VENAFI TRUST PROTECTION PLATFORM

Integration Guide

Applicable Devices:
KMES Series 3

TABLE OF CONTENTS

[1] DOCUMENT INFORMATION

[1.1] DOCUMENT OVERVIEW

The purpose of this document is to provide information regarding the configuration of the Futurex KMES Series 3 for integration with Venafi Trust Protection Platform (TPP) through its Adaptable CA functionality.

This document focuses on steps specific to Trust Protection Platform integration and assumes basic setup of the KMES Series 3 has been performed. For additional information and setup instructions for the KMES Series 3, see the relevant user guide. This document also assumes basic setup of Venafi Trust Protection Platform has been performed.

[1.2] ABOUT VENAFI TRUST PROTECTION PLATFORM

From Venafi's Trust Protection Platform datasheet: "Venafi Trust Protection Platform manages, secures and protects keys and certificates, delivering an enterprise-grade platform that provides enterprise-wide security, operational efficiency and organizational compliance."

[2] INTEGRATION WITH THE VENAFI TRUST PROTECTION PLATFORM

The use of hardware security modules (HSM) is one of the strongest methods of protecting the certificate issuance process. Venafi's Trust Protection Platform integrates with Futurex's KMES Series 3 to offload certificate lifecycle management to a FIPS 140-2 Level 3 validated HSM, using strong cryptography to guard against key compromise, reduce fraud risk, and thwart insider attacks. Additionally, the KMES Series 3 enables administrators to manage multiple certificate issuance policies from a single device and offers turnkey integration with Futurex's Hardened Enterprise Security Platform, allowing it to form the cornerstone of an organization's overall core cryptographic infrastructure.

[2.1] WHAT IS ADAPTABLE CA?

This document refers frequently to Adaptable CA. Adaptable CA is Trust Protection Platform's integration method for third-party or non-natively supported certificate authority platforms, such as the KMES Series 3.

[3] PREREQUISITES

Before following the steps in this integration guide, the following prerequisite items must be installed and configured:

- Venafi Trust Protection Platform
- Futurex KMES Series 3 with minimum application version 6.1.2.4, the Registration Authority license enabled, and initial setup steps completed
- Futurex PowerShell scripts downloaded from the Venafi Marketplace

[4] INSTALLATION AND CONFIGURATION: KMES SERIES 3

[4.1] ENABLE HOST API COMMANDS

To enable Trust Protection Platform integration, six Host API commands must be unblocked in the KMES Series 3. These Host API commands can be enabled and disabled through the Host API Options window on the Configuration tab.

- RKLO: Login User
- RKRK: Retrieve Generated Keys
- RAUX: Upload Request (X.509 CSR)
- RAYX: Approve Requests
- RAGX: Retrieve Request (X.509 CSR)
- RASX: Manipulate Signed Request

[4.2] SETTING UP PKI-BASED APPLICATION AUTHENTICATION

The KMES Series 3 supports authenticating applications using PKI certificates. These are generated on the KMES Series 3 and imported into Trust Protection Platform using steps outlined later in this document.

Establishing an application authentication PKI ensures the Trust Protection Platform server is trusted and eliminates the reliance on solely having a username and password to authenticate. For these reasons, PKI-based application authentication is Futurex's recommended method. The process of setting up PKI-based application authentication is outlined in detail in the Initial Setup section of the KMES Series 3 user guide.

At a high level, the process of setting up PKI-based authentication requires the following steps be completed:

1. Create or import a trusted certificate authority that will be used to authenticate Trust Protection Platform.
2. Enable and configure the Host API port.
3. Configure global settings for application users.
4. Configure the application user group.
5. Whitelist application IDs within the user group.
6. Export the TLS credential as a PFX/PKCS #12 file.
7. Install the certificate on the server running Trust Protection Platform.

[4.3] USER, GROUP, AND POLICY PERMISSIONS

The table below outlines the most commonly used permission structure for users, user groups, and issuance policies on the KMES Series 3. These permissions may differ slightly depending on the environment and should be viewed as representative of a typical environment, not necessarily a set of mandatory permissions.

User, Group, or Policy Type	Permission
Uploading Users	USE permissions over the certificate container and issuing chain.

User, Group, or Policy Type	Permission
	USE permissions over the approval group.
Approving Users	USE permissions over the approval group.
Uploading Groups	Manage Certificates -> Upload Manage Certificates -> Export
Approving Groups	Manage Signing Approvals -> Approve
Issuance Policies	Manage Signing Approvals -> Approve If a single user is used, "Allow single group for upload and approval" enabled

[4.4] CREATE USER GROUPS AND USERS

Trust Protection Platform supports two options for user credential management. The single user role option establishes one user per issuance policy that is permitted to submit certificate issuance requests, approve or deny requests, or revoke certificates. The dual user role option establishes two users per issuance policy, with one permitted only to submit certificate issuance requests and one permitted only to approve or deny issuance requests or revoke issued certificates.

For a greater degree of administrative separation as well as adherence to principles of role-based access control, Futurex recommends using the dual user method.

The term "users" on the KMES Series 3 is equivalent to the term "credentials" on Trust Protection Platform. To maintain consistency with product user interfaces, those terms are used interchangeably throughout this integration guide, depending on which product is being referenced.

This integration guide does not contain a comprehensive list of all user group and user configuration parameters, but addresses the items specifically required for integration with Trust Protection Platform.

[4.4.1] USER GROUP CREATION – SINGLE USER ROLE OPTION

Users on the KMES Series 3 must belong to a user group. When setting up a single user to control all aspects of certificate requesting, approval, and revocation, the high-level steps below must be performed.

1. Select **Users** from the left toolbar on the KMES Series 3 application. The *Users* menu will open.
2. Right-click on **Admin Group** and select **Add** -> **Group**. The *User Group Editor* window will appear.
3. Set the number of users required to log in to **1**.
4. Under the *Permissions* tab, enable the necessary permissions. See the section above entitled Permissions for more detail.
5. Configure the remaining group settings with parameters appropriate for your organization. For more detail on all options, see the KMES Series 3 user guide.

[4.4.2] USER GROUP CREATION – DUAL USER ROLES OPTION (RECOMMENDED)

When setting up two users, one to submit certificate issuance requests and one to approve or reject them as well as revoke certificates, the high-level steps below must be performed.

1. Select **Users** from the left toolbar on the KMES Series 3 application. The *Users* menu will open.
2. Right-click on **Admin Group** and select **Add** -> **Group**. The *User Group Editor* window will appear.
3. Set the number of users required to log in to **1**.
4. Under the *Permissions* tab, enable the following permissions:
    a. **Manage Certificates**: Export and Upload
5. Configure the remaining group settings with parameters appropriate for your organization. For more detail on all options, see the KMES Series 3 user guide.

Next, configure a second group using the same steps outlined above, but enabling the Approve permission under the **Manage Signing Approvals** permission category instead.

[4.5] CREATE SIGNING APPROVAL GROUP

To enable certificate signing approval workflows in the KMES Series 3, a signing approval group must be created using the following steps:

1. Select **Signing Approval** from the left toolbar on the KMES Series 3. The *Signing Approval* menu will open.
2. Right-click, select **Add Approval Group**, and choose a name for the group.

After creating a signing approval group, make note of the group name, as it will need to be referenced in the Adaptable CA driver, which is detailed later in this document.

[4.6] DEFINE CERTIFICATE ISSUANCE POLICIES

One of the primary advantages of the KMES Series 3 is that it allows Trust Protection Platform users to manage multiple certificate issuance policies from a single device.

1. Create the issuing certificate tree.
    a. Create or import the needed CAs and generate an issuing certificate that will be used for issuing certificates.
    b. Define permissions on the CA container and select the option to apply permissions to children recursively.
2. Assign an issuance policy. Further detail on issuance policies is contained in the KMES Series 3 user guide.
3. Set the number of users required to log in to **1**.
4. Under the *Permissions* tab, enable the following permissions:
    a. **Manage Certificates**: Export and Upload
    b. **Manage Signing Approvals**: Approve
5. Configure the remaining group settings with parameters appropriate for your organization. For more detail on all options, see the KMES Series 3 user guide.

After creating or importing an issuing certificate tree and issuance policy, make note of the CA name and the issuance policy name, as they will need to be referenced in either the Adaptable CA driver or as a custom field,

both of which are detailed later in this document.

[5] CONFIGURING THE ADAPTABLE CA DRIVER

Two PowerShell scripts are required for connecting the KMES Series 3 to Trust Protection Platform's Adaptable CA interface:

- Futurex KMES CA.ps1
- FuturexCreateCustomFields.ps1

Futurex KMES CA.ps1 must be copied into the AdaptableCA scripts folder, which is typically found at **C:\Program Files\Venafi\Scripts\AdaptableCA**.

FuturexCreateCustomFields.ps1 may be run from anywhere, as long as it's able to connect to Trust Protection Platform's web SDK. As Trust Protection Platform will attempt to enumerate the script as if it's a driver, Futurex recommends NOT placing it in the AdaptableCA scripts folder.

[5.1] CONFIGURING THE KMES SERIES 3 POWERSHELL DRIVER

To connect to a KMES Series 3, Trust Protection Platform uses a PowerShell configuration file containing user-defined parameters. This file can be opened in a text editor and contains the following fields:

```
##################
# Configuration #
##################

# Address of the KMES Host API
$global:ServerHost = "<KMES SERIES 3 HOSTNAME OR IP>";

# Port of the KMES Host API
$global:ServerPort = "<KMES SERIES 3 HOST API PORT>";

# Container name associated with issuing certificate
$global:ContainerName = "<CONTAINER NAME ON THE KMES SERIES 3>";

# Name of the issuing certificate
$global:IssuingCertificate = "<ISSUING CERTIFICATE ON THE KMES SERIES 3>";
```

To use multiple KMES Series 3 servers or even different issuing certificates, the user will need to create additional copies of the driver script with different filenames and manually change the variables for each instance required. If the driver script's filename is changed, it will appear in Trust Protection Platform with a different name.

[5.2] CONFIGURING THE CUSTOM FIELDS POWERSHELL SCRIPT

The second PowerShell file, FuturexCreateCustomFields.ps1, is a script that defines two custom fields in Trust Protection Platform. These are used for defining the approval group within the KMES Series 3 that will control approvals of issuance requests, as well as defining X.509 extension profiles. X.509 extension profiles allow users to define the type of certificate being deployed. This must match an option defined for the relevant issuance policy.

These fields are optional and can provide additional levels of granular control over Venafi policies for certificate attributes and issuance structure. These two fields are currently the only ones supported by Futurex and Venafi.

These custom fields must be added using this script and cannot be manually added inside the Venafi application itself.

To configure the script, open FuturexCreateCustomFields.ps1 in a text editor and change the following variables to ones appropriate for the Venafi Trust Protection Platform installation.

```
# “Configuration”
$SdkUri = "<VENAFI TRUST PROTECTION PLATFORM HOSTNAME OR IP>"
$SdkUser = "<VENAFI TRUST PROTECTION PLATFORM USERNAME>"
$SdkPass = "<VENAFI TRUST PROTECTION PLATFORM PASSWORD>"
```

Once these changes have been made, the script can be run in PowerShell. This script only needs to be run once on each server running Venafi, regardless of how many KMES Series 3 units or issuance policies are defined.

In order to allow custom X.509 extensions to be defined in Trust Protection Platform when creating certificates, “Allow User-Defined Extensions” must be checked in the issuance policy. If this is not checked, custom extensions will be ignored and only what is defined in the issuance policy on the KMES Series 3 will be used.

[6] CONFIGURING THE VENAFI TRUST PROTECTION PLATFORM

[6.1] CREDENTIAL MANAGEMENT

After creating user groups and users on the KMES Series 3, they must be added to Trust Protection Platform. On Trust Protection Platform, these are referred to as credentials.

The instructions contained in this section assume two separate users are being used, one to submit certificate issuance requests and one to approve or reject them as well as revoke certificates, which is Futurex's recommended configuration. A single user to perform all operational tasks may also be used.

[6.1.1] DEFINE USER CREDENTIALS

To define user credentials, perform the following steps:

1. Log into Trust Protection Platform.
2. Select **Manage** and then **Credentials** from the toolbar menu.

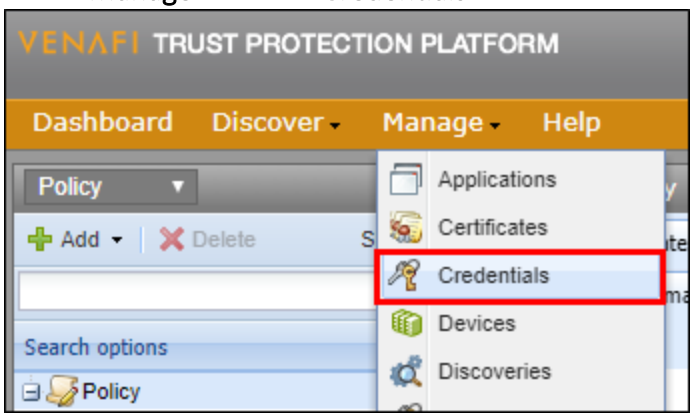

FIGURE: DEFINE USER CREDENTIALS

3. In the *Policy* menu, click **Add** and under the *Credential* category, select **Username Credential**.
4. In the *Username Credential* window, add the username and password created on the KMES Series 3 earlier in the integration process, along with any other settings needed for the environment, such as a credential expiry date.
5. Click **Save** to save the credential.
6. Repeat steps 2-4 for each additional user needed.

[6.1.2] DEFINE TLS CLIENT CERTIFICATE CREDENTIALS

TLS client certificates are used to mutually authenticate with the KMES Series 3, allowing only authorized operation and establishing an encrypted tunnel to prevent man-in-the-middle eavesdropping on traffic.

To define TLS client certificate credentials, perform the following steps:

1. Log into Trust Protection Platform.
2. Select **Manage** and then **Credentials** from the toolbar menu.

3. In the *Policy* menu, click **Add** and under the *Credential* category, select **Certificate Credential**.

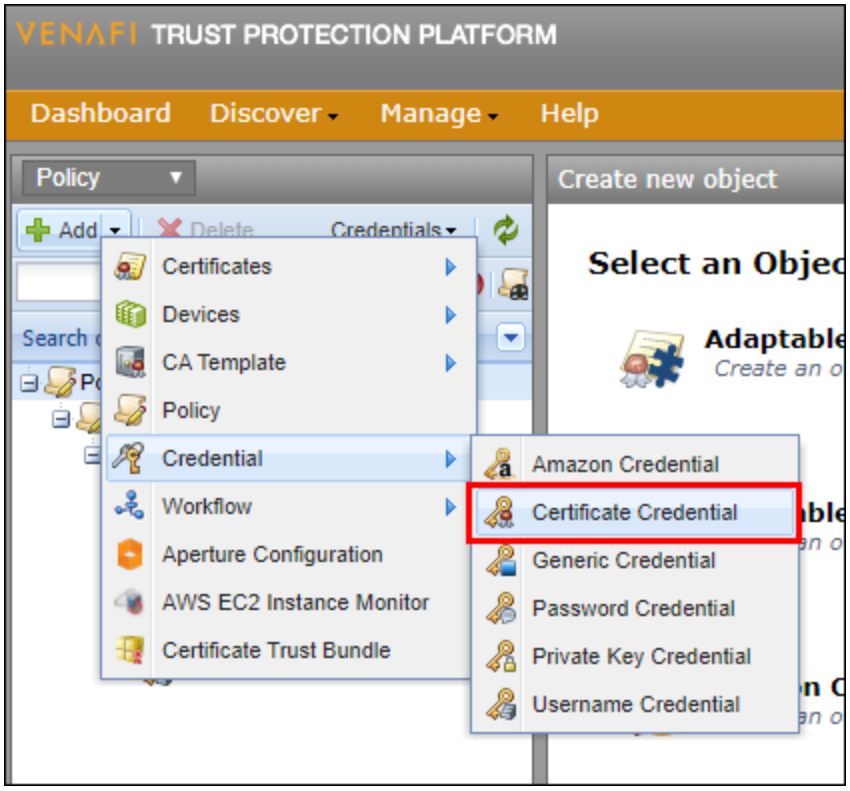

FIGURE: DEFINE TLS CLIENT CERTIFICATE CREDENTIALS

4. In the *Certificate Data* section, choose the option to import a certificate and select the binary-encoded PFX/PKCS #12 certificate that was exported from the KMES Series 3 earlier in this integration guide.
5. Specify the corresponding private key password and begin the import process.
6. Once the certificate has imported, select the **Save** button to complete the process.

[6.2] CA TEMPLATE CREATION

To create CA templates, perform the following steps:

1. Log into Trust Protection Platform.
2. Select **Manage** and then **Policies (all)** from the toolbar menu.
3. In the *Policy* tree, right-click on **Certificate Authorities** and select **Add** -> **CA Template** -> **Adaptable**. The *Add New Adaptable* window will appear.

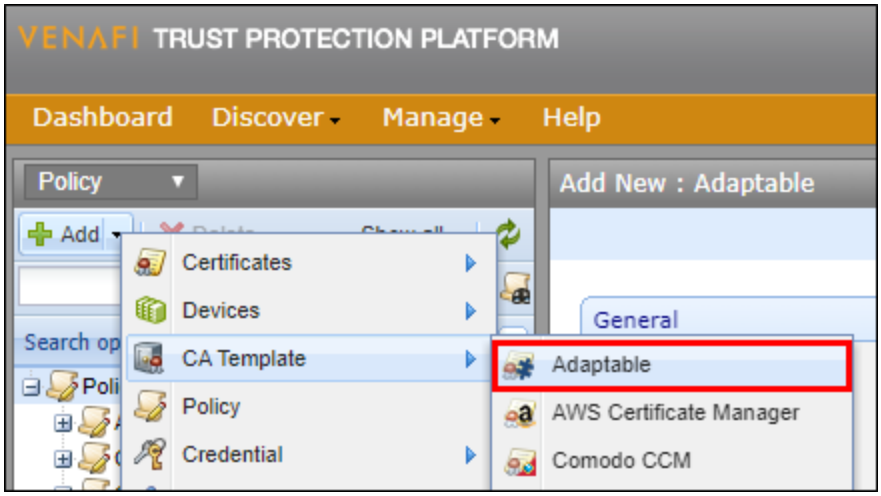

FIGURE: CA TEMPLATE CREATION

4. Define the following General and Connection fields:
    a. **CA Name**: the desired CA name.
    b. **Username Credential**: the first credential created earlier in the integration process.
    c. **Certificate Credential**: the TLS client certificate created earlier in the integration process.
    d. **Secondary Credential**: the second credential, if applicable, created earlier in the integration process.
    e. **PowerShell Script**: Futurex KMES CA
5. If custom X.509 extensions or Futurex approval groups are desired, define them in the Custom Fields section. Note that for these to be visible, the custom fields PowerShell script defined earlier in this document must have been successfully run.
6. Select **Validate** to test the connection and authentication with the KMES Series 3. The process may take anywhere from 10 to 20 seconds.

[6.3] CERTIFICATE POLICY CREATION

To create certificate policies, perform the following steps:

1. Log into Trust Protection Platform.
2. Select **Manage** and then **Certificates** from the toolbar menu.
3. In the *Policy* tree, navigate to the desired child certificate tree, right-click on it, and select **Add** -> **Policy**. The *Add New Policy* window will appear.
4. Define the policy name and any other desired settings and select **Save**.
5. Return to the *Certificates* section of the *Policy* tree, navigate to the desired child certificate tree, and select the **Certificate** tab.
6. In the *Other Information* section, click the drop-down next to CA Template and choose the **Set value here** option.
7. Open the file browser using the **…** button and select **KMES Adaptable CA**.
8. Select the **Save** button to complete the process.

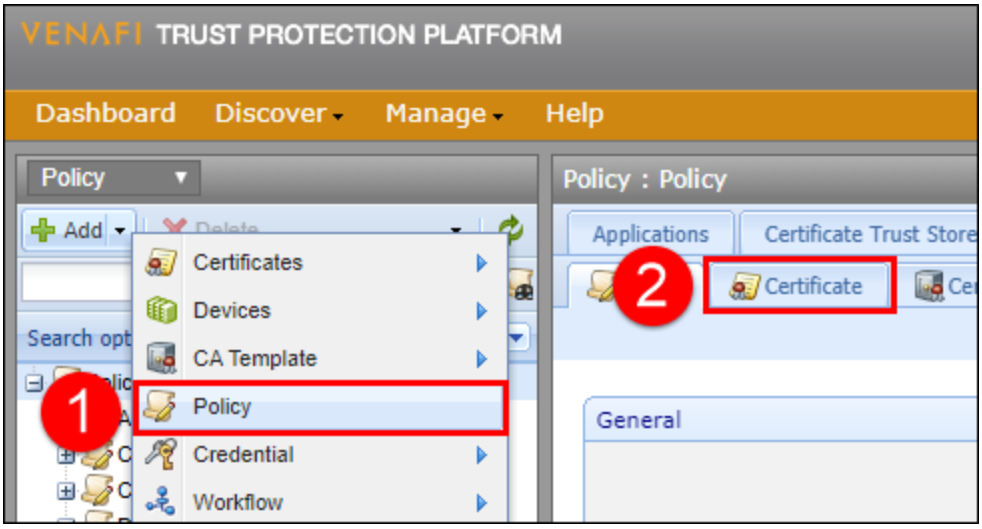

FIGURE: CERTIFICATE POLICY CREATION

[7] TROUBLESHOOTING

[7.1] ERROR MESSAGES

If an error is encountered, the KMES Series 3 will provide an error message that is displayed within Trust Protection Platform. Most functions provide a description of the error and the entire Excrypt API response containing the error provided by the KMES Series 3's Host API.

When troubleshooting error messages with Futurex's support team, providing the entire message displayed by Trust Protection Platform can speed the diagnosis and resolution.

Error Message	Description
X509 SIGNING NOT ALLOWED	Caused by a lack of upload permissions in the issuance policy.
NO PERMISSIONS	A general error resulting from a lack of permissions for that particular task.
INSUFFICIENT APPROVAL GROUP PERMISSION	A specific error for when a user has view permissions over an approval group but cannot use the approval group.
INVALID REQUEST IDS	Occurs when the correct IDs are used but the approving group doesn't have permissions to view them, so the KMES Series 3 believes them to be invalid.
NOT ALLOWED TO APPROVE YOUR OWN UPLOAD	The same user is being used for both upload and approval. If this is intended, then the restriction can be relaxed in the issuance policy via the "Allow single group for upload and approval" option in the KMES Series 3 configuration.
BAD LOGIN ATTEMPT	User credentials could not be validated. Possible causes include an incorrect or nonexistent username or incorrect permissions.

APPENDIX A: XCEPTIONAL SUPPORT

In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

ENGINEERING CAMPUS

864 Old Boerne Road

Bulverde, Texas, USA 78163

Phone: +1 830-980-9782

+1 830-438-8782

E-mail: info@futurex.com

XCEPTIONAL SUPPORT

24x7x365

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com