Protegrity Data Security Platform Licensing Guide 9.0.0.0

Created on: Nov 19, 2024

Notice

Copyright

Protegrity products are protected by and subject to patent protections;

Patent: *https://www.protegrity.com/patents*.

The Protegrity logo is the trademark of Protegrity Corporation.

NOTICE TO ALL PERSONS RECEIVING THIS DOCUMENT

Some of the product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective owners.

Windows, Azure, MS-SQL Server, Internet Explorer and Internet Explorer logo, Active Directory, and Hyper-V are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SCO and SCO UnixWare are registered trademarks of The SCO Group.

Sun, Oracle, Java, and Solaris are the registered trademarks of Oracle Corporation and/or its affiliates in the United States and other countries.

Teradata and the Teradata logo are the trademarks or registered trademarks of Teradata Corporation or its affiliates in the United States and other countries.

Hadoop or Apache Hadoop, Hadoop elephant logo, Hive, and Pig are trademarks of Apache Software Foundation.

Cloudera and the Cloudera logo are trademarks of Cloudera and its suppliers or licensors.

Hortonworks and the Hortonworks logo are the trademarks of Hortonworks, Inc. in the United States and other countries.

Greenplum Database is the registered trademark of VMware Corporation in the U.S. and other countries.

Pivotal HD is the registered trademark of Pivotal, Inc. in the U.S. and other countries.

PostgreSQL or Postgres is the copyright of The PostgreSQL Global Development Group and The Regents of the University of California.

AIX, DB2, IBM and the IBM logo, and z/OS are registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

Table of Contents

Chapter 1

Introduction to this Document

This document is intended to provide a general overview of licensing and to explain its importance and impact on Protegrity products.

The document answers the following questions:

- What is the difference between a temporary and validated license?
- How can you request a validated license?
- What happens if the license expires?
- How are you notified when your license is due to expire?
- What are the features included in a validated license?

It is strongly recommended that you read all sections of the document to make sure you understand how the licensing affects the ESA installation, ESA upgrade, trusted appliances cluster licensing, and protectors' licensing.

1.1 Sections contained in this Guide

The guide is broadly divided into the following sections:

- *Section 1 Introduction to this Guide* defines the purpose and scope for this Guide. In addition, it explains how information is organized in this Guide.
- *Section 2 Protegrity Products Licensing* provides information about the product licensing and how to handle temporary licenses.
- *Section 3 Obtaining a Validated License* provides information about validating a license.
- *Section 4 Non-Licensed Product* provides information about handling expired licenses and so on.
- *Section 5 Cluster Licensing* provides information about how to handle licensing in HA and TAC setup.
- *Section 6 Upgraded Products Licensing* provides about how licensing is affected based on the version you are upgrading from to the latest ESA release.

1.2 Accessing the Protegrity documentation suite

This section describes the methods to access the *Protegrity Documentation Suite* using the *My.Protegrity* portal.

Chapter 2

Protegrity Products Licensing

To prevent unauthorized use of the Protegrity Data Security Platform and prevent illegal copying and distribution, Protegrity supports licensing. The licenses provided by Protegrity are unique and non-transferable. They permit product usage for the term specified in your agreement with Protegrity.

The benefit to you, as our customer, the Protegrity license provides additional security to the product and supports a legal agreement stipulating the rights and liabilities of both parties.

2.1 License Agreement

The License Agreement is a contract between the licensor and purchaser, establishing the purchaser's right to use the software.

The Protegrity License Agreement stipulates the license expiry date and the number of affected Protectors. The License Agreement also predefines the functionality which is available after the license expiry date.

For specific details about your particular licensing terms, refer to your License Agreement provided by Protegrity.

2.2 License Types

When your Enterprise Security Administrator (ESA) is installed, a temporary license is applied to it by default.

If you have an older version of ESA, and you are going to upgrade it to latest version of ESA, then perform the upgrade as explained in *Upgraded Products Licensing*.

The temporary license which is created during installation allows you to use ESA, Policy management, and ten protectors for 30 days starting from the day you installed ESA. When the temporary license expires, you are able to log on to ESA, but you have restricted permissions for using it.

For more information, refer *Expired License*.

To continue using the ESA with full administrative permissions, you must obtain a validated license provided by Protegrity. The validated license has an expiry date which is determined by the License Agreement between your company and Protegrity.

> **Note:** If the license status is *invalid*, then contact *Protegrity Support*.

2.3 Temporary and Validated License Characteristics

This section explains types of licenses and characteristics of each license.

The following table describes the characteristics of each type of license. The license characteristics explain the key points of each license and show how they differ from each other.

Table 2-1: Characteristics of Different License Types

Characteristics	Temporary License	Validated License
Obtaining a license	Installed by default during ESA installation.	Requested using ESA Web UI.
Updating a license	Not applicable	Requested using ESA Web UI.
Warning alerts before expiry of the license date	30 days prior to expiry date. The alerts appear as start-up messages when you log into ESA. The alerts can also be configured using email, and are available in the ESA logs and logs received from the Protection Points.	
Cluster licensing	Can only be used on a particular node where it was created during installation.	Stipulated by the License Agreement. For details, refer to *Cluster Licensing*.

The following table describes the features of each type of license. The license features explain the functionality that is available when the license is valid.

Table 2-2: Functionality of Different License Types

Features	Temporary License	Validated License
Number of Protectors included	Maximum 10	Stipulated by the License Agreement: • Number of Protectors or • Maximum 500 Protectors
Data protection types	Encryption and Tokenization are enabled	Encryption enabled. Tokenization can be disabled or enabled.
License duration	30 days (from the day ESA is installed).	Stipulated by the License Agreement: • Number of days or • Perpetual (never expiring)
Post-expiration functionality	• Policy management disabled • Policy deployment disabled • Protection disabled • Re-protection disabled • Unprotection enabled	Stipulated by the License Agreement: • Policy management and/or • Policy enforcement

The number of protectors includes the total number of the following which you have purchased:

- Database Protector
- Application Protector
- File Protector
- Big Data Protector
- Teradata nodes

> **Note:** Each node protected by Big Data Protector and each node protected by Database Protector for Teradata counts as one protector.

This restricts the number of protection points that can be included in your policy.

Data protection types are the methods of protection that can be applied to your data. Data protection types determine the type of data elements that can be created for your data security policy.

License duration is defined by a start and an end date. If you have purchased a perpetual license, then no end date is specified.

If your license has expired, then you have limited functionality, as defined in your licence agreement with Protegrity.

Policy management will restrict functionality that is not supported by your validated license. For example, you cannot create data elements of a protection type that is not included in your validated license. If you create data elements for tokenization under your temporary license, but your validated license does not allow tokenization, then you receive an error if a protector attempts to use that data element after the policy is redeployed.

Chapter 3

Obtaining a Validated License

You can obtain the **validated license** using the ESA Web UI. Obtaining the validated license is a two-step process consisting of requesting the ESA license and ESA license activation.

Both of these steps are performed from the Licenses pane, available in the ESA Web UI (refer to the following screenshot). Only a user with ESA Administrative permissions can request and activate the license.

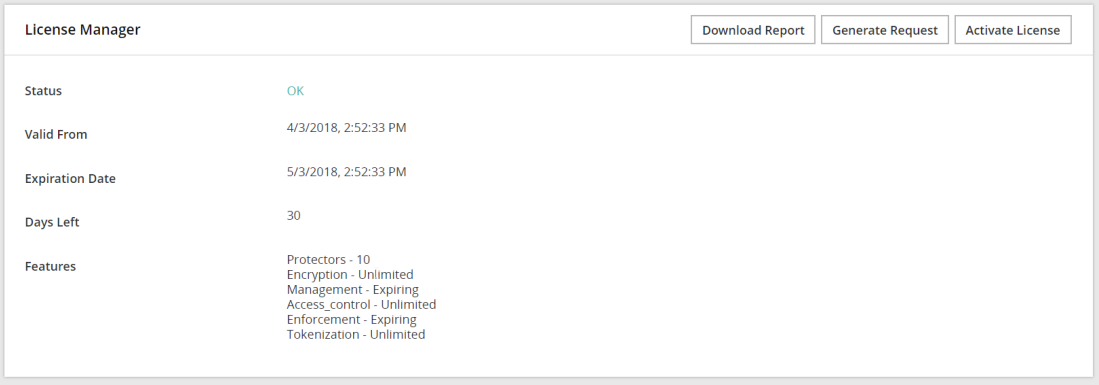

Figure 3-1: Activate License Screen

3.1 Requesting a License

You can request a validated ESA license while your temporary license is valid, or invalid, or has already expired.

➤ To request an ESA license:

1. As an ESA administrator, proceed to **Settings** > **Licenses**
2. In the Licenses pane, click the **Generate** button.
3. Save the automatically generated *licenserequest.xml* file to the local disk.
4. Send the license request file to *licensing@protegrity.com*.

3.2 Activating a License

After submitting your license request, you receive an email with a license file called license.xml. This file includes the original data retrieved from the license request, expiration date, and additional information, if required.

Before you begin

> **Note:** If there is a License Agreement between your company and Protegrity, then you receive the validated license by the end of the following business day.

To activate an ESA license:

1. Save the *license.xml* file to your local disk when you receive it from Protegrity
2. As an ESA administrator, proceed to **Settings** > **Licenses**.
3. Click **Activate License**.
4. In the Licenses pane, click **Browse**.
5. Select the *license.xml* file.
   You are notified about success or failure of the activation process.

   > **Note:** You do not need to restart ESA and any data protectors to activate the validated license. However, if you have policies deployed to protection points with a temporary license, then you must re-deploy the policies with the validated license.

   The license file is stored in an encrypted format on the ESA file system after it is activated.

   > **Caution:** Modifying either the temporary or validated license file leads to license deactivation.

3.3 Updating a License

You may need to update your current license when it has expired or if you want to add more data protectors or features to your license.

The process of updating the license is the same as when you apply for a new license. You need to submit a new license request and send an email to *licensing@protegrity.com* with the information about what you would like to change in your current license.

For details, refer to *Requesting a License*.

Chapter 4

Non-Licensed Product

The following paragraph explains the state of a Protegrity product when it is considered non-licensed, that is when the license has expired (for details refer to *Expired License*) or when it has been corrupted and, therefore, invalid (for details refer to *Corrupted (Invalid) License*).

If a license, either temporary or validated, has expired or has been corrupted, then you are able to request a validated license using the ESA Web UI. However, the availability of functionality depends on the license state and the license itself. The following paragraphs explain how the state of a license affects the permissions and availability of functionalities.

4.1 License Expiry Notification

On the ESA Web UI, a message in the Notification pane reminds you that your license is due to expire. This reminder message appears every day from one month prior to the expiry date.

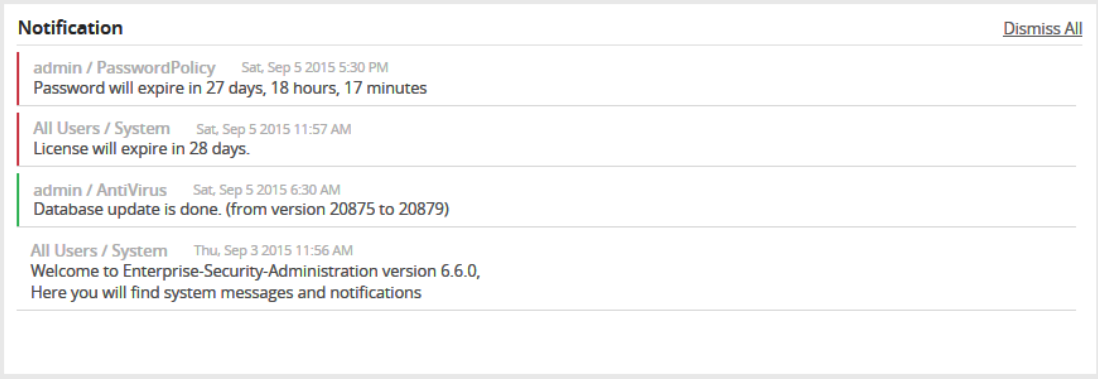

Figure 4-1: License Expiry Notification

4.2 Expired License

A license expires depending on the expiry time and date settings in the license file. In the Notification pane of the ESA Web UI, **Expired** license status is displayed.

The following changes in **Policy management** are applied when a temporary or validated license expires:

- When the current system date passes the expiration date, ESA purges all active sessions.
- At a moment when the current system date has passed the expiration date, the Policy Management is disconnected from the Hub Controller and a connection error message displays.
- On subsequent login to **Policy** management, all controls that enable users to modify policy configuration and deploy policies remain disabled. The status bar displays the message *License expired, logged in as Security Viewer*.

Upon expiration the **policy enforcement** restrictions are applied as follows:

- For a temporary license, only decryption is allowed.
- For a validated license, policy enforcement is in effect as stipulated by the License Agreement.

Table 4-1: Functionality Restrictions on Expired Licenses

Expired License Functionality	Management	Enforcement	Management & enforcement	No Management and enforcement enabled
Protectors with Structured policy	Change policy configuration (existing data elements, existing data stores, and so on) and deploy a policy	Allowed operations: • Unprotect (U) • Protect (P) • Re-protect (R) • Delete (D)	• Change policy configuration (existing data elements, existing data stores, and so on) • URPD operations	Only Unprotect operation is allowed
Protectors with Unstructured policy		• Protecting / Unprotecting files/ folders/ volumes. • Delegation / Undelegation	• Change policy configuration (existing data elements, existing data stores, etc.) • Protecting/ Unprotecting files/ folders/volumes • Delegation/ Undelegation	• Deny creating volumes • Deny protecting new files and folders • Deny delegation • Allow access to already protected files and folders • Allow unprotecting files and folders • Allow undelegation.

4.3 Corrupted (Invalid) License

If a license has been corrupted, in the Licenses pane of the ESA Web UI, then the **Invalid** license status is displayed.

If a license has been corrupted, in the Licenses pane of the ESA Web UI, then the Invalid license status is displayed.

A license may be corrupted in the following cases:

- License file has been changed manually
- License file has been deleted
- System date and time has been modified prior to when the license was applied to the product.

Caution: You MUST NOT change the system date and time to an earlier date and time (time earlier than the license has been generated) since it can lead to license deactivation. The daylight saving time change is done automatically.

Caution: You MUST NOT edit or delete the license file saved on ESA since it can lead to license deactivation.

If a temporary or validated license becomes invalid, then the following occurs:

1. Attempts to log in to **Policy** management fail and displays the message ***`License is Invalid`***, thus no policy administration is possible.

2. Protectors treat an invalid license in the same way as an expired license. Depending on the license which is corrupted, the following is applied:
   - Only unprotect is possible,if the temporary license is corrupted.
   - If the validated license is corrupted, then policy enforcement remains non-functional.

> **Note:** If policy enforcement is white listed in the validated license, then the license file is not affected with time/date changes.

However, if the validated license with white listed policy enforcement has been edited manually or deleted, the validated license becomes invalid.

4.4 License Alerts

When a license is about to expire, already expired or invalid, Hub Controller and PEP Server generate WARNING logs at start-up and once per day. The ESA Web UI and **Policy** management generate alert notifications about license status.

When a license is about to expire, already expired or invalid, Hub Controller and PEP Server generate WARNING logs at start-up and once per day. The ESA Web UI and Policy management generate alert notifications about license status.

Once the system detects that the current system date is less than or equal to 30 days from the expiration date, an audit event is generated. For the temporary license, the system generates alerts once the ESA is installed.

Once the license is expired or becomes invalid, the Data Security Platform produces logs and notifications informing you of the license status change (refer to the following tables for details).

You also view alerts in the ESA Web UI when you log in, and in the Licenses pane. In the **Expiration Date** field, there will be notification about how many days are left before the license expires and notification about the current license status.

You can also set up separate email notification alerts when licenses are about to expire using the ESA Web UI (refer to *Enterprise Security Administrator Guide*).

The following table lists the system notifications and alerts about the status of the license at risk.

Table 4-2: Alerts and Notifications when License at Risk

Alert type	ESA alerts	Protection point alerts	Cumulative alerts information
• License is about to expire • License is expired • License is invalid	License status in the ESA Web UI homepage.	WARNING generated by PEP Server in `pepserver.log` once per hour and upon PEP Server restart.	ESA Web UI Events Forensics
	License status in the ESA Web UI Licenses pane.		
	WARNING generated by Hub Controller in pepserver.log once per day and upon Hub Controller restart.		Protegrity Reports

Chapter 5

Cluster Licensing

Protegrity provides functionality for creating a cluster and, beginning with Release 6.6.x, an ESA appliance cluster primarily for use in disaster recovery (DR) scenarios. This allows you to create a trusted network of appliances with replication between ESA hosts. The procedure you follow for requesting licenses will depend upon the type of license agreement you have with Protegrity.

There are two types of restrictions that can be applied to your Protegrity license. A Configuration Lock is not machine specific and therefore can be used on other nodes in a cluster. A Node Lock is specific to the machine address of the node, and therefore cannot be used on other nodes. The stronger of the two restrictions, the Node Lock, will always take precedence when it is applied.

The descriptions of these restrictions follow:

License Agreement	Configuration Lock	Node Lock
Perpetual License	Always applied	Not applied.
Term License	Always applied	Applied as stipulated by your License Agreement with Protegrity.

The procedure you follow for requesting license files for your cluster are explained in the following sections.

Caution: These procedures must be followed ONLY when your Protegrity license agreement stipulates that the Node Lock is applied. If your license agreement only has the Configuration Lock applied, then you can use the same license file for all nodes.

5.1 Licensing Trusted Appliance Cluster

From Release 6.6.x onwards, we offer customers the functionality to create an appliance cluster, primarily for use in disaster recovery (DR) scenarios. This allows you to create a trusted network of appliances with replication between appliances hosts. Depending upon the type of license agreement you have with Protegrity, you may be required to request a new validated license file when adding nodes to your appliance cluster. You must refer to your Protegrity License Agreement for specific terms.

➤ To obtain a license for an ESA cluster:

1. Create an ESA cluster as explained in the *Protegrity Appliances Overview Guide*.
2. Using the Web Interface on each individual node, generate a license request file and save it on your local disk under a name different than the default, for example, *licenserequest2.xml*.
3. Send an email to *licensing@protegrity.com* including all license request files obtained in step 3. In the email, state that you need a license for an ESA trusted appliances cluster.

4. When you receive the single Protegrity license, activate it on one of the ESA nodes as explained in section *3.2 Activating a License*.
5. Export the policy to all other ESA nodes in the cluster.

> **Note:** When you add a new node to an existing cluster, you must create a new license request for each node in the cluster, including the new node, and send it to Protegrity.

Chapter 6

Upgraded Products Licensing

If you have an ESA of a previous version and you want to upgrade it, then the ESA license will be affected by the upgrade.