Protegrity Data Security Platform Feature Guide 9.1.0.5

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 Guide

This guide provides a general overview of the updated features in this release and guidelines on how to use these features.

1.1 Sections contained in this Guide

This section provides a short description about the sections contained in this guide.

The guide is broadly divided into the following sections:

- Section *1 Introduction to this Guide* defines the purpose of the guide and how information is organized in this guide.
- Section *2 What's New* provides an overview of the new features, starting from the release 9.1.0.5 through release 7.0.
- Section *3 Deprecated Features* provides an overview of the features that are deprecated starting from the release 9.1.0.5 through release 7.0.
- Section *4 Deprecated Releases and Products* provides information about the deprecated releases and products.
- Section *6 New Protectors* describes the new protectors, starting from the release 7.1.

1.2 Accessing the Protegrity documentation suite

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

1.2.1 Viewing product documentation

The **Product Documentation** section under **Resources** is a repository for Protegrity product documentation. The documentation for the latest product release is displayed first. The documentation is available in the HTML format and can be viewed using your browser. You can also view and download the *.pdf* files of the required product documentation.

1. Log in to the *My.Protegrity* portal.
2. Click **Resources** > **Product Documentation**.
3. Click a product version.
   The documentation appears.

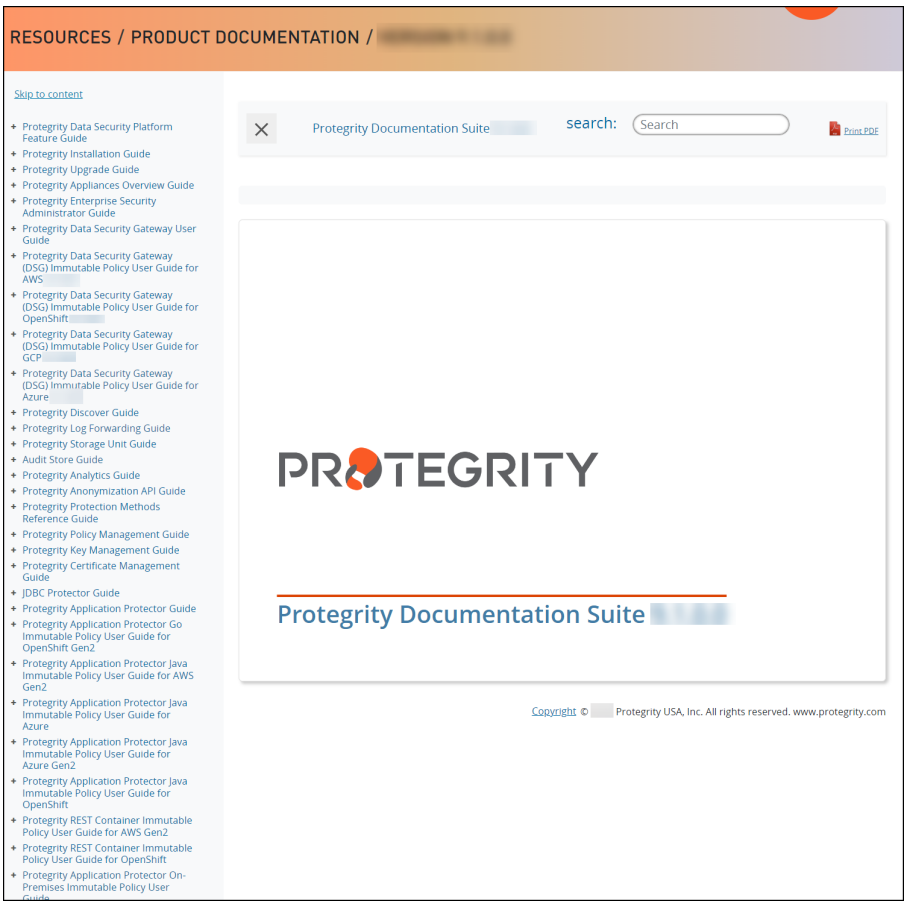

Figure 1-1: Documentation

4. Expand and click the link for the required documentation.
5. If required, then enter text in the **Search** field to search for keywords in the documentation.
   The search is dynamic, and filters results while you type the text.
6. Click the **Print PDF** icon from the upper-right corner of the page.
   The page with links for viewing and downloading the guides appears. You can view and print the guides that you require.

1.2.2 Downloading product documentation

This section explains the procedure to download the product documentation from the *My.Protegrity* portal.

1. Click **Product Management** > **Explore Products**.
2. Select **Product Documentation**.
   The **Explore Products** page is displayed. You can view the product documentation of various Protegrity products as per their releases, containing an overview and other guidelines to use these products at ease.
3. Click **View Products** to advance to the product listing screen.
4. Click the **View** icon ( ) from the **Action** column for the row marked **On-Prem** in the **Target Platform Details** column.
   If you want to filter the list, then use the filters for: **OS**, **Target Platform**, and **Search** fields.
5. Click the icon for the action that you want to perform.

Chapter 2

What's New

This section provides information about the new features that have been added in the Protegrity Data Security Platform releases, starting from the release 9.1.0.5 through release 7.2.0.

The following table lists the features in chronological order, starting from the Release 9.1.0.5 through Release 7.2.0.

Table 2-1: New/Updated Features

New/Updated Feature	Description
9.1.0.5	
Data Security Gateway (DSG) Container Dynamic Policy Update	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 3.1.0.5 The Data Security Gateway (DSG) Container represents a new form factor for the DSG. It is intended to be deployed on Kubernetes running on the Amazon Elastic Kubernetes Service (Amazon EKS) and Azure Kubernetes Service (AKS) environments. This release supports dynamic policy updates from the ESA. • Section ***General Architecture*** in the *Protegrity Data Security Gateway (DSG) Container Dynamic Policy Update User Guide 3.1.0.5*.
9.1.0.2	
Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS) support in Member Source (MBS)	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.1.0.2 Use Active Directory type external source with LDAPS to retrieve information for users and user groups from Active Directory. The LDAPS uses TLS/SSL as a transmission protocol to create secure communication to the directory server. For more information, refer to: • in *Protegrity Policy Management Guide 9.1.0.5*
Azure Active Directory (Azure AD)	**Affected Products:** Appliances **Applicable from Release:** 9.1.0.2 Azure AD allows access to external (Azure portal) and internal resources (corporate appliances). With Azure AD feature you can manage user access to the appliance by importing the required users or groups to the appliance, and assigning specific roles to them. For more information, refer to • *Working with Azure AD* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

New/Updated Feature	Description
Azure Active Directory (Azure AD) Member Source	**Affected Products:** Appliances **Applicable from Release:** 9.1.0.2 Use the Azure AD type external source to retrieve information for users and user groups from an Azure AD, which organizes corporate information on users, machines, and networks in a structural database. For more information, refer to • *Configuring Azure AD Member Source* in the *Protegrity Policy Management Guide 9.1.0.5*
9.1.0.1	
The Amazon S3 tunnel settings have been enhanced to provide the support for connecting the DSG to any endpoint URL other than the Amazon S3 bucket	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.1.0.1 A new parameter, "AWS Endpoint URL", is introduced in the S3 tunnel settings. Using this parameter, the user can configure the S3 tunnel to add any endpoint URL other than the Amazon S3 bucket. It also supports the Google Cloud Storage. If the URL is not specified, then by default the DSG will connect to the Amazon S3 bucket. For more information, refer to • *Amazon S3 Object* in the *Data Security Gateway Guide 3.1.0.1.*
The Amazon S3 tunnel settings have been enhanced to provide the support for specifying the path to the CA bundle.	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.1.0.1 A new parameter, "Path to CA Bundle", is introduced in the S3 tunnel settings. Using this parameter, the user can provide the path to the CA bundle if the endpoint is other than Amazon S3 bucket. If the user has installed the S3 on-premise using the self-signed certificate, then specify that path to the CA bundle in this parameter. For more information, refer to section: • *Amazon S3 Object* in the *Data Security Gateway Guide 3.1.0.1.*
On the DSG Web UI, a new option is added at the rule level to view the Ruleset configuration in the JSON format.	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.1.0.1 When the user uses the Dynamic CoP, in the header you need to pass the Ruleset details in the JSON format. To retrieve the Ruleset details in the JSON format, you can use the option "View Configuration" on a particular rule and click the "Copy" button to copy the data. This copied JSON data can be passed in the header of the Dynamic CoP to protect the sensitive data. For more information, refer to section: • *Table: Ruleset Sub Menu UI Columns* in the *Data Security Gateway Guide 3.1.0.1.*
Support for the Common Internet File System (CIFS) tunnel is added in the DSG with a new implementation	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.1.0.1

New/Updated Feature	Description
	In previous versions of DSG, the file was mounted on the disk. With the new implementation, the file will be mounted in the memory instead of the disk. For more information, refer to section: • *CIFS Tunnel* in the *Data Security Gateway Guide 3.1.0.1.*
The *max_599_retries* parameter is added for the HTTP Gateway Servece	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.1.0.1 The "max_599_retries" parameter is added to the Outbound Transport Settings field of the HTTP Gateway Service. Using this parameter, you can configure the maximum number of retries for the request sent to the server. The minimum value of the parameter is 1 and the maximum value is 5. For more information, refer to section: • *HTTP Gateway* in the *Data Security Gateway Guide 9.1.0.1.*
Enhanced the DSG Transaction metrics logging by supporting new metrics for different operations	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.1.0.1 The DSG Transaction Metrics logging is improved to include http outbound metrics, such as, "http_outbound_response_code", "http_outbound_count_new_connections", "http_outbound_error_details", "http_outbound_time_request", "http_outbound_time_total", and so on for the HTTP service. For more information, refer to section: • *Transaction Metrics Logging* in the *Data Security Gateway Guide 3.1.0.1.*
Added the support for the Error Metrics Logging.	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.1.0.1 Error Metrics allow a user to view details about errors, which are encountered while processing a file. Error metrics logging feature can be enabled at the service level. This metrics is logged in the *gateway.log* file and the "Log Viewer" screen. The errors encountered while processing the CSV or Fixed Width payloads will only be captured in the error metrics. For more information, refer to section: • *Error Metrics Logging* in the *Data Security Gateway Guide 3.1.0.1.*
9.1.0.0	
Support for Azure Storage Blob	**Affected Products:** Application Protector **Applicable from Release:** 9.1.0.0 The Application Protector Java Immutable Policy Container for OpenShift enables you to upload the policy package as an Azure Storage Blob to the Azure Storage Container. For more information about the support for Azure Storage Blob, refer to: • Section in *Protegrity Application Protector Java Immutable Policy User Guide for OpenShift 9.1.0.0*

New/Updated Feature	Description

Application Protector Java Immutable Policy Container for Azure Gen2	**Affected Products:** Application Protector
	
	Applicable from Release: 9.1.0.0
	
	The Application Protector Java Immutable Policy Container represents a new form factor for the Java Application Protector. The Container is intended to be deployed on Kubernetes running on the Azure Kubernetes Service (AKS) environment. The Gen2 release supports the following new features:
	
	• *Support for Immutable Service APIs* - The Immutable Application Protector Java now uses the Immutable Service Export API to create policy packages. As a result, the Get ESA Policy container is no longer required. The Helm charts for deploying the Sample Application container have also been enhanced and updated.
	For more information about the new architecture, refer to:
	  • Section in the *Protegrity Application Protector Java Immutable Policy User Guide for Azure Gen2 9.1.0.0*.
	• *Inclusion of the source file for the Sample Application* - The installation package includes Dockerfile and the source file for the Sample Application, which allows you to build the custom image for the Sample Application container.
	For more information about the support for Dockerfiles, refer to:
	  • Section in the *Protegrity Application Protector Java Immutable Policy User Guide for Azure Gen2 9.1.0.0*.
	• *Removal of Init Container* - The Init container has been deprecated and its functionality has been integrated with the Sample Application container. As a result, the IAP Java deployment now includes only the Sample Application container.
	For more information about the new architecture, refer to:
	  • Section in the *Protegrity Application Protector Java Immutable Policy User Guide for Azure Gen2 9.1.0.0*.

Cloud support (Google Cloud Platform) for external Key stores	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.1.0.0 Protegrity supports the Google Cloud Platform (GCP) Cloud HSM. It can be used to ensure the life cycles of keys work the same as they would on-premise. For more information about the support to Cloud HSM, refer to: • Section in *Key Management Guide 9.1.0.0.*
Parsing users from a DN instead of querying the LDAP server	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.1.0.0 By default, a user is authenticated by parsing the User Login Attribute from the Distinguished Name that has been initially retrieved by the Member Source Service, instead of querying the external LDAP server. This option is applicable only if the Group Member is DN option is enabled while configuring the Member Source. In this case, the members must be listed using their fully qualified name, such as their Distinguished Name. If the ESA is unable to parse the DN or if the DN is not available in the specified format, then the user is authenticated by querying the external LDAP server. For more information about Parsing users from a DN instead of querying the LDAP server, refer to:

New/Updated Feature	Description
	• Section ***Configuring LDAP Member Source*** in *Protegrity Policy Management Guide 9.1.0.0.*
Log Forwarding Guide 9.1.0.0	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.0.0.0 The Log Forwarding Guide replaces the Log Management Guide. This guide covers the information and steps for forwarding logs to an external SIEM. For more information about the Log Forwarding Guide, refer to: • Section in *Protegrity Log Forwarding Guide 9.1.0.5*
Application Protector (AP) Go Immutable Policy Container for OpenShift Gen2 9.1.0.0	**Affected Products:** Application Protector **Applicable from Release:** 9.1.0.0 The Application Protector Go Immutable Policy Container represents a new form factor that is being developed for the Application Protector Go. The Container is intended to be deployed on Kubernetes residing on any of the OpenShift on-premise setup. For more information about the Application Protector Go Immutable Policy Container for OpenShift Gen2, refer to: • Section in *Protegrity Application Protector Go Immutable Policy User Guide for OpenShift Gen2 9.1.0.0*
Extended the second generation of Unicode with a new tokenizer	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.1.0.0 Unicode Gen2 allows you to define and use large alphabets with up to 100000 code points. The new SLT_X_1 tokenizer can only be used to create the data elements for protectors with version 9.1.0.0 and higher. For more information about the SLT_X_1 tokenizer, refer to: • Section in the *Protegrity Protection Methods Reference Guide 9.1.0.0*
Unicode Gen2 Data Element with Extended Alphabet Range	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.1.0.0 The Unicode Gen2 token element creates length-preserved Unicode tokens. It allows you to leverage existing internal alphabets or create custom alphabets by defining code points, thus creating tokens that can be of the same character set as the input data or customized as per requirements. The SLT_X_1 tokenizer supports large alphabets from 161-100K code points and the SLT_1_3 tokenizer supports small alphabets from 10-160K code points. The extended code point range in hex is from U+0020 to U+3FFFF. The Left Right settings have been enabled for the Unicode Gen2 tokenizer type. For more information about Unicode Gen2 token element, refer to: • Section in the *Protegrity Protection Methods Reference Guide 9.1.0.0*

New/Updated Feature	Description
Recursive search	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.1.0.0 When the Recursive Search button is enabled, you can search the active directory recursively. After you upgrade the ESA version, Recursive Search is disabled, by default, for all the existing active directory member sources. For more information about Unicode Base64 token element, refer to: • Section in the *Protegrity Policy Management Guide 9.1.0.0*
Updated the Postgres driver version	**Affected Products:** Appliances **Applicable from Release:**9.1.0.0 Updated the Postgres driver to v32.3.1
AWS Systems Manager	**Affected Products:** Appliances **Applicable from Release:** 9.1.0.0 AWS Systems Manager allows you to manage and operate the infrastructure on AWS. Using the Systems Manager console, you can view operational data from multiple AWS services and automate operational tasks across the AWS services. For more information about the AWS Systems Manager, refer to: • Section in Protegrity Appliances Overview Guide 9.1.0.0
Option to delete multiple certificates on the Web UI	**Affected Products:** Appliances **Applicable from Release:** 9.1.0.0 The Web UI certificate page allows you to select multiple certificates and perform the delete operation. For more information about the Certificate Management, refer to: • Section in Protegrity Certificate Management Guide 8.1.0.0
Updated the OpenSSH version	**Affected Products:** Appliances **Applicable from Release:**9.1.0.0 The OpenSSH is updated to version 8.4p1-2~bpo10+1.
Enhanced readability for Logs	**Affected Products:** Appliances **Applicable from Release:** 9.1.0.0 The information about 'username' and 'IP address' is added in the logs for various operations.
Transaction Metrics	**Affected Products:** Data Security Gateway (DSG)

New/Updated Feature	Description
	Applicable from Release: 9.1.0.0 Added new transaction metrics for different protocols • Section ***12 Transaction Metrics Logging*** in Data Security Gateway Guide 3.1.0.0
Max 599 retries	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.1.0.0 The "max_599_retries" parameter is added to the Outbound Transport Settings field of the HTTP Gateway Service. Using this parameter, you can configure the maximum number of retries for the request sent to the server. The minimum value of the parameter is 1 and the maximum value is 5. • Section ***15.1.3 HTTP Gateway*** in Data Security Gateway Guide 3.1.0.0
9.0.0.0	
Protegrity Discover	**Affected Products:** Protegrity Discover **Applicable from Release:** 9.1.0.5 Protegrity Discover 3.0.2.0 supports the following features: • Support for NLP spaCy Tokenization You can update the *tokenizer_config* parameter, which is found in the *classifiers.json* file, to specify the delimiters that can be used to split the input data into individual tokens that can be processed by the spaCy module. For more information about the *tokenizer_config* parameter, refer to: • Section ***6.4.2.1.7 Updating the Spacy Patterns Tab*** in *Protegrity Discover Guide 3.0.2.0* • Support for Additional File Metadata The *file_metadata* attribute displays the metadata related to the files, such as, file type, date created, file size, and date modified. For more information about the additional file metadata, refer to: • Section ***Appendix J File Metadata Collected in Filestores*** in *Protegrity Discover Guide 3.0.2.0* • Support for Classification using Metadata You can now classify the metadata using datastore coordinates and file metadata. You can also test the metadata expressions that have been specified in the **Metadata** tab using the **Test Metadata JSON** area in the **Testbed** tab. For more information about classifying the metadata, refer to: • Section ***6.4.2.1.2 Updating the Metadata Tab*** in *Protegrity Discover Guide 3.0.2.0* • Section ***6.4.2.1.8 Testing the Classifier*** in *Protegrity Discover Guide 3.0.2.0* • Support for retrieving the Data Elements from the ESA You can integrate Protegrity Discover with the ESA, which allows you to associate the data elements configured in the ESA with the classifiers. For more information about retrieving the data elements from the ESA, refer to:

New/Updated Feature	Description
	• Section ***Section 6.8 Retrieving ESA Data Elements*** in *Protegrity Discover Guide 3.0.2.0* • Support for IAM Role You can scan the AWS S3 buckets using the **IAM Role (Instance profile)** authentication method. For more information about support for IAP roles, refer to: • Section ***Section 6.4.1.1 Creating a Discover Job*** in *Protegrity Discover Guide 3.0.2.0* • Section ***Appendix C Scan Job Advanced Configuration Settings*** in *Protegrity Discover Guide 3.0.2.0* • Support for Azure Blob Storage Protegrity Discover can now scan data within the Azure Blob Storage. For more information about support for Azure Blob Storage, refer to: • Section ***Chapter 3 System Architecture*** in *Protegrity Discover Guide 3.0.2.0* • Support for SSL-Enabled Hive Cluster Protegrity Discover can now scan data within an SSL-enabled Hive server. For more information about support for SSL-Enabled Hive Cluster, refer to: • Section ***Section 5.1.2.1 Adding a New Datastore*** in *Protegrity Discover Guide 3.0.2.0* • View a list of all the scans in the **Scan Results** tab The **Scan Results** screen enables you to view a list of all the scans that you have performed. For more information about the **Scan Results** screen, refer to: • Section ***Section 6.3 Scan Results*** in *Protegrity Discover Guide 3.0.2.0* • Migrate data from Version 3.0.0.0 to 3.0.2.0 You can migrate the Protegrity Discover data, such as, the repository and classifier data, from version 3.0.0.0 to 3.0.2.0. For more information about migrating data from version 3.0.0.0 to 3.0.2.0, refer to: • Section ***Section 4.4 Migrating Protegrity Discover Data from Version 3.0.0.0 to 3.0.2.0*** in *Protegrity Discover Guide 3.0.2.0* • Version 2 of the Protegrity Discover REST APIs A new version of the Protegrity Discover REST APIs has been released. The response body shows a list of classifiers. The classification records are grouped under the respective classifier. For more information about version 2 of the Protegrity Discover REST APIs, refer to: • Section ***Chapter 11 Protegrity Discover REST APIs*** in *Protegrity Discover Guide 3.0.2.0* • Scanning of Apache Avro files Protegrity Discover allows you to scan Apache Avro files. For more information about the supported file formats, refer to: • Section ***Appendix D: Supported File Formats*** in *Protegrity Discover Guide 3.0.2.0*

New/Updated Feature	Description
	• Improved Kerberos configuration Protegrity Discover has been enhanced to simplify the process of requesting a Kerberos ticket. In addition, you can periodically run a Discover job that requires Kerberos authentication. For more information about the improved Kerberos configuration, refer to: • Section ***Section 7.5.1 Kerberos Configuration Manager*** in *Protegrity Discover Guide 3.0.2.0*
Log Forwarding Guide 9.0.0.0	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.0.0.0 The Log Forwarding Guide replaces the Log Management Guide. This guide covers the information and steps for forwarding the logs to an external SIEM. For more information about the Log Forwarding Guide, refer to: • Section ***Introduction to Logging*** in *Protegrity Log Forwarding Guide 9.1.0.5*
CoP export API for only Containers	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.0.0.0 The DSG configurations can be exported through an API. The CoP export API will extract the required directories and files and create a *CoP* package. This CoP package can be only used in the containers to import the DSG configurations. For more information about exporting the CoP package through an API, refer to: • Section ***Appendix H: API for Exporting CoP*** in the *Data Security Gateway User Guide 3.0.0.0.*
Sub-clustering for the DSG nodes in the cluster	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.0.0.0 The sub-clustering feature will allow the user to group the DSG nodes in the cluster. A node group can be associated with each DSG node in the cluster. The user can push the configurations to a specific node group, which will be associated with a set of DSG nodes in the cluster. For more information about sub-clustering, refer to: • Section ***11 Overview of Sub-Clustering*** in the *Data Security Gateway User Guide 3.0.0.0.*
Python version is upgraded from v2.7 to v3.10	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 9.0.0.0 The Python version used in the DSG has been upgraded from v2.7 to v3.10. The UDFs written in Python v2.7 will not be compatible with Python v3.10. For more information about migrating the UDFs from python 2.7 to python 3.10, refer to: • Section ***24 Appendix I: Migrating the UDFs to Python 3*** in the *Data Security Gateway User Guide 3.0.0.0.*

New/Updated Feature	Description
Immutable Policy REST Container for AWS Gen2	**Affected Products:** Application Protector **Applicable from Release:** 9.0.0.0 The Immutable Policy REST Container represents a new form factor for the Application Protector REST. The Container is intended to be deployed on Kubernetes running on the Amazon Elastic Kubernetes Service (Amazon EKS) environment. The Gen2 release supports the following new features: • *Support for Immutable Service APIs* - The REST Container now uses the Immutable Service Export API to create policy packages. As a result, the Get ESA Policy container is no longer required. The Helm charts for deploying the AP-REST container have also been enhanced and updated. For more information about the new architecture, refer to: ◦ Section ***Architecture and Components*** in the *Protegrity REST Container Immutable Policy User Guide for AWS Gen2 9.1.0.0*. • *Inclusion of the Dockerfile for the AP-REST Container* - The installation package includes Dockerfile, which allows you to build the custom image for the AP-REST container. For more information about the support for Dockerfiles, refer to: ◦ Section ***Appendix D: Using the Dockerfile to Build Custom Images*** in the *Protegrity REST Container Immutable Policy User Guide for AWS Gen2 9.1.0.0*. • *Removal of Init Container* - The Init container has been deprecated and its functionality has been integrated with the AP-REST container. As a result, the AP-REST deployment now includes only the AP-REST container. For more information about the new architecture, refer to: ◦ Section ***Architecture and Components*** in the *Protegrity REST Container Immutable Policy User Guide for AWS Gen2 9.1.0.0*. • *Support for OAuth Authentication* - The REST container supports the use of OAuth authentication functionality, which enables you to authenticate the REST API requests sent from the client application to the REST container. For more information about the OAuth authentication functionality, refer to: ◦ Section ***Enabling the Authentication Functionality*** in the *Protegrity REST Container Immutable Policy User Guide for AWS Gen2 9.1.0.0*.
Application Protector (AP) Golang	**Affected Products:** Application Protector **Applicable from Release:** 9.0.0.0 Application Protector Golang (AP Go) is an API that integrates with the client application or user using a common interface to protect data, regardless of where and how the processing is done in the backend. **Note:** The AP Go protector has been released with limited functionality and limited availability for the *9.0.0.0* release. This will be enhanced in future releases and would be available on the *MyProtegrity* portal. For more information about AP Go, refer to: • Section ***Application Protector Golang*** in the *Protegrity Application Protector Guide 9.0.0.0*

New/Updated Feature	Description
Application Protector (AP) On-Premises Immutable Policy	**Affected Products:** Application Protector **Applicable from Release:** 9.0.0.0 Immutable Application Protector (IAP) On-premises solution for Java, C, Python, Golang. It enables you to protect the sensitive data present on various on-premise systems without the need to be connected to the administrator system. For more information about the architecture of the IAP On-premises protector, refer to: • Section ***Architecture and Components*** in the *Protegrity Application Protector On-Premises Immutable Policy 9.0.0.0 User Guide*
Application Protector Java Immutable Policy Container for AWS EC2 Gen2	**Affected Products:** Application Protector **Applicable from Release:** 9.0.0.0 The Immutable Java Application Protector for AWS EC2 represents a new form factor for the Java Application Protector. The Protector is intended to be deployed on an AWS EC2 instance using AWS CloudFormation Templates. The Gen2 release supports the following new features: • *Support for Immutable Service APIs* - The Immutable Application Protector Java now uses the Immutable Service Export API to create policy packages. As a result, the Get ESA Policy CloudFormation Template is no longer required. The CloudFormation Template for deploying the Sample Application have also been enhanced and updated. For more information about the new architecture, refer to: • Section ***Architecture and Components*** in the *Protegrity Application Protector Java Immutable Policy User Guide for AWS EC2 Gen2 9.1.0.0*.
Application Protector Java Immutable Policy Container for AWS Gen2	**Affected Products:** Application Protector **Applicable from Release:** 9.0.0.0 The Application Protector Java Immutable Policy Container represents a new form factor for the Java Application Protector. The Container is intended to be deployed on Kubernetes running on the Amazon Elastic Kubernetes Service (Amazon EKS) environment. The Gen2 release supports the following new features: • *Support for Immutable Service APIs* - The Immutable Application Protector Java now uses the Immutable Service Export API to create policy packages. As a result, the Get ESA Policy container is no longer required. The Helm charts for deploying the Sample Application container have also been enhanced and updated. For more information about the new architecture, refer to: • Section ***Architecture and Components*** in the *Protegrity Application Protector Java Immutable Policy User Guide for AWS Gen2 9.1.0.0*. • *Inclusion of the source file for the Sample Application* - The installation package includes Dockerfile and the source file for the Sample Application, which allows you to build the custom image for the Sample Application container. For more information about the support for Dockerfiles, refer to: • Section ***Appendix D: Using the Dockerfile to Build Custom Images*** in the *Protegrity Application Protector Java Immutable Policy User Guide for AWS Gen2 9.1.0.0*. • *Removal of Init Container* - The Init container has been deprecated and its functionality has been integrated with the Sample Application container. As a result, the IAP Java deployment now includes only the Sample Application container.

New/Updated Feature	Description
	For more information about the new architecture, refer to: • Section ***Architecture and Components*** in the *Protegrity Application Protector Java Immutable Policy User Guide for AWS Gen2 9.1.0.0*.
Audit Store uses Elasticsearch version 7.10.2	**Affected Products:** Appliances **Applicable from Release:** 9.0.0.0 The Audit Store is upgraded to use Elasticsearch version 7.10.2.
Migration utility for configurations and logs	**Affected Products:** Appliances and Protectors **Applicable from Release:** 9.0.0.0 The CLI Manager includes migration tools for migrating the configurations and log. A clean-up tool is also included for removing the temporary indexes created after performing the migration. For more information about the tools, refer to: • Section ***Analytics Migration Tools*** in the *Protegrity Data Security Platform Upgrade Guide Release 9.0.0.0.*
8.1.0.1	
Data Security Gateway 2.6.0.1 Patch Release	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 8.1.0.1 The Protegrity Data Security Gateway v2.6.0.1 can be upgraded from an earlier DSG release to DSG v2.6.0.1 using a patch. For more information about upgrading the Data Security Gateway (DSG), refer to: • Section ***9 Upgrading to DSG v2.6.0.1*** in the *Data Security Gateway User Guide 2.6.0.1*
SNMPTRAPD	**Affected Products:** Appliances **Applicable from Release:** 8.1.0.1 The snmptrapd is a service that sends messages to the manager in the form of traps. The SNMP traps are alert messages that are configured in the manager in such a way that an event occurring at the client immediately triggers a report to the manager. For more information about the Immutable Service API, refer to: • Section ***Configuring SNMP*** in the *Appliances Overview Guide 8.1.0.1.*
Immutable Service API	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.1.0.1 The Immutable Service API enables you to export the immutable policy from the API so that it can be used by Immutable Gen 2 protectors. For more information about the Immutable Service API, refer to:

New/Updated Feature	Description
	• Section ***Appendix B: APIs for Immutable Protectors*** in the *Protegrity APIs, UDFs, and Commands Reference Guide 8.1.0.1.* For more information about the installing the Immutable Service patch, refer to: • Section ***Appendix B: Installing the Immutable Service on the ESA to Export Policy for Immutable Protectors in the*** in the *Protegrity Installation Guide 8.1.0.1.*
Signature Verification	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.1.0.1 Signature Verification is introduced in Protegrity Analytics to verify the integrity of logs from Protectors v8.1.0.0 and above. For more information about signature verification, refer to: • Section ***Verifying Signatures*** in the *Protegrity Analytics Guide 8.1.0.1* • Section ***Creating a Scheduled Task*** in the *Protegrity Analytics Guide 8.1.0.1* • Section ***Alert for Signature Verification Failures*** in the *Protegrity Analytics Guide 8.1.0.1*
8.1.0.0	
Support for Spark SQL Encryption UDFs	**Affected Products:** Big Data Protector **Applicable from Release:** 8.1.0.0 Starting from the BDP 8.1.0.0 release, support for Encryption UDFs has been added for the Spark SQL protector. The Protegrity Spark SQL Encryption UDFs provide functions that encrypt, decrypt, and re-encrypt the data. For more information on the Spark SQL Encryption UDFs, refer to: • Section *ptyStringEnc() ptyStringEnc()* in the *APIs UDFs and Commands Reference Guide 8.1.0.0* • Section *ptyStringDec() ptyStringDec()* in the *APIs UDFs and Commands Reference Guide 8.1.0.0* • Section *ptyStringReEnc() ptyStringReEnc()* in the *APIs UDFs and Commands Reference Guide 8.1.0.0*
Big Data Protector 8.1.0.0 support for CDP Private Cloud Base (CDP-PVC-Base), version 7.1 environment	**Affected Products:** Big Data Protector **Applicable from Release:** 8.1.0.0 Starting from v8.1.0.0, the Big Data Protector supports CDP Private Cloud Base (CDP-PVC-Base), version 7.1 environment. For more information about installing the Big Data Protector from Cloudera Manager, refer to: • Section ***Installing Big Data Protector using CDP Private Cloud Base (CDP-PVC-Base) Native Installer*** in the *Protegrity Installation Guide Release 8.1.0.0*. For more information about configuring the Big Data Protector, refer to: • Section ***Setting the BDP Configuration for CDP-DC Distribution*** in the *Protegrity Big Data Protector Guide Release 8.1.0.0*.

New/Updated Feature	Description
XML with Tree-of-Trees (ToT) codec	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 8.1.0.0 Starting from the DSG 2.6.0.0 release, the XML with Tree-of-Trees (ToT) codec can be used to extract and transform multiple XML element in one extract rule. For more information about the XML with ToT codec, refer to: • Section ***13.3.1.2.7 XML with Tree-of-Trees (ToT) Payload*** in the *Data Security Gateway User Guide 2.6.0.0*
WebSocket Secure (WSS) Service	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 8.1.0.0 The WebSocket Secure (WSS) service is introduced in the DSG 2.6.0.0 release. You can use the WSS service to pass through data as-is. The WSS is a communication protocol that provides bi-directional communication between a client and a server over a single established connection. For more information about the WSS service, refer to: • Section ***13.1.4 WebSocket Secure (WSS) Gateway*** in the *Data Security Gateway User Guide 2.6.0.0*
Log Forwarder for Protectors to forward logs to the Audit Store in PSU	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.1.0.0 The Log Forwarder component on Protectors 8.1.0.0 is configured to forward audit logs to the Audit Store in the PSU. For more information about the Log Forwarder, refer to: • Section ***13.2 Installing the Log Forwarder on Protectors*** in the *Data Security Gateway User Guide 2.6.0.0* • Section ***2.1 Logging Architecture*** in the *Protegrity Log Management Guide 8.1.0.0*
Unicode Gen2 Data Element	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.1.0.0 The Unicode Gen2 token element creates length-preserved Unicode tokens. It allows you to leverage existing internal alphabets or create custom alphabets by defining code points, thus creating tokens that can be of the same character set as the input data or customized as per requirement. For more information about the Unicode Gen2 data element, refer to: • Section ***Unicode Gen2*** in the *Protegrity Protection Methods Reference Guide 8.1.0.0*
Monitor Data Element	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.1.0.0

New/Updated Feature	Description
	The Monitor data element is generally used for auditing. As an organization, if you plan to monitor and assess users that are trying to access the data, you must opt for the Monitor data method. For more information about the Monitor data element, refer to: • Section ***Monitor*** in the *Protegrity Protection Methods Reference Guide 8.1.0.0*
Masking Data Element	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.1.0.0 As an organization, if you plan to restrict access such that only users with required privileges can view sensitive data, while other users view masked data, the Masking data element can be used. For more information about the Masking data element, refer to: • Section ***Masking*** in the *Protegrity Protection Methods Reference Guide 8.1.0.0*
Unicode Base64 Token Element	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.1.0.0 The Unicode Base64 token element provides enhanced performance when tokenizing Unicode data in comparison to the Unicode token element. This token element uses Base64 encoding instead of Base62 encoding resulting in better performance but with three additional characters, namely *+*, */*, and *=*. For more information about Unicode Base64 token element, refer to: • Section ***Unicode Base64*** in the *Protegrity Protection Methods Reference Guide 8.1.0.0*
Auto rollover of audit indices	**Affected Products:** Appliances **Applicable from Release:** 8.1.0.0 The *Rollover Index* task has been added to the scheduler in Analytics. This task automatically rotates indices to reduce the size of individual indices. For more information about the Rollover Index task, refer to: • Section ***Creating a Scheduled Task*** in the *Protegrity Analytics Guide 8.1.0.0*
Role management for the Audit Store cluster nodes	**Affected Products:** Appliances **Applicable from Release:** 8.1.0.0 The roles for the appliances in the Audit Store cluster can be set to Master, Data, and Ingest as required. This helps balance the load on the Appliance for processing logs. For more information about role management, refer to: • Section ***Working with Roles*** in the *Audit Store Guide 8.1.0.0*
Log forwarding capability to external SIEM software	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.1.0.0

New/Updated Feature	Description
	The logs generated on an Appliance or Protector can now be forwarded to an external database. This allows you to use your own database with Protegrity software for logging and analytics. The auditing capabilities provided by Protegrity Analytics depends on the database configuration. For more information about using an external database, refer to: • Section ***Sending Logs to an External Location*** in the *Protegrity Log Management Guide 8.1.0.0*
Configuring security for the Log Forwarder	**Affected Products:** Protectors **Applicable from Release:** 8.1.0.0 The authentication for the *Log Forwarder* present on the Protector can be configured for sending logs to the Audit Store. By default, *Anonymous* authentication is set up on the Protector for forwarding logs to the Audit Store. You can customize the authentication to use *Basic Authentication* or *Certificate Authentication*. For more information about using an external database, refer to: • Section ***Configuring Security for the Log Forwarder*** in the *Audit Store Guide 8.1.0.0*
8.0.0.0	
Protegrity Discover	**Affected Products:** Protegrity Discover **Applicable from Release:** 8.0.0.0 Protegrity Discover 3.0.0.0 supports the following features: • Scanning of MySQL and PostgreSQL databases For more information about the supported databases, refer to: • Section ***5 Capabilities and Support*** in *Protegrity Discover Guide 3.0.0.0* • Packaging the ODBC driver file for the EXAsol database For more information about the packaged driver files, refer to: • Section ***5 Capabilities and Support*** in *Protegrity Discover Guide 3.0.0.0* • Scanning of files that are stored on the Hadoop File Distributed System (HDFS) For more information about the support for HDFS, refer to: • Section ***3 System Architecture*** in *Protegrity Discover Guide 3.0.0.0* • Section ***5 Capabilities and Support*** in *Protegrity Discover Guide 3.0.0.0* • Section ***Appendix C: Scan Job Advanced Configuration Settings*** in *Protegrity Discover Guide 3.0.0.0* • Scanning of Apache Parquet files For more information about the supported file formats, refer to: • Section ***Appendix D: Supported File Formats*** in *Protegrity Discover Guide 3.0.0.0* • Exporting and importing of classifiers For more information about exporting and importing of classifiers, refer to: • Section ***6.3.2.3 Exporting Classifiers*** in *Protegrity Discover Guide 3.0.0.0*

New/Updated Feature	Description
	• Section ***6.3.2.4 Importing Classifiers*** in *Protegrity Discover Guide 3.0.0.0* • Configuring the size of the input data that can be processed by the spaCy module For more information about configuring the size of the input data, refer to: • Section ***6.7 Managing the Appliance Information*** in *Protegrity Discover Guide 3.0.0.0* • Retrieving the data from a database table randomly, instead of only sequentially For more information about retrieving the data from a database table randomly, refer to: • Section ***Appendix C: Scan Job Advanced Configuration Settings*** in *Protegrity Discover Guide 3.0.0.0* • Deploying the product on Google Cloud Platform (GCP) and Azure For more information about deploying the product on GCP and Azure, refer to: • Section ***4.3 Installing Protegrity Discover on Cloud Platforms*** in *Protegrity Discover Guide 3.0.0.0* • Using third-party applications, such as, CyberArk, to store the password of the datastore that you want to scan For more information about integrating Protegrity Discover with CyberArk, refer to: • Section ***Appendix H: Integrating Protegrity Discover with CyberArk*** in *Protegrity Discover Guide 3.0.0.0* • Scanning of data using REST APIs For more information about using REST APIs, refer to: • Section ***6.4.2 Viewing REST API Logs*** in *Protegrity Discover Guide 3.0.0.0* • Section ***6.4.3 Viewing REST API Analytics*** in *Protegrity Discover Guide 3.0.0.0* • Section ***Appendix G: Understanding Protegrity Discover-specific Permissions*** in *Protegrity Discover Guide 3.0.0.0* • Section ***Appendix I: Using Protegrity Discover REST APIs*** in *Protegrity Discover Guide 3.0.0.0* • Using the webhook functionality For more information about using webhooks, refer to: • Section ***Appendix J: Using Webhooks*** in *Protegrity Discover Guide 3.0.0.0*
Protegrity Storage Unit	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.0.0.0 The Protegrity Storage Unit is an appliance for scaling the Audit Store cluster. For more information about the Protegrity Storage Unit, refer to: • Section ***Working with the Protegrity Storage Unit*** in the *Protegrity Storage Unit Guide 8.0.0.0.*
Log handling	**Affected Products:** Appliances and pre-8.0.0.0 Protectors **Applicable from Release:** 8.0.0.0

New/Updated Feature	Description
	The logging system is enhanced and provides better log handling and management. Logs received by the Appliance are forwarded to the Audit Store. For more information about log handling, refer to: • Section ***Introduction to Logging*** in the *Protegrity Log Management Guide 8.0.0.0*
Audit Store	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.0.0.0 The Audit Store is a repository of all the logs generated by Appliances and Protectors. In addition to storing logs, it provides the capability for searching and retrieving logs quickly. For more information about the Audit Store, refer to: • Section ***Introduction to the Audit Store*** in the *Audit Store Guide 8.0.0.0.*
Protegrity Analytics	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.0.0.0 Prtoegrity Analytics reads and displays audit data from the Audit Store. Analyze the audit data in Analytics using reports, graphs, and alerts. For more information about Protegrity Analytics, refer to: • Section ***Introduction to Insight Analytics*** in the *Protegrity Analytics Guide 8.0.0.0*
Certificates added for Audit Store clustering	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.0.0.0 Certificates are added for secure communication between the Appliance and the Audit Store and for communication between the Audit Store nodes. For more information about the Audit Store certificates, refer to: • Section ***7. Certificates in PLUG*** in the *Certificate Management Guide 8.0.0.0*
Case-preserving and Position-preserving Tokenization	**Affected Products:** Appliances, AP Java Protector on a Linux platform, Teradata Database Protector, Oracle Database Protector on RHEL platform, and Big Data Protector on a Cloudera distribution **Applicable from Release:** 8.0.0.0 If you are working with the *Alpha-Numeric (0-9, a-z, A-Z)* token type and the *SLT_2_3* tokenizer, then you can specify additional tokenization options for case-preservation and position-preservation. For more information about the case-preserving and position-preserving tokenization options, refer to: • Section ***3.3.7 Case-preserving and Position-preserving Tokenization*** in the *Protection Methods Reference Guide 8.0.0.0*

New/Updated Feature	Description
	• Section ***4.1.1.1 Creating a Case-Preserving and Position-Preserving Data Element*** in the *Policy Management Guide 8.0.0.0.*
DevOps API deployment updates	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.0.0.0 The DevOps API specification is improved to enable the following operations: • Deployment of a specific policy or trusted application to a data store • Deployment of one data store • Ability to access the existing API and the new API solutions to support backward compatibility The additional deploy operations are provided to support deployment of a specific data store or multiple data stores. For more information about the DevOps API deployment updates, refer to: • Section ***Appendix A: DevOps REST APIs*** in the *APIs, UDFs, and Commands Reference Guide 8.0.0.0*
Logfacade and Logfacade Legacy services	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.0.0.0 The Logfacade and Logfacade Legacy services receive audits from the protectors and send it to the Audit Store, which is then used by the Protegrity Analytics. For more information about the Logfacade and Logfacade Legacy services, refer to: • Section ***5.7.1 Services*** in the *Appliances Overview Guide 8.0.0.0*
Meteringfacade service	**Affected Products:** Appliances and Protectors **Applicable from Release:** 8.0.0.0 The Meteringfacade service collects the total count of successful protect, unprotect, and reprotect operations from the connected protectors. The total count is then sent at periodic intervals, which is 20 minutes as configured in the *pepserver.cfg* configuration file, to the Audit Store for further analysis. For more information about the Meteringfacade service, refer to: • Section ***5.7.1 Services*** in the *Appliances Overview Guide 8.0.0.0*
Single Sign-On for Appliances	**Affected Products:** Appliances **Applicable from Release:** 8.0.0.0 Single Sign-on (SSO) is a feature that enables users to authenticate multiple applications by logging in to a system only once. On the Protegrity appliances, you can utilize the Kerberos SSO mechanism to login to the appliance. The users log in to the system with their domain credentials for accessing the appliances, such as, the ESA or DSG. For more information about the SSO service, refer to:

New/Updated Feature	Description
	• Section ***18 Accessing Appliances using Single Sign-On (SSO)*** in the *Appliances Overview Guide 8.0.0.0*
GRand Unified Boot (GRUB2) Loader	**Affected Products:** Appliances **Applicable from Release:** 8.0.0.0 In the Protegrity appliances, GRUB version 2 (GRUB2) is used for loading the kernel. The GRUB menu can be protected by setting a username and password. For more information about the GRUB service, refer to: • Section ***4.4.7 Securing the GRand Unified Bootloader (GRUB*** in the *Appliances Overview Guide 8.0.0.0*
Azure Cloud Utility	**Affected Products:** Appliances **Applicable from Release:** 8.0.0.0 The Azure Cloud Utility is an appliance component that is available for supporting features specific to the Azure Cloud Platform. For Protegrity appliances, this component must be installed to utilize the services of Azure Accelerated Networking and Azure Linux VM agent. When you upgrade or install the appliance from an Azure v8.0 image, the Azure Cloud Utility is installed automatically on the appliance. For more information about the Azure Cloud Utility, refer to: • Section ***16.2 Azure Cloud Utility*** in the *Appliances Overview Guide 8.0.0.0*
Mandatory Access Control	**Affected Products:** Appliances **Applicable from Release:** 8.0.0.0 Mandatory Access Control (MAC) is a security approach that allows or denies an individual to access resources on a system. Among many implementations of MAC, Application Armor (AppArmor) is a security module that protects the operating system and its applications from threats. On the Protegrity appliances, AppArmor is enabled to protect the different OS features, such as, antivirus, trusted appliances cluster, proxy authentication, and so on. For more information about the AppArmor, refer to: • Section ***18 Mandatory Access Control (MAC) in the Appliances Overview Guide*** in the *Appliances Overview Guide 8.0.0.0*
Auditing Service	**Affected Products:** Appliances **Applicable from Release:** 8.0.0.0 The Linux Auditing System is a tool/utility that allows to monitor events occurring in a system. It is integrated with the kernel to monitor the system operations. For more information about the AppArmor, refer to: • Section ***4.3.4 Auditing Service*** in the *Appliances Overview Guide 8.0.0.0*
7.2.1	

New/Updated Feature	Description
Application Protector (AP) Python	**Affected Products:** Application Protector **Applicable from Release:** 7.2.1 Starting from version 7.2.1, a new protector, AP Python, has been provided. AP Python provides native APIs that can be utilized with Python to protect, unprotect, or reprotect the data as it is stored or retrieved. For more information about Application Protector (AP) Python, refer to: • Section ***Application Protector (AP) Python*** in the *Application Protector Guide 7.2.1.* For more information about installing Application Protector (AP) Python, refer to: • Section ***Installing Application Protector (AP) Python*** in the *Installation Guide 7.2.1.*
Data Security Gateway 2.4.1 ISO, Patch, and Cloud Releases	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.2.1 The Protegrity Data Security Gateway v2.4.1 can be installed as a node using an ISO, upgraded from an earlier DSG release using a patch, or can be installed on cloud platforms namely, Azure, AWS, and GCP. For more information about installing the Data Security Gateway (DSG), refer to: • Section ***8.1 Installing the DSG On-Premise*** in the *Data Security Gateway User Guide 2.4.1* • Section ***9 Upgrading to DSG v2.4.1*** in the *Data Security Gateway User Guide 2.4.1* • Section ***8.2.3 Installing the Data Security Gateway (DSG) on Microsoft Azure*** in the *Data Security Gateway User Guide 2.4.1* • Section ***8.2.1 Installing Data Security Gateway (DSG) on Amazon Web Services (AWS)*** in the *Data Security Gateway User Guide 2.4.1* • Section ***8.2.2 Installing the Data Security Gateway (DSG) on Google Cloud Platform (GCP)*** in the *Data Security Gateway User Guide 2.4.1*
JSON with Tree-of-Trees (ToT)	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.2.1 Starting from the DSG 2.4.1 release, the JSON ToT payload allows you to use the advantages offered by *Tree-of-Trees* to extract the JSON payload from the request and provide protection according to the data element defined. For more information about using JSON with Tree-of-Trees (ToT), refer to: • Section ***13.3.1.2.11 JSON with Tree-of-Trees (ToT)*** in the *Data Security Gateway User Guide 2.4.1*
Support for Futurex HSM	**Affected Products:** Appliances **Applicable from Release:** 7.2.1 The procedure to configure the Futurex HSM client version 4.20 for Debian 9 with OpenSSL version 1.0.2 is provided in the *Key Management Guide 7.2.1*. For more information about switching from Soft HSM to Futurex HSM, refer to:

New/Updated Feature	Description
	• Section ***7.2.2 Switching from Soft HSM to Futurex HSM*** in the *Key Management Guide 7.2.1*
Data Security Gateway ISO and Cloud Releases	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.2.1 The Protegrity Data Security Gateway v2.4.0 can be installed as a node using an ISO or can be installed on cloud platforms namely, AWS, GCP, and Azure. For more information about installing the Data Security Gateway (DSG), refer to: • Section ***8.1 Installing the DSG On-Premise*** in the *Data Security Gateway User Guide 2.4.0* • Section ***8.2.1 Installing Data Security Gateway (DSG) on Amazon Web Services (AWS)*** in the *Data Security Gateway User Guide 2.4.0* • Section ***8.2.2 Installing the Data Security Gateway (DSG) on Google Cloud Platform (GCP)*** in the *Data Security Gateway User Guide 2.4.0* • Section ***8.2.3 Installing the Data Security Gateway (DSG) on Microsoft Azure*** in the *Data Security Gateway User Guide 2.4.0*
Big Data Protector with CDH and Cloudera Manager 6.3	**Affected Products:** Big Data Protector **Applicable from Release:** 7.2.1 The Big Data Protector 7.2.1 is certified with the CDH and Cloudera Manager, version 6.3. For more information about installing Big Data Protector 7.2.1 using the CDH Native Installer, refer to: • Section ***Installing Big Data Protector using CDH Native Installer*** in the *Installation Guide 7.2.1* • Section ***Upgrading Big Data Protector using CDH Native Installer*** in the *Upgrade Guide 7.2.1*
Teradata Database Protector version 16.20	**Affected Products:** Teradata Database Protector **Applicable from Release:** 7.2.1 The Teradata Database Protector version 16.20 is certified for the 7.2.1 release. For more information about installing the Teradata Database Protector version 16.20 for the 7.2.1 release, refer to: • Section ***Installing and Uninstalling Teradata Database Protector*** in the *Installation Guide 7.2.1*
AWS Cloud Utility Product	**Affected Products:** Appliance Framework **Applicable from Release:** 7.2.1 The AWS Cloud Utility is a cloud-based utitlities are services that handle the computing and processing of data on the cloud. Local applications interact with the cloud services for various purposes, such as, data storage, data computing, and so on. AWS offers a variety of cloud-based utilities for computing, storage, analytics, networking, and management. Protegrity appliances leverage the the AWS cloud utilities for storing logs and metrics. The following AWS utilities are included for the appliances:

New/Updated Feature	Description
	• AWS CloudWatch for collecting logs and metrics from appliances and storing them on AWS • Key Management System (KMS) Encrypting and decrypting data • AWS CLI for configuring and managing AWS services For more information about the AWS Cloud Utility Product, refer to: • Section ***Working with Cloud-based Applications*** in the *Appliance Overview Guide 7.2.1*
Rotation of default passwords	**Affected Products:** Appliance Framework **Applicable from Release:** 7.2.1 Rotation of default passwords: For appliance images that are delivered on cloud platforms, the users, such as, root, admin, local_admin, and viewer, are provided with a default set of passwords. When you run the appliance OS keys rotation process, a screen to change the passwords for the default users appears. It is recommended to change the passwords for the users to enhance the security of the appliance. For more information about the rotation of default passwords, refer to: • Section ***Rotate Appliance OS Keys*** in the *Appliance Overview Guide 7.2.1*
Codebook Re-shuffling	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.2.1 Starting from DSG 2.4.0, the Codebook Re-shuffling feature can be used for generating unique tokens for protected values across different DSG nodes. Codebook Re-shuffling support has been enhanced to support all tokenization data elements as listed: • Alpha (a-z, A-Z) • Alpha-Numeric (0-9, a-z, A-Z) • Binary • Credit Card (0-9) • Date (YYYY-MM-DD) • Date (DD/MM/YYYY) • Date (MM/DD/YYYY) • DateTime Date (YYYY-MM-DD HH:MM:SS MMM) • Decimal (numeric with decimal point and sign) • Email • Integer • Lower ASCII (Lower part of ASCII table) • Numeric (0-9) • Printable • Uppercase Alpha (A-Z) • Uppercase Alpha-Numeric (0-9, A-Z) • Unicode For more information about the Codebook Re-shuffling feature, refer to: • Section ***Codebook Re-shuffling*** in the *Data Security Gateway Guide 2.4.0*

New/Updated Feature	Description
Minimize Output option in JSON codec	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.2.1 The DSG sends an indented JSON response as a default when using the JSON codec. If in cases where the DSG Ruleset is deeply nested, the *Minimize Output* option can be used to reduce CPU overhead. For more information about the *Minimize Output* field, refer to: • Section ***JSON Payload*** in the *Data Security Gateway User Guide 2.4.0*
Enhanced Learn Mode Log Cleanup scheduled task	**Affected Products:** Data Security Gateway **Applicable from Release:** 7.2.1 This section includes information about editing the **Learn Mode Log Cleanup** scheduled task to support archival in hours and minutes along with days. For more information about editing the Learn Mode Log Cleanup scheduled task, refer to: • Section ***Learn Mode*** in the *Data Security Gateway Guide 2.4.0*
Private keys uploaded to DSG are encrypted	**Affected Products:** Data Security Gateway **Applicable from Release:** 7.2.1 For private keys or encrypted private key types uploaded, the DSG ensures that the keys in the DSG ecosystem are always present in an encrypted format. For more information about key encryption, refer to: • Section ***Keys Subtab*** in the *Data Security Gateway Guide 2.4.0* • Section ***Uploading Keys*** in the *Data Security Gateway Guide 2.4.0*
UDF codec enhanced to include blacklisted modules and methods	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.2.1 The UDF codec has been enhanced to blacklist vulnerable modules and methods that can defined as part of the UDF payload. As part of the security enhancements, the *gateway.json* file includes the *globalUDFSettings* key. This key and the corresponding value defines a list of vulnerable modules and methods that are blacklisted. If any blacklisted method is required to be unblocked, then the *Rule Advanced Settings* field can be set to unblock the required method. For more information about the UDF codec enhancement, refer to: • Section ***Advanced Rule Settings in UDFs*** in the *Data Security Gateway User Guide 2.4.0*
Date and Datetime Tokenizer Updates for Cutover Dates of the Gregorian Calendar	**Affected Products:** Appliances, Oracle Database Protector, and Application Protector Java **Applicable from Release:** 7.2.1 The Date and Datetime tokenizers are updated to mitigate the data loss issue observed with the application systems that do not accept the cutover Dates of the Gregorian Calendar. As the cutover Dates with the interval *1582-10-05* to *1582-10-14* are converted internally to *1582-10-15*, data loss

New/Updated Feature	Description
	occurs as the system is not capable to return the actual Date value during the de-tokenization. Some application systems perform the conversion by adding ten days to the source date. **Note:** While the problems occur in Oracle and Java, the fix was made to the tokenizer that is used by all the systems for ensuring token compatibility across platforms. For more information about the Date and Datetime Tokenizer Updates for Cutover Dates of the Gregorian Calendar, refer to: • Section ***Date (YYYY-MM-DD, DD/MM/YYYY, MM.DD.YYYY)*** *Date (YYYY-MM-DD, DD/MM/YYYY, MM.DD.YYYY)* in the *Protection Methods Reference Guide 7.2.1*. • Section ***Datetime (YYYY-MM-DD HH:MM:SS)*** *Datetime (YYYY-MM-DD HH:MM:SS)* in the *Protection Methods Reference Guide 7.2.1*.
7.2.0	
Insight Discovery	**Affected Products:** Insight Discovery **Applicable from Release:** 7.2.0 Insight Discovery 2.1.0 supports the scanning of files that are stored on the Hadoop File Distributed System (HDFS). For more information about the support for HDFS, refer to: • Section ***3 System Architecture*** in *Protegrity Insight Discovery 2.1.0* • Section ***5 Capabilities and Support*** in *Protegrity Insight Discovery 2.1.0* • Section ***5.1 Extending the Support to Other Systems*** in *Protegrity Insight Discovery 2.1.0* • Section ***6.3.1.1 Creating a Data Discovery Task*** in *Protegrity Insight Discovery 2.1.0* • Section ***Appendix C: Scan Task Advanced Configuration Settings*** in *Protegrity Insight Discovery 2.1.0*
Big Data Protector with CDH and Cloudera Manager 6.3	**Affected Products:** Big Data Protector **Applicable from Release:** 7.2.0 Starting from the 7.2.0 release, the Big Data Protector 7.2.0 is certified with the CDH and Cloudera Manager, version 6.3. For more information about installing Big Data Protector 7.2.0 using the CDH Native Installer, refer to: • Section ***Installing Big Data Protector using CDH Native Installer*** in the *Installation Guide 7.2.0*
Data Security Gateway (DSG)	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.2.0 The Protegrity Data Security Gateway v2.2.3 includes feature updates, such as, support for Azure AD in the SAML codec, support for user defined headers, and enhancements to the XML codec to include additional parsing parameters. For more information about installing the Data Security Gateway (DSG), refer to:

New/Updated Feature	Description
	• Section ***7 Installing the DSG*** in the *Data Security Gateway User Guide 2.2.3* • Section ***Appendix I: Using Data Security Gateway (DSG) on Amazon Web Services (AWS)*** in the *Data Security Gateway User Guide 2.2.3* • Section ***Appendix J: Using Data Security Gateway (DSG) on Google Cloud Platform (GCP)*** in the *Data Security Gateway User Guide 2.2.3* • Section ***Appendix I: Using Data Security Gateway (DSG) on Amazon Web Services (AWS)*** in the *Data Security Gateway User Guide 2.2.3*
Azure AD support added for SAML codec	**Affected Products:** Data Security Gateway **Applicable from Release:** 7.2.0 With support for SAML, user authentication and authorization can be manged uniformly for multiple applications on the same network. For more information about the SAML codec, refer to: • Section ***Security Assertion Markup Language (SAML) Codec*** in the *Data Security Gateway Guide 2.2.3*
User Defined Headers	**Affected Products:** Data Security Gateway **Applicable from Release:** 7.2.0 User Defined Headers are meant to provide additional information about an HTTP Response Header that can be helpful for troubleshooting purposes. The User Defined Headers can include information such as custom cookies, state information, and provide information to the load balancer, for example, CPU utilization of a particular node behind the load balancer. For more information about user defined headers, refer to: • Section ***12.3.1.6.8 User Defined Headers*** in the *Data Security Gateway Guide 2.2.3*
Advanced XML Parser	**Affected Products:** Data Security Gateway **Applicable from Release:** 7.2.0 Configure advanced parsing parameter options for the XML payload. This field accepts parsing options in the JSON format. The parsing options are of the Boolean data type. For example, the parsing parameter, `remove_comments`, accepts the values as `true` or `false`. For more information about advanced XML parser, refer to: • Section ***12.3.1.2.6 XML Payload*** in the *Data Security Gateway Guide 2.2.3*
Big Data Protector with CDH and Cloudera Manager 5.14	**Affected Products:** Big Data Protector **Applicable from Release:** 7.2.0 Starting from the 7.2.0 release, the Big Data Protector 7.2.0 is certified with the CDH and Cloudera Manager, version 5.14. For more information about installing Big Data Protector 7.2.0 using the CDH Native Installer, refer to:

New/Updated Feature	Description
	• Section ***Installing Big Data Protector using CDH Native Installer*** in the *Installation Guide 7.2.0* • Section ***Upgrading Big Data Protector using CDH Native Installer*** in the *Upgrade Guide 7.2.0*
Automatic Rotation of Master Key (MK) and Data Store Keys (DSK)	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.2.0 Starting from the version 7.2.0 release, the MK and DSK are set for automatic rotation ten days prior to the Originator Usage Period (OUP) expiration date. The OUP for a key is the period during which the data can be protected using the key. For more information about the automatic rotation of Master Key (MK) and Data Store Keys (DSK), refer to: • Section ***Key Rotation*** in the *Key Management Guide 7.2.0*
The test HSM connection from the ESA Web UI	**Affected Products:** Appliances **Applicable from Release:** 7.2.0 Starting from the version 7.2.0 release, you can test connection to the active HSM from the ESA Web UI. For more information about the test HSM connection feature from the ESA Web UI, refer to: • Section ***Switching from Soft HSM to HSM*** in the *Key Management Guide 7.2.0* • Section ***Switching from the HSM to the Soft HSM*** in the *Key Management Guide 7.2.0*
The rotation of the Master Key (MK) from the ESA Web UI	**Affected Products:** Appliances **Applicable from Release:** 7.2.0 Starting from the version 7.2.0 release, you can rotate the MK from the ESA Web UI. For more information about rotating the Master Key (MK) from the ESA Web UI, refer to: • Section ***Rotating the Master Key*** in the *Key Management Guide 7.2.0*
Switching the HSM modules from the ESA Web UI	**Affected Products:** Appliances **Applicable from Release:** 7.2.0 Starting from the version 7.2.0 release, you can switch the HSM modules from the ESA Web UI. For more information about switching the HSM modules from the ESA Web UI, refer to: • Section ***Switching HSM Modules*** in the *Key Management Guide 7.2.0*
Policy Management Initialization	**Affected Products:** Appliances **Applicable from Release:** 7.2.0 When you install and log in to the ESA for the first time, you must initialize the Policy Management (PIM), which creates the keys-related data and the policy repository. In a Cloud-

New/Updated Feature	Description
	based installation, this step helps to create a new instance of the required keys-related data instead of inheriting the data from the virtual image template. For more information about initializing the Policy Management data on the ESA Web UI, refer to: • Section ***Initializing the Key Management*** in the *Key Management Guide 7.2.0* • Section ***Initializing the Policy Management*** in the *Policy Management Guide 7.2.0*
Member Source Server Replacement	**Affected Products:** Appliances **Applicable from Release:** 7.2.0 Starting from the version 7.2.0 release, the member source server is replaced with the Member Source API micro-service. With the implementation of this micro-service, the **DPS Member Source Server Connectivity** tool is deprecated from the CLI Manager and functionality to configure database connection for the member sources is provided from the ESA Web UI. For more information about the member source server replacement, refer to: • Section ***Configuring Database Member Source*** in the *Policy Management Guide 7.2.0*
Short Data Tokenization for Unicode Tokenizer	**Affected Products:** Appliances, Big Data Protector, Application Protector, and Teradata Database Protector **Applicable from Release:** 7.2.0 Starting from the version 7.2.0 release, the short data tokenization property is enabled for the Unicode data elements and this property is supported by the protectors with version 7.2 or higher. For more information about short data tokenization for Unicode data elements, refer to: • Section ***Protegrity Tokenization*** in the *Protection Methods Reference Guide 7.2.0* • Section ***Creating Data Elements for Structured Data*** in the *Policy Management Guide 7.2.0* **Caution:** The DSG provides limited support for data elements with Short Data for Unicode tokens. Additional functionality or enhancements will be delivered as part of future release(s).
DevOps REST APIs	**Affected Products:** Appliances **Applicable from Release:** 7.2.0 The DevOps REST APIs include the Policy Management REST APIs and appliance-specific information APIs. The Policy Management REST APIs are used to create or manage the policies. The policy management functions performed from the ESA Web UI can also be performed using the REST APIs. In addition, the read-only information about the appliance is also available using the REST API. For more information about using the policy management functions through the REST APIs, refer to: • Section ***Appendix A: DevOps REST APIs*** in the *APIs, UDFs, and Commands Reference Guide 7.2.0*
JSON Web Tokens (JWT)	**Affected Products:** Appliances

New/Updated Feature	Description
	Applicable from Release: 7.2.0 In the version 7.2.0 release, using JWT, you can authorize users to access the REST APIs. For more information about JWT, refer to: • Section ***Working with Tokens*** in the *Appliances Overview Guide 7.2.0.*
Support for ODSEE	**Affected Products:** Appliances **Applicable from Release:** 7.2.0 Starting from the version 7.2.0 release, appliances support ODSEE as an external directory. For more information about restricting the brute force attack, refer to: • Section ***Sample ODSEE Configuration*** in the *Appliances Overview Guide 7.2.0.*
SSH Keys protected by Passphrase	**Affected Products:** Appliances **Applicable from Release:** 7.2.0 Starting from the version 7.2.0 release, you can upload the SSH Keys that are protected by Passphrase from the Web UI. For more information about SSH Keys protected by Passphrase, refer to: • Section ***Secure Shell (SSH) Keys*** in the *Appliances Overview Guide 7.2.0.*
7.1 Maintenance Release 4 (MR4)	
Support for MS SQL version 2019 on the MS SQL Database Protector	**Affected Products:** Database Protector **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) The MS SQL Database Protector supports the MS SQL version 2019. For more information about the MS SQL Database Protector, refer to: • Section ***MS SQL Server Database Protector*** in the *Database Protector Guide* • Section ***Installing and Uninstalling MS SQL Database Protector*** in the *Installation Guide*
Support for Greenplum version 6.0 on the Greenplum Database Protector	**Affected Products:** Database Protector **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) The Greenplum Database Protector supports the Greenplum version 6.0. For more information about the Greenplum Database Protector, refer to: • Section ***Pivotal Greenplum Database Protector*** in the *Database Protector Guide* • Section ***Installing and Uninstalling the Greenplum Database Protector*** in the *Installation Guide*
Support for Oracle version 19c on the Oracle Database Protector	**Affected Products:** Database Protector **Applicable from Release:** 7.1 Maintenance Release 4 (MR4)

New/Updated Feature	Description
	The Oracle Database Protector supports the Oracle version 19c. For more information about Oracle Database Protector, refer to: • Section ***Oracle Database Protector*** in the *Database Protector Guide* • Section ***Installing and Uninstalling Oracle Database Protector*** in the *Installation Guide*
File Protector	**Affected Products:** File Protector **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) The Protegrity File Protector provides a transparent solution for encrypting and protecting sensitive files. The File Protector can protect directories and sub-directories in real-time. As the File Protector operates at the file-system level, it ensures that the sensitive data is in protected form, whenever the file is accessed. The File Protector solution enables the applications and processes to transparently encrypt and decrypt files and directories. In this case, no modifications are required for the applications and processes. For more information about the File Protector, refer to: • Section ***Introduction to the File Protector*** in the *File Protector Guide*
DSG instance on Amazon Web Services (AWS)	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) The DSG 2.2.1 release is now compatible with ESA 7.1 MR4 on AWS. For more information about Using Data Security Gateway (DSG) on Amazon Web Services (AWS), refer to: • Section ***Appendix I: Using Data Security Gateway (DSG) on Amazon Web Services (AWS)*** in the *Data Security Gateway User Guide 2.2.1*
DSG instance on Azure	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) The DSG 2.2.1 release is now compatible with ESA 7.1 MR4 on Azure. For more information about Using Data Security Gateway (DSG) on Microsoft Azure, refer to: • Section ***Appendix K: Using Data Security Gateway (DSG) on Microsoft Azure*** in the *Data Security Gateway User Guide 2.2.1*
DSG instance on Google Cloud Platform (GCP)	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) The DSG 2.2.1 release is now compatible with ESA 7.1 MR4 on GCP. For more information about Using Data Security Gateway (DSG) on Google Cloud Platform (GCP), refer to: • Section ***Appendix J: Using Data Security Gateway (DSG) on Google Cloud Platform (GCP)*** in the *Data Security Gateway User Guide 2.2.1*

New/Updated Feature	Description
Open ports on Appliances	**Affected Products:** Appliances **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) The ports that must be open for all the Protegrity appliances are now enhanced in 7.1 MR4. • Section ***Open Listening Ports*** in the *Appliances Overview Guide*
Strengthening RSA Keys	**Affected Products:** Appliances **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) From 7.1 MR4, the private key length for certificates must be at least 1024-bit. For more information about private key length for certificates, refer to: • Section ***To upload certificates or CRL*** in the *Certificate Management Guide*
Reference information about the *pepserver.cfg* configuration file	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) A single source of reference information for the parameters present in the *pepserver.cfg* configuration file is now added to the documentation. For more information about the parameters present in the *pepserver.cfg* configuration file, refer to: • Section ***Appendix A. PEP Server Configuration File*** in the *Installation Guide 7.1*
Search criteria for filtering members from AD and LDAP	**Affected Products:** Appliances **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) The information about the usage of search filters when working with member or user filters from member sources, such as AD and LDAP, is now added to the documentation. For more information about using search filters for filtering the members from AD and LDAP, refer to: • Section ***Filtering Members from AD and LDAP Member Sources*** in the *Policy Management Guide 7.1*
OS Users	**Affected Products:** Appliances and DSG **Applicable from Release:** 7.1 Maintenance Release 4 (MR4) From 7.1 MR4, the OS users that are available in the system are listed. For more information about the OS Users, refer to: • Section ***OS Users in Appliances***
FUSE File Protector	**Affected Products:** File Protector **Applicable from Release:** 7.1

New/Updated Feature	Description
	The Filesystem in Userspace (FUSE) is an open source framework that enables you to develop a file system in the user space. The FUSE File Protector (FUSE FP) is based on the open source FUSE-based file system. The FUSE FP uses the FUSE framework for protecting files and directories. The FUSE framework is enhanced to support encryption, decryption, and other file protection features.s For more information about the FUSE File Protector, refer to: • Section ***Using the FUSE FP*** in the *FUSE File Protector*
7.1 Maintenance Release 3 (MR3)	
Presto Protector	**Affected Products:** Database Protector **Applicable from Release:** 7.1 Maintenance Release 3 (MR3) In the big data environment, the Presto protector is used together with Hive to process queries and provide data warehousing capabilities to the organization. Based on the Presto client query, the Presto Protector performs data security operations on sensitive data stored in HDFS. For more information about the Presto Protector, refer to: • Section ***Presto Protector*** in the *Database Protector Guide 7.1*. • Section ***Installing and Uninstalling Presto Protector*** in the *Installation Guide 7.1*. • Section ***Presto Protector User Defined Functions*** in the *APIs, UDFs, and Commands Reference Guide 7.1*. • Section ***Tokenization Types*** in the *Protections Methods Reference Guide 7.1*. • Section ***Appendix C: Empty String Handling by Protectors*** in the *Protection Methods Reference Guide 7.1*. • Section ***Appendix D: NULL Handling by Protectors*** in the *Protection Methods Reference Guide 7.1*.
Security Enhancements based on CIS recommendations	**Affected Products:** Appliances **Applicable from Release:** 7.1 Maintenance Release 3 (MR3) To mitigate timing attacks, you can minimise the time intervals for invalid login responses. For more information about reducing the time intervals, refer to: • Section ***Preferences*** in the *Appliances Overview Guide*
Password Policy OS Users	**Affected Products:** Appliances **Applicable from Release:** 7.1 Maintenance Release 3 (MR3) You can enforce policy restrictions for the OS and LDAP user accounts. For more information about enforcing the policy restrictions for the OS and LDAP user accounts, refer to: • Section ***Strengthening Password Policy*** in the *Appliances Overview Guide*
FPVE-Core Protector	**Affected Products:** File Protector

New/Updated Feature	Description
	Applicable from Release: 7.1 Maintenance Release 3 (MR3) The FPVE-Core provides full disk encryption solution at the volume, or disk, or partition level. The data written to the volume is encrypted and decrypted upon read. The FPVE-Core based volume protection encrypts volume partitions which contains sensitive information. The volume Encryption offered by FPVE Core is a data at rest type of protection. The FPVE-Core is recommended in setups where access to volumes is managed by file system level permissions and only encrypted data stores on the volume. For more information about the FPVE-Core Protector, refer to: • Section ***Features of the FPVE-Core*** in the *FPVE-Core Protector*
7.1 Maintenance Release 2 (MR2)	
Installation of Big Data Protector on an HDP Cluster using Cloudbreak	**Affected Products:** Big Data Protector **Applicable from Release:** 7.1 Maintenance Release 2 (MR2) Starting from the version 7.1 MR2 release, you can utilize Cloudbreak to create an HDP cluster and install Big Data Protector on it. For more information about installing Big Data Protector on an HDP Cluster using Cloudbreak, refer to: • Section ***Using Cloudbreak to Install the Big Data Protector*** in the *Installation Guide* • Section ***Installing Big Data Protector on a New Node using Cloudbreak*** in the *Installation Guide*
ESA on Azure	**Affected Products:** Appliances **Applicable from Release:** 7.1 Maintenance Release 2 (MR2) Starting from the version 7.1 MR2 release, you can deploy the ESA on the Azure Cloud Platform. For more information about the ESA on the Azure Cloud Platform, refer to: • Section ***Appendix: Using Protegrity Appliances on Azure*** in the *Appliance Overview Guide*
Network Interface Card (NIC) Bonding	**Affected Products:** Appliances **Applicable from Release:** 7.1 Maintenance Release 2 (MR2) Starting from version 7.1 MR2 release, you can add multiple NICs for network redundancy and fault tolerance. For more information about the NIC Bonding, refer to: • Section ***NIC Bonding*** in the *Data Security Gateway User Guide 2.2.0*
Consul Implementations	**Affected Products:** Appliances **Applicable from Release:** 7.1 Maintenance Release 2 (MR2) Starting from version 7.1 Maintenance Release 2 (MR2), Consul is implemented on TAC to improve network bandwidth and performance.

New/Updated Feature	Description
	For more information about the Consul, refer to: • Section ***Trusted Appliances Cluster (TAC)*** in the *Appliance Overview Guide*
7.1 Maintenance Release 1 (MR1)	
Re-enablement of SLT_2_6 tokenizer	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.1 Maintenance Release 1 (MR1) Starting from version 7.1 Maintenance Release 1 (MR1), you can create data elements using the SLT_2_6 tokenizer. The newly created data elements using the SLT_2_6 tokenizer from v7.1 MR1 onwards is deployable to protectors with versions 7.1 MR1 and higher. For more information about the re-enablement of the SLT_2_6 tokenizer, refer to: • Section ***Tokenization Properties*** in the *Protection Methods Reference Guide 7.1*. • Section ***Tokenization Types*** in the *Protection Methods Reference Guide 7.1*.
7.1	
Adding a default gateway to a Network Interface Card (NIC)	**Affected Products:** Appliances **Applicable from Release:** 7.1 Starting from version 7.1, you can add a default gateway for every NIC that is added to the appliance. For more information about the default gateway for every NIC, refer to: • Section ***Configuring default gateway for Network Interfaces*** in the *Data Security Gateway User Guide 2.1*
ESA Repository Key (ERK) Rotation	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.1 Starting from the version 7.1 release, the ESA Repository Key (ERK) can be rotated using the ESA Web UI. It can be rotated either manually or automatically. The supported states for ERK are Active, Deactivated, Compromised, and Destroyed. For more information about the ESA Repository Key (ERK) Rotation, refer to: • Section ***Key Rotation*** in the *Key Management Guide 7.1*. • Section ***Viewing ESA Repository Key (ERK) Information*** in the *Key Management Guide 7.1*.
Importing Custom Files	**Affected Products:** Appliances **Applicable from Release:** 7.1 Starting from version 7.1, you can import or export custom files between appliances that are in a cluster. For more information about importing or exporting custom files, refer to: • Section ***Exporting Custom Files*** in the *Appliances Overview Guide* • Section ***Upgrading to v7.1 MR4*** in the *Upgrade Guide*

New/Updated Feature	Description
Metering for Protegrity Prime customers	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.1 The Metering feature essentially counts successful protect and reprotect operations for each protector. The pricing for the Protegrity Prime customers is derived from the reported number of counts. For more information about the metering feature for Protegrity Prime customers, refer to: • Section ***Metering Overview*** in the *Data Security Platform Licensing*.
Format Preserving Encryption (FPE)	**Affected Products:** Appliances, Application Protector, Big Data Protector, and Teradata Database Protector **Applicable from Release:** 7.1 Protegrity supports Format Preserving Encryption (FPE) using National Institute of Standards and Technology (NIST) approved FF1 (Format preserving, Feistel based, type 1) mode of operation with AES-256 block cipher encryption algorithm. The data types supported are as follows: • Numeric (0-9) • Alpha (a-z, A-Z) • Alpha-Numeric (0-9, a-z, A-Z) • Credit Card (0-9) • Unicode Basic Latin and Latin-1 Supplement Alpha • Unicode Basic Latin and Latin-1 Supplement Alpha-Numeric For more information about the Format Preserving Encryption (FPE), refer to: • Section ***Protegrity Format Preserving Encryption*** in the *Protection Methods Reference Guide 7.1*. • Section ***Appendix C: Empty String Handling by Protectors*** in the *Protection Methods Reference Guide 7.1*. • Section ***Appendix D: NULL Handling by Protectors*** in the *Protection Methods Reference Guide 7.1*. • Section ***Creating a Structured FPE Data Element*** in the *Policy Management Guide 7.1*.
7.0.1	
SASL integration for user authentication	**Affected Products:** Appliances and Protectors **Applicable from Release:**7.0.1 SP2 The SASL integration ensures that when users are imported from external LDAP, a user with the same name is recreated in the internal LDAP. When the user accesses the data security platform, ESA authorizes the user and communicates with the external LDAP for authenticating the user. This implementation ensures that organizations are not forced to modify their LDAP configuration to accommodate the data security platform. For more information about the SASL, refer to: • Section ***Proxy Authentication*** in the *Appliance Overview Guide*
IMS Database Protector	**Affected Products:** z/OS Protectors

New/Updated Feature	Description
	Applicable from Release: 7.0.1 SP1 IMS Database Protector for z/OS is a set of products that provides capabilities for encrypting and decrypting data on IMS database. The entire database segment will be encrypted and decrypted using IMS Database Protector. Additionally, the protector has compression facility to compress data on segment before encryption and decompress the data after decryption. For more information about the IMS Database Protector, refer to ***The IMS Solutions on Mainframe z/OS*** in the *z/OS Protector Guide*.
Google Dataproc Installer	**Affected Products:** Big Data Protector **Applicable from Release:** 7.0.1 Starting from the Big Data Protector, version 7.0.1 release, an installer for the Google Dataproc environment is being provided. For more information about the Google Dataproc Installer for Big Data Protector, refer to: • Section ***Installing Big Data Protector on a Dataproc Cluster*** in the *Installation Guide* • Section ***Cloud Environment-specific Requirements*** in the *Big Data Protector Guide*
Amazon EMR Installer	**Affected Products:** Big Data Protector **Applicable from Release:** 7.0.1 Starting from the Big Data Protector, version 7.0.1 release, an installer for the Amazon EMR environment is being provided. For more information about the Amazon EMR Installer for Big Data Protector, refer to: • Section ***Installing Big Data Protector on Amazon EMR*** in the *Installation Guide* • Section ***Installing Big Data Protector on a New EMR Cluster*** in the *Installation Guide* • Section ***Installing Big Data Protector on an Existing EMR Cluster*** in the *Installation Guide* • Section ***Cloud Environment-specific Requirements*** in the *Big Data Protector Guide*
String encryption UDFs for Hive	**Affected Products:** Big Data Protector **Applicable from Release:** 7.0.1 The string encryption UDFs are provided to encrypt, decrypt, and reencrypt *string* data type for the Hive protector. For more information about the String encryption UDFs for Hive, refer to: • Section ***ptyStringEnc()*** in the *Protegrity APIs, UDFs, Commands Reference Guide* • Section ***ptyStringDec()*** in the *Protegrity APIs, UDFs, Commands Reference Guide* • Section ***ptyStringReEnc()*** in the *Protegrity APIs, UDFs, Commands Reference Guide* • Section ***Protegrity Encryption*** in the *Protection Methods Reference Guide*
Char(n) tokenization UDFs for Hive	**Affected Products:** Big Data Protector **Applicable from Release:** 7.0.1

New/Updated Feature	Description
	The character tokenization UDFs are provided to protect, unprotect, and reprotect *char(n)* data type for the Hive protector. For more information about the Char(n) tokenization UDFs for Hive, refer to: • Section ***ptyProtectChar()*** in the *Protegrity APIs, UDFs, Commands Reference Guide* • Section ***ptyUnprotectChar()*** in the *Protegrity APIs, UDFs, Commands Reference Guide* • Section ***ptyReprotect() - Char data*** in the *Protegrity APIs, UDFs, Commands Reference Guide* • Section ***Support by Protegrity Products*** in the *Protection Methods Reference Guide*
Data Security Gateway (DSG) instance on Amazon Web Services (AWS)	**Affected Products:** Data Security Gateway (DSG) **Applicable from Release:** 7.0.1 The DSG 2.0 release is compatible with ESA 7.0.1 on AWS For more information about the DSG Instance on AWS, refer to: • Section *23 Appendix J: Using Protegrity Cloud Gateway (PCG) on Amazon Web Services (AWS)* in the *Data Security Gateway User Guide 2.0.1*
Allow Short Data	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.0.1 Starting from the version 7.0.1 release, length preserving short tokens are created if the length of the source data that needs to be tokenized is less than the entry length of the Static Lookup Table (SLT). This feature is supported by the following length preserving tokens: • Numeric (0-9) • Alpha (a-z, A-Z) • Upper-case Alpha (A-Z) • Alpha-Numeric (0-9, a-z, A-Z) • Upper-case Alpha-Numeric (0-9, A-Z) • Printable • Lower ASCII • Email For more information about the short data tokenization, refer to: • Section ***Protegrity Tokenization*** in the *Protection Methods Reference Guide 7.0.1* • Section ***Creating Data Elements for Structured Data*** in the *Policy Management Guide 7.0.1* • Section ***Creating a Structured FPE Data Element*** in the *Policy Management Guide 7.0.1*
FIPS Mode	**Affected Products:** Appliances **Applicable from Release:** 7.0.1 The crypto operations using the ESA Repository Key (ERK) and Data Store Key (DSK) are now supported using the FIPS 140-2 Level 1 non-certified crypto module using the PKCS#11 API specification. For more information about the FIPS mode, refer to: • Section ***Crypto Operations using FIPS Mode*** in the *Key Management Guide 7.0.1*.

New/Updated Feature	Description
External Groups	**Affected Products:** Appliances **Applicable from Release:** 7.0.1 Starting from version 7.0.1 release, you can import users from external directory services to ESA automatically or manually. For more information about the External Groups, refer to: • Section ***External Groups*** in the *Appliance Overview Guide*
RADIUS Authentication	**Affected Products:** Appliances **Applicable from Release:** 7.0.1 Starting from version 7.0.1 release, the RADIUS protocol is supported as a part of two factor authentication. For more information about the RADIUS Authentication, refer to: • Section ***Remote Authentication Dial-up Service (RADIUS) Authentication*** in the *Appliance Overview Guide*
Node assignment to data stores	**Affected Products:** Appliances **Applicable from Release:** 7.0.1 When nodes are registered with a data store, the access can be restricted to specific nodes for security reasons. The allowed servers can now identify a node using either the node IP address or the proxy IP address. For more information about the node assignment to data stores, refer to: • Section***Adding Allowed Servers to the Data Store*** in the *Policy Management Guide 7.0.1*
7.0	
Automated Product Installation	**Affected Products:** z/OS Protectors **Applicable from Release:** 7.0 Starting from z/OS protector, version 7.0 release, the installation procedure of z/OS PEP Server on Open MVS and Cryptographic Server is automated. The automated way to edit *pepserver.cfg* is enhanced. Also, logs from *pepserver.log* file are written on system console at CSRV start-up. For more information about the Automated Installation, refer to ***Sample Codes for Automated Installation*** in the *z/OS Protector Guide*.
Spark SQL Protector	**Affected Products:** Big Data Protector **Applicable from Release:** 7.0 The Protegrity Spark SQL protector provides native UDFs that can be utilized with Spark Scala to protect, unprotect, or reprotect the data as it is stored or retrieved.

New/Updated Feature	Description
	For more information about the Spark SQL protector, refer to: • Section ***Spark SQL*** in the *Big Data Protector Guide* • Section ***Spark SQL UDFs*** in the *Protegrity APIs, UDFs, Commands Reference Guide*
CDH Native Installer	**Affected Products:** Big Data Protector **Applicable from Release:** 7.0 Starting from the Big Data Protector, version 7.0 release, a native installer for the Cloudera environment is being provided. This new installer simplifies the task of installing, configuring, and managing Big Data Protector using Cloudera Manager. For more information about the CDH Native Installer for Big Data Protector, refer to: • Section ***Installing Big Data Protector using CDH Native Installer*** in the *Installation Guide* • Section ***Upgrading Big Data Protector using CDH Native Installer*** in the *Upgrade Guide*
Ambari Native Installer	**Affected Products:** Big Data Protector **Applicable from Release:** 7.0 Starting from the Big Data Protector, version 7.0 release, a native installer for the Ambari environment is being provided. This new installer simplifies the task of installing, configuring, and managing Big Data Protector using the Ambari UI. For more information about the Ambari Native Installer for Big Data Protector, refer to: • Section ***Installing Big Data Protector using Ambari Native Installer*** in the *Installation Guide* • Section ***Upgrading Big Data Protector using Ambari Native Installer*** in the *Upgrade Guide*
Protector Proxy	**Affected Products:** Protectors **Applicable from Release:** 7.0 In ESA 7.0 the DPS proxy has been enhanced to improve scalability to support more nodes communicating with ESA via the proxy that is now renamed to Protector Proxy. The Protector proxy is a standalone component, packaged along with the protector archive. When the protector archive is extracted it will have a separate installable for the protector proxy. For more information about the Protector Proxy, refer to: • Section ***Protector Proxy Installation*** in the *Installation Guide 7.0* • Section ***Teradata Database Protector*** in the *Database Protector Guide 7.0* • Section ***Netezza Database Protector*** in the *Database Protector Guide 7.0*
Service Dispatcher	**Affected Products:** Appliances **Applicable from Release:** 7.0

New/Updated Feature	Description
	This is a new network layer that makes the ESA appliance more scalable and is more efficient in utilizing system resources. This framework is termed as the Service Dispatcher, and it is the central component in the Appliance framework that routes the requests between various components. This service dispatcher is exposed in the Web UI and CLI. You can start and stop the service dispatcher from the Web UI and the CLI. The service dispatcher performance can be tuned only from the CLI as necessary. For more information about the Service Dispatcher feature, refer to: • Section ***3.3 Appliance Services*** in the *Appliance Overview Guide* • Section ***4.6.6 Service Dispatcher Tuning*** in the *Appliance Overview Guide*
Certificates Management	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.0 Certificate Management 7.0 provides certificate based authentication, increased strength of certificate keys, and the ability to replace the "seed" self-signed Protegrity certificates with their CA based certificates. For more information about the Certificates Management, refer to: • Section ***Certificates in ESA*** in the *Certificate Management Guide 7.0* • Section ***Certificate Management in ESA*** in the *Certificate Management Guide 7.0* • Section ***Certificate Management for Protectors*** in the *Certificate Management Guide 7.0* • Section ***Certificates in DSG*** in the *Certificate Management Guide 7.0* • Section ***Replicating Certificates in a Trusted Appliances Cluster (TAC)*** in the *Certificate Management Guide 7.0* • Section ***Validating Certificates*** in the *Certificate Management Guide 7.0*
Key Management	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.0 Secure key generation through Soft HSM internal to ESA. Keys are governed by NIST 800-57 standard and generated from a non-certified FIPS 140-2 Level 1 module. Added functionality to switch to an external HSM. Keys remain within secure perimeter of ESA thus ensuring improved data security. For more information about the Key Management, refer to: • Section ***Protegrity Key Management*** in the *Key Management Guide 7.0* • Section ***Working with Keys***in the *Key Management Guide 7.0* • Section ***Appendix B: Safenet: Switching HSM Modules*** in the *Key Management Guide 7.0*
Policy Management	**Affected Products:** Appliances and Protectors **Applicable from Release:** 7.0 The Enterprise Security Administrator (ESA) 7.0 provides a complete re-design of the user interface for Policy Management.

New/Updated Feature	Description
	For more information about the Policy Management, refer to: • Section ***Policy Management in ESA*** in the *Policy Management Guide 7.0* • Section ***Policy Deployment in Protectors*** in the *Policy Management Guide 7.0* • Section ***Components of a Policy*** in the *Policy Management Guide 7.0* • Section ***Creating and Deploying Policies*** in the *Policy Management Guide 7.0* • Section ***Policy Deployment Feedback*** in the *Policy Management Guide 7.0* • Section ***Policy Management Audit Events*** in the *Policy Management Guide 7.0*
High Availability	**Affected Products:** Appliances **Applicable from Release:** 7.0 High Availability provides a solution for single-point-of-failure (SPOF) problem. It follows a active-passive setup where one ESA is the primary node and the other ESA is secondary node. For more information about the High Availability, refer to: • Section ***Scalability and Availability in Protegrity Products*** in the *Scalability and Availability Guide*

Chapter 3

Deprecated Features

The following table lists the deprecated features in the Protegrity Data Security Platform releases, starting from the release 9.1.0.5 through release 7.0.

Table 3-1: Deprecated Features

Platform Release	Deprecated Feature	Affected products	Description
9.0.0.0	The Samba package is deprecated	DSG	Starting from the DSG 3.0.0.0 release, the Samba package is deprecated for the security reasons. The CIFS tunnel configuration will not be supported in this release.
	The support for HSM integration is deprecated	DSG	Starting from the DSG 3.0.0.0 release, the Label-External IV used with the HSM integration will not be supported from this release.
	The Log Management Guide is deprecated	ESA and PSU	The Log Forwarding Guide replaces the Log Management Guide.
	The steps to forward logs to an external Elasticsearch are deprecated	ESA and PSU	The steps to send logs to an Elasticsearch is removed from the the Audit Store guide. The supported external SIEMs are covered in the Log Forwarding guide.
8.1.0.0	PEP return code *45* is deprecated	Protectors	The Policy Management logs are now available from the Audit Store by navigating to the **ESA Web UI** > **Insight Analytics** > **Forensics**.
	In the the *pepserver.cfg*, the following sections and related configurations are deprecated. • Audit configuration • Disk space management	Protectors	Starting from the version 8.1.0.0 release, the **Log Forwarder** is responsible for handling audits and forwarding them to the **Audit Store**. The deprecated Audit and Disk space configurations are auto handled by the **Log Forwarder** configurations. For more information about **Log Forwarder**, refer to the section *Installing the Log Forwarder on Protectors* in the *Protegrity Installation Guide 8.1.0.0*.
	The following appliance logs that could be accessed from the ESA CLI Manager and the ESA Web UI are deprecated • Hubcontroller • PIM Cluster Service • Soft HSM Gateway • HSM Gateway	ESA	The Policy Management logs are now available from the Audit Store by navigating to the **ESA Web UI** > **Insight Analytics** > **Forensics**. For more information about the Audit Store, refer to the *Audit Store Guide 8.1.0.0*.

Platform Release	Deprecated Feature	Affected products	Description
	• Member Source Service • DevOps Service		
	The *logging.conf* file is deprecated.	ESA	The logging level at the platform level can be configured in the *hubcontroller.env* file. For more information about editing logging levels, contact Protegrity support.
	The *ILM* scheduled task is deprecated.	ESA	Starting from the version 8.1.0.0 release, the *ILM* scheduled task is replaced with the *ILM Multi Export* scheduled task for automatically exporting logs. This is available in the **ESA Web UI** > **Analytics** > **Scheduler** > **Tasks** > **Add New Task**. For more information about the scheduled tasks, refer to the *Protegrity Analytics Guide 8.1.0.0*.
8.0.0.0	Policy Management logs from the **ESA Web UI** > **Logs** > **Policy Management** screen	Appliances	Starting from the version 8.0.0.0 release, the Policy Management logs are now available from the Audit Store by navigating to the **ESA Web UI** > **Analytics** > **Forensics**. For more information about the Audit Store, refer to the *Audit Store Guide 8.1.0.0*.
	Generate *Metering Report* button from the **ESA Web UI** > **License** screen	Appliances and Protectors	Starting from the version 8.0.0.0 release, the *Meteringfacade* service collects the total count of successful protect, unprotect, and reprotect operations from the connected protectors. The total count is then sent at periodic intervals, which is 20 minutes, to the Audit Store for further analysis. For more information about Metering, refer to section *Viewing the Metering Information* in the *Analytics Guide Release 8.1.0.0*. For more information about the Audit Store, refer to the *Audit Store Guide 8.1.0.0*.
7.2.0			
	Switching the HSM modules from the CLI Manager	Appliances and Protectors	The switching of the HSM modules from the CLI Manager is deprecated from the v7.2.0 release and is now available through the ESA Web UI. For more information about switching the HSM modules from the ESA Web UI, refer to the section ***Switching HSM Modules*** in the *Key Management Guide*.
	Rotation of the Master Key from the CLI Manager	Appliances and Protectors	The rotation of the Master Key from the CLI Manager is deprecated from the v7.2.0 release and is now available through the ESA Web UI. For more information about rotating the Master Key (MK) from the ESA Web UI, refer to the section ***Rotating the Master Key*** in the *Key Management Guide*.
	DPS Member Source Server Connectivity tool from the CLI Manager	Appliances and Protectors	With the implementation of the Member Source API micro-service in the v7.2.0 release, the **DPS Member Source Server Connectivity** tool is deprecated from the CLI Manager. The functionality to configure database connection for the member sources is provided from the ESA Web UI.

Platform Release	Deprecated Feature	Affected products	Description
			For more information about configuring database connection for the member sources, refer to the section ***Configuring Database Member Source*** in the *Policy Management Guide*.
	HDFS File Protector (HDFSFP)	Big Data Protector	Starting from the Big Data Protector 7.2.0 release, the HDFS File Protector (HDFSFP) is deprecated. The HDFSFP-related sections are retained to ensure coverage for using an older version of Big Data Protector with the ESA 7.2.0.
7.1			
	HAWQ Protector	Big Data Protector	Starting from the version 7.1 Maintenance Release 3 (MR3), the HAWQ protector is deprecated.
	DTP2 protection method	Appliances and Protectors	Starting from the version 7.1, Maintenance Release 1 (MR1), the DTP2 protection method is deprecated. For assistance in switching to a different protection method, contact Protegrity.
7.0.1			
	Time access settings	Appliances	Starting from the version 7.0.1 release, the time access settings that can be set on a role or data element are no longer supported in ESA v7.0.1. The policies deployed to protectors, v6.6.5 through v6.5 SP2, are set to default time access. The default time access is 24/7.
	Role validity settings	Appliances	Starting from the version 7.0.1 release, the role validity settings with start date and end date are no longer supported in ESA v7.0.1. This feature is already handled within Active Directory (AD).
	HBase Protector Migration Utility	Big Data Protector	Starting from the version 7.0.1 release, the HBase protector Migration utility is no longer supported.

Chapter 4

Deprecated Releases and Products

End of Support (EOS) for Protegrity platform versions up to and including 7.1.x (7.1, 7.1 MR1, 7.1 MR2, 7.1 MR3, 7.1 MR4).

The support for the *Protegrity Platform versions 7.0.1 and prior to 7.0.1*, as well as for *File Protector Gateway*, the *Protection Server*, and all *Protectors running on the Solaris operating system*, has previously expired in accordance with the prior End of Support announcements for such versions.

As long as you have a valid Maintenance and Support contract or subscription license in effect, you may take delivery of any later versions up to then-current versions without any additional license or maintenance fees; however, these versions are no longer eligible for Support as of the EOS date.

We encourage reviewing our Current Release (9.1.0.3) which offers new and improved functionality and technology designed to manage the complex security issues in today's enterprise.

As per our End of Support (EOS) policy, the release to end support as of the following date, which is four (4) years after the initial general availability of the first product release on the respective version.

Protegrity Platform Release Version	**End of Support Date**
7.1 (7.1, 7.1 MR1, 7.1 MR2, 7.1 MR3, 7.1 MR4)	December 30, 2022
7.0.1	September 15, 2021
6.6.5	December 1, 2020
6.6.4	August 1, 2020
6.6.3	June 1, 2020
6.6.0 6.6.1 6.6.2	March 1, 2020

Chapter 5

New Protectors

The following is the list of new Protegrity protectors that have been added in the respective releases.

- Spark SQL Protector for Big Data Protector, starting from the 7.0 release
  For more information about the Spark SQL protector, refer to the *Protegrity Big Data Protector Guide Release 7.2.0*.
- IMS Database Protector for z/OS, starting from the 7.0.1 release
  For more information about the IMS Database Protector, refer to the *z/OS Protector Guide 7.0.1*.
- FPVE-Core Protector for File Protector, starting from the 7.1 release
  For more information about the FPVE-Core Protector, refer to the *Protegrity FPVE-Core User Guide Release 7.1*.
- File Protector, starting from the 7.1 release
  For more information about the File Protector, refer to the *Protegrity File Protector Guide 7.1*.
- Presto Protector, starting from the 7.1 release
  For more information about the Presto Protector, refer to the *Protegrity Database Protector Guide 7.2.0*.
- FUSE File Protector, starting from the 7.1 release
  For more information about the Presto Protector, refer to the *Protegrity FUSE File Protector Guide Release 7.1*.
- Application Protector (AP) Python, starting from the 7.2.0 release
  For more information about the AP Python, refer to the *Protegrity Application Protector Guide 7.2.0*.

5.1 Spark SQL Protector

Spark is an execution engine that carries out batch processing of jobs in-memory and handles a wider range of computational workloads. In addition to processing a batch of stored data, Spark is capable of manipulating data in real time.

Spark leverages the physical memory of the Hadoop system and utilizes Resilient Distributed Datasets (RDDs) to store the data in-memory and lowers latency, if the data fits in the memory size. The data is saved on the hard drive only if required. As RDDs are the basic units of abstraction and computation in Spark, you can use the protection and unprotection APIs, provided by the Spark protector, when performing the transformation operations on an RDD.

The Protegrity Spark SQL protector provides native UDFs that can be utilized with Spark Scala to protect, unprotect, or reprotect the data as it is stored or retrieved.

For more information about the Protegrity Spark protector, refer to the *Protegrity Big Data Protector Guide Release 7.2.0*.

5.2 IMS Database Protector

IMS Database Protector for z/OS is a set of products that provides capabilities for encrypting and decrypting data on IMS database. The entire database segment will be encrypted and decrypted using IMS Database Protector.

IMS Database Protector has compression facility to compress data on segment before encryption and decompress the data after decryption.

The product uses standard IMS segment edit/compression exit routine to invoke the encryption or decryption.

Protegrity has three ways to protect data in IMS database.

- PTYPIMS DBDEXIT
- PTYPIMSC DBDEXIT
- Protegrity z/OS Application protector (PTYPSLL/PTYPSLI)

For more information about the IMS Database Protector, refer to *z/OS Protector Guide 7.0.1*.

5.3 FPVE-Core Protector

The FPVE-Core provides full disk encryption solution at the volume, or disk, or partition level. The data written to the volume is encrypted and decrypted upon read.

The FPVE-Core based volume protection encrypts volume partitions which contains sensitive information. The volume Encryption offered by FPVE Core is a data at rest type of protection.

The FPVE-Core is recommended in setups where access to volumes is managed by file system level permissions and only encrypted data stores on the volume.

For more information about the FPVE-Core Protector, refer to *Protegrity FPVE-Core User Guide Release 7.1*.

5.4 Presto Protector

Presto, a distributed SQL engine, enables you to leverage its ability to query across disparate data sources to run interactive analytic queries.

In the Big Data environment, Presto is used together with Hive to process queries and provide data warehousing capabilities to the organization.

In this release, based on the Presto client query, Presto Protector performs data security operations on the sensitive data stored in Hadoop Distributed File System (HDFS). The user permissions and roles defined in the ESA data security policy define whether the user can view the protected data or clear data.

For more information about the Presto Protector, refer to *Protegrity Database Protector Guide 7.2.0*.

5.5 File Protector

The Protegrity File Protector provides a transparent solution for encrypting and protecting sensitive files. The File Protector can protect directories and sub-directories in real-time. As the File Protector operates at the file-system level, it ensures that the sensitive data is in protected form, whenever the file is accessed. The File Protector solution enables the applications and processes to transparently encrypt and decrypt files and directories. In this case, no modifications are required for the applications and processes. User can protect files or directories using the File Protector command set. After the protection is configured, the File Protector automatically allows access when the required policy is loaded for the application or user.

For more information about the File Protector, refer to *Protegrity File Protector Guide Release 7.1*.

5.6 FUSE File Protector

The Filesystem in Userspace (FUSE) is an open source framework that enables you to develop a file system in the user space. The FUSE File Protector (FUSE FP) is based on the open source FUSE-based file system.

The FUSE FP uses the FUSE framework for protecting files and directories. The FUSE framework is enhanced to support encryption, decryption, and other file protection features.

For more information about the FUSE File Protector, refer to *Protegrity FUSE File Prote ctor Guide Release 7.1*.

5.7 Application Protector Python

The AP Python provides native APIs that can be utilized with Python to protect, unprotect, or reprotect the data as it is stored or retrieved.

Protegrity Application Protector (AP) Python provides APIs that integrates with the customer application to protect data.

You can use the AP Python in the following modes:

- *Production mode* - Customers can use the AP Python APIs to protect, unprotect and reprotect the production data.
- *Development mode* - Customers can use the AP Python APIs along with a set of sample users and data elements that can be used to simulate the behavior of the APIs in the production environment. This mode can be used to test the integration of the customer application with the AP Python APIs.

For more information about the AP Python, refer the *Protegrity Application Protector Guide 7.2.0*.

5.8 Application Protector NodeJS

The AP NodeJS provides native APIs that can be utilized with applications developed using NodeJS to protect, unprotect, or reprotect the data as it is stored or retrieved.

Protegrity Application Protector (AP) NodeJS provides APIs that integrates with the customer application to protect data.

For more information about the AP NodeJS, refer the *Protegrity Application Protector Guide 9.1.0.0*.

5.9 Application Protector .Net

The Protegrity Application Protector (AP) .Net provides APIs that integrate with the customer application to protect, unprotect, and reprotect sensitive data.

The AP .Net can be used with any customer application that is developed using the .Net Core and C# programming language.

For more information about the AP .Net, refer the *Protegrity Application Protector Guide 9.1.0.0*.