Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – CLIENT CONFIGURATIONS

VERSION 2.0

Fortanix Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

Welcome to the Fortanix Data Security Manager (DSM) Client Configuration User Guide. This document describes how to configure the various configuration options for the Fortanix DSM Clients.

1.1 OVERVIEW

Currently, the Fortanix DSM clients are configured locally through configuration files and environment variables. With the Client Configuration feature in the Fortanix DSM UI, you can set the default configurations for clients such as PKCS11 in the Fortanix DSM accounts and groups and the PKCS11 clients will automatically get these values. This makes it simpler to configure a large number of clients.

NOTE: You can set the client config values at the Fortanix DSM account/group/app level using the `client_configuations` field. You can also use an App to call `GET /sys/v1/apps/client_configs` to get the client config value outside of the client.

2.0 DEFINITIONS

- **Fortanix Data Security Manager** -

  Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

- **Accounts** -

  An Fortanix DSM account is the top-level container for security objects managed by the Fortanix DSM. An account is generally associated with an organization, rather than an individual. Security objects, groups, and applications belong to exactly one account. Different accounts are fully isolated from each other. *See support for more information.*

- **Users** -

  Users are associated with an email address. A user can be a member of one or more accounts.

Depending on permissions, users can:

- Perform management operations like adding or modifying users or groups
- Create security objects
- Change properties of security objects
- Review logs of Fortanix DSM activity

⚠ **Users cannot perform cryptographic operations. Only applications can perform cryptographic operations.**

- **Groups** -

  A group is a collection of security objects created by and accessible by users and applications which belong to the group. The user who creates a group automatically gets assigned the role of the group administrator. You can add more users to the group in the role of administrators or auditors. You can also add applications to the group to enable the applications to create and use security objects in that group. *See support for more information.*

  Access policies are set at the group level, so all security objects in a group share the same access policy. Any number of users and/or applications can be assigned to a group. *Some examples of usage of groups are given in the Authorization section.*

  Quorum policies can also be set at group level. A Quorum policy mandates that all security sensitive operations in that group would require a quorum approval. Such operations include using a key for cryptographic operations or deleting or updating a group. *See Quorum Policy for more information.*

- **Applications** -

  An application can use Fortanix DSM to generate, store, and use security objects, such as cryptographic keys, certificates, or an arbitrary secret. Applications can authenticate to Fortanix DSM using an API key (a secret token) or a TLS client certificate. An application can interact with Fortanix DSM using the REST APIs or using the PKCS#11, JCE, or CNG providers. *See support for more information.*

- **Fortanix Data Security Manager Security Objects** –

  A security object is any datum stored in Fortanix DSM (for example a key, a certificate, a secret, or other security objects). Each security object is assigned to exactly one group. Users and applications assigned to the group have permission to see the security object and to perform operations on it. *See support for more information.*

3.0 SETTING CLIENT CONFIGURATION OPTIONS

Using the Client Configuration setting in the Fortanix DSM UI you can set the default options for the Fortanix DSM clients such as PKCS #11 and other common clients.

3.1 SETTING THE CONFIGURATION OPTIONS FOR THE COMMON CLIENTS

To set the default options for the account-level Fortanix DSM Common client:

1. Go to the Fortanix DSM **Account settings** page and select the **CLIENT CONFIGURATION** tab.
2. On the Client Configuration page, select the **COMMON** tab to configure the common clients.

To set the default options for the group-level Fortanix DSM Common client:

1. Go to the detailed view of a Fortanix DSM group, and in the **INFO** tab scroll to the Client Configuration (Advanced) section and click **ADD CONFIGURATION** to add a new configuration.
2. On the Client Configuration page, select the **COMMON** tab to configure the common clients.

NOTE: The group-level Client configuration settings for the Common client will override the account-level configuration settings. This is an advanced configuration.

The following table lists the Common client configuration options.

NAME	DESCRIPTION
Retry timeout	When API calls that allow retrying fail with error codes, select this option to allow the client library to retry the API call up to the specified timeout in milliseconds.

Logging	Select this option to log all function calls made into the client library based on the following settings:
	• **System**: Selecting this option instructs the client library to use System logging facilities. On Linux, this would use Syslog for instance.
	• **Level**: This is the minimum log level to produce log messages. The default option is **info**. Select one of the following options to log messages when making a function call to the client library:
	  ○ **off**: if you do not want to log any messages.
	  ○ **error**: if you want to log any errors preventing one or more functionalities from properly functioning.
	  ○ **warn**: if you want to log warnings that indicate that something unexpected happened.
	  ○ **info**: if you want to log all the information such as errors, warnings, and any informational messages.
	  ○ **debug**: Setting this to debug would cause additional debugging information to be logged which might be helpful in debugging errors.
	  ○ **trace**: if you want to log all the details about the behaviour of the client library. It is mostly diagnostic and is more granular and finer than the **debug** log level.
	  **NOTE**: Each log level above will also include all messages from the previous log level. For example, the log level **trace** will include errors, warnings, informational messages, debugging information, and all other details about the client library.
	• **File**: Select this option to configure the file that is used to log all the function calls made into the client library. The following options can be configured.
	  ○ **Path**: Enter the log file path used by the client library.

	○ **Set file size**: Select the maximum log file size in KB before the log file is rotated. The values that can be selected are 16, 32, 64, 128, or 256. ○ **Set max files**: Configure the maximum number of log files to keep after rotation.

3.2 SETTING THE CONFIGURATION OPTIONS FOR THE PKCS #11 CLIENT

To set the default options for the account-level Fortanix DSM PKCS #11 client:

1. Go to the Fortanix DSM **Account settings** page and select the **CLIENT CONFIGURATION** tab.
2. On the Client Configuration page, select the **PKCS#11** tab to configure the PKCS #11 clients.

To set the default options for the group-level Fortanix DSM PKCS #11 client:

1. Go to the detailed view of a Fortanix DSM group, and in the **INFO** tab scroll to the Client Configuration (Advanced) section and click **ADD CONFIGURATION** to add a new configuration.
2. On the Client Configuration page, select the **PKCS#11** tab to configure the PKCS#11 clients.

NOTE: The group-level Client configuration settings for the PKCS#11 client will override the account-level configuration settings. This is an advanced configuration.

The following table lists the PKCS #11 client configuration options.

NAME	DESCRIPTION
Fake RSA X9.31 keygen support	Select this option to allow the PKCS #11 mechanism `CKM_RSA_X9_31_KEY_PAIR_GEN` to be specified when generating RSA keys in X9.31 generation procedure.

Signing AES key as HMAC	Select this option to create an AES key while specifying either the `CKA_SIGN` or `CKA_VERIFY` attributes in the template. This will result in an HMAC key being created in the backend. The key should still appear as an "AES key" from a PKCS #11 perspective.
Prevent duplicate opaque objects	Select this option to prevent creating a duplicate opaque object. This would skip creating new Opaque objects if there is an existing Opaque object with the same `CKA_LABEL`.
Opaque objects are not certificates	Fortanix DSM versions prior to 2.1.633 did not support `certificate` objects and the PKCS #11 library creates certificates using `opaque` object type. If your on-prem DSM cluster or your DSM SaaS account was created after that release (circa May 2018), then you can safely turn this on so that `C_FindObjects` queries run faster.
Max concurrent requests	Select this option to limit the number of concurrent HTTP requests the PKCS #11 client can make to the Fortanix DSM per slot. This effectively limits the number of concurrent API calls the client can make. This can be used to prevent a client from consuming too many resources. If set to **0**, no limit is imposed.
Exact key ops	Select this option to explicitly specify the key operations in the attribute template when creating a key instead of the

	PKCS#11 having to specify the default key operations. The key created using the template will contain exactly the key ops that the user specified in the template. However, when no key operation attributes (apart from `CKA_MODIFIABLE` or `CKA_DESTROYABLE`) are specified, the PKCS #11 client will assign some default keyops (for user convenience). For more details, refer to the PKCS11-Developer's Guide.

3.3 SETTING THE CONFIGURATION OPTIONS FOR THE KMIP CLIENT

To set the default options for the account-level Fortanix DSM KMIP client:

1. Go to the Fortanix DSM **Account settings** page and select the **CLIENT CONFIGURATION** tab.
2. On the Client Configuration page, select the **KMIP** tab to configure the KMIP client.

To set the default options for the group-level Fortanix DSM KMIP client:

1. Go to the detailed view of a Fortanix DSM group, and in the **INFO** tab scroll to the Client Configuration (Advanced) section and click **ADD CONFIGURATION** to add a new configuration.
2. On the Client Configuration page, select the **KMIP** tab to configure the KMIP clients.

NOTE: The group-level Client configuration settings for the KMIP client will override the account-level configuration settings. This is an advanced configuration.

The app-level client configuration settings for the KMIP client can be set using the Fortanix DSM REST API and after you set it, a read-only view of the setting will be visible in the detailed view of the Fortanix DSM app in the UI.

The following table lists the KMIP client configuration options.

NAME	DESCRIPTION
Allow secrets with unknown operations (verify/Derive/Wrap/ unwrap)	Enable this option to allow a "Secret" object to be created with `VERIFY`/`DERIVE_KEY`/`WRAP_KEY`/`UNWRAP_KEY` operations from a KMIP client.

4.0 REFERENCES

For more details about the Fortanix DSM Common Client and the PKCS #11 client, refer to the Developer's Guide – PKCS#11 Library.

5.0 DOCUMENT INFORMATION

5.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/4764402409876-User-s-Guide-Client-Configurations

5.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com