可とします。	MIRAIsMain[PASSWORDCHECK]SW=OFF

No	制限事項	補足
19	複数病院対応機能が有効の場合の制限事項です。 MIRAIs ログイン時にログイン施設の変更を行う場合、DDS 社指紋認証画面を終了し、手動でユーザーID、パスワードの入力を行う動きとする。	複数病院対応機能は下記設定の場合有効となります。 MIRAIs[複数病院対応]SW=ON

3. DDS 社指紋認証環境の構築

既に DDS 社指紋認証機能がインストール済みの場合、本手順は不要です。

3-1.ハードウェア要件およびシステム要件

インストール前にハードウェア要件およびシステム要件に関して、『[EVE MA はじめにお読みください.pdf](#)』を確認してください。

※『[EVE MA はじめにお読みください.pdf](#)』マニュアルは DDS 社より提供されている媒体に含まれています。

3-2.指紋認証機能のインストール

『[EVE MA インストールマニュアル.pdf](#)』の「3.サーバー構築」に従い環境の構築を行う。

※『[EVE MA インストールマニュアル.pdf](#)』マニュアルは DDS 社より提供されている媒体の「Document」フォルダー直下に含まれています。

下記項目を確認してから環境構築を行ってください。

- ・「Windows Logon Lite」方式でログインを行うため「仮想スマートカード」を利用する場合の手順は不要となります。

- ・「AD アクセス用ユーザー」「AD LDS アクセス用ユーザー」「AD LDS インスタンス名」を下記内容で設定する。

設定名	推奨設定名
ドメインのユーザー	
AD アクセス用ユーザー名	ADAccessUser
AD アクセス用パスワード	Adaccess#pass
AD LDS インスタンス	
AD LDS インスタンス名	MAdb
AD LDS アクセス用ユーザー名	DBAdmin
AD LDS アクセス用パスワード	Db#admin

AD アクセス用ユーザー：EVE MA サーバーやツールが AD のアクセス時に内部的に使用するユーザー

AD LDS アクセス用ユーザー：EVE MA サーバーが AD LDS インスタンスに接続するためのユーザー

- ・AD LDS に設定するプラグインは以下となります。

プラグイン名	説明
d1000.mldf	必須のプラグイン
p50006.mldf	ID Manager を利用する場合に必要なプラグイン
p50008.mldf	Windows Logon Lite を利用する場合に必要なプラグイン
u21.mldf	紋認証時を利用する場合に必要なプラグイン

3-3.EVE MA 管理用端末の環境構築

『[【EVE MA 管理用端末】 - 環境構築手順書.docx](#)』を参照し管理者用の端末を構築する。

3-4.EVE MA 管理者用ドメインユーザーの作成

本手順は管理者用端末で行います。

「Active Directory ユーザーとコンピューター」から、EVE MA 管理者用のドメインユーザーを作成します。

※ドメインの管理者権限のあるユーザーでユーザーの作成を行ってください。

※既存のユーザーを管理者として設定する場合は、この作業は不要です。

設定名	推奨設定名
ドメインのユーザー	
EVE MA 管理者用ユーザー名	maadmin
EVE MA 管理者用パスワード	maadmin

3-5.EVE MA 初期ユーザー作成と EVE MA 管理者権限付与

本手順は EVE MA サーバーで行います。

PC の Administrator 権限のあるユーザーで設定を行います。

EVE MA サーバーで下記コマンドを実行し「3-4.EVE MA 管理者用ドメインユーザーの作成」で作成した EVE MA 管理者用のユーザーを EVE MA へ作成し、EVE MA の管理者権限を与える。

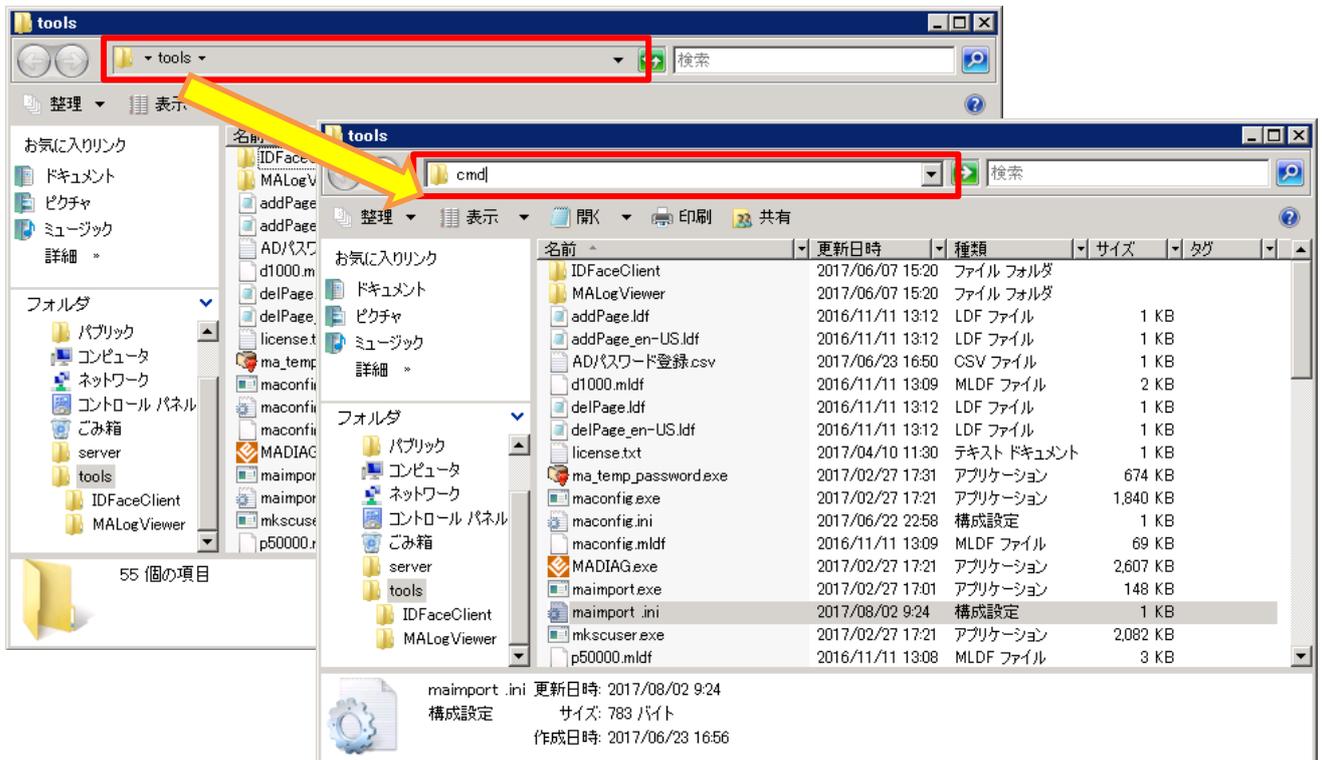
【EVE MA へユーザーを作成するコマンド】

```
maconfig.exe --create-user-entry maadmin@<DNS ドメイン名> --password maadmin
```

【ユーザーへ EVE MA の管理者権限を与えるコマンド】

```
maconfig.exe --enable-administrator maadmin@<DNS ドメイン名>
```

1. EVE MA サーバーにコピーした「tools」フォルダーを開き、アドレスバーに「cmd」と入力して「Enter」キーを押下する。



2. コマンドプロンプトが起動するので下記コマンドを実行する。

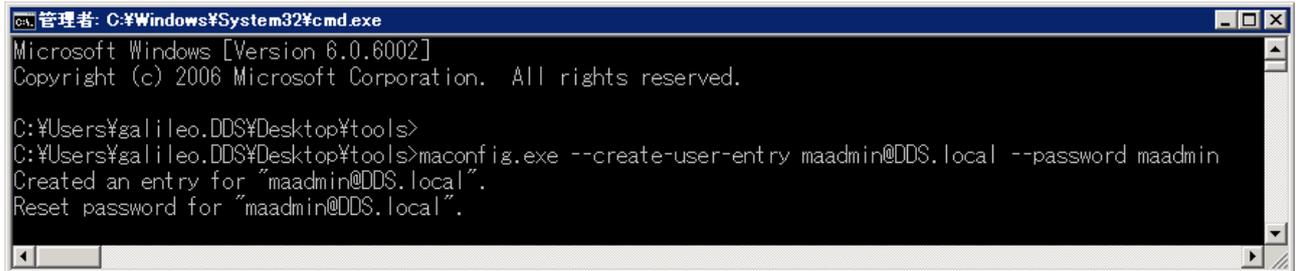
```
maconfig.exe --create-user-entry maadmin@<DNS ドメイン名> --password maadmin
```

実行結果に下記内容が表示されることを確認する。

Created an entry for " maadmin@<DNS ドメイン名>".

Reset password for " maadmin@<DNS ドメイン名>".

※「<DNS ドメイン名>」と「--」の間にスペースを入れる事。スペースを入れない場合正常にコマンドが実行されません。



```

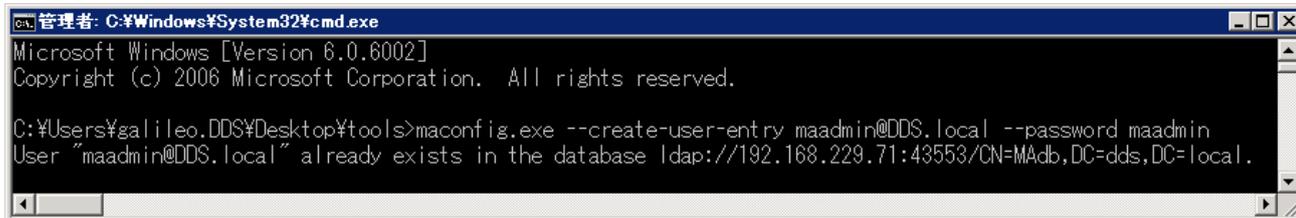
管理 管理者: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\galileo.DDS\Desktop\tools>
C:\Users\galileo.DDS\Desktop\tools>maconfig.exe --create-user-entry maadmin@DDS.local --password maadmin
Created an entry for "maadmin@DDS.local".
Reset password for "maadmin@DDS.local".

```

実行結果に下記内容が表示された場合、以下手順が必要となります。

User "maadmin@<DNS ドメイン名>" already exists in the database ldap:// < AD LDS
サーバー IP アドレス >:< AD LDS インスタンスポート番号 >:< AD LDS インスタンス
識別名 >.



```

管理 管理者: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\galileo.DDS\Desktop\tools>maconfig.exe --create-user-entry maadmin@DDS.local --password maadmin
User "maadmin@DDS.local" already exists in the database ldap://192.168.229.71:43553/CN=MAdb,DC=dds,DC=local.

```

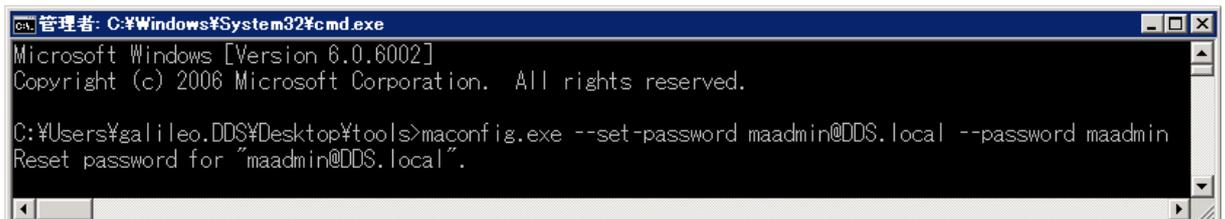
下記コマンドでパスワードの再設定を行う。

※「<DNS ドメイン名>」と「--」の間にスペースを入れる事。スペースを入れない場合正常にコマンドが実行されません。

```
maconfig.exe --set-password maadmin@<DNS ドメイン名> --password maadmin
```

実行結果に下記内容が表示されることを確認する。

Reset password for "maadmin@<DNS ドメイン名>"



```

管理 管理者: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\galileo.DDS\Desktop\tools>maconfig.exe --set-password maadmin@DDS.local --password maadmin
Reset password for "maadmin@DDS.local".

```

3. コマンドプロンプトが起動するので下記コマンドを実行する。

```
maconfig.exe --enable-administrator maadmin@<DNS ドメイン名>
```

実行結果に下記内容が表示されることを確認する。

Enabled administrative privileges to user " maadmin@<DNS ドメイン名>".

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\galileo.DDS\Desktop\tools>maconfig.exe --create-user-entry maadmin@DDS.local --password maadmin
Created an entry for "maadmin@DDS.local".
Reset password for "maadmin@DDS.local".

C:\Users\galileo.DDS\Desktop\tools>maconfig.exe --enable-administrator maadmin@DDS.local
Enabled administrative privileges to user "maadmin@DDS.local".
    
```

4. 「EVE MA Server Service」サービスの再起動を行う。



※ 「コントロール パネル」すべてのコントロール パネル項目管理ツール」にある「サービス」を起動し、「EVE MA Server Service」サービスの再起動を行う

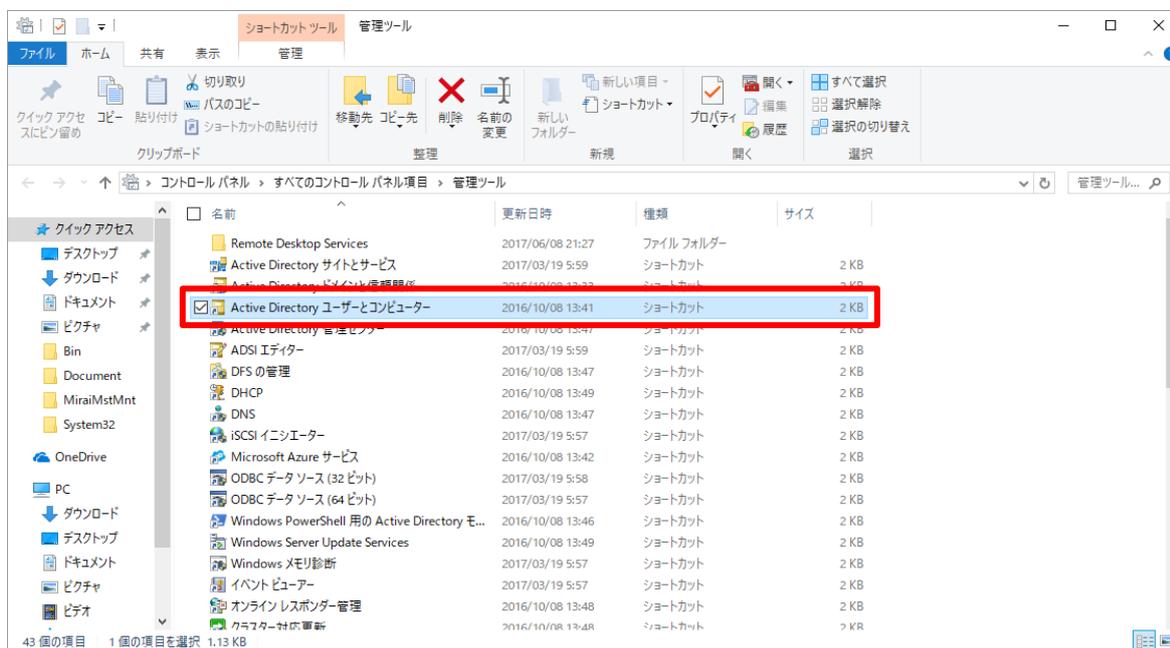
3-6.EVE MA 管理ツールにログオンする

本手順は管理者用端末で行います。

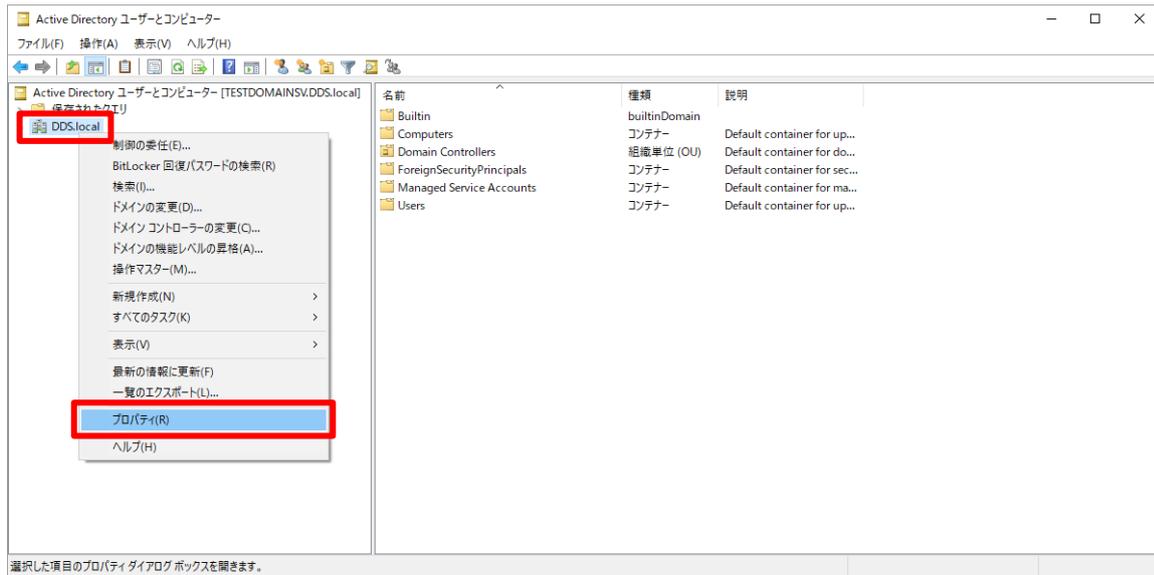
1. 「コントロールパネル」を起動し「管理ツール」を選択する。



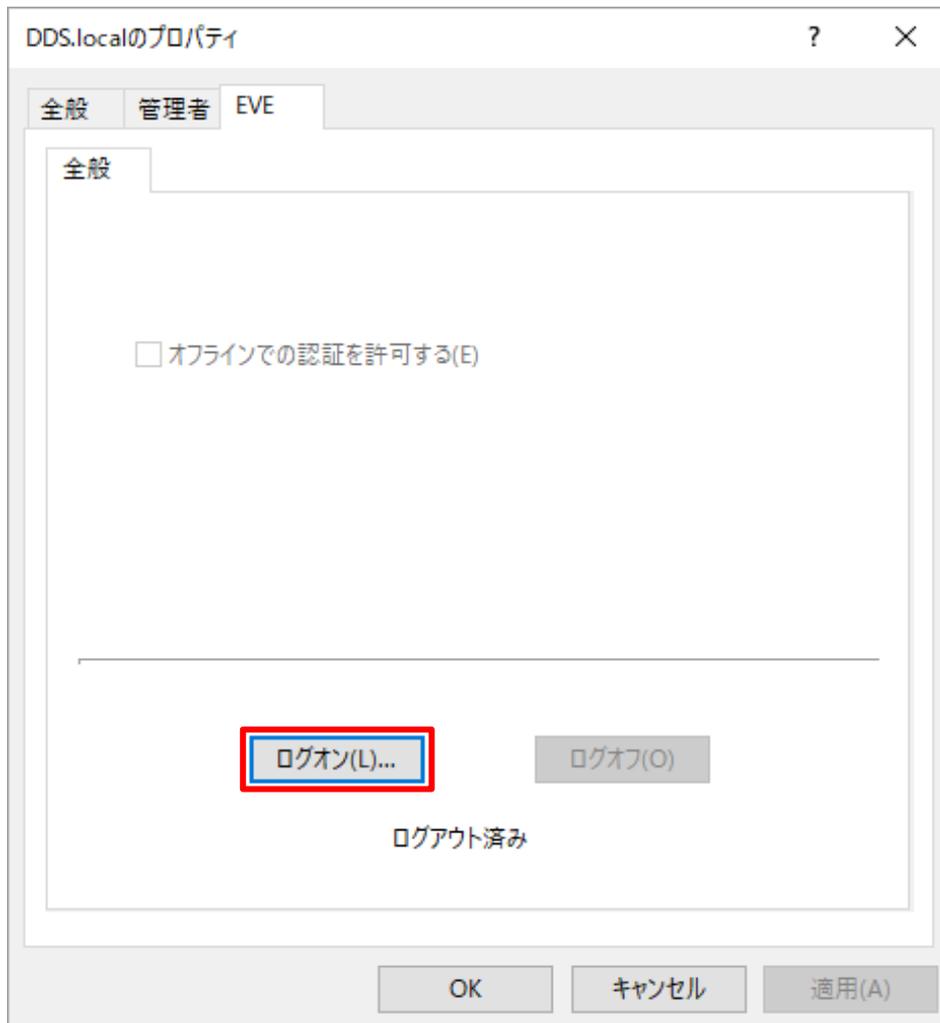
2. 「Active Directory ユーザーとコンピューター」を選択する。



3. ドメインを選択し、右クリックメニューの「プロパティ」を選択する。



4. 「EVE」タブを選択し、「ログオン」ボタンを押下する。



- 「ユーザー名」に「3-4.EVE MA 管理者用ドメインユーザーの作成」で作成したユーザーを指定し、「パスワード」欄にパスワードを入力してログインする。

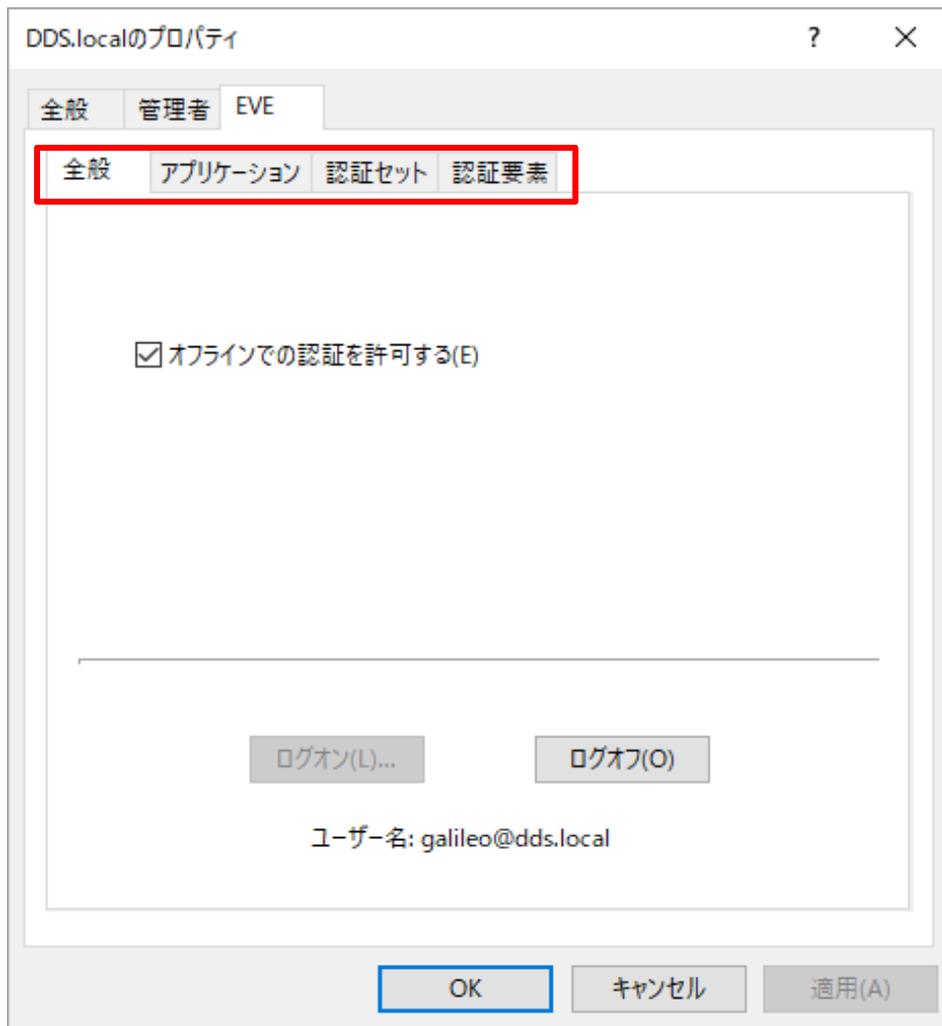


※手順書通り設定を行った場合ユーザー名、パスワードは以下となります。

ユーザー名 : maadmin@<DNS ドメイン名>

パスワード : maadmin

6. 「EVE」 タブに「全般」「アプリケーション」「認証セット」「認証要素」タブが表示されたことを確認する。



4. ID Manager の設定

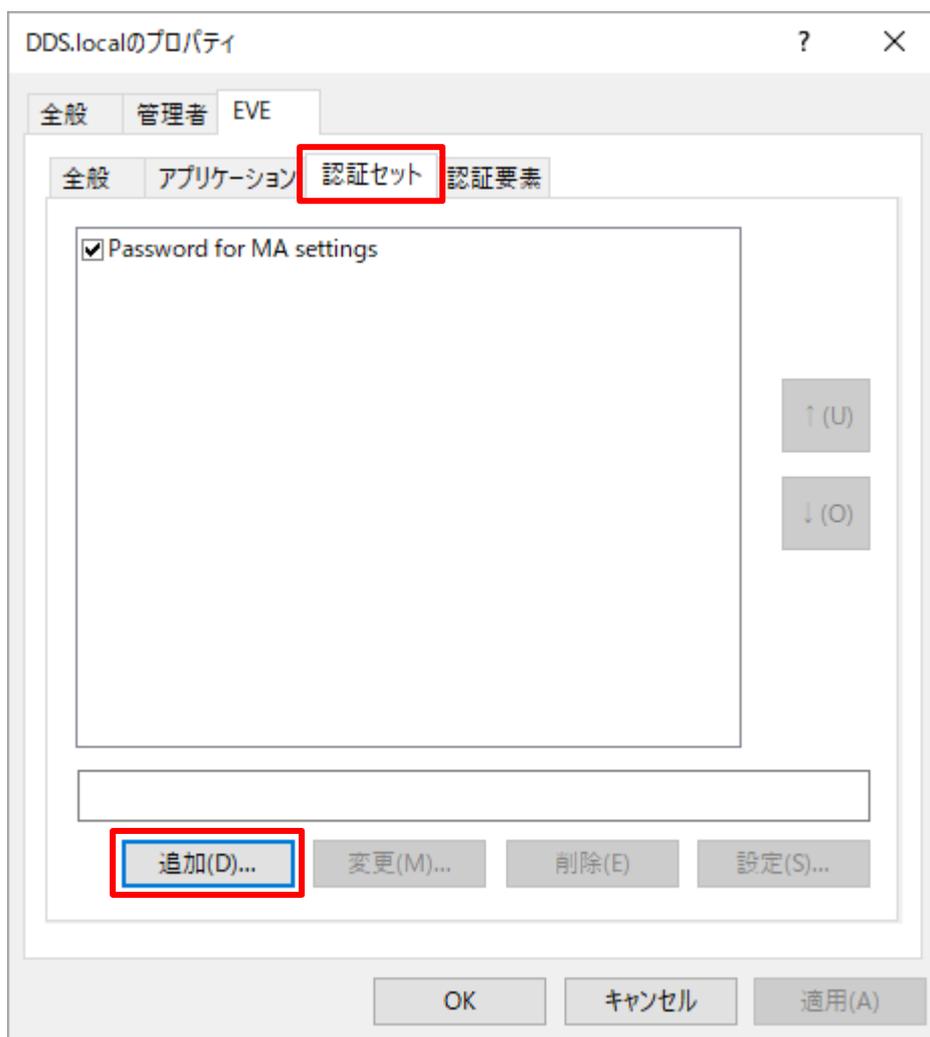
本手順は管理者用端末で行います。

以降の手順は MIRAIs と連携する為の設定となります。

4-1. 認証セットの追加

指紋認証キット「UBF-neo」「UBF-Tri」にて指紋認証を行う際に必要な認証セットを追加する。

1. 管理ツールを起動し「EVE」タブを選択する。
「認証セット」タブを選択し、「追加」ボタンを押す。



2. 認証セット名に「指紋認証」と入力する

認証セットの追加

認証セット名(N):
指紋認証

説明(D):

選択可能な認証要素(V):
Password
Hybrid Fingerprint

必要な認証要素(Q):

追加(A) >
< 削除(R)

↑(U)
↓(O)

オンラインでの認証を許可する(L)
 オフラインでの認証を許可する(E)
 常に表示する(S)
 管理ツール以外でも使用する(H)

OK キャンセル

3. 選択可能な認証要素から「Hybrit Fingerprint」を選択し、「追加」ボタンを押下する。

認証セットの追加

認証セット名(N):
指紋認証

説明(D):

選択可能な認証要素(V):
Password
Hybrid Fingerprint

必要な認証要素(Q):

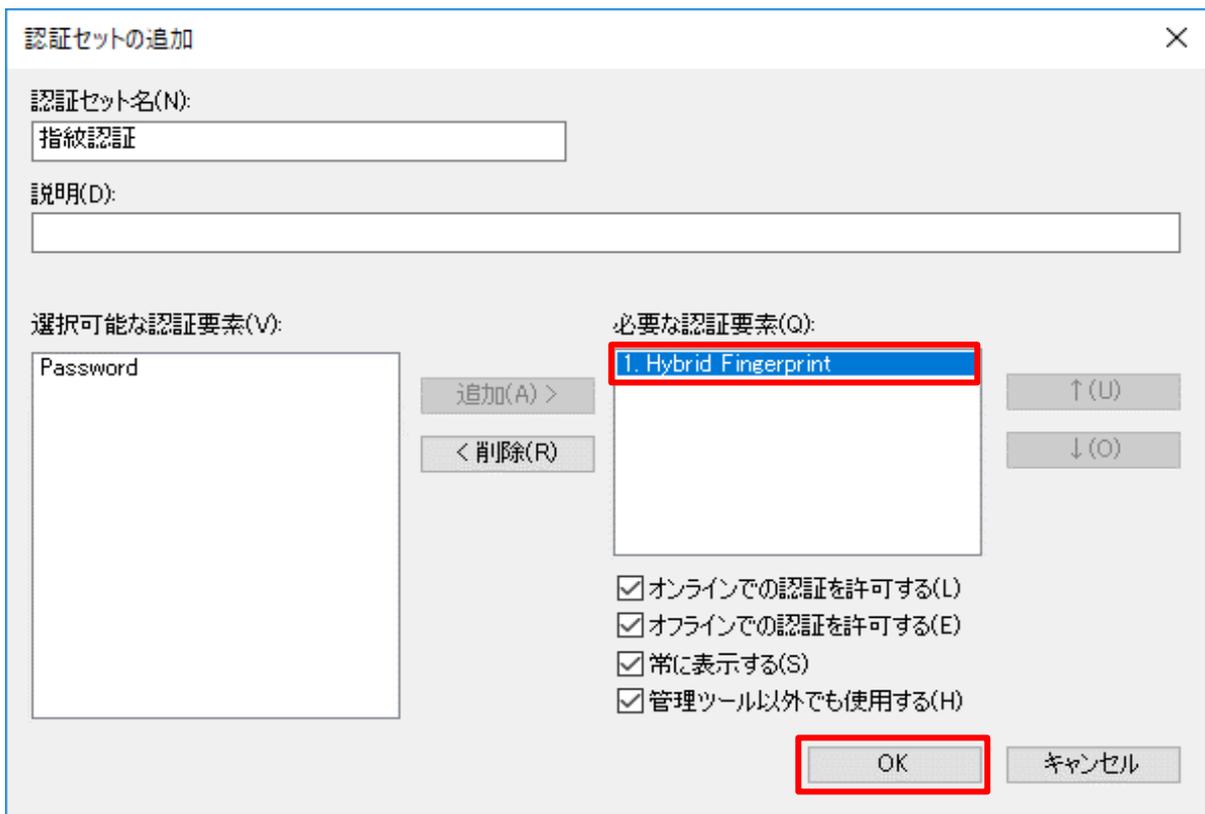
追加(A) >
< 削除(R)

↑(U)
↓(O)

オンラインでの認証を許可する(L)
 オフラインでの認証を許可する(E)
 常に表示する(S)
 管理ツール以外でも使用する(H)

OK キャンセル

4. 必要な認証要素に「Hybrit Fingerprint」が追加されている事を確認して、「OK」ボタンを押下する。



5. 認証セットに「指紋認証」が追加されたことを確認する。



4-2. 共通アプリケーションの設定

共通アプリケーションは、複数のユーザーが共通して利用するアプリケーションです。
EVE MA 管理者で EVE MA 管理ツールから登録を行ってください。

現地の環境に合わせて設定が必要な共通アプリケーションを選択してください。
尚、現場で使用していない機能に関するアプリケーションの追加を行っても他の機能に影響はありません。どのアプリケーションを追加していいかわからない場合は全てのアプリケーションの追加を行ってください。

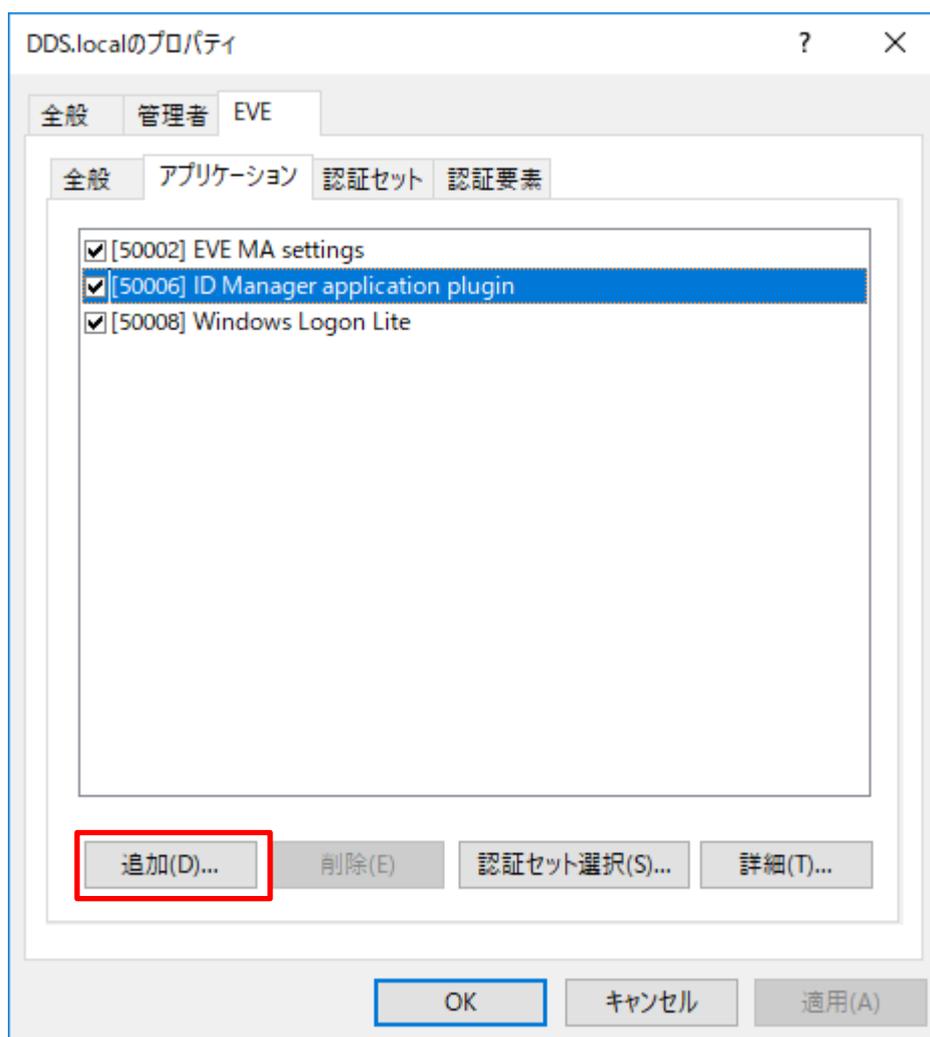
追加対象となる共通アプリケーションは以下となります。

アプリケーション名	必須	説明
MIRAI _s ログイン	必須	MIRAI _s ログイン時に必要となります。
スクリーンセーバー・離席時		MIRAI _s スクリーンセーバー、もしくは、離席機能を使用時に必要
カルテ印刷		カルテ画面からカルテ印刷を起動する際にログイン画面を表示する設定にしている場合必要。 ※以下設定の場合 MIRAI _s [SIMON] PIDSW=0 かつ KartePrint[PermissionCheck] SpoolerKrtMode=2
カルテ印刷・単体起動		カルテ印刷単体起動時にログイン画面を表示する設定にしている場合必要。 ※以下設定の場合 MIRAI _s [SIMON] PIDSW=0 かつ KartePrint[PermissionCheck] SpoolerSingleMode=2
マスターメンテナンス		マスターメンテナンス起動時にログイン画面を表示する設定にしている場合必要。 ※以下設定の場合 MIRAIMSTMNT[STARTMENU] STARTMENUSW=1
オーダー通知		オーダー通知からカルテを起動する際に MIRAI _s のログイン機能を使用しない設定にしている場合必要。 ※以下設定の場合 OrderCheck [MIRAISMAIN] LOGIN=OFF

4-2-1. ID Manager アプリケーションを追加する

※以降の手順「4-2-1.ID Manager アプリケーションを追加する」～「4-2-3.対象アプリケーションを登録する」は「MIRAIs ログイン」の設定手順となります。

1. EVE MA 管理ツールにログオンしてドメインのプロパティを開き、[EVE] - [アプリケーション]を表示します。
2. 「[50006] ID Manager application plugin」を選択して [追加] ボタンをクリックします。



3. [ID Manager アプリケーションの追加] 画面で名称などを設定します。

このダイアログボックスは「ID Manager アプリケーションの追加」を示しています。入力された情報は以下の通りです。

項目	値
アプリケーション ID(I):	61000 (61000 ~ 65999)
アプリケーション名(N):	MIRAI: ログイン
説明(D):	

4-2-2. 詳細の設定

1. 「4-2-1 ID Manager アプリケーションを追加する」で追加したアプリケーションを選択して「詳細」ボタンを押下する。

このダイアログボックスは「DDS.localのプロパティ」の「アプリケーション」タブを示しています。リスト内のアプリケーションは以下の通りです。

アプリケーション名	チェック
[50002] EVE MA settings	<input checked="" type="checkbox"/>
[50006] ID Manager application plugin	<input checked="" type="checkbox"/>
[50008] Windows Logon Lite	<input checked="" type="checkbox"/>
[ID Manager:61000] MIRAI: ログイン	<input checked="" type="checkbox"/>

この画面には「追加(D)...」、「削除(E)」、「認証セット選択(S)...」、「詳細(D)...」のボタンがあります。この中で「詳細(D)...」ボタンが赤い枠で強調されています。

2. 「送出情報の選択、形式」の「ユーザーIDの種類、形式」「パスワードの種類」を下記内容で設定する。

項目	設定内容
ユーザーIDの種類、形式	Windows ログオン時のユーザー名（ユーザー名のみ、ドメイン名は送出不し）
パスワードの種類	Windows ログオン時のパスワード

MIRAIis ログインの詳細 (ID Manager:61000)

アプリケーション名(N):
MIRAIis ログイン

説明(D):

50006-1: アプリケーションの設定
監視対象アプリケーション情報が設定されています
編集(E)... クリア(L)

50006-2: 登録制限
 一般ユーザーによる、ID、パスワードの更新を許可する(U)

50006-3: 送出情報の選択、形式

ユーザー ID の種類、形式(S)
Windows ログオン時のユーザー名 (ユーザー名のみ、ドメイン名は送出不し)

パスワードの種類(P)
Windows ログオン時のパスワード

OK キャンセル

4-2-3. 対象アプリケーションを登録する

アプリケーションの詳細画面で「編集」ボタンをクリックすると、「アプリケーションの登録」画面が表示されます

MIRAI's ログインの詳細 (ID Manager:61000)

アプリケーション名(N):
MIRAI's ログイン

説明(D):

50006-1: アプリケーションの設定
監視対象アプリケーション情報が設定されています
編集(E)... クリア(L)

50006-2: 登録制限
 一般ユーザーによる、ID、パスワードの更新を許可する(U)

50006-3: 送出情報の選択、形式
ユーザー ID の種類、形式(S)
Windows ログオン時のユーザー名 (ユーザー名のみ、ドメイン名は送出しない) ▼
パスワードの種類(P)
Windows ログオン時のパスワード ▼

OK キャンセル

「アプリケーションの登録」画面

4-2-3-1. 詳細画面の設定

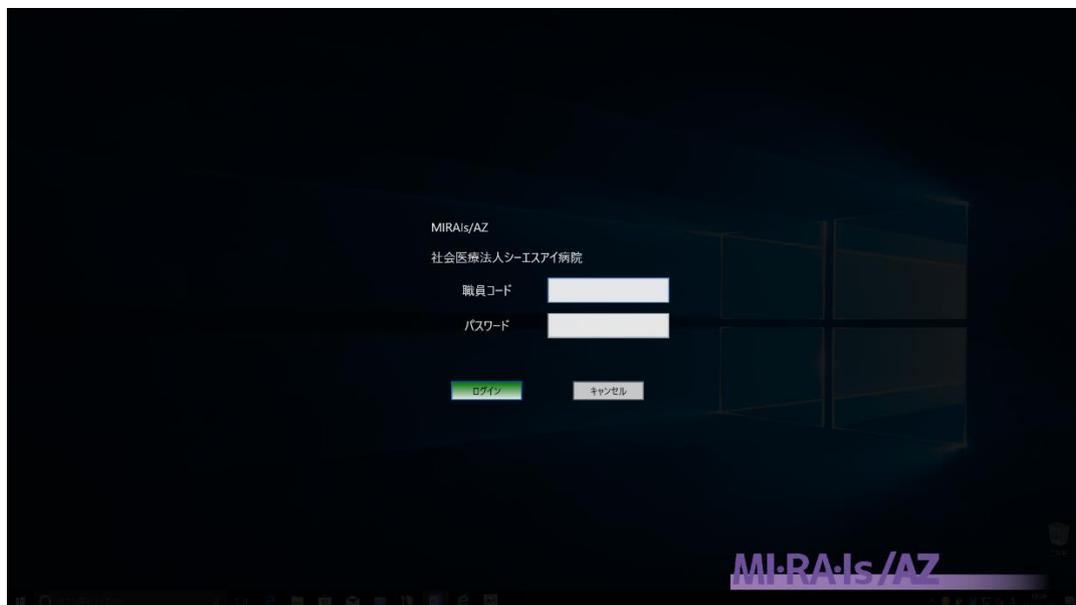
下記項目の設定を行う。

項目	設定内容
認証画面をロックする方法	ウィンドウをロック
ログインした画面は一定期間、検出を行わない	OFF
コントロールの取得に拡張モードを使用する	OFF

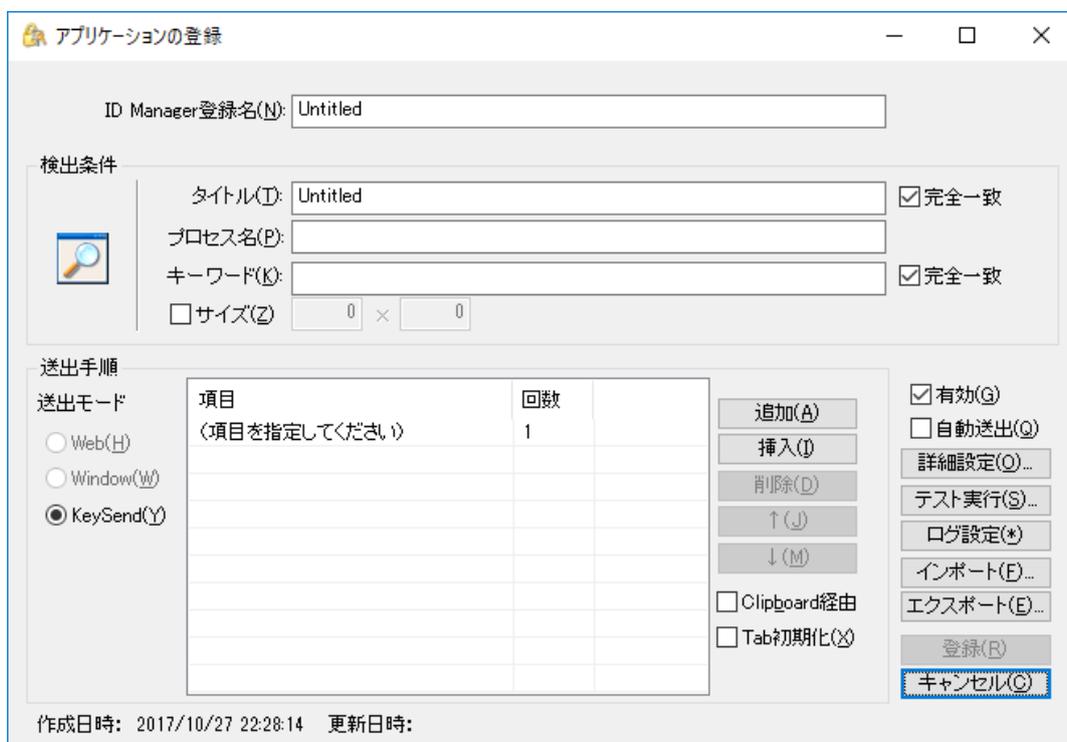
4-2-3-2. 対象アプリケーションを認識する

1. 「対象アプリケーション」と「アプリケーションの登録」を起動する。

「MIRAI_s ログイン画面」

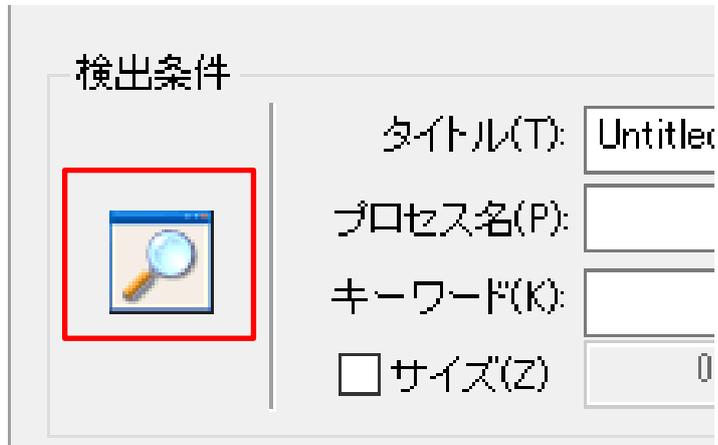


「アプリケーションの登録」

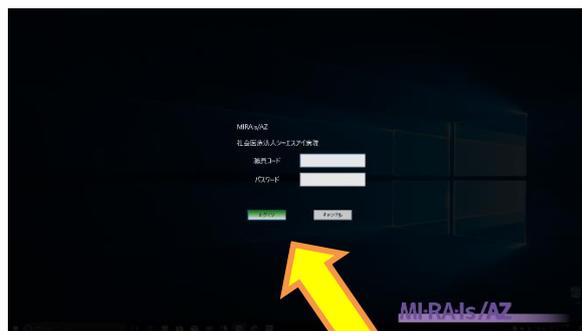


2. 「アプリケーションの登録」画面で虫めがねアイコンを、対象アプリケーションにドラッグ & ドロップします。

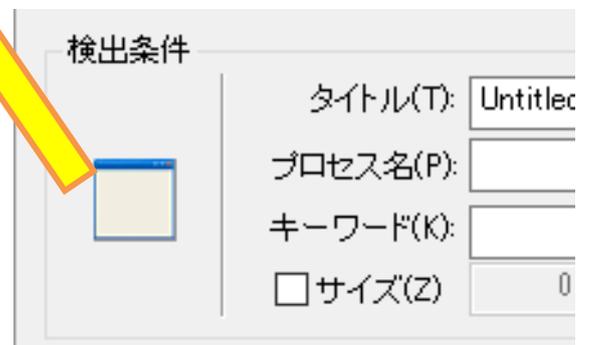
虫めがねアイコン



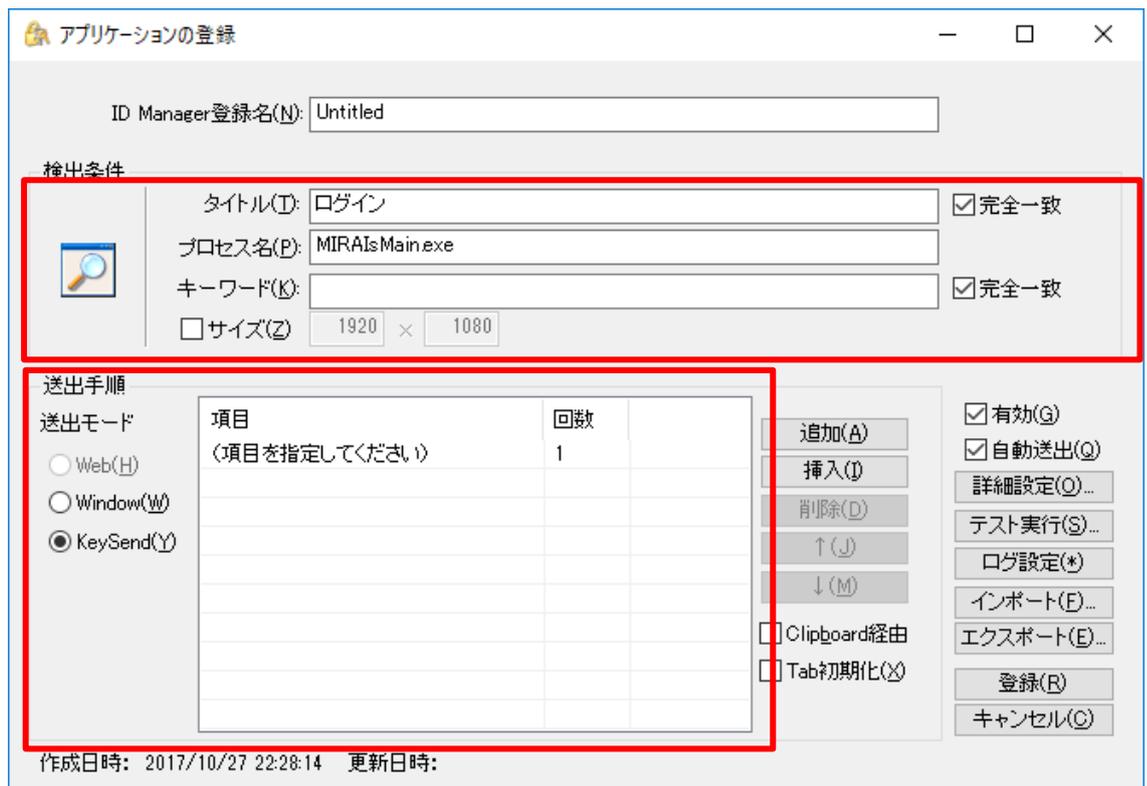
虫めがねアイコンを、対象アプリケーションにドラッグ & ドロップする。
「MIRAIcs ログイン画面」



「アプリケーションの登録」



3. 虫めがねアイコンをドロップすると、自動取得したアプリケーションの情報がアプリケーション登録画面に表示されます。



4-2-3-3. アプリケーションの登録画面の設定

以下表に従い各項目の設定を行う。

<その他>

項目	設定内容
ID Manager 登録名	MIRAIs ログイン
有効	ON
自動検出	ON

アプリケーションの登録

ID Manager登録名(N): MIRAIs ログイン

検出条件

タイトル(T): ログイン 完全一致

プロセス名(P): MIRAIsMain.exe

キーワード(K): 完全一致

サイズ(Z) 1920 x 1080

送出手順

送出モード

Web(H)

Window(W)

KeySend(Y)

項目	回数
(項目を指定してください)	1

Clipboard経由

Tab初期化(X)

有効(G)

自動送出(O)

作成日時: 2017/10/27 22:28:14 更新日時: 2017/10/27 22:29:58

<検出条件>

項目	設定内容
タイトル	ログイン
タイトルの完全一致	ON
プロセス名	MIRAIsmain.exe
キーワード	(未設定)
キーワードの完全一致	OFF
サイズチェックボックス	OFF

アプリケーションの登録

ID Manager登録名(N): MIRAIsmain ログイン

検出条件

タイトル(T): ログイン 完全一致

プロセス名(P): MIRAIsmain.exe

キーワード(K): 完全一致

サイズ(Z) 266 x 129

送出手順

送出手順

送出手順モード

Web(H)

Window(W)

KeySend(Y)

項目	回数
(項目を指定してください)	1

追加(A) 挿入(I) 削除(D) ↑(J) ↓(M)

Clipboard経由 Tab初期化(X)

有効(G) 自動送出(Q)

詳細設定(O)... テスト実行(S)... ログ設定(*)

インポート(F)... エクスポート(E)...

登録(R) キャンセル(C)

作成日時: 2017/08/08 14:44:06 更新日時: 2017/10/27 21:56:12

<送出手順>

項目	設定内容
送出モード	KeySend
送出モードの登録項目	ユーザーID
	Tab キー
	パスワード
	Tab キー
	Enter キー

アプリケーションの登録

ID Manager登録名(N): MIRAIs ログイン

検出条件

タイトル(T): ログイン 完全一致

プロセス名(P): MIRAIsmain.exe

キーワード(K): 完全一致

サイズ(Z) 266 × 129

送出手順

送出モード

Web(H)

Window(W)

KeySend(Y)

項目	回数
ユーザーID	1
Tabキー	1
パスワード	1
Tabキー	1
Enterキー	1
(項目を指定してください)	1

追加(A)

挿入(I)

削除(D)

↑(J)

↓(M)

Clipboard経由

Tab初期化(X)

有効(G)

自動送出(Q)

詳細設定(O)...

テスト実行(S)...

ログ設定(*)

インポート(F)...

エクスポート(E)...

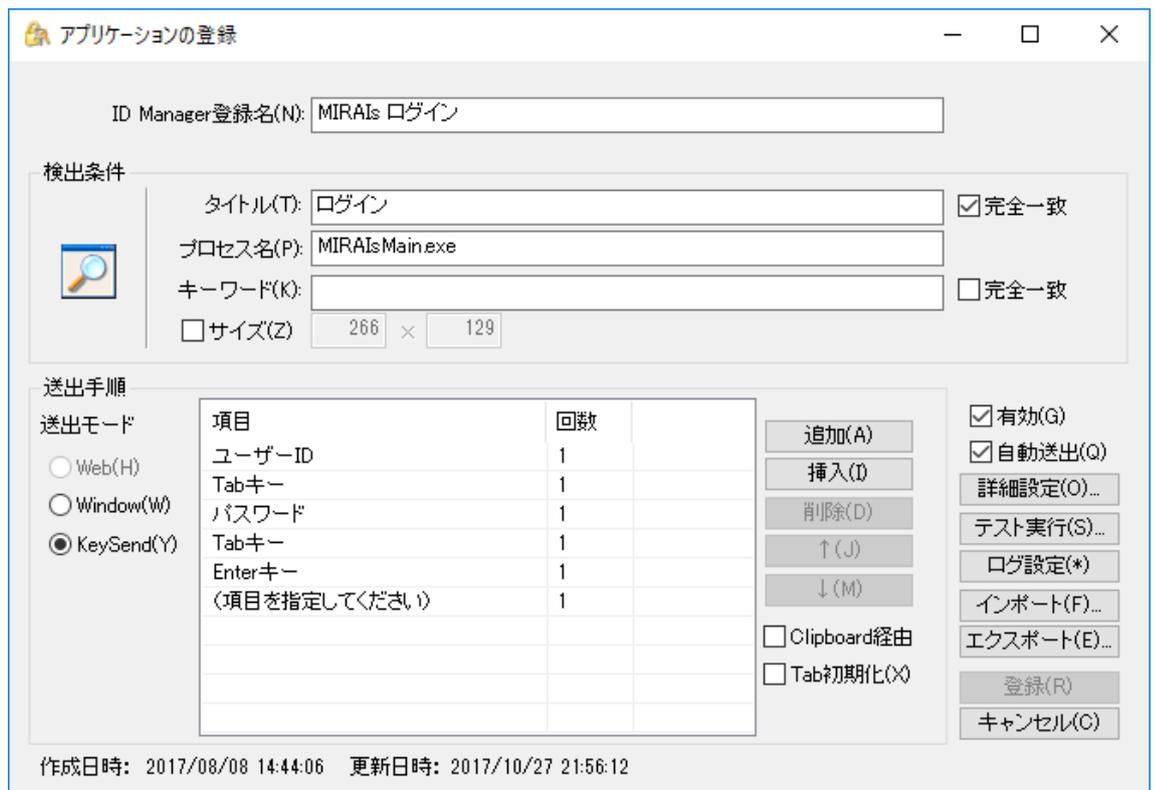
登録(R)

キャンセル(C)

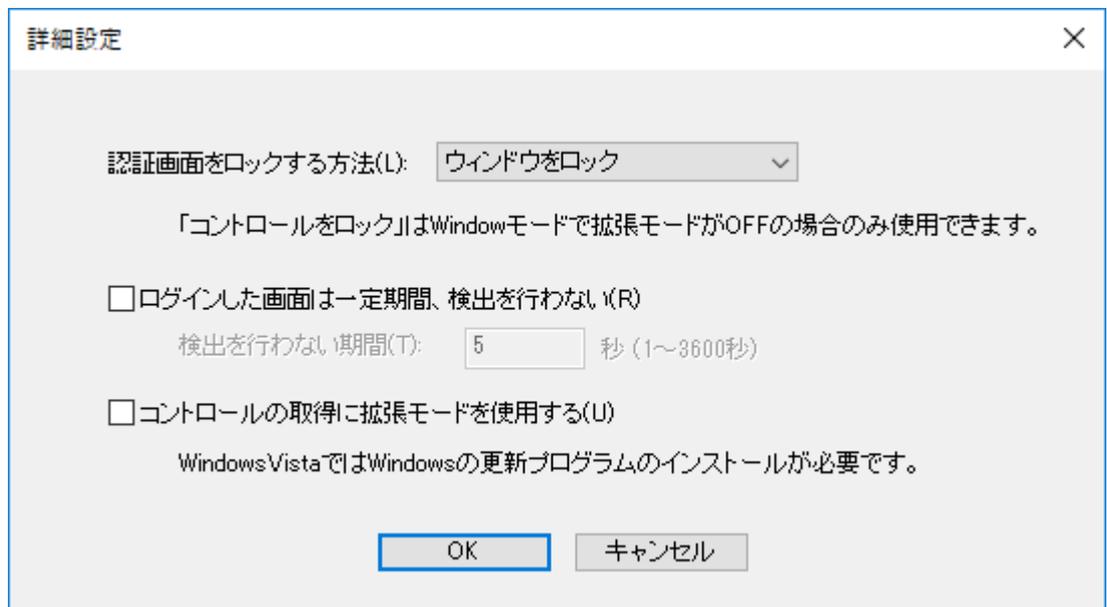
作成日時: 2017/08/08 14:44:06 更新日時: 2017/10/27 21:56:12

設定後の画面イメージ

【アプリケーションの登録画面】



【詳細設定画面】



4-2-4. ID Manager アプリケーションの設定内容一覧

「MIRAI_s ログイン」以外に追加が必要なアプリケーションがあった場合は、「4-2-1.ID Manager アプリケーションを追加する」～「4-2-3.対象アプリケーションを登録する」の手順を参考にしてアプリケーションの追加を行ってください。

また、以下に「全アプリケーション共通項目」とアプリケーション毎の「タイトル」と「プロセス名」を一覧にまとめています。

4-2-4-1. 全アプリケーション共通項目

<詳細画面>

項目	設定内容
ユーザーIDの種類、形式	Windows ログオン時のユーザー名 (ユーザー名のみ、ドメイン名は送付しない)
パスワードの種類	Windows ログオン時のパスワード

<アプリケーション登録画面の設定>

<その他>

項目	設定内容
ID Manager 登録名	該当のアプリケーション名
有効	ON
自動検出	ON

<検出条件>

項目	設定内容
タイトル	「4-2-4-2「タイトル」と「プロセス名」」を参照
タイトルの完全一致	ON ※「マスターメンテナンス」のみ OFF とする。
プロセス名	「4-2-4-2「タイトル」と「プロセス名」」を参照
キーワード	(未設定)
キーワードの完全一致	OFF
サイズチェックボックス	OFF

<送出手順>

項目	設定内容
送出モード	KeySend
送出モードの登録順	ユーザーID
	Tab キー
	パスワード
	Tab キー
	Enter キー

4-2-4-2. 「タイトル」と「プロセス名」

「アプリケーション登録画面の設定/検出条件」の「タイトル」と「プロセス名」はアプリケーション毎に異なる為、以下に設定内容を記載します。

アプリケーション名	タイトル	プロセス名
MIRAIs ログイン	ログイン	MIRAIsMain.exe
スクリーンセーバー・ 離席時	ログイン	MIRAIsLeavesDesk.exe
カルテ印刷	ログイン	Karte.exe
カルテ印刷 - 単体起動	ログイン	MIRAIs.KartePrint.KartePrintMain.exe
マスターメンテナンス	MIRAIs マスターメ ンテナンス	MSACCESS.EXE
オーダー通知	ログイン	OrderCheck.exe

4-2-4-3. アプリケーションの登録画面設定イメージ

【マスターメンテナンス】

アプリケーションの登録

ID Manager登録名(N): マスターメンテナンス

検出条件

タイトル(T): MIRAIs マスターメンテナンス 完全一致

プロセス名(P): MSACCESS.EXE

キーワード(K): 完全一致

サイズ(Z) 1930 × 1054

送出手順

送出モード

Web(H)

Window(W)

KeySend(Y)

項目	回数
ユーザーID	1
Tabキー	1
パスワード	1
Tabキー	1
Enterキー	1
(項目を指定してください)	1

追加(A)

挿入(I)

削除(D)

↑(J)

↓(M)

Clipboard経由

Tab初期化(X)

有効(G)

自動送出(Q)

詳細設定(O)...

テスト実行(S)...

ログ設定(*)

インポート(F)...

エクスポート(E)...

登録(R)

キャンセル(C)

作成日時: 2017/08/08 16:09:43 更新日時: 2017/10/27 22:00:03

※マスターメンテナンスのログイン画面の検出を行うとタイトルに Version [x.x.xxxx] の表示がされます。Version [x.x.xxxx]を削除して、完全一致のチェックボックスを OFF とする。

【スクリーンセーバー・離席時】

アプリケーションの登録

ID Manager登録名(N): スクリーンセーバー・離席時

検出条件

タイトル(T): ログイン 完全一致

プロセス名(P): MIRAIIsLeavesDesk.exe

キーワード(K): 完全一致

サイズ(Z) 1920 × 1080

送出手順

送出モード

Web(H)

Window(W)

KeySend(Y)

項目	回数
ユーザーID	1
Tabキー	1
パスワード	1
Tabキー	1
Enterキー	1
〈項目を指定してください〉	1

追加(A)

挿入(I)

削除(D)

↑(J)

↓(M)

Clipboard経由

Tab初期化(X)

有効(G)

自動送出(Q)

詳細設定(O)...

テスト実行(S)...

ログ設定(*)

インポート(F)...

エクスポート(E)...

登録(R)

キャンセル(C)

作成日時: 2017/10/26 13:47:56 更新日時: 2017/10/27 21:59:02

【カルテ印刷】

アプリケーションの登録

ID Manager登録名(N): カルテ印刷

検出条件

タイトル(T): ログイン 完全一致

プロセス名(P): Karte.exe

キーワード(K): 完全一致

サイズ(Z) 266 × 129

送出手順

送出モード

Web(H)

Window(W)

KeySend(Y)

項目	回数
ユーザーID	1
Tabキー	1
パスワード	1
Tabキー	1
Enterキー	1
〈項目を指定してください〉	1

追加(A)

挿入(I)

削除(D)

↑(J)

↓(M)

Clipboard経由

Tab初期化(X)

有効(G)

自動送出(Q)

詳細設定(O)...

テスト実行(S)...

ログ設定(*)

インポート(F)...

エクスポート(E)...

登録(R)

キャンセル(C)

作成日時: 2017/08/08 15:58:01 更新日時: 2017/10/27 21:57:37

【カルテ印刷 - 単体起動】

アプリケーションの登録

ID Manager登録名(N): カルテ印刷・単体起動

検出条件

タイトル(T): ログイン 完全一致

プロセス名(P): MIRAIIs.KartePrint.KartePrintMain.exe

キーワード(K): 完全一致

サイズ(Z) 266 × 119

送出手順

送出モード

Web(H)

Window(W)

KeySend(Y)

項目	回数
ユーザーID	1
Tabキー	1
パスワード	1
Tabキー	1
Enterキー	1
〈項目を指定してください〉	1

追加(A)

挿入(I)

削除(D)

↑(J)

↓(M)

Clipboard経由

Tab初期化(X)

有効(G)

自動送出(Q)

詳細設定(O)...

テスト実行(S)...

ログ設定(*)

インポート(F)...

エクスポート(E)...

登録(R)

キャンセル(C)

作成日時: 2017/08/08 16:03:48 更新日時: 2017/10/27 21:58:22

【オーダー通知】

アプリケーションの登録

ID Manager登録名(N): オーダー通知

検出条件

タイトル(T): ログイン 完全一致

プロセス名(P): OrderCheck.exe

キーワード(K): 完全一致

サイズ(Z) 0 × 0

送出手順

送出モード

Web(H)

Window(W)

KeySend(Y)

項目	回数
ユーザーID	1
Tabキー	1
パスワード	1
Tabキー	1
Enterキー	1
〈項目を指定してください〉	1

追加(A)

挿入(I)

削除(D)

↑(J)

↓(M)

Clipboard経由

Tab初期化(X)

有効(G)

自動送出(Q)

詳細設定(O)...

テスト実行(S)...

ログ設定(*)

インポート(F)...

エクスポート(E)...

登録(R)

キャンセル(C)

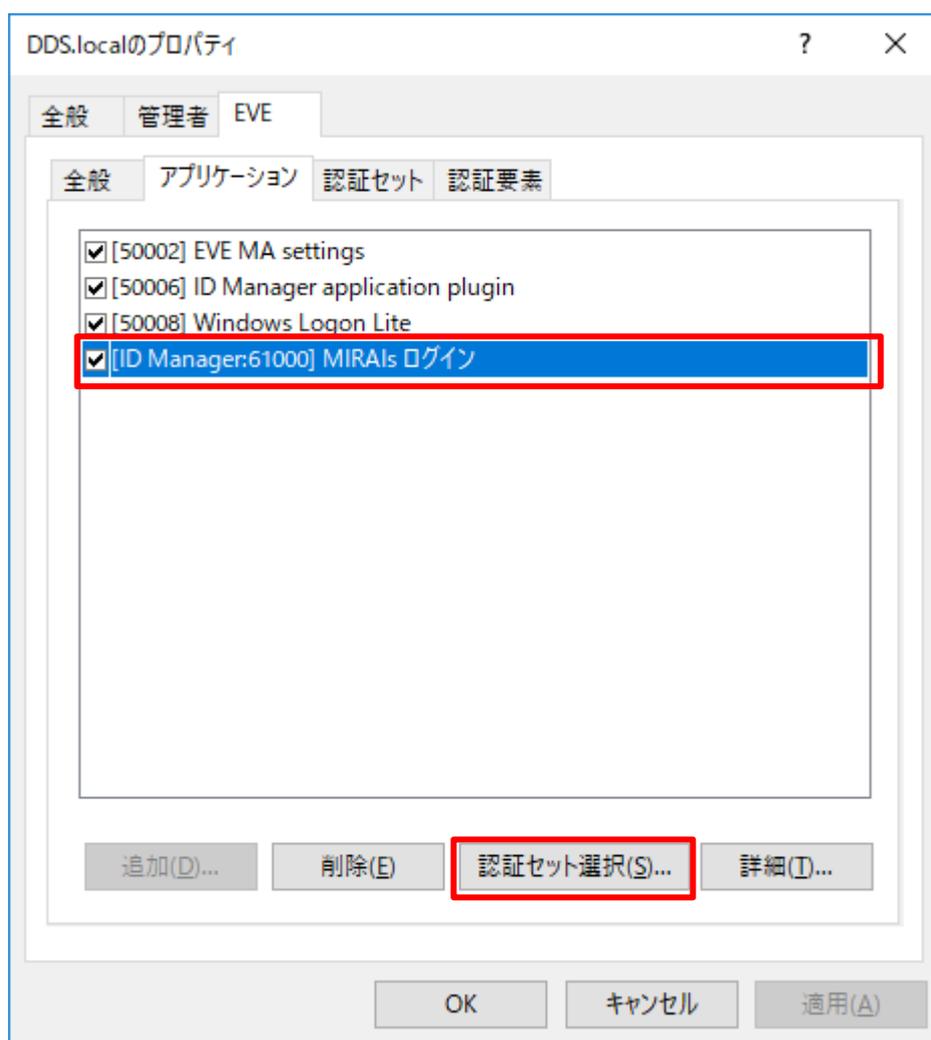
作成日時: 2017/08/08 16:13:49 更新日時: 2017/10/27 21:58:50

4-3. 認証セットの設定

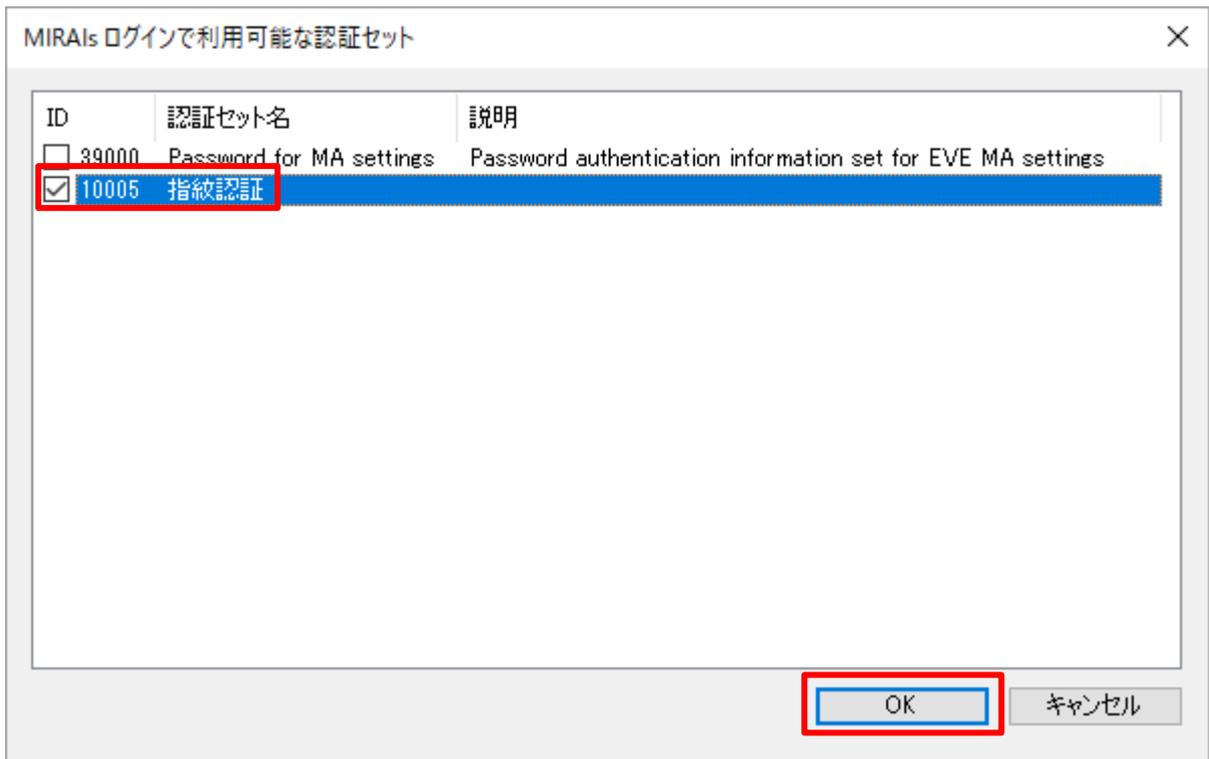
「4-2. 共通アプリケーションの設定」で追加した ID Manager アプリケーションに「4-1. 認証セットの追加」で追加した「指紋認証」の認証セットを設定します。

本手順は「[50008] Windows Logon Lite」と追加した全ての ID Manager アプリケーションに対して行ってください。行わなかった場合認証画面が起動しません。

1. 認証セットを追加する ID Manager アプリケーションを選択し「認証セット選択」ボタンを押下する。



2. 「指紋認証」のチェックボックスにチェックを付け「OK」ボタンを押下する。



4-4.ID Manager のリロード

ID Manager で設定を変更した場合、リロードを行い変更内容を反映させる。

ID Manager アイコン



1.ID Manager のアイコンの右クリックメニューから「リロード」を選択する。



2.リロード中はアイコンが変更します



3.アイコンが元に戻るまで待機します。



5. クライアント端末の環境構築

5-1. クライアント端末のセットアップ

クライアント端末の環境構築は、MIRAIs を使用している全ての端末で必要となります。
環境構築方法は「【クライアント用端末】 - 環境構築手順書.docx」を参照してください。

6. 指紋登録

6-1. ユーザーの作成

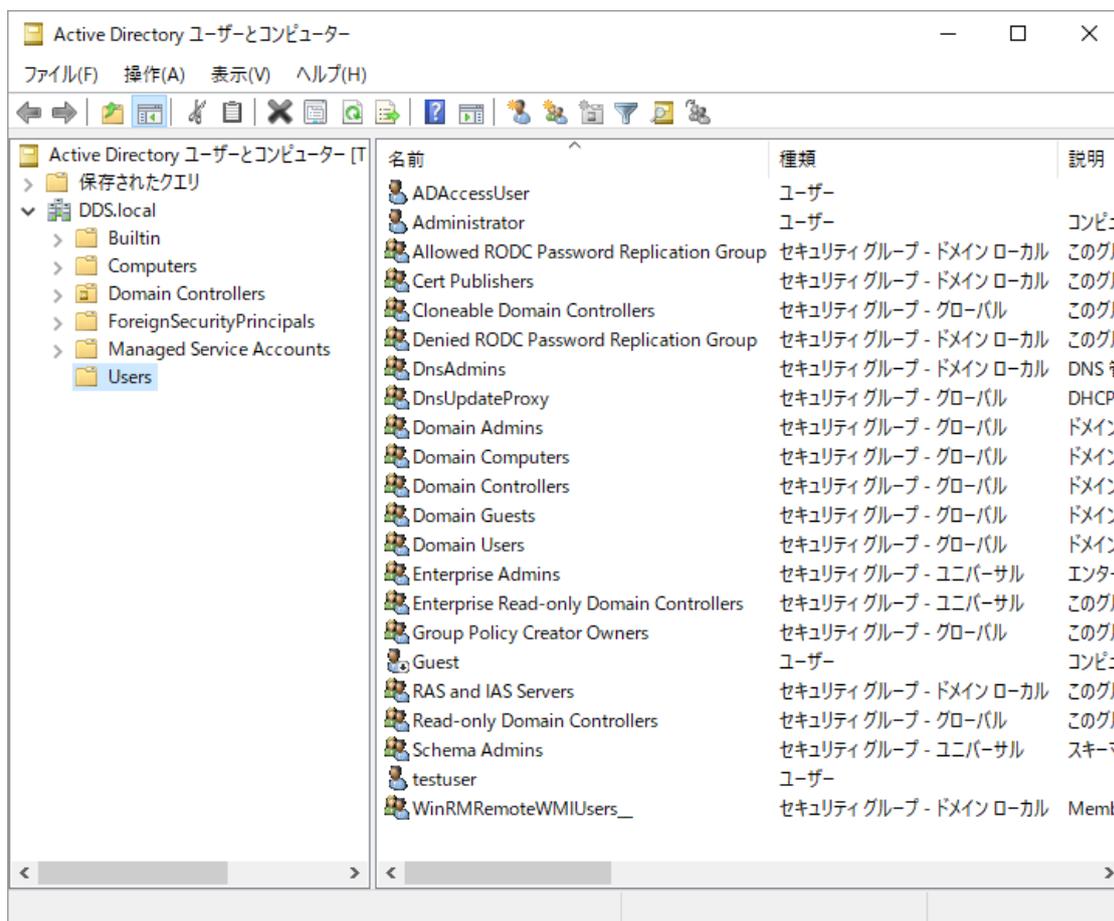
管理用端末で「Active Directory ユーザーとコンピューター」を起動してドメインユーザーの作成を行う。※既存のユーザーに対し指紋登録を行う場合、ユーザーの作成は不要です。

6-2. 指紋登録

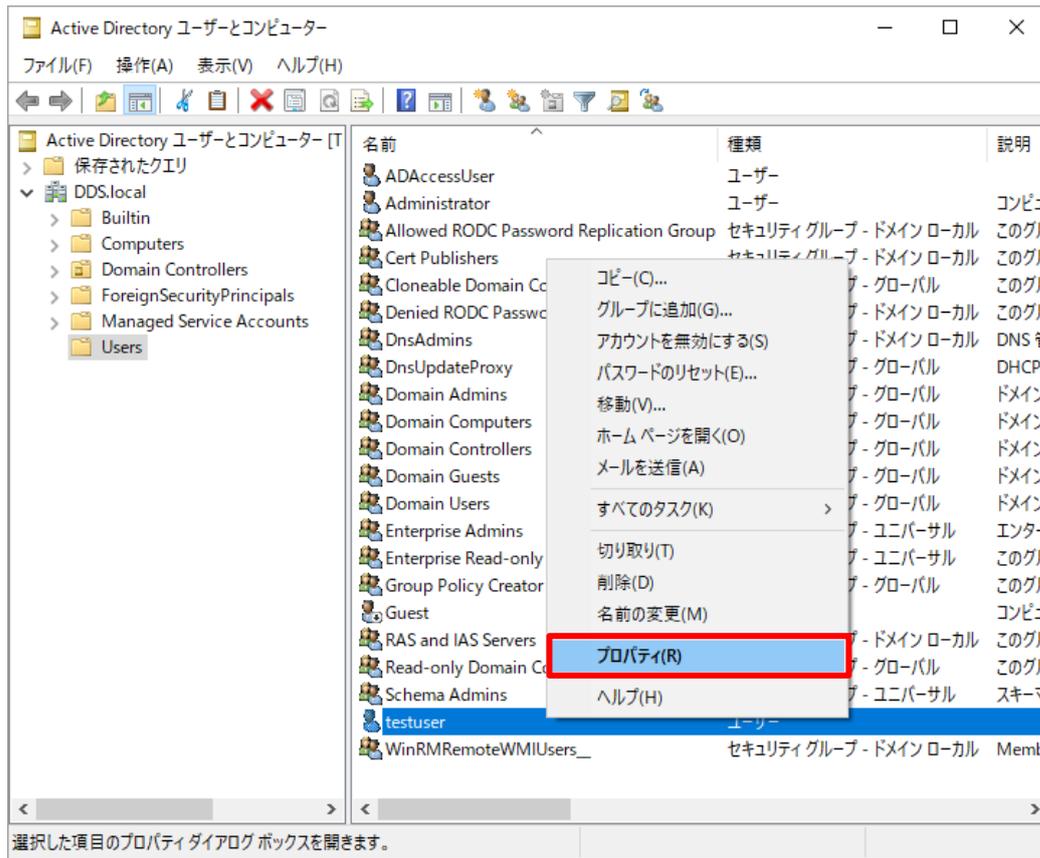
管理者用端末から指紋の認証を行います。

※クライアント端末での指紋の登録は行えないため、管理者用端末から指紋の登録を行います。

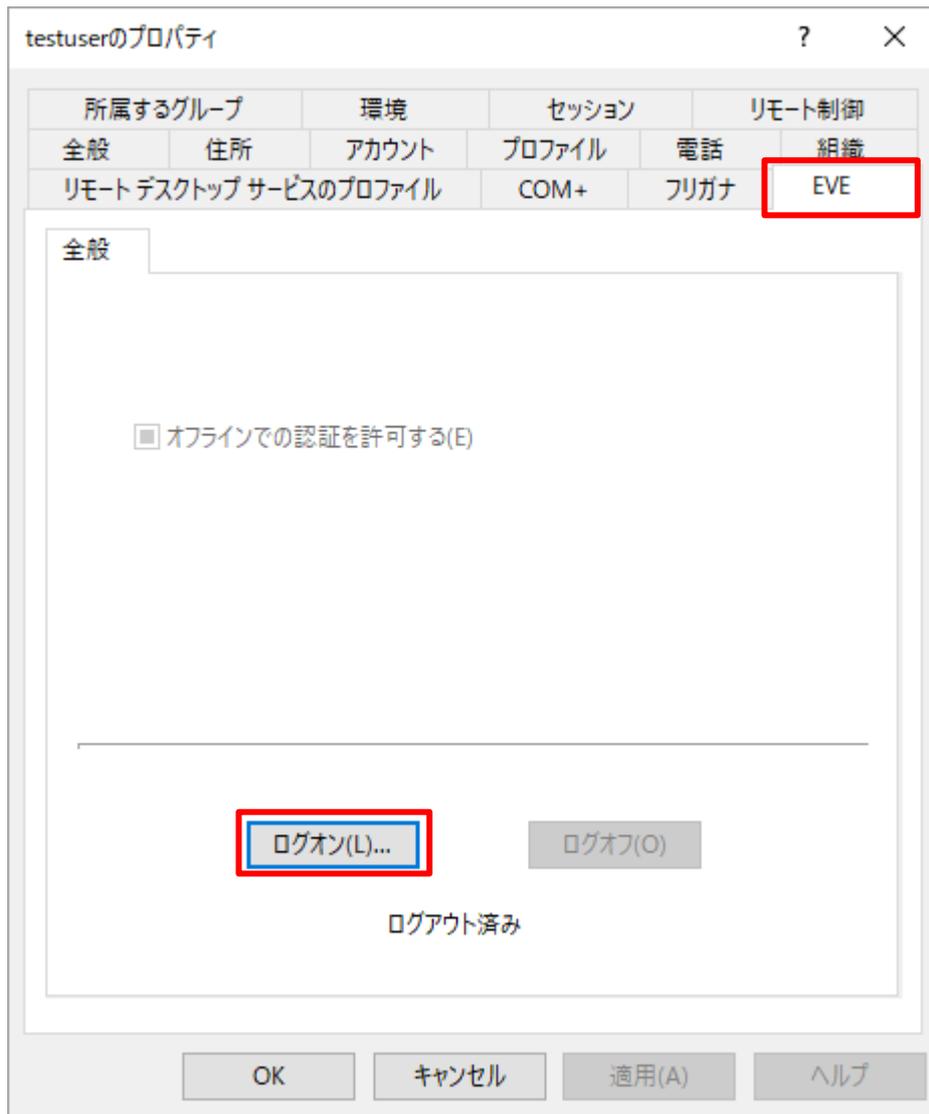
1. 「Active Domain ユーザーとコンピューター」を起動する。



2.指紋登録を行うユーザーを選択し、右クリックメニューからプロパティを開く。



3. 「EVE」タブを選択し、「ログオン」ボタンを押下する。



4. 「ユーザー名」に「3-4. EVE MA 管理者用ドメインユーザーの作成」で作成したユーザーを指定し、「パスワード」欄にパスワードを入力してログインする。

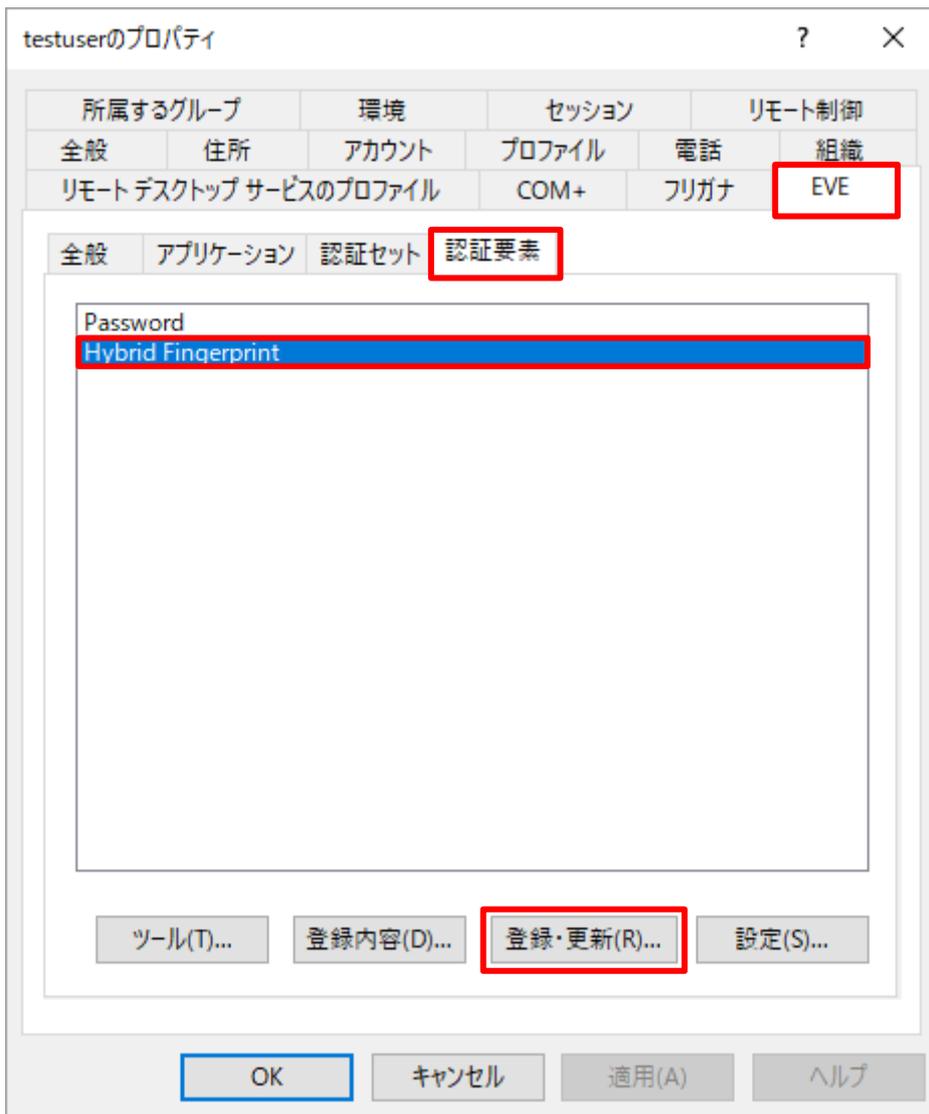


※手順書通り設定を行った場合ユーザー名、パスワードは以下となります。

ユーザー名 : maadmin@<DNS ドメイン名>

パスワード : maadmin

5. 「EVE」タブ→「認証要素」タブ→「Hybrid Fingerprint」の順に選択し「登録・更新」ボタンを押下する。

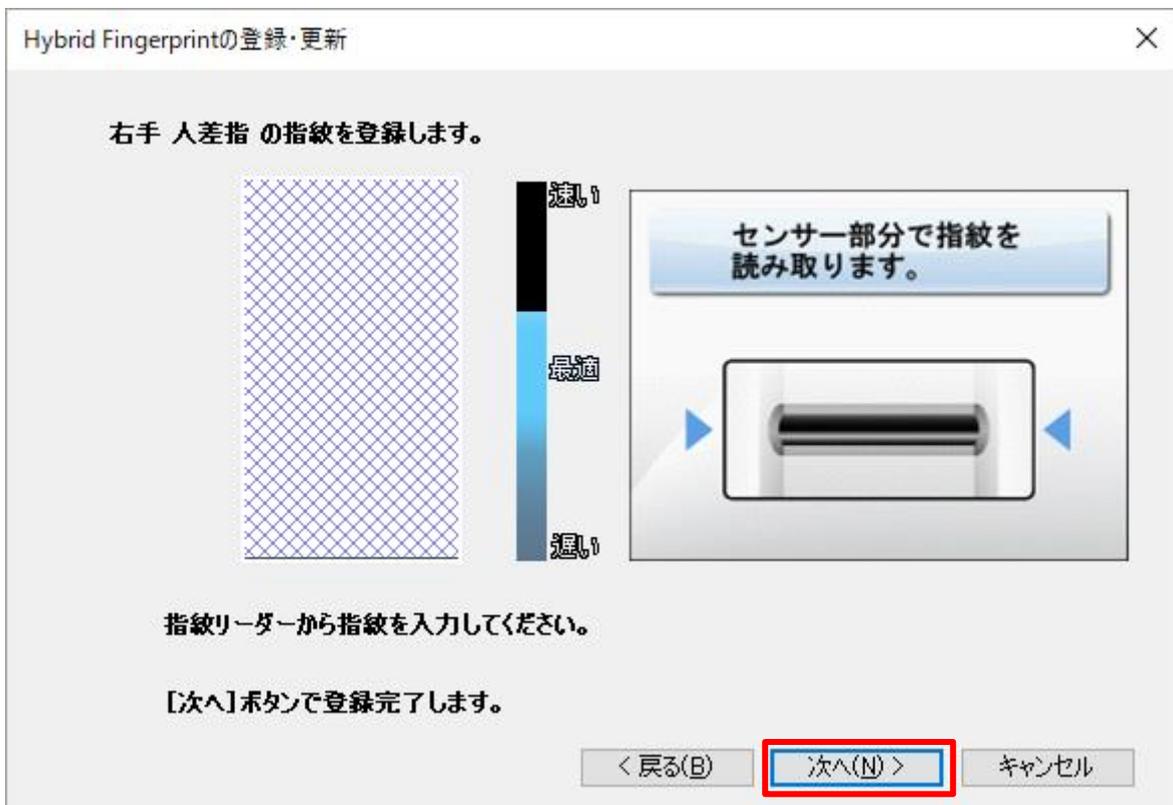


6.指紋を登録する指を選択し、「追加、更新」にチェックを付け「次へ」ボタンを押下する。



7.指紋認証キットで指紋の登録を行い「次へ」ボタンを押下する。

※3回以上認証を行うと「次へ」ボタンが有効になる。



8. 「次へ」 ボタンを押下する。



9. 「キャンセル」 ボタンを押下して画面を閉じる。指紋情報の追加、更新、削除を行う場合は続けて行う。

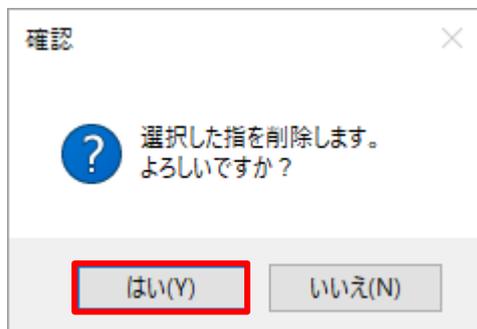


<指紋の削除>

- 1.指紋情報を登録している指を選択し「削除」にチェックを付け「次へ」ボタンを押下する。

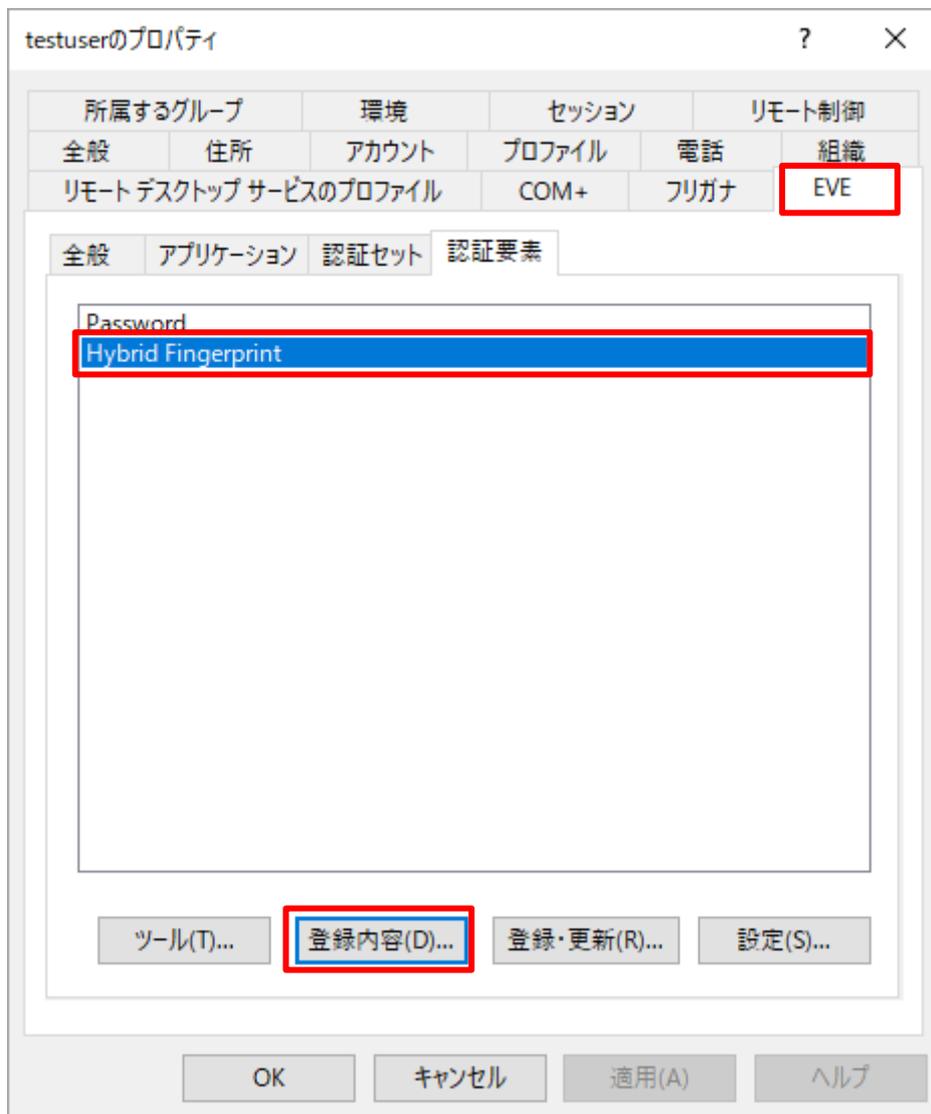


- 2.「はい」ボタンを押下する。



<指紋登録情報の確認>

1. 「EVE」タブ→「認証要素」タブ→「Hybind Fingerprint」の順に選択し「登録内容」ボタンを押下する。



2.指紋登録内容を確認する。



7. 職員マスター（ComStaff）の設定

※本手順は全ての職員に対して行ってください。設定を行わない場合正常にログインが行えません。
職員マスター（ComStaff）の「職員コード」と「パスワード」を「ドメインユーザーのユーザー名、パスワード」と同じ設定にする。

ComStaffの項目	登録する値
職員コード	ドメインユーザーのユーザー名
パスワード	ドメインユーザーのパスワード

※新規職員に対し指紋を登録する場合、職員マスターに新規で職員の追加を行い「職員コード」と「パスワード」を「ドメインユーザーのユーザー名、パスワード」と同じ設定にしてください。

※既存職員に対し指紋を登録する場合、「職員コード」と「パスワード」を「ドメインユーザーのユーザー名、パスワード」と同じ設定にしてください。

職員マスター（ComStaff）

The screenshot shows a registration form with the following fields and annotations:

- 職員コード** (Employee Code): A text input field highlighted with a red box. A callout bubble points to it with the text "ドメインユーザーのユーザー名" (Domain user's username).
- パスワード** (Password): A text input field highlighted with a red box. A callout bubble points to it with the text "ドメインユーザーのパスワード" (Domain user's password).
- Other fields include: 病院コード (Hospital Code), 部署病棟コード (Department/Ward Code), 職種コード (Job Code), カナ氏名 (Kana Name), 漢字氏名 (Kanji Name), 免許コード 1 (License Code 1), 免許日付 1 (License Date 1), 免許コード 2 (License Code 2), and 免許日付 2 (License Date 2).

【補足】

DDS 社指紋認証キットで指紋認証を行った際、EVE MA サーバーに登録している指紋情報を元にドメインサーバーからユーザー名とパスワードを取得し MIRAI^s へログインを行います。
本手順を行わなかった場合、指紋情報と職員情報の紐付けが行えないためログインできません。

8. 関連設定ファイル

8-1.MIRAI.xml

セクション名	エントリー名	エントリーコメント
SIMON	PIDSW	指紋認証ログオンの使用／未使用フラグを設定 0:未使用 1:使用 (NEC) 2:使用 (SecuSearch) 3:使用 (NEC 指ハイブリッド認証)
複数病院対応	SW	複数病院対応の使用有無 ON : 使用する OFF : 使用しない (既定値)

8-2.KartePrint.xml

セクション名	エントリー名	エントリーコメント
PermissionCheck	SpoolerMain Mode	MIRAI.xml からのカルテ印刷起動時に、利用権チェックを行うかを設定 0 : ログイン画面を表示しない。利用権チェックも行わない。 1 : ログインを行った操作者の利用権にて、メニュー・ボタンの使用可否を制御する 2 : MIRAI.xml [SIMON] PIDSW の設定に従って、ID パスワード入力、または指紋認証によるチェックを行う
	SpoolerKrtMode	カルテからのカルテ印刷起動時に、利用権チェックを行うかを設定 0 : ログイン画面を表示しない。利用権チェックも行わない。 1 : ログインを行った操作者の利用権にて、メニューの使用可否を制御する 2 : MIRAI.xml [SIMON] PIDSW の設定に従って、ID パスワード入力、または指紋認証によるチェックを行う
	SpoolerSingleMode	カルテ印刷単独起動時に、利用権チェックを行うかを設定 0 : ログイン画面を表示しない。 利用権チェックも行わない。 1 : ID パスワード入力によるチェックを行う

8-3. SeatOff.xml

セクション名	エントリー名	エントリーコメント
SEATOFF	MENU	MIRAIs メイン、カルテ、クリティカルパスで[離席]起動ボタンを表示するかどうか。 ON : 表示する OFF : 表示しない

8-4. OrderCheck.xml

セクション名	エントリー名	エントリーコメント
MIRAISMAIN	LOGIN	カルテ及び指示受け起動時のログインをオーダー通知で行うか、MIRAIsMain で行うかを設定します。 ON : MIRAIsMain でログインする (オーダー通知の操作者パネル等が非表示になる) ※ログイン後にカルテや指示受けは起動しない。 OFF : オーダー通知でログインする (既定値)

8-5. MIRAIMSTMNT.xml

セクション名	エントリー名	エントリーコメント
STARTMENU	STARTMEN USW	利用権メンテナンス使用の切り替え 0 : 利用権メンテナンスに関係なく、マスタメンテの起動・全てのマスタの利用を可能にする (既定値) 1 : ログイン画面を起動画面とし、マスタメンテ用利用権メンテナンスで設定した職種と利用できるマスタのみ、マスタメンテの起動・マスタの利用を可能にする

DDS 指紋認証環境構築手順

初版 2017年12月22日

 株式会社シーエスアイ

〒003-0029 札幌市白石区平和通15丁目北1番21号
電話：011-861-1500 FAX：011-861-1510