

フローティングライセンス サーバー設定手順書

～ソフトウェア認証編～

第1版

Index

0.はじめに	1
1.動作環境	2
2.Sentinel RTEのインストール方法	3
3.フィンガープリントの作成方法	4
4.ライセンスファイルの適用方法	5
5.Sentinel RTEの設定方法	7
6.Identity Stringの作成方法	9
7.MDiA独自設定の追加方法	12
8.注意点	13
9.Sentinel RTEのアンインストール方法	14
10.トラブルシューティング	15

0.はじめに

- ・ ソフトウェア認証は、Model Dr. MDiA v4.3.0以降の認証方法です。
v4.3.0以降と過去バージョンをフローティングライセンスで併用したい場合は、
問い合わせ窓口までご相談ください。
- ・ 本ドキュメントはライセンスサーバー側の設定のみが記載されています。
クライアント側の設定は「クイックスタートガイド.pdf」に記載されている
<フローティングライセンスの場合>を参照してください。

1.動作環境

- ・フローティングライセンスを使用するためには、
Sentinel RTEをサーバーとなるPCにセットアップする必要があります。
- ・Sentinel RTEは下記Windows環境にインストールできます。
クライアントOSでもサーバーOSでも問題ありませんが、安定稼働の観点ではサーバーOSが望ましいです。
 - ・ Windows 10
 - ・ Windows 11
 - ・ Windows Server 2016
 - ・ Windows Server 2019
 - ・ Windows Server 2022
- ・ソフトウェア認証作業について、
Sentinel RTEを下記のタイミング時に使用します。
 - ①フローティングライセンス初回設定時
 - ②認証サーバーPC変更時
 - ③フローティングライセンス更新時
 - ④MDiA使用PC変更時

各作業タイミングで実施する作業内容が異なりますので、下記表をご確認ください。

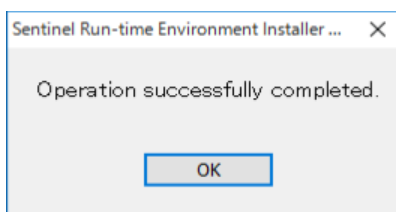
作業内容	フローティング ライセンス初回設定時	認証サーバPC 変更時	フローティング ライセンス更新時	MDiA使用PC 変更時
2.Sentinel RTEのインストール方法	○	○	×	×
3.フィンガープリントの作成方法	○	○	×	×
4.ライセンスファイルの適用方法	○	○	○	×
5.Sentinel RTEの設定方法	○	○	×	×
6.Identity Stringの作成方法	○	○	×	○
7.MDiA独自設定の追加方法	○	○	×	×

2.Sentinel RTEのインストール方法

- ・ 認証サーバーとするインストール先の環境（PC）にて、以下の手順に従ってインストールをお願いします。

①コマンドプロンプトを「管理者として実行」で開きます。

② 弊社提供の「**haspdinst_112987.exe**」を①で開いたコマンドプロンプト上で「**haspdinst_112987.exe -install**」を入力して実行します。
以下のメッセージが出てきたら、セットアップは完了です。



③ブラウザで以下のページにアクセスします。

<http://localhost:1947>

④Sentinel ACCのページが表示されれば、インストールは完了です。



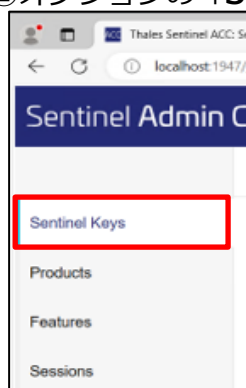
3.フィンガープリントの作成方法

- ・フローティングライセンスファイル作成時のインプットとなるフィンガープリントファイル (拡張子が.c2vのファイル) の作成 及び 送付をお願いします。

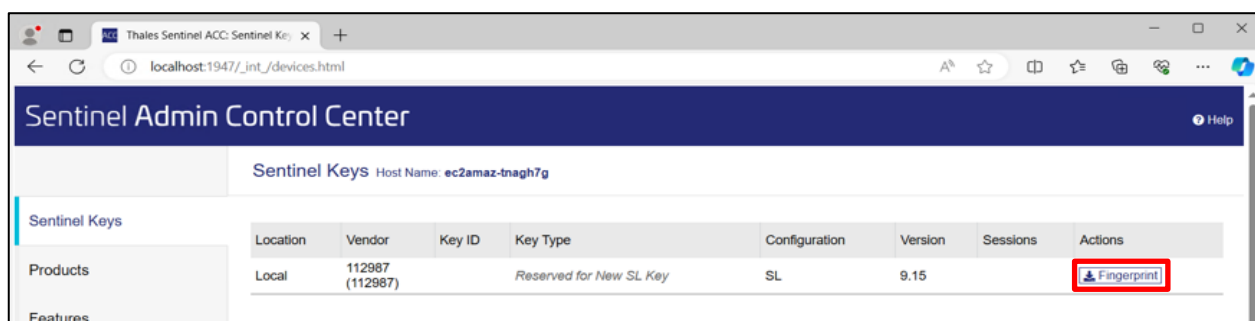
①ブラウザで以下のページにアクセスします。

<http://localhost:1947>

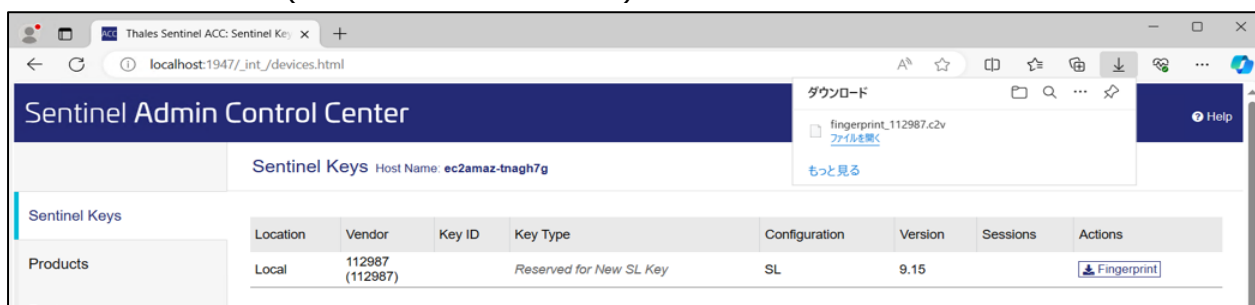
②オプションの「**Sentinel Keys**」をクリックします。



③Vendor=**112987**、Key Type=**Reserved for New SL Key** のキー情報が表示されたら、「Fingerprint」ボタンをクリックします。



④フィンガープリント(拡張子が.c2vのファイル)が作成されるので、任意の場所に保存します。



⑤フィンガープリントを弊社まで送付してください。

以上で、フィンガープリントの作成は完了です。

弊社にて、フィンガープリント受領後、

フローティングライセンスファイル(拡張子が.V2CPのファイル)を作成、送付します。

4.ライセンスファイルの適用方法

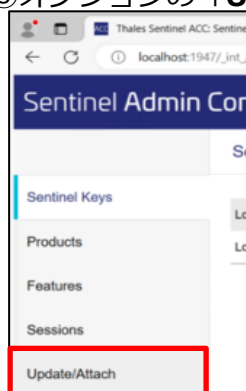
- ・弊社より送付されたフローティングライセンスファイル(拡張子が.V2CPのファイル)を Sentinel RTEにインストールして頂くようお願いします。

①弊社より送付されたフローティングライセンスファイルを取得、解凍します。

②ブラウザで以下のページにアクセスします。

<http://localhost:1947>

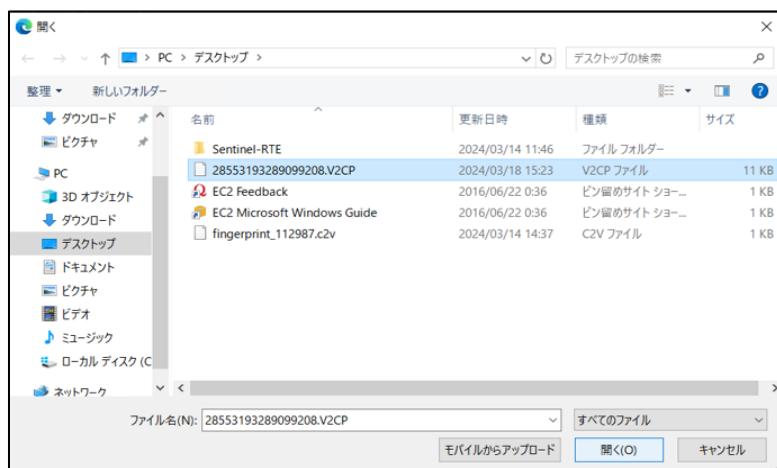
③オプションの「**Update/Attach**」をクリックします。



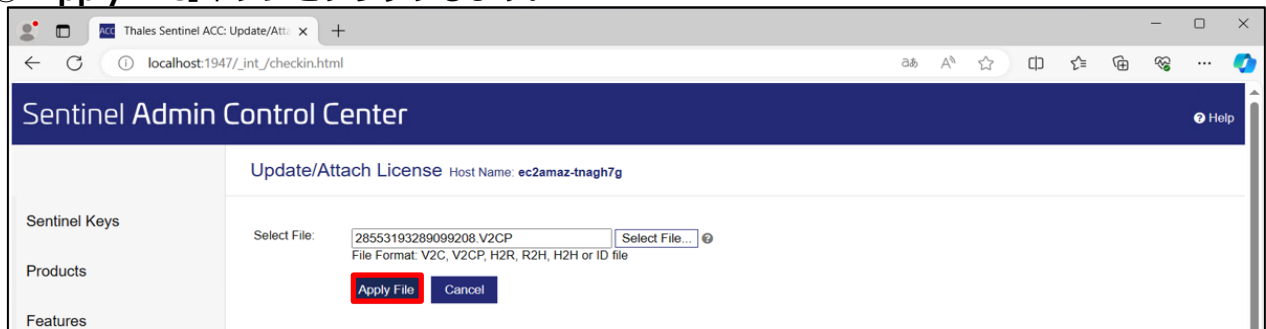
④Update/Attach Licenseのページが開いたら、「**Select File...**」をクリックします。



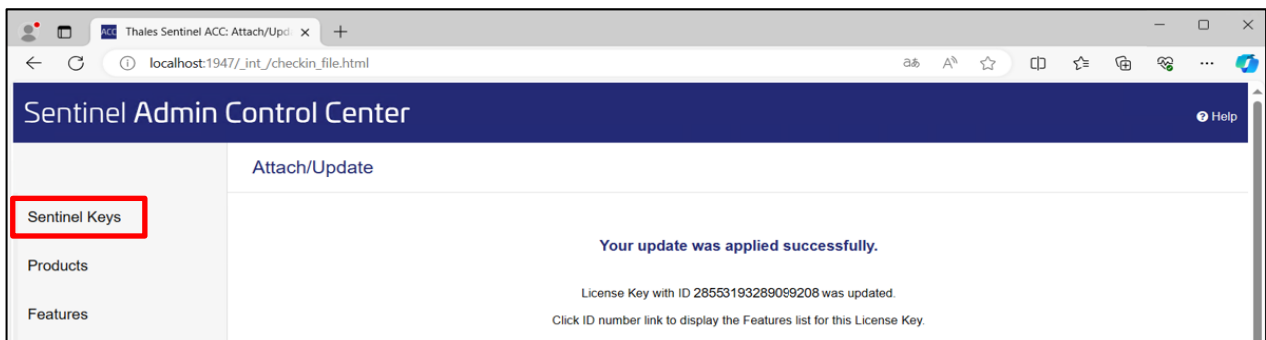
⑤取得したフローティングライセンスファイルを選択して「**開く**」ボタンをクリックします。



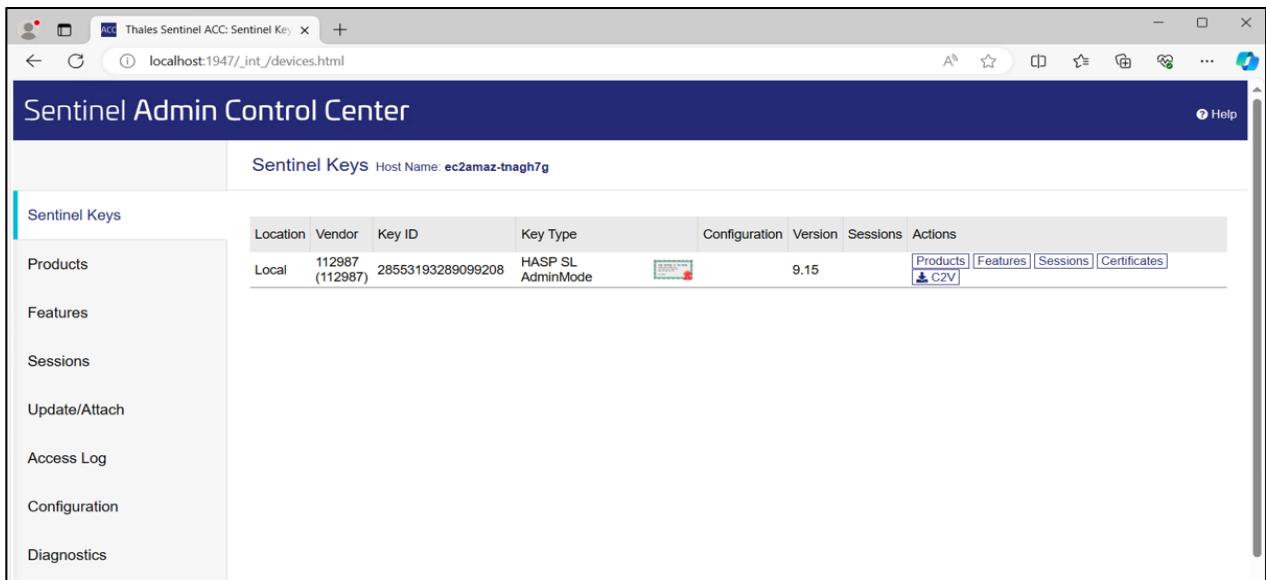
⑥「**Apply File**」ボタンをクリックします。



⑦メッセージ「**Your update was applied successfully**」が表示されたら、オプションの「**Sentinel Keys**」をクリックします。



Key ID=フローティングライセンスファイル名、Key Type=HASP SL AdminModeのキー情報が表示されたら、適用完了です。



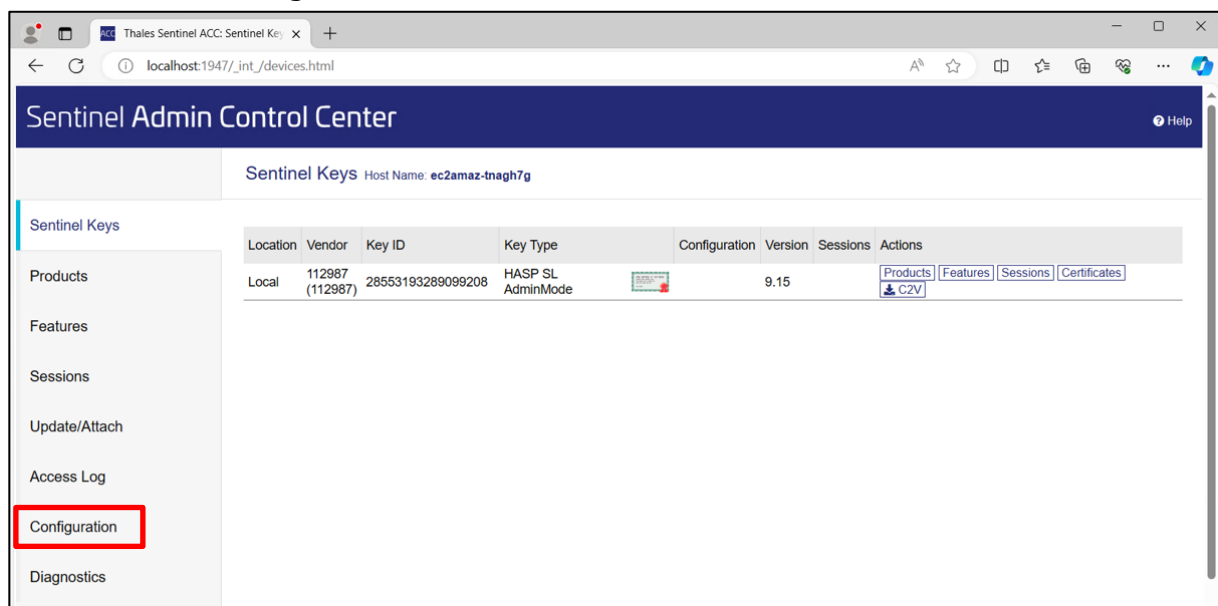
5.Sentinel RTEの設定方法

- ・ライセンスサーバーPCに接続できるようSentinel RTEの設定をお願いします。

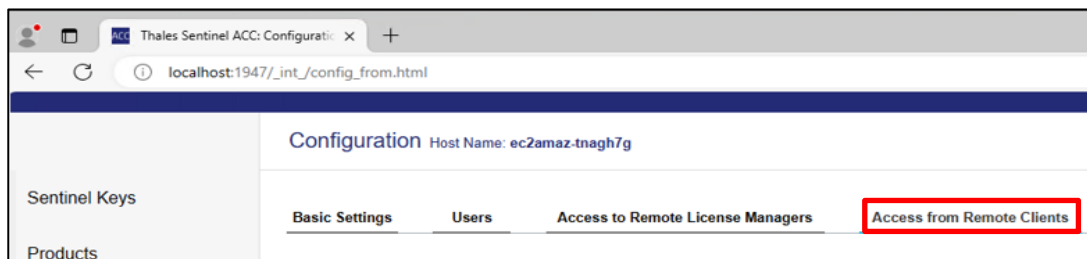
①ブラウザで以下のページにアクセスします。

<http://localhost:1947>

②オプションの「Configuration」をクリックします。



③「Access from Remote Clients」タブをクリックします。



④「Access from Remote Clients」タブ以下の設定を行います。

- ・ **Allow Access from Remote Clients** で
「**Identifiable clients only. Non-cloud licenses cannot be accessed.**」を選択します。
- ・ **Public Address for Access With Identity and ACC** にクライアントから接続可能なサーバーのIPアドレスを入力します。
- ・ **Access Restrictions** に「**allow=all**」を入力します。

The screenshot shows the 'Configuration' page for a host named 'ec2amaz-tnagh7g'. The 'Access from Remote Clients' tab is selected. The settings are as follows:

- Allow Access from Remote Clients:** Three radio buttons are present. The first, 'Identifiable clients only. Non-cloud licenses cannot be accessed.', is selected and highlighted with a red box. The other two are 'No one' and 'Cloud licenses require identity. Other licenses are accessible by all clients.' A red note below states: 'Note: Regardless of the option selected, remote machines using a client identity cannot access non-cloud licenses.'
- Public Address for Access With Identity and ACC:** A text field containing '54.79.9.187' is highlighted with a red box.
- Trusted Client:** An empty text field.
- Public Port for Access With Identity:** A checkbox for 'Listen for clients also on port 80' is unchecked.
- Store Identity Secrets:** Two radio buttons are present. The first, 'Plain text', is selected.
- Access Restrictions:** A text field containing 'allow=all' is highlighted with a red box.

At the bottom left, there is a link 'Show Recent Client Access'. At the bottom right, a note states: 'The entries are evaluated in the order in which they are specified. As soon as a match is found, evaluation stops. allow=all is implicitly added to end of list.'

⑤「Submit」ボタンをクリックしたら完了です。

The screenshot shows the bottom of the configuration page with three buttons: 'Submit', 'Cancel', and 'Set Defaults'. The 'Submit' button is highlighted with a red box.

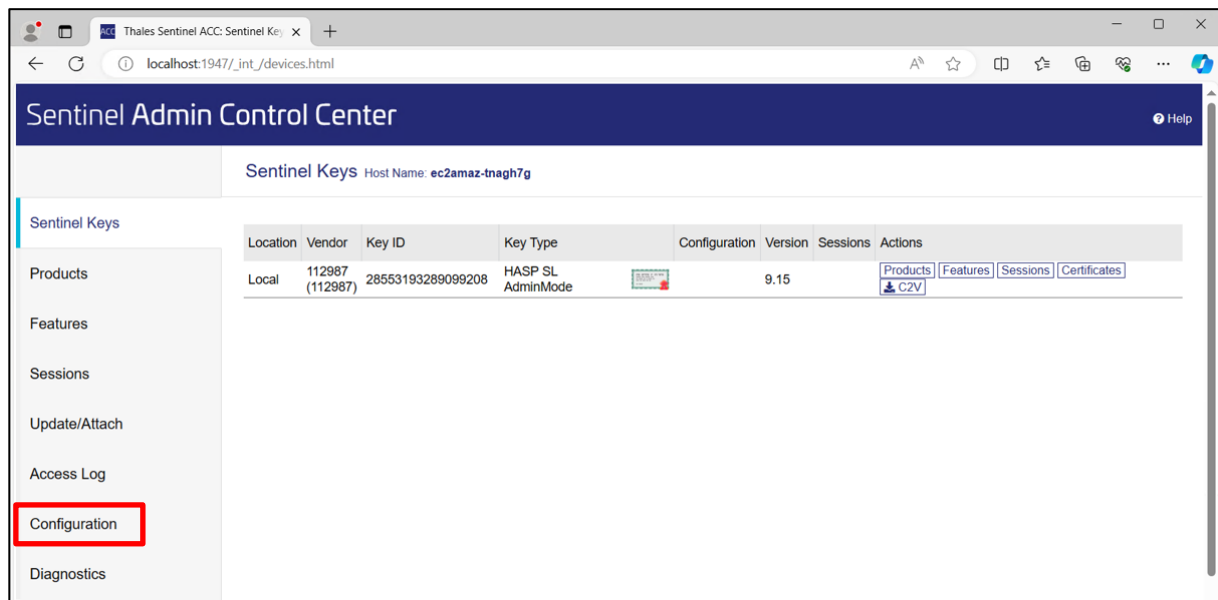
6.Identity Stringの作成方法

- 登録したキー情報を使用して、ライセンス認証用ファイル Identity Stringの作成をお願いします。
※Identity StringはライセンスサーバーPCに接続するためのPC固有の認証用ファイルとなります。
Identity StringはMDiAを使用するPC毎に作成します。
MDiAを10台のPCで使用する場合は、10件が必要です。

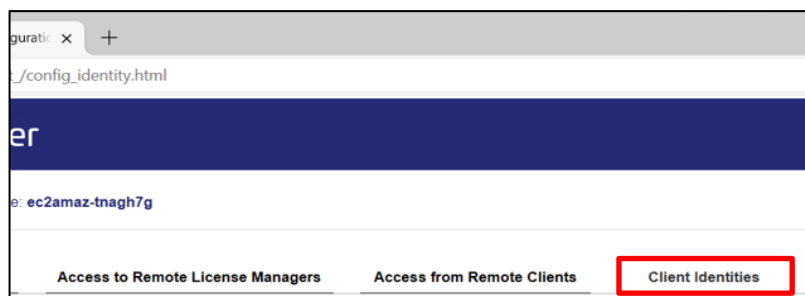
①ブラウザで以下のページにアクセスします。

<http://localhost:1947>

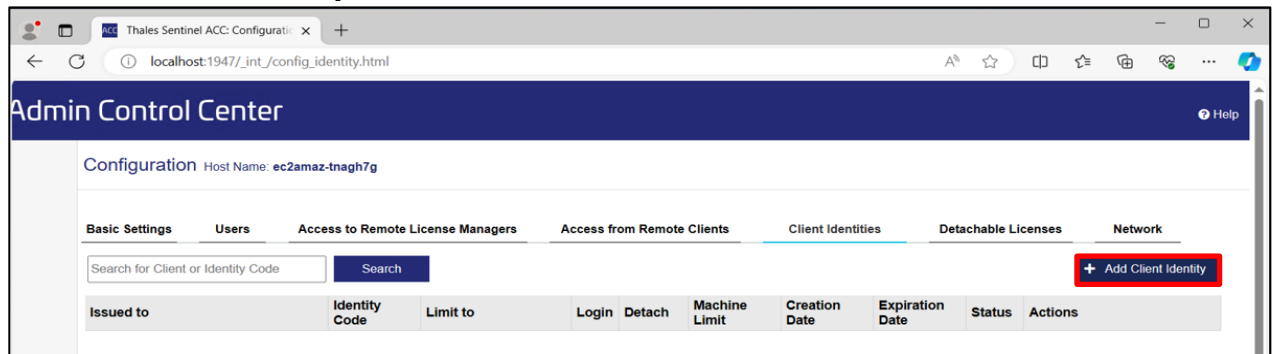
②オプションの「Configuration」をクリックします。



③「Clients Identities」タブをクリックします。



④「Add Clients Identity」ボタンをクリックします。



⑤「Add Clients Identity」の設定を行います。

- **Issued to** にクライアントPC名を入力します。
- **Limit to** に「4.ライセンスファイルの適用方法」で作成した Key ID=フローティングライセンスファイル名を入力します。
- **Maximum Number of Auto-registered Machiens** に1(固定値)を入力します。

The screenshot shows the 'Add Client Identity' form. The 'Issued to' field contains 'Test_PC'. The 'Identity String' field contains 'EMM33XI: oBWAAQCBEJWJFIZHKJrOzJ1qVDJYyYA'. The 'Limit to' field contains '28553193289099208'. The 'Maximum Number of Auto-registered Machines' dropdown is set to '1'. The 'Expiration Date' field is empty, and the 'Never Expires' checkbox is checked. Red boxes highlight the 'Test_PC' field, the 'Limit to' field, and the 'Maximum Number of Auto-registered Machines' dropdown.

⑥「Copy Identity String」ボタンをクリックします。

The screenshot shows the 'Add Client Identity' form with the same data as the previous one. A red box highlights the 'Copy Identity String' button, which is located next to the 'Identity String' field.

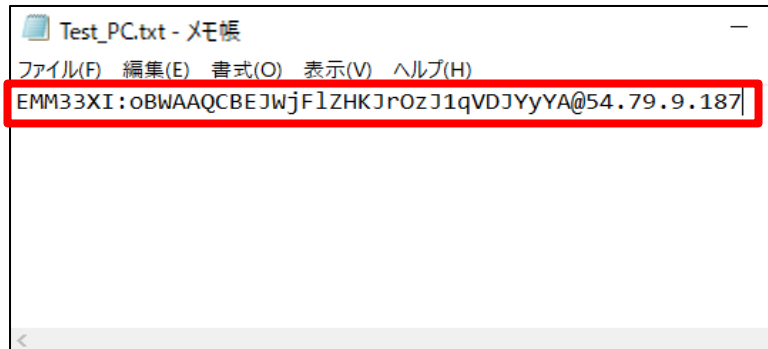
⑦メモ帳を開き、Ctrlキー+Vキーを押します。

Identity Stringの内容が貼り付けられるので、下記内容で保存します。

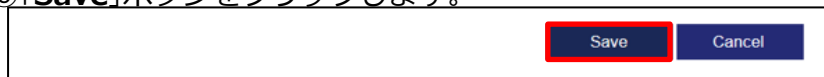
名称： クライアントPC名

形式： テキスト ファイル(.txt)

場所： 任意



⑧「**Save**」ボタンをクリックします。



⑨⑦で保存したファイルを該当のクライアントPCに送付します。

MDiA Managerでのライセンス認証時に使用しますので、任意の場所に配置してください。

以降のクライアント側の設定は「クイックスタートガイド.pdf」に記載されている
<フローティングライセンスの場合>を参照してください。

以上で、Identity Stringの作成は完了です。

7.MDiA独自設定の追加方法

- ・ ライセンスサーバーPCに、フローティングライセンス用のMDiA独自設定※を追加します。
※MDiA認証のタイムアウト設定 及び フローティングライセンス専用機能の利用設定です。
- ①弊社提供の「MDiAFloatingSetting.bat」を実行します。
（「MDiAFloatingSetting」フォルダ内に格納されています。）
以下のメッセージが出てきたら、設定追加は完了です。



8.注意点

- ・別のサーバー（PC）への変更を行う場合、弊社へご連絡ください。
- ・使用ポートは「**1947**」となりますので、ファイアウォール等で遮断されている場合は解放をお願いします。
- ・クライアントPC側の認証先（iniファイル）を設定する必要があるため、
認証サーバーPCのIPアドレス（推奨：固定IP）またはコンピューター名について
アプリケーション使用ユーザーへの周知をお願いします。

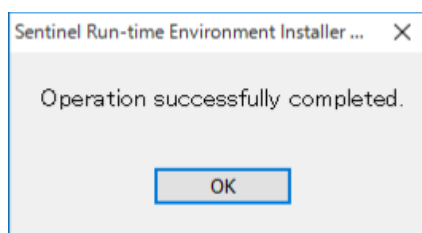
9.Sentinel RTEのアンインストール方法

- ・ 以下の手順に従ってアンインストールをお願いします。

① コマンドプロンプトを「管理者として実行」で開きます。

② 弊社提供の「**haspdinst_112987.exe**」を①で開いたコマンドプロンプト上で「**haspdinst_112987.exe -remove**」を入力して実行します。

以下のメッセージが出てきたら、アンインストールは完了です。



10.トラブルシューティング

症状	原因	確認方法
Sentinel RTE設定ページ (http://localhost:1947) を表示できない	Sentinelサービスが 起動していない	Windowsのサービス「Sentinel LDK License Manager」の 状態が開始になっているか確認してください。
Sentinelサービスの状態 が、開始にならない場合	Windowsの別サービ スと競合(コンフリク ト)が発生している	以下の手順で競合しているサービスを確認してください。 ① Windowsのシステム構成(コントロールパネル >管理ツ ール >システム構成)を開く ② サービス タブを開く ③ 「Microsoft のサービスをすべて隠す(H)」にチェックを つける ④ 「すべて無効(D)」をクリックする ⑤ 目的のサービス (RTE の場合、Sentinel LDK License Manager) が動作するか確認する ⑥ Microsoft 以外のサービスが全て無効の状態で作動する 場合、上記を繰り返し、コンフリクトしている サービス を特定し除去する
クライアント側からアク セス可能に関わらず、 認証できない	通信ポート1947を 別のアプリケーションが占有している	以下の手順で占有状況を確認してください。 ① コマンドプロンプトから “netstat -ano” と入力し、ア クティブな接続の一覧を表示する ② ローカルアドレス列で、目的のポート 1947 の行を特定 し、PID 番号を控えておく ③ タスクマネージャーを起動 >表示(V) >列の選択(S) > PID (プロセス ID) にチェックをつける ④ PID 列から、②で控えておいた番号を特定し、イメージ 名が hasplms.exe であることを確認する