Protegrity Policy Management Guide 9.1.0.4

Created on: Nov 19, 2024

Notice

Copyright

Table of Contents

Chapter 1

Introduction

This guide provides details on the policy management functionality provided by Protegrity Data Security Platform.

The value of any company or its business is in its data. The company or business suffers serious issues if an unauthorized user gets access to the data. Therefore, it becomes necessary for any company or business to protect its data.

The data may contain sensitive information like personally identifiable information, company secrets such as pricing information or intellectual property etc. The process of protecting sensitive data to protect the privacy and personal identity of individuals is called De-Identification.

When de-identifying data, the analysis consists of:

- **Anonymization** – In anonymization, the intent is to protect privacy by sanitizing any information that could lead to the individual being identified. The de-identified data cannot be re-identified. It includes methods like encryption, masking etc.
- **Pseudonymization** – In pseudonymization, artificial identifiers or pseudonyms replace the identifying data within a data record. The de-identified data can be re-identified only to authorized users. It includes methods like vaultless tokenization.

The Protegrity methodology together with policy management provides a framework for designing and delivering enterprise data security solutions. Data security solutions, when adopted within an organization, ensures the security of information assets. One of the key components of data security is a policy.

Policy is a set of rules that defines how sensitive data needs to be protected. These policies are designed or created and then distributed to locations in the enterprise, where data needs to be protected.

Policy management is a set of capabilities for creating, maintaining, and distributing the policies.

The following section explains the workflow for policy management in ESA.

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* defines the purpose of the guide and how information is organized in this guide.
- Section *2 Policy Management in ESA* provides information about the concept of Policy Management in ESA.
- Section *3 Policy Deployment in Protectors* describes about how policy deployment functions on protectors.
- Section *4 Initializing the Policy Management* describes describes the steps to initialize the Policy Management (PIM) to load the Policy Management-specific information on the ESA Web UI.

- Section *5 Components of a Policy* describes about the components of a Policy and how they function.
- Section *6 Creating and Deploying Policies* describes how to create and deploy policies.
- Section *7 Deploying Data Stores to Protectors* describes the procedure to deploy data stores to protectors.
- Section *8 Managing Policy Components* describes about how to manage the Policy Components.
- Section *9 Policy Deployment Feedback* provides conceptual information about the collective status of deployed policies, nodes and trusted applications combined with the deploy statuses by the PEP servers running on various protector nodes.

1.2 Accessing the Protegrity documentation suite

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

Chapter 2

Policy Management in ESA

This section discusses about Policy Management in ESA.

The policy each organization creates within ESA is based on requirements with relevant regulations. A policy helps you to determine, specify and enforce certain data security rules. These data security rules are as shown in the following figure.

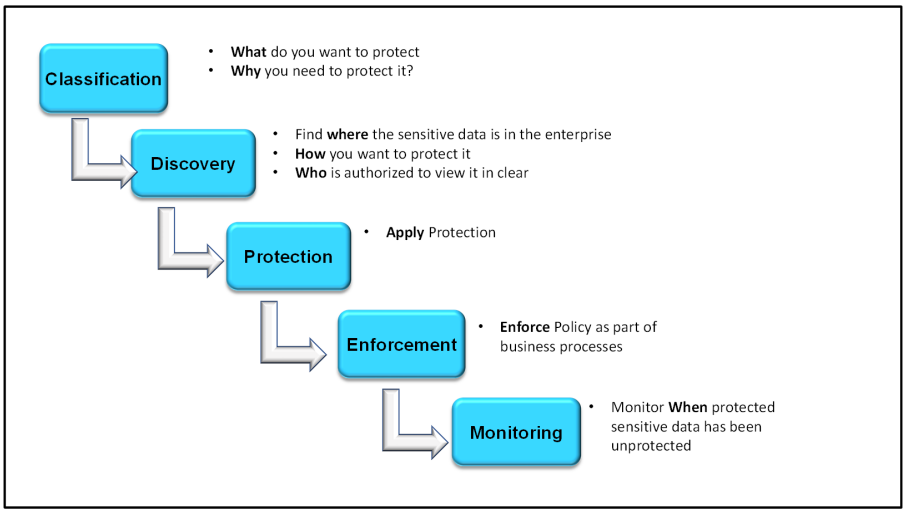


Figure 2-1: Protegrity Data Security Methodology

2.1 Classification

This section discusses about the classification of Policy Management in ESA.

- **What do you want to protect?**

  The data that is to be protected needs to be classified. This step determines the type of data that the organization considers sensitive. The compliance or security team will choose to meet certain standard compliance requirements with specific law or regulation, such as the Payment Card Industry Data Security Standard (PCI DSS) or the Health Information Portability and Accessibility Act (HIPAA).

  In ESA, you classify the sensitive data fields by creating ‘Data Elements’ for each field or type of data.

- **Why do you need to protect?**

  The fundamental goal of all IT security measures is the protection of sensitive data. The improper disclosure of sensitive data can cause serious harm to the reputation and business of the organization. Hence, the protection of sensitive data by avoiding identity theft and protecting privacy is for everyone’s advantage.

2.2 Discovery

This section discusses about the discovery of Policy Management in ESA.

- **Where is the data located in the enterprise?**

  The data protection systems are the locations in the enterprise to focus on as the data security solution is designed. Any data security solution identifies the systems that contains the sensitive data.

- **How you want to protect it?**

  Data protection has different scenarios which require different forms of protection. For example, tokenization is preferred over encryption for credit card protection. The technology used must be understood to identify a protection method. For example, if a database is involved, Protegrity identifies a Protector to match up with the technology used to achieve protection of sensitive data.

- **Who is authorized to view it in the clear?**

  In any organization, the access to unprotected sensitive data must be given only to the authorized stakeholders to accomplish their jobs. A policy defines the authorization criteria for each user. The users are defined in the form of members of roles. A level of authorization is associated with each role which assigns data access privileges to all members in the role.

2.3 Protection

The Protegrity Data Security Platform delivers the protection through a set of Data Protectors. The Protegrity Protectors meet the governance requirements to protect sensitive data in any kind of environment. ESA delivers the centrally managed policy set and the Protectors locally enforce them. It also collects audit logs of all activity in their systems and sends back to ESA for reporting.

2.4 Enforcement

The value of any company or its business is in its data. The company or business suffers serious issues if an unauthorized user gets access to the data. Therefore, it becomes necessary for any company or business to protect its data. The policy is created to enforce the data protection rules that fulfils the requirements of the security team. It is deployed to all Protegrity Protectors that are protecting sensitive data at protection points.

2.5 Monitoring

As a policy is enforced, the Protegrity Protectors collects audit logs in their systems and reports back to ESA. Audit logs helps you to capture authorized and unauthorized attempts to access sensitive data at all protection points. It also captures logs on all changes made to policies. You can specify what types of audit records are captured and sent back to ESA for analysis and reporting.

Chapter 3

Policy Deployment in Protectors

This section discusses about Policy Management in Protectors.

The following image illustrates how the policies defined in the ESA reach the protectors. When a policy is deployed in the ESA, the protectors pull the policy and related metadata at frequent intervals. If any change is made to the policy, the ESA does not push the changes immediately to the protector, but rather waits for a pull request from the protector. There can be multiple scenarios when any change in policy is made.

> **Note:**
> The deployment scenario explained in this section applies to Pull protectors from v6.6.x, v7.x.x, and v8.x.x.x.

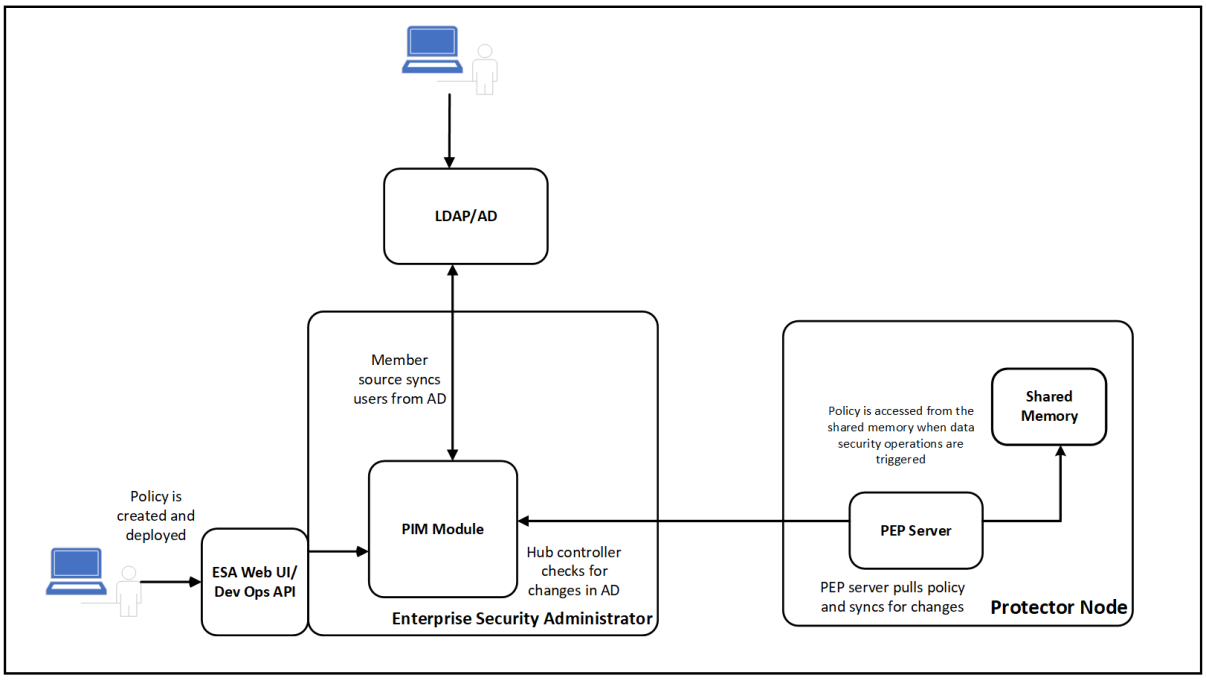


Figure 3-1: Policy Management in Protectors

Protector-related information

The following table provides information about key elements that provide information about whether the PEP server is connected to ESA, adding new members from the LDAP to the ESA, and so on.

Table 3-1: Protector-related Key Information

Protector-related Information	Reference
The Nodes screen provides information about the protector node health. It provides information, such as if the node is up, whether policy is successfully deployed, and so on.	• For more information, refer to the section *Policy Deployment Feedback.*

Protector-related Information	Reference
	• For more information about policy deployment status on each protector node where policy is deployed, refer to *Working with Nodes*.
If new members are added to the organizational LDAP, the ESA adds these members to the member source and subsequently to the policy. The policy is deployed automatically based on the role definition.	• For more information about how to pull new members from the LDAP to the ESA AD, refer to the section *Working with Member Sources*. • For more information about how to add these new members to the roles in the policy, refer to the section *Working with Roles*.

Chapter 4

Initializing the Policy Management

When you install and log in to the ESA Web UI for the first time, you must initialize the Policy Management (PIM), which creates the keys-related data and the policy repository. In a Cloud-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. This section describes the steps to initialize the Policy Management (PIM) to load the Policy Management-specific information on the ESA Web UI.

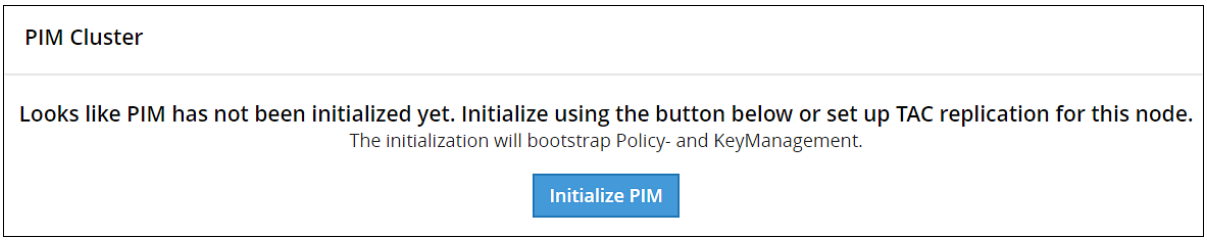
Before you begin

> **Note:**
> When you try to access any of the Policy Management or Key Management screens on the ESA Web UI, a request to initialize the PIM appears.

> **Caution:** Prior to the installation of protectors, ensure that you perform the following steps to initialize the Policy Management.

To initialize the Policy Management:

1. On the ESA Web UI, click **Policy Management**
2. Click any option available in the Policy Management area.
   The following screen to initialize PIM appears.



3. Click **Initialize PIM**.
   A confirmation message box appears.
4. Click **Ok**.
   The policy management information appears in the Policy Management area.

Chapter 5

Components of a Policy

This section discusses about components of a policy.

A policy comprises of multiple components that work together to enforce protection at the protection endpoints.The role component and policy is tied closely. Any changes made to the organization LDAP, such as a user linked to a role is added or deleted, result in an update to the policy. When a policy is deployed in ESA, the protectors pull the policy and related metadata at frequent intervals, which can be as less as an hour. So, when a change in policy is detected due to LDAP changes, the protector pulls the policy.

5.1 Working With Data Elements

Data elements consist of a set of data protection properties to protect sensitive data. This set consists of different token types, encryption algorithms, and encryption options. The most important of these properties are the methods that you use to protect sensitive data.

Some data elements can be set up to use key IDs. A data element can have multiple instances of keys for the same data element and this binds the key ID with the cryptographic text.

For more information about the protection methods, refer to *Protection Methods Reference Guide 9.1.0.5*.

You can create data elements for the following data types:

- **Structured Data:** Structured Data provides the properties that support column-level database protection, and capabilities to integrate policies into applications, with an API. Protegrity provides the ability to protect sensitive data in the individual columns in a database table. When protecting applications, it becomes necessary to integrate an API into the application.
- **Unstructured Data:** Unstructured Data Files are a common mechanism for communicating information and moving data between data stores in the enterprise. Unstructured Data provides the properties supporting file protection. The file protection capabilities enable the protection of sensitive data as it traverses the enterprise or as it rests within files.

The protection methods include, tokenization, encryption, FPE, monitoring, and masking. Depending on the protection type, you need to specify the additional protection settings.

Tokenization

Tokenization is supported for structured data only. The following different tokenization types are supported for structured data types:

- Numeric
- Integer (2 bytes, 4 bytes, and 8 bytes)
- Credit Card
- Alpha
- Upper-case Alpha
- Alpha-Numeric
- Upper Alpha-Numeric
- Lower ASCII
- Printable
- Date YYYY-MM-DD
- Date DD/MM/YYYY
- Date MM.DD.YYYY
- Datetime
- Decimal
- Unicode
- Unicode Base64
- Unicode Gen2
- Binary
- Email

Format Preserving Encryption

Format Preserving Encryption (FPE) is supported for structured data only. The following data types are supported by FPE:

- Numeric (0-9)
- Alpha (a-z, A-Z)
- Alpha-Numeric (0-9, a-z, A-Z)
- Credit Card (0-9)
- Unicode Basic Latin and Basic Latin-1 Supplement Alpha
- Unicode Basic Latin and Basic Latin-1 Supplement Alpha-Numeric

For more information about FPE, refer to section *Protegrity Format Preserving Encryption* in the *Protection Methods Reference Guide 9.1.0.5*.

Encryption

The following table shows the different encryption algorithms supported for structured and unstructured data.

Table 5-1: Encryption Algorithms

Algorithms	Structured Data	Unstructured Data
3DES	√	√
AES-128	√	√
AES-256	√	√
HMAC-SHA1	√	
CUSP 3DES	√	
CUSP AES-128	√	
CUSP AES-256	√	

Algorithms	Structured Data	Unstructured Data
DTP2-3DES	√	
DTP2-AES-128	√	
DTP2-AES-256	√	
DTP2-SHA1	√	

Caution: 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.

Encryption options

The following table describes the encryption options available when you create a data element.

Table 5-2: Encryption Options

Feature	Description	Algorithms
Initialization Vector (IV)	A block of bits required to allow a cipher to be executed in any of several streaming modes of operation to produce a unique stream, independent from other streams produced by the same encryption key, without having to go through a re-keying process.	3DES, AES-128, AES-256
Integrity Check (CRC)	A type of function that takes as input a data stream of any length and produces as output a value of a certain fixed size. A CRC can be used as a checksum to detect alteration of data during transmission or storage.	3DES, AES-128, AES-256, CUSP 3DES, CUSP AES-128, CUSP AES-256
Key ID	An identifier that associates encrypted data with the protection method so that the data can be decrypted regardless of where it ultimately resides. A data element can have multiple instances of key IDs associated with it.	3DES, AES-128, AES-256, CUSP 3DES, CUSP AES-128, CUSP AES-256

The following figure shows the **New Data Element** screen.

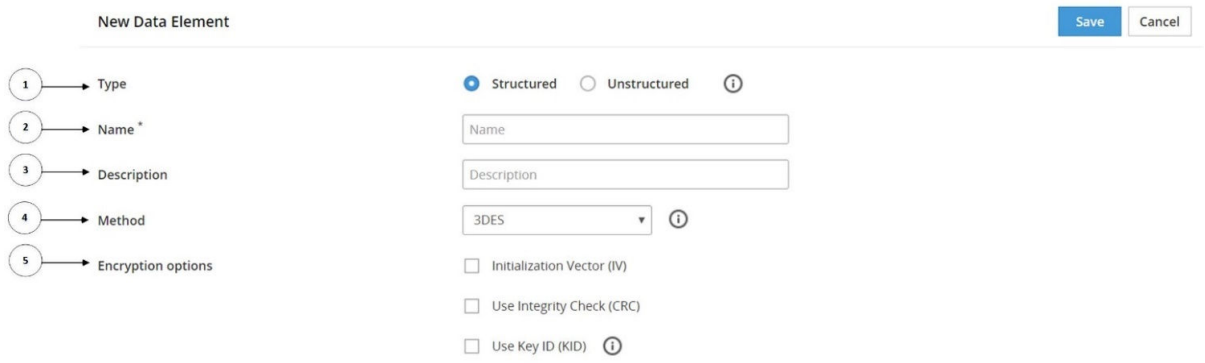


Figure 5-1: New Data Element Screen

The following table provides the description for each element available on the of the ESA Web UI.

Table 5-3: Data Element Fields

Callout	UI Element	Description
1	Type	Type of data element you require to create, structured or unstructured.
2	Name	Unique name identifying the data element.
3	Description	Text describing the data element.
4	Method	Tokenization, encryption, masking, and monitoring methods.
5	Encryption Options/Tokenize Options	Based on the method selected, the tokenization or the encryption options change.

Key ID Specifics

Key IDs are a way to correlate a data element with its encrypted data.

For more information on Key IDs, refer to the section *Encryption Properties(IV, CRC, Key ID)* in *Protection Methods Reference Guide 9.1.0.5*.

If key ID is enabled for a data element, then multiple keys can be created for a single data element, but only one key at a time is used for encryption.

If the data element is set up to use key IDs, then you can create a new key for the data element with a different key id.

When you create a data element with the Key ID, the data element is displayed with a UID in the *Preactive* state, in the **Keys** tab for the specific data element.

If the state of the new key is *Preactive*, then you cannot create a new key.

When you deploy a policy with this data element, the system uses the new key ID. The current ID displays in Active status.

When you click **Create New Key**, all policies using this data element automatically change from Deployed to Ready to Deploy. When you deploy the policy, the old key becomes Deactivated and the state of the new key changes from *Preactive* to *Active*. To activate the new key, all policies using this data element should be redeployed to use the new key.

For more information about deploying polices, refer to section *Creating and Deploying Policies*.

Monitor

Monitoring is supported for structured data only.

The **Monitor** protection method is generally used for auditing. As an organization, if you plan to monitor and assess users that are trying to access the data, then you must opt for the Monitor data method. This element does not restrict any data security operation for any user, but instead audits attempts to add, access or change data by users. The audit logs generated at the protection point are forwarded to the log management system.

Masking

The Masking protection method is supported for structured data only.

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 method can be used. Considering that the sensitive data is residing in the protection endpoint in clear, based on how the Masking data element is configured, users are granted view access. The masking data element as a default considers all users as restricted users and displays masked sensitive data. If any user must be granted access to view clear data, then it must be configured through roles.

5.1.1 Creating Data Elements for Structured Data

You create a structured type of data elements for Database, Application Protector, or Big Data Protector (without *HDFSFP*) policies. This section describes the steps to create a numeric token data element for a structured data type.

To create a structured data element:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Elements & Masks** > **Data Elements**.
2. Click **Add New Data Element**.
   The **New Data Element** screen appears.
3. Select **Structured** from **Type**.
4. Type a unique name for the data element in the **Name** textbox.

   > **Note:** Ensure that the length of the data element name does not exceed 55 characters.

5. Type the required description for the data element in the **Description** textbox.
6. Select **Tokenization** from the **Method** drop-down.
7. Select **Numeric (0-9)** from the **Data Type** drop down.
   For more information about the different data types, refer to the *Protection Methods Reference Guide 9.1.0.5*.
8. Select the required tokenizer from the **Tokenizer** drop-down.
   For more information about the different token elements, refer to the *Protection Methods Reference Guide 9.1.0.5*.
9. Type the required numbers in the **From Left** and **From Right** text box.
   For more information on the maximum and minimum input values for these fields, refer to the section *Minimum and Maximum Input Length* in the *Protection Methods Reference Guide 9.1.0.5*.
10. If the token length needs to be equal to the provided input, then select the **Preserve length** check box.
11. Select the required short data tokenization settings in the **Allow Short Data** drop-down.
    If you require short data tokenization with existing data that was previously not protected using short data enabled data element, then you must do the following:
    a. Unprotect the existing data with the old data element.
    b. Create a new data element that is enabled with short data.
    c. Reprotect the unprotected data with the new short data enabled data element.

    For more information about length preservation and short data tokenization, refer to section *Length Preserving* and *Short Data Tokenization* in *Protection Methods Reference Guide 9.1.0.0*.

    > **Note:**
    > If you are create a short data token in a policy and then deploy the policy, the **Forensics** displays a policy deployment warning indicating that the data element has unsupported settings.
    >
    > For protectors v7.x.x, the warning appears as a cautionary and can be ignored. The policy is deployed successfully.

12. Click **Save**.

A message *Data Element has been saved successfully* appears.

5.1.1.1 Creating a Case-Preserving and Position-Preserving Data Element

You can create an alpha-numeric data element that preserves the case of the alphabets and position of the alphabets and numbers for the output tokenized value. This section describes the steps to create a case-preserving and position-preserving *Alpha-Numeric (0-9, a-z, A-Z)* data element.

To create a Case-preserving and Position-preserving *Alpha-Numeric (0-9, a-z, A-Z)* data element:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Elements & Masks** > **Data Elements**.
2. Click **Add New Data Element**.
   The **New Data Element** screen appears.
3. Select **Structured** from **Type**.
4. Type a unique name for the data element in the **Name** textbox.

   Note: Ensure that the length of the data element name does not exceed 55 characters.

5. Type the required description for the data element in the **Description** textbox.
6. Select **Tokenization** from the **Method** drop-down.
7. Select **Alpha-Numeric (0-9,a-z,A-Z)** from the **Data Type** drop-down box.
8. Select the *SLT_2_3* tokenizer from the **Tokenizer** drop-down.

   Note:
   You can specify the case-preserving and position-preserving tokenization options when using the *SLT_2_3* tokenizer and *Alpha-Numeric (0-9, a-z, A-Z)* token type only.

9. Select **Preserve Position** to preserve the position of characters in the tokenized value.
10. Select **Preserve Case** to preserve the case and position in the tokenized value.

    Note:
    If you select the *Preserve Case* property, then the *Preserve Position* property is also selected, by default. Hence, the position of the alphabets and numbers is preserved along with the casing of the alphabets in the output tokenized value.

    If you are selecting the *Preserve Case* or *Preserve Position* property, then the following additional properties are set.

    - The *Preserve Length* property is enabled and *Allow Short Data* property is set to *Yes*, by default. These two properties are not modifiable.
    - The retention of characters or digits from the left and the right are disabled, by default. The *From Left* and *From Right* properties are both set to zero.

11. Click **Save**.
    A message *Data Element has been saved successfully* appears.

5.1.1.2 Creating a Structured FPE Data Element

This section describes the steps to create a structured FPE data element.

To create a structured FPE data element:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Elements & Masks** > **Data Elements**.
2. Click **Add New Data Element**.
   The **New Data Element** screen appears.
3. Select **Structured** from **Type**.
4. Type a unique name for the data element in the **Name** textbox.

> **Note:** Ensure that the length of the data element name does not exceed 55 characters.

5. Type the required description for the data element in the **Description** textbox.
6. Select **FPE NIST 800-38G** from the **Method** drop-down.
7. Select a data type from the **Plaintext Alphabet** drop-down.
8. Select the encoding type from the **Plaintext Encoding** drop-down.

> **Note:** If you are using Format Preserving Encryption (FPE) and Byte APIs, then ensure that the encoding, which is used to convert the *string* input data to *bytes*, matches the encoding that is selected in the **Plaintext Encoding** drop-down for the required FPE data element.

9. Configure the minimum input length from the **Minimum Input Length** text box.
10. Select the tweak input mode from the **Tweak Input Mode** drop-down.
    For more information about the tweak input mode, refer to the section *Tweak Input* in the *Protection Methods Reference Guide 9.1.0.5*.
11. Select the short data configuration from the **Allow Short Data** drop-down.

> **Note:** FPE does not support data less than 2 bytes, but you can set the minimum message length value accordingly.

    For more information about length preservation and short tokens, refer to section *Length Preserving* in *Protection Methods Reference Guide 9.1.0.5*.

> **Note:**
> If you are create a short data token in a policy and then deploy the policy, the **Forensics** displays a policy deployment warning indicating that the data element has unsupported settings.
>
> For protectors v6.6.x, the warning indicates that short data tokens and data elements cannot be deployed. The policy is deployed.
>
> For protectors v7.x.x, the warning appears as a cautionary and can be ignored. The policy is deployed successfully.

12. Enter the required input characters to be retained in the clear in the **From Left** and **From Right** text box.
    For more information about this setting, refer to the section *Left and Right Settings* in the *Protection Methods Reference Guide 9.1.0.5*.
13. Configure any special numeric data handling request, such as Credit Card Number (CCN), in the **Special numeric alphabet handling** drop-down.
    For more information about handling special numeric data, refer to the section *Handling Special Numeric Data* in the *Protection Methods Reference Guide 9.1.0.5*.
14. Click **Save**.

A message *Data Element has been saved successfully* appears.

5.1.2 Creating Data Elements for Unstructured Data

You create an unstructured type of data elements for File Protector or Big Data Protector (with *HDFSFP*) policies. This section describes the steps to create a data element for an unstructured data type.

To create an unstructured data element:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Elements & Masks** > **Data Elements**.
2. Click **Add New Data Element**.
   The **New Data Element** screen appears.
3. Select **Unstructured** from **Type**.
4. Type a unique name for the data element in the **Name** textbox.

   > **Note:** Ensure that the length of the data element name does not exceed 55 characters.

5. Type the required description for the data element in the **Description** textbox.
6. Select one of the following encryption methods from the **Method** drop-down:
   - 3DES
   - AES-128
   - AES-256
7. If you want to enable multiple instances of keys with the data element, then check the **Use Key ID (KID)** checkbox.
8. Click **Save**.

A message *Data Element has been saved successfully* appears.

5.2 Working with Alphabets

This section provides information about the **Alphabets** tab in the **Data Elements & Masks** screen.

The Unicode Gen2 token type gives you the liberty to customize how the protected token value is returned. It allows you to leverage existing internal alphabets or create custom alphabets by defining code points.

The Alphabets tab applies to a Unicode Gen2 data element. Though some alphabets are preloaded, you can also create custom alphabets using code points. This flexibility allows you to create token values in the same Unicode character set as the input data.

For more information about the code points and considerations around creating alphabets, refer to the section *Code Points in Unicode Gen2 Token Type* in the *Protegrity Protection Methods and Reference Guide 9.1.0.5*.

The following figure shows the **Alphabet** screen.

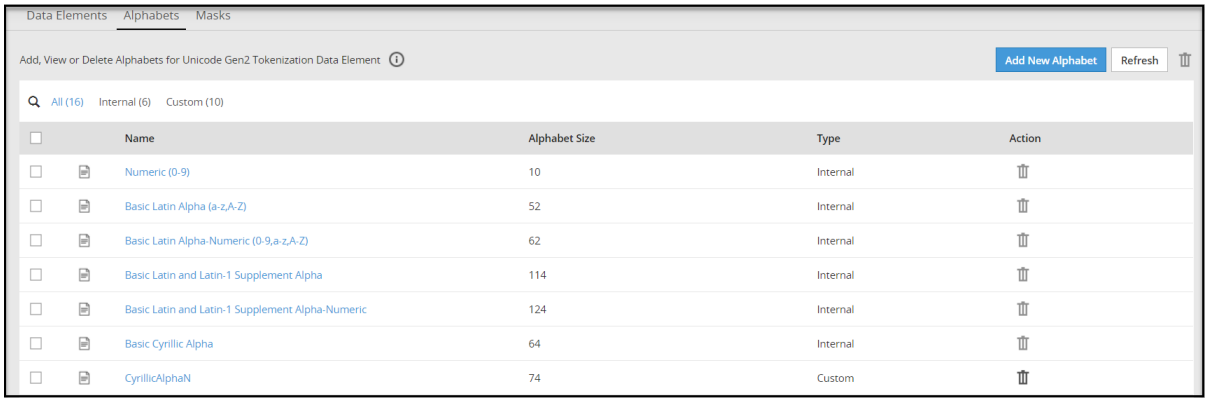


Figure 5-2: Alphabet Screen

5.2.1 Creating an Alphabet

The following procedure describes the steps to create an alphabet. An alphabet can include multiple alphabet templates, for example, an alphabet can be created to generate a token value, which is a mix of Numeric and Cyrillic characters.

To create an alphabet:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Elements & Masks** > **Alphabets**.
2. Click **Add New Alphabet**.
   The **New Alphabet** screen appears.
3. Enter a unique name for the alphabet in the **Name** text box.
4. Under the **Alphabet** tab, click **Add** to add existing alphabets or custom code points to the new alphabet.
   The *Add Alphabet entry* screen appears.

> **Note:** If you plan to use multiple alphabet entries to create a token alphabet, then click **Add** again to add other alphabet entries.

> **Note:** Ensure that code points in the alphabet are supported by the protectors using this alphabet.

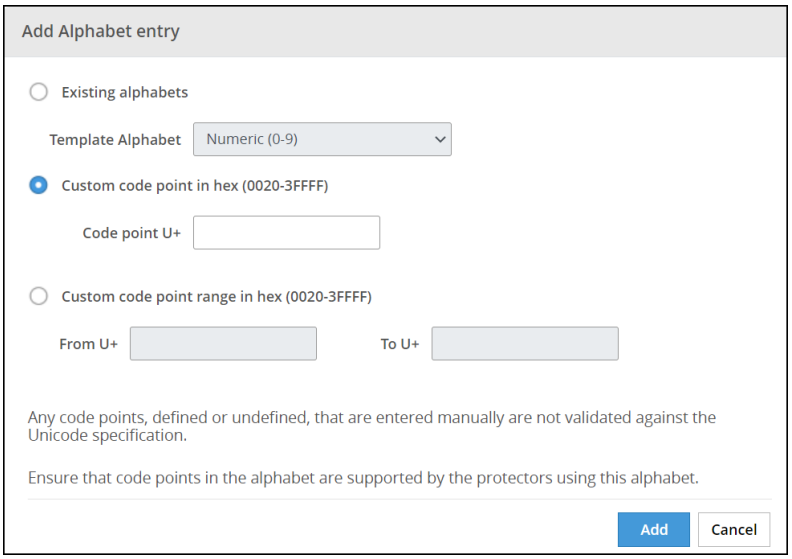


Figure 5-3: Add Alphabet entry screen

5. Select either an existing alphabet, create a custom code points, or define a range of code points.
   The following options are available for creating an alphabet.

   Important: For the *SLT_1_3* tokenizer, you must include a minimum of 10 code points and a maximum of 160 code points.

   Important: For the *SLT_X_1* tokenizer, you must include a minimum of 161 code points and a maximum of 100k code points.

   Table 5-4: Alphabet options

Alphabet option	Description
Existing Alphabets	Select one of the existing alphabets. The list includes internal and custom alphabets.
Custom code point in hex (0020-3FFFF)	Add custom code points that will be used to generate the token value.
Custom code point range in hex (0020-3FFFF)	Add a range of code points that will be used to generate the token value. **Note:** When creating an alphabet using the code point range option, note that the code points are not validated. For more information about consideration related to defining code point ranges, refer to the section *Code Point Range in Unicode Gen2 Token Type* in the *Protegrity Protection Methods and Reference Guide 9.1.0.0*.

6. Click **Add** to add the alphabet entry to the alphabet.
7. Click **Save** to save the alphabet.

   Important: Only the alphabet characters that are supported by the OS fonts are displayed on the Web UI.

A message *Alphabet has been created successfully* appears.

5.3 Working with Masks

This section provides information about the **Masks** tab in the **Data Elements & Masks** screen.

Masks are a pattern of symbols and characters, that when imposed on a data field obscures its actual value to the viewer of that data. For example, you might want to mask out characters from credit cards and Social Security numbers. Masks can obscure data completely or partially. For example, a partial mask might display the last four digits of a credit card on a grocery store receipt.

For more information about the Masks option, refer to the section *Masks* in the *Protegrity Protection Methods and Reference Guide 9.1.0.5*.

The following figure shows the **New Mask** screen.

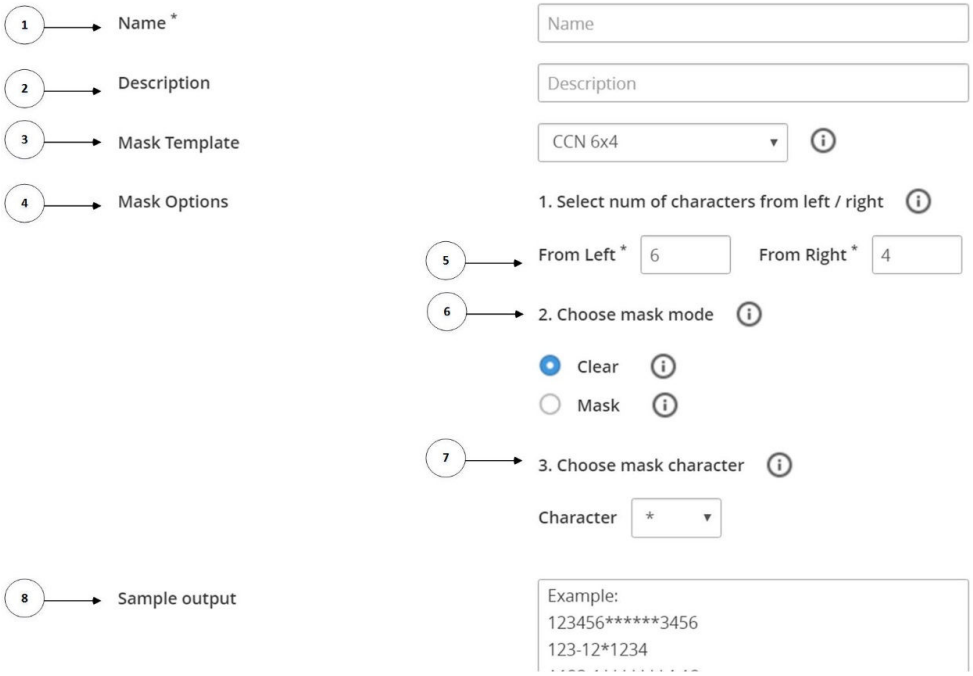


Figure 5-4: New Mask Screen

The following table provides the description for each element available on the Web UI.

Table 5-5: Mask Fields

Callout	UI Element	Description
1	Name	Unique name to identify the mask.
2	Description	Text describing the mask.
3	Mask Template	Mask templates for masking the data.For more information about the mask templates, refer to *Table 3-5 Mask Templates*.
4	Mask Options	Following options are available to mask the data: • Mask character • Mask Mode • Selection of characters
5	From Left / From Right	Select the text to be masked from left and from the right.
6	Mask Mode	If the masking is in clear or masked.
7	Mask Character	The character to mask the data.
8	Sample Output	The output based on the select template and mask mode.

The following table shows the different mask mode templates.

Table 5-6: Mask Templates

Mask Template	Mask Mode-Clear	Mask Mode-Mask
CCN- 6*4	Template to retain six characters from left and four characters from right in clear. For example, 123456******3456 123-12*1234	Template to mask six characters from left and four characters from right. For example, ******789012**** ******-****

Mask Template	Mask Mode-Clear	Mask Mode-Mask
	A123-1*******4-12	******234-123****
CCN 12*0	Template to retain 12 characters from left and no characters from right in clear. For example, 123456789012**** 123-12-1234 A123-1234-12*****	Template to mask 12 characters from left but no characters from right. For example, **********3456 ********** **********34-12
CCN 4*4	Template to retain four characters from left and four characters from right in clear. For example, 1234********3456 123-***1234 A123*********4-12	Template to mask four characters from left and four characters from right. For example, ****56789012**** ****12-**** ****-1234-123****
SSN x-4	Template to retain no characters from left but only four characters from right in clear. For example, **********3456 *******1234 **********4-12	Template to mask no characters from left but four characters from right. For example, 123456789012**** 123-12-**** A123-1234-123****
SSN 5-x	Template to retain five characters from left but no characters from right. For example, 12345********** 123-1****** A123-**********	Template to mask five characters from left but no characters from right. For example, *****67890123456 *****2-1234 *****1234-1234-12

5.3.1 Creating a mask

The following procedure describes the steps to create a mask with the CCN-6*4 template with mask mode as clear.

To create a mask:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Elements & Masks** > **Masks**.
2. Click **Add New Mask**.

The **New Mask** screen appears.

3. Enter a unique name for the mask in the **Name** text box.
4. Enter the required description for the mask in the **Description** textbox.
5. Select **CCN 6X4** from the **Mask Template** drop-down.
6. Select **Clear** from **Mask Mode**.
7. Select the required masking character from the **Character** drop-down.
8. Click **Save**.

A message *Mask has been saved successfully* appears.

5.4 Working with Trusted Applications

The Trusted Applications (TA) is an entity that defines which system users and applications are authorized to run the Application Protector (AP) Java to protect data. Any application or its system user, must be added in the Trusted Application to use the AP Java. These custom applications and the authorized system users, are added to the Trusted Application.

Trusted Application does not support the capability of adding multiple users and applications in a single Trusted Application instance. In a Trusted Application, you can add only one application and its corresponding system user. If you want to add multiple users and applications, then you must create Trusted Application for each application and its corresponding system user.

5.4.1 Creating a Trusted Application

The following procedure describes the steps to create a trusted application.

➤ To make an application trusted:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Trusted Applications**.
2. Click **Add New Trusted Application**.
   The **New Trusted Application** screen appears.

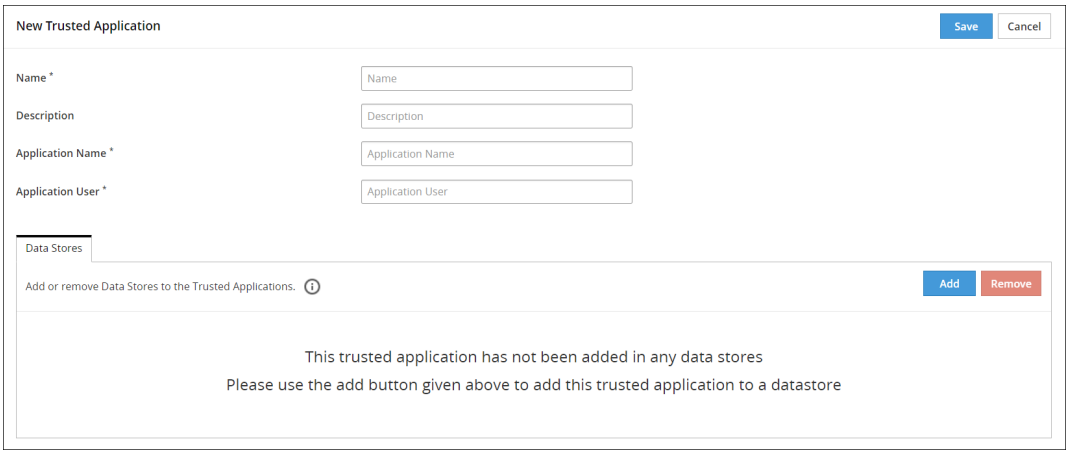


Figure 5-5: New Trusted Application Screen

3. Type a unique name to the trusted application in the **Name** textbox.
4. Type the required description to the trusted application in the **Description** textbox.

5. Type the name of the AP Java, AP Python or AP Go application in the **Application Name** textbox.

   Note: The maximum length of an Application Name is up to 64 characters.

   Note: In case of AP Java and AP Go applications, ensure that you specify the complete module or package name.

   Note:
   In the application name, you can type the asterisk (*) wild card character to represent multiple characters or the question mark (?) wild card character to represent a single character. You can also use multiple wild card characters in the application name.

   For example, if you specify *Test_App** as the application name, then you can use applications with names, such as, *Test_App1* or *Test_App123* to perform security operations.

   Caution:
   Use wild card characters with discretion, as they can potentially lead to security threats.

6. Type the user of the AP Java, AP Python or AP Go application in the **Application User** textbox.

   Note:
   In the application user name, you can type the asterisk (*) wild card character to represent multiple characters or the question mark (?) character to represent a single character. You can also use multiple wild card characters in the application user name.

   For example, if you specify *User** as the application user name, then you can have users with names, such as, *User1* or *User123* to perform security operations.

   Caution:
   Use wild card characters with discretion, as they can potentially lead to security threats.

7. If an audit record is required every time a trusted application loads the AP Java jar file or invokes the AP Python or AP Go APIs, then select the **Successful Audit** slider to generate audit logs.
8. Click **Save**.

A message *Trusted Application has been created successfully* appears.

5.4.2 Linking Data Store to a Trusted Application

You link a data store with the trusted application to specify the location where to deploy the trusted application. Using the following steps, you can link a trusted application to a data store.

To link a trusted application to a data store:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Trusted Applications**.
   The list of all the trusted applications appear.

2. Select the required trusted application.
   The screen to edit the trusted application appears.
3. Under the Data Stores tab, click **Add**.
   The screen to add the data stores appears.
4. Select the required data stores.
5. Click **Add**.

A message *Select Data Stores have been added to Trusted Application successfully* appears.

5.4.3 Deploying a Trusted Application

This section describes the steps to deploy a trusted application.

Deploying a trusted application consists of the following two states:

- *Readying the Trusted Application for deployment*
- *Deploying the Trusted Application*

5.4.3.1 Readying the Trusted Application for deployment

The following procedure describes the steps to make a trusted application ready for deployment.

Before you begin
After you link data stores to your trusted application, it is ready to be deployed to the protector nodes.

➤ To make a trusted application ready for deployment:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Trusted Applications**.
   The list of all the trusted applications appear.
2. Select the required trusted application.
   The screen to edit the trusted application appears.
3. Click **Ready to Deploy**.

A message *Trusted Application has been marked ready to deploy* appears.

The **Deploy** action is active.

5.4.3.2 Deploying the Trusted Application

The following procedure describes the steps to deploy the trusted application.

Before you begin
You deploy the policy to the data store after the trusted application is ready for deployment. If no data stores are linked with the trusted application, then the deployment of the trusted application fails.

➤ To deploy the trusted application:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Trusted Applications**.
   The list of all the trusted applications appear.
2. Select the required application that is in the ready to deploy state.
   The screen to edit the trusted application appears.
3. Click **Deploy**.

A message *Trusted application has been successfully deployed* appears.

The ESA PEP server stores the trusted application information in the database and then publishes it to the shared memory. During deployment, the PEP server of the Application Protector Java accesses this information from the shared memory. It validates the information and in the event of validation failure, generates an audit log entry with the detailed information.

5.5 Working with Member Sources

The Member Sources are the physical locations of users and user groups to be involved in the policies.

The users can come from the following types of sources:

- User directory, such as:
  - LDAP
  - Posix LDAP
  - Active Directory
- Database
  - Teradata
  - Oracle
  - SQL Server
  - DB2
  - PostgreSQL
- File

Using these source types, you configure the connection to a directory to retrieve information on the users and the user groups available.

When you configure the connection to any member source, you can verify if the connection parameters that you have specified are correct and the users and groups can be retrieved from the member source. On clicking **Test** adjacent to the member source entry from the list or from the respective member source screen, the **Test Member Source Connection** dialog box displays the status with the following parameters: connection, authentication, groups, and users.

> **Note:**
> The password length of a member source on some platforms may have a limitation.

5.5.1 Configuring File Member Source

You use the File type to obtain users or user groups from a text file. These text files reference individual members and groups of members.

In Policy Management, the *exampleusers.txt* and *examplegroups.txt* are sample member source files that contain a list of users or groups respectively. These files are available on the ESA Web UI. You can edit them to add multiple user name or user groups.

The *examplegroups.txt* has the following format.

```
[Examplegroups]
<groupusername1>
<groupusername2>
<groupusername3>
```

Note: Ensure that the file has read permission set for Others.

Important:
Ensure that the *\U* character is not present in the *exampleusers.txt* or *examplegroups.txt* files.

5.5.1.1 Viewing the List of Users and Groups in the Sample Files

This sections describes the steps to view the list of users and groups in the sample files.

To view list of users and groups in the sample files:

1. On the ESA Web UI, navigate to **Settings** > **Systems** > **Files**.
2. Click **View**, corresponding to *exampleusers.txt* or *examplegroups.txt* under **Policy Management-Member Source Service User Files** and **Policy Management-Member Source Service Group Files** respectively.

The list of users in the *exampleuser.txt* file or *examplegroups.txt* file appear.

5.5.1.2 Creating File Member Source

This section describes the procedure on how to create a file member source.

To create file member source:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Source** > **Member Sources**.
2. Click **Add New Member Source**.
   The **New Member Source** screen appears.
3. Type a unique name of the file member source in the **Name** textbox.
4. Type the required description in the **Description** textbox.
5. Select **File** from the **Source Type** drop-down list.
6. Select **Upload file** from the **User File** drop-down list.
7. Click the **Browse..** ( ) icon to open the file browser.
8. Select the required file.

9. Click **Upload File** ( ) icon.
   A message *User File has been uploaded successfully* appears.
10. Select **Upload file** from the **User File** drop-down list.
11. Click the **Browse..** ( ) icon to open the file browser.
12. Select the required file.
13. Click **Upload File** ( ) icon.
    A message *Group File has been uploaded successfully* appears.
14. Click **Save**.

A message *Member Source has been created successfully* appears.

5.5.2 Configuring Database Member Source

This section explains the process to configure a Database Member Source.

You use the Database type to obtain users from database, such as, SQL Server, Teradata, DB2, PostgreSQL, or Oracle. An ODBC connection to the database must be setup to retrieve user information.

The following table describes the connection variable settings for the databases supported in Policy Management.

Table 5-7: Database Types and DSN Names

Database Type	Database
SQLSERVER	System DSN Name (ODBC) For example, *SQLSERVER_DSN*.
TERADATA	System DSN Name (ODBC) For example, *TD_DSN*.
ORACLE	Transport Network Substrate Name (TNSNAME).
DB2	System DSN Name (ODBC) For example, *DB2DSN*.
POSTGRESQL	System DSN Name For example, *POSTGRES*.

5.5.2.1 Creating Database Member Source

This section describes the procedure on how to create a database member source.

To create a Database Member Source:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Source** > **Member Sources**.
2. Click **Add New Member Source**.
   The **New Member Source** screen appears.
3. Type a unique name for the file member source in the **Name** text box.

4. Type the required description in the **Description** text box.
5. Select **Database** from the **Source Type** drop-down list.
6. Select one of the following database from the **Source** drop-down list.
   - Teradata
   - Oracle
   - SQL Server
   - DB2
   - PostgreSQL
7. To enable the usage of a custom data source name, switch the **Use Custom DSN** toggle.
   a. Enter the custom data source name in the **DSN** text box.
      Ensure that the specified DSN is present in the *odbc.ini* configuration file located in the */opt/protegrity/mbs/conf/* directory.
8. If you are selecting the Oracle database as the source database, then enter the service name in the **Service Name** text box.

   > **Note:**
   > This step is applicable for the Oracle database only.

9. If you are not using *Custom DSN*, then the following steps are applicable.
   a. Enter the database name in the **Database** text box.
   b. Enter the host name in the **Host** text box.
   c. Enter the port to connect to the database in the **Port** text box.
10. Enter the username in the **Username** text box.
11. Enter the password in the **Password** text box.
12. Click **Save**.

The message *Member Source has been created successfully* appears.

5.5.3 Configuring LDAP Member Source

This section provides information on how to configure Lightweight Directory Access Protocol (LDAP) Member Source.

Before you begin

You use the Lightweight Directory Access Protocol (LDAP) type user source to retrieve information on users and user groups from a LDAP Server, which facilitates users and directory services over an IP network and provides Web Services for Application Protector.

To create an LDAP member source:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Source** > **Member Sources**.
2. Click **Add New Member Source**.
   The **New Member Source** screen appears.
3. Type a unique name of the file member source in the **Name** textbox.
4. Type the required description in the **Description** textbox.

5. Select **LDAP** from the **Source Type** drop-down list.
6. Select **LDAP** from the **Source Type** drop-down list.
   The **LDAP Member Source** screen appears

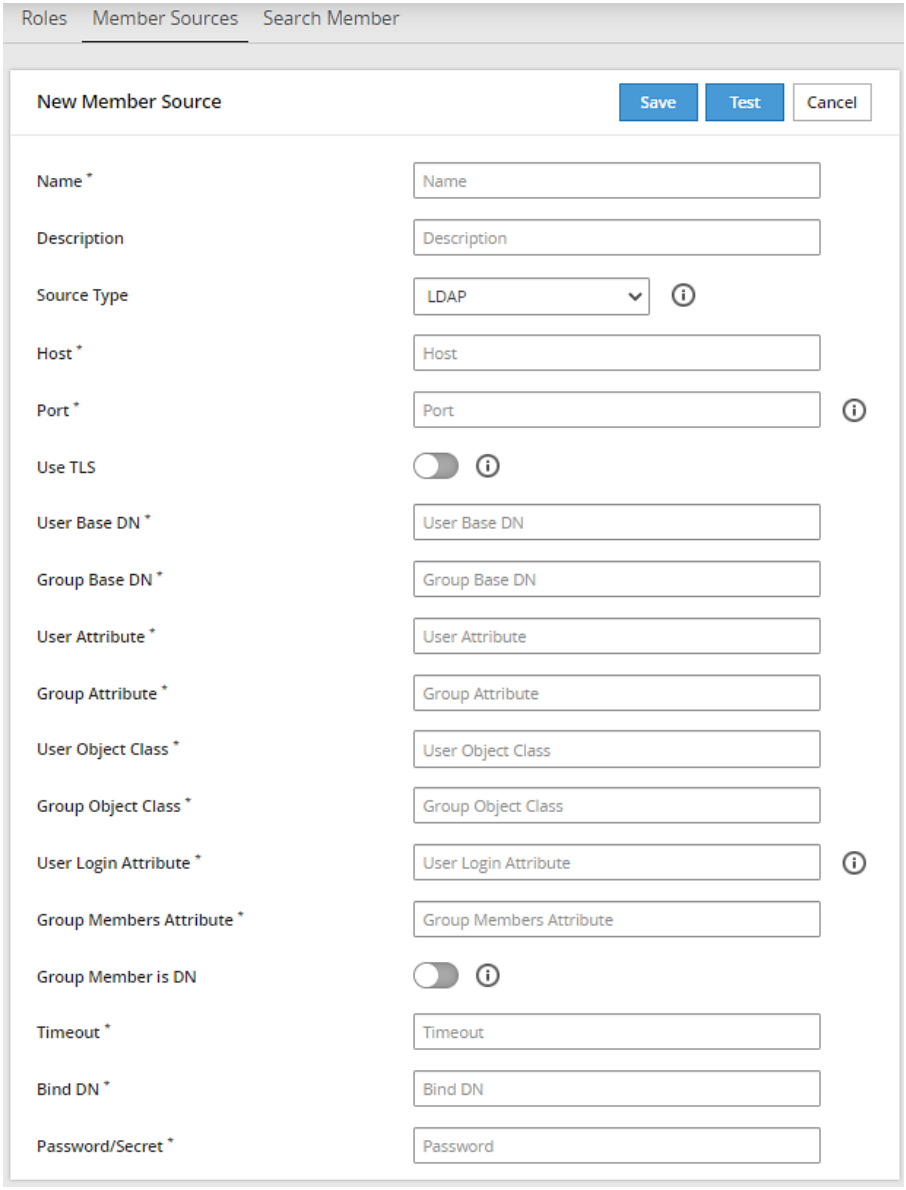


Figure 5-6: LDAP Member Source screen

.

7. Enter the required information in the LDAP member source fields.
   The following table describes the directory fields for LDAP member sources.

Table 5-8: LDAP Fields

Field Name	Description
Host	The Fully Qualified Domain Name (FQDN), or IP of the directory server. Port The network port on the directory server where the service is listening.
Port	The network port on the directory server where the service is listening.
Use TLS	The TLS is enabled to create a secure communication to the directory server. LDAPS, which is deprecated, is no longer the supported protocol. TLS is the only supported protocol.
User Base DN	The base distinguished name where users can be found in the directory. The user Base DN is used as the user search criterion in the directory.

Field Name	Description
Group Base DN	The base distinguished name where groups can be found in the directory. The group base dn is used as a group search criterion in the directory.
User Attribute	The Relative Distinguished Name (RDN) attribute of the user distinguished name.
Group Attribute	The RDN attribute of the group distinguished name.
User Object Class	The object class of entries where user objects are stored. Results from a directory search of users are filtered using user object class.
Group Object Class	The object class of entries where group objects are stored. Results from a directory search of groups are filtered using group object class.
User Login Attribute	The attribute intended for authentication or login.
Group Members Attribute	The attribute that enumerates members of the group.
Group Member is DN	The members may be listed using their fully qualified name, for example, their distinguished name or as in the case with the Posix user attribute (cn) value.
Timeout	The timeout value when waiting for a response from the directory server.
Bind DN	The DN of a user that has read access, rights to query the directory.
Password/Secret	The password of the user binding to the directory server

Note: Parsing users from a DN instead of querying the LDAP server: 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.

8. Click **Save**.

A message *Member Source has been created successfully* appears.

5.5.4 Configuring Posix LDAP Member Source

You use Posix LDAP to retrieve information on users and user groups from an internal LDAP Server that uses the Posix schema.

Before you begin
You can retrieve users and user groups from any external LDAP and Posix LDAP. The internal LDAP available on ESA, uses the Posix schema. Thus, when using ESA, it is recommended to use Posix LDAP to configure the connection with the internal ESA LDAP.

To create a Posix LDAP member source:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Source** > **Member Sources**.
2. Click **Add New Member Source**.
   The **New Member Source** screen appears.
3. Type a unique name of the file member source in the **Name** textbox.
4. Type the required description in the **Description** textbox.
5. Select **Posix LDAP** from the **Source Type** drop-down list.
   The **Posix LDAP Member Source** screen appears.

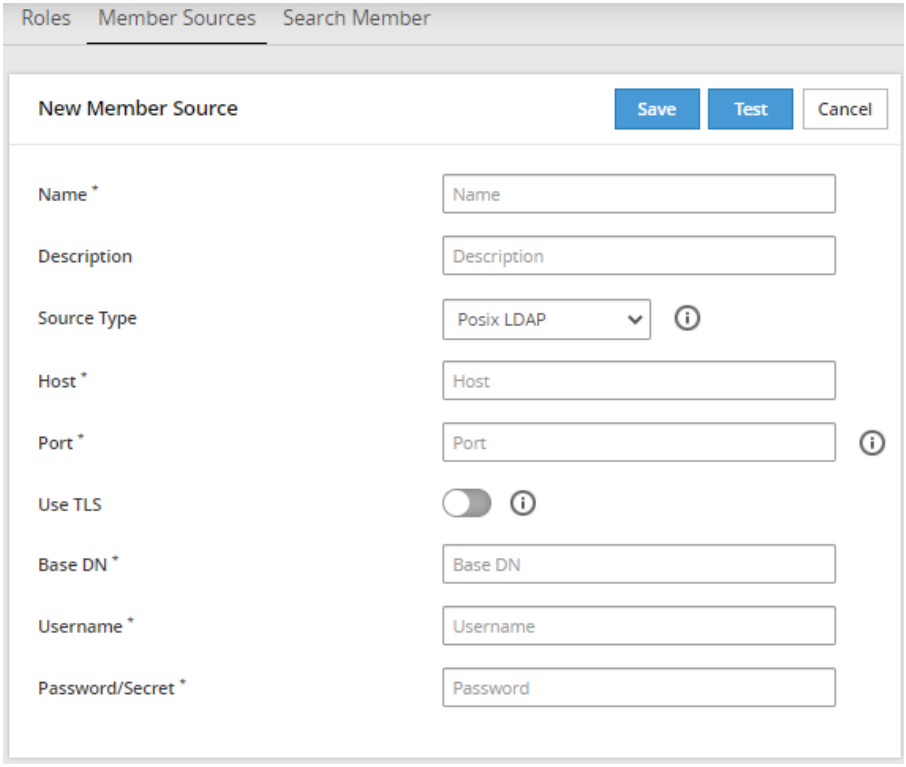


Figure 5-7: Posix LDAP Member Source screen

6. Enter the required information in the directory fields.
   The following table describes the directory fields for Posix LDAP member source.

Table 5-9: Posix LDAP Fields

Field Name	Description
Host	The Fully Qualified Domain Name (FQDN), or IP of the directory server.
Port	The network port on the directory server where the service is listening.
Use TLS	The TLS can be enabled to create a secure communication to the directory server.
Base DN	The base distinguished name where users can be found in the directory.
Username	The username of the Posix LDAP server.
Password/Secret	The password of the user binding to the directory server.

7. Click **Save**.

A message *Member Source has been created successfully* appears.

5.5.5 Configuring Active Directory Member Source

You use the Active Directory type external source to retrieve information on users and user groups from an Active Directory, which organizes corporate information on users, machines, and networks in a structural database.

➤ To create an Active Directory member source:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Source** > **Member Sources**.
2. Click **Add New Member Source**.
   The **New Member Source** screen appears.

3. Type a unique name of the file member source in the **Name** textbox.
4. Type the required description in the **Description** textbox.
5. Select **Active Directory** from the **Source Type** drop-down list.
   The **Active Directory Member Source** screen appears.

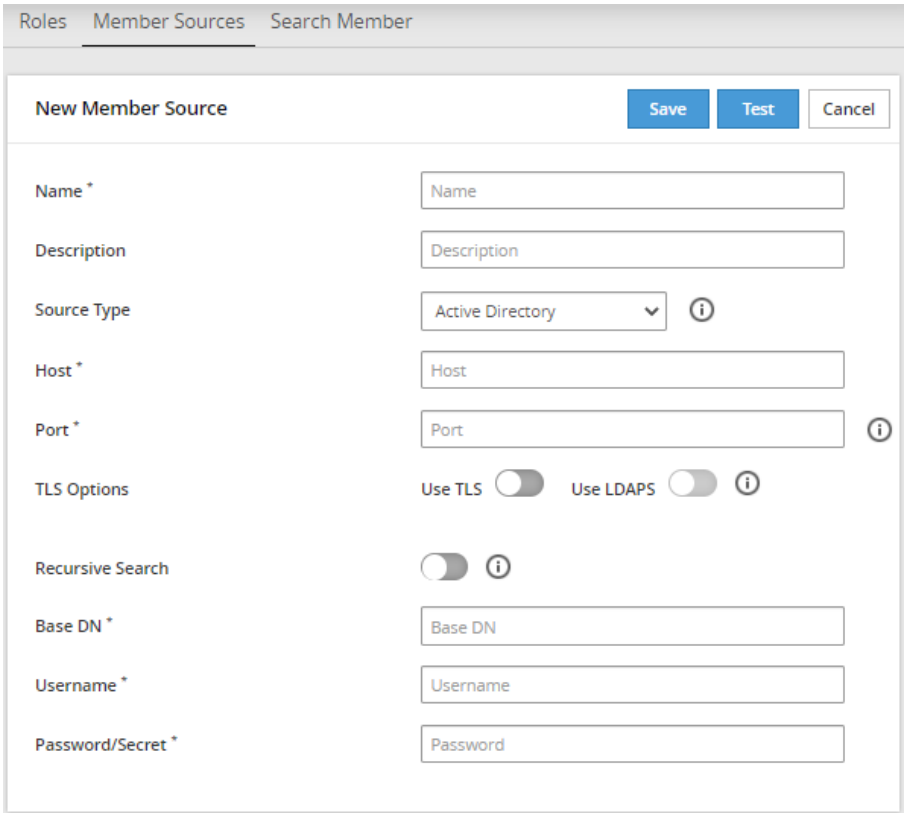


Figure 5-8: Active Directory Member Source screen

6. Enter the required information in the directory fields.
   The following table describes the directory fields for Active Directory member sources.

Table 5-10: Directory Fields

Field Name	Description
Host	The Fully Qualified Domain Name (FQDN), or IP of the directory server.
Port	The network port on the directory server where the service is listening.
TLS Options	• The **Use TLS** option can be enabled to create secure communication to the directory server. • The **Use LDAPS** option can be enabled to create secure communication to the directory server. LDAPS uses TLS/SSL as a transmission protocol. **Note:** Selection of the LDAPS option is dependent on selecting the TLS option. If the TLS option is not selected, then the LDAPS option is not available for selection.
Recursive Search	The recursive search can be enabled to search the user groups in the active directory recursively. For example, consider a user group U1 with members User1, User2, and Group1, and Group1 with members User3 and User4. If you list the group members in user group U1 with recursive search enabled, then the search result displays User1, User2, User3, and User4.
Base DN	The base distinguished name where users can be found in the directory.
Username	The username of the Active Directory server.
Password/Secret	The password of the user binding to the directory server.

7. Click **Save**.

A message *Member Source has been created successfully* appears.

5.5.6 Configuring Azure AD Member Source

You 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.

To create an Azure AD member source:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Sources** > **Member Sources**.
2. Click **Add New Member Source**.
   The **New Member Source** screen appears.
3. Type a unique name of the Azure AD member source in the **Name** textbox.
4. Type the required description in the **Description** textbox.
5. Select **Azure AD** from the **Source Type** drop-down list.
   The **Azure AD Member Source** screen appears.

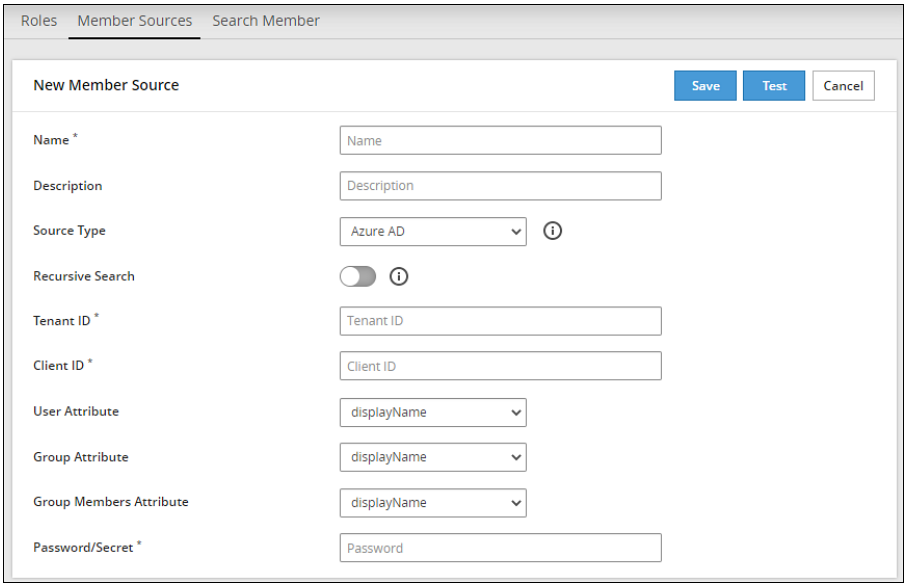


Figure 5-9: Azure AD Member Source screen

6. Enter the required information in the directory fields.
   The following table describes the directory fields for the Azure Active Directory member sources.

Table 5-11: Azure AD Fields

Field Name	Description
Recursive Search	The recursive search can be enabled to search the user groups in the Azure AD recursively.
Tenant ID	The unique identifier of the Azure AD instance
Client ID	The unique identifier of an application created in Azure AD
User Attribute	The Relative Distinguished Name (RDN) attribute of the user distinguished name. The following user attributes are available:

Field Name	Description
	• *displayName* - The name displayed in the address book for the user. • *userPrincipalName* - The user principal name (UPN) of the user. • *givenName* - The given name (first name) of the user. • *employeeId* - The employee identifier assigned to the user by the organization. • *id* - The unique identifier for the user. • *mail* - The SMTP address for the user. • *onPremisesDistinguishedName* - Contains the on-premises Active Directory distinguished name (DN). • *onPremisesDomainName* - Contains the on-premises domainFQDN, also called dnsDomainName, synchronized from the on-premises directory. • *onPremisesSamAccountName* - Contains the on-premises samAccountName synchronized from the on-premises directory. • *onPremisesSecurityIdentifier* - Contains the on-premises security identifier (SID) for the user that was synchronized from the on-premises setup to the cloud. • *onPremisesUserPrincipalName* - Contains the on-premises userPrincipalName synchronized from the on-premises directory. • *securityIdentifier* - Security identifier (SID) of the user, used in Windows scenarios.
Group Attribute	The RDN attribute of the group distinguished name. The following group attributes are available: • *displayName* - The display name for the group. • *id* - The unique identifier for the group. • *mail* - The SMTP address for the group. • *onPremisesSamAccountName* - Contains the on-premises SAM account name synchronized from the on-premises directory. • *onPremisesSecurityIdentifier* - Contains the on-premises security identifier (SID) for the group that was synchronized from the on-premises setup to the cloud. • *securityIdentifier* - Security identifier of the group, used in Windows scenarios.
Group Members Attribute	The attribute that enumerates members of the group. **Note:** Ensure to select the same *Group Members Attribute* as the *User Attribute*. The following group members attributes are available: • *displayName* - The name displayed in the address book for the user. • *userPrincipalName* - The user principal name (UPN) of the user. • *givenName* - The given name (first name) of the user. • *employeeId* - The employee identifier assigned to the user by the organization. • *id* - The unique identifier for the user. • *mail* - The SMTP address for the user. • *onPremisesDistinguishedName* - Contains the on-premises Active Directory distinguished name (DN). • *onPremisesDomainName* - Contains the on-premises domainFQDN, also called dnsDomainName, synchronized from the on-premises directory. • *onPremisesSamAccountName* - Contains the on-premises samAccountName synchronized from the on-premises directory. • *onPremisesSecurityIdentifier* - Contains the on-premises security identifier (SID) for the user that was synchronized from the on-premises setup to the cloud. • *onPremisesUserPrincipalName* - Contains the on-premises userPrincipalName synchronized from the on-premises directory.

Field Name	Description
	• *securityIdentifier* - Security identifier (SID) of the user, used in Windows scenarios.
Password/Secret	The client secret is the password/secret of the Azure AD application.

7. Click **Save**.

A message *Member Source has been created successfully* appears.

5.6 Working with Roles

The authorization criteria for each user is defined in form of members of roles. Roles determine and define the unique data access privileges for each member. Each role is associated with a level of authorization granted to all its members, including specific data access privileges.

The following figure shows the New Role screen.

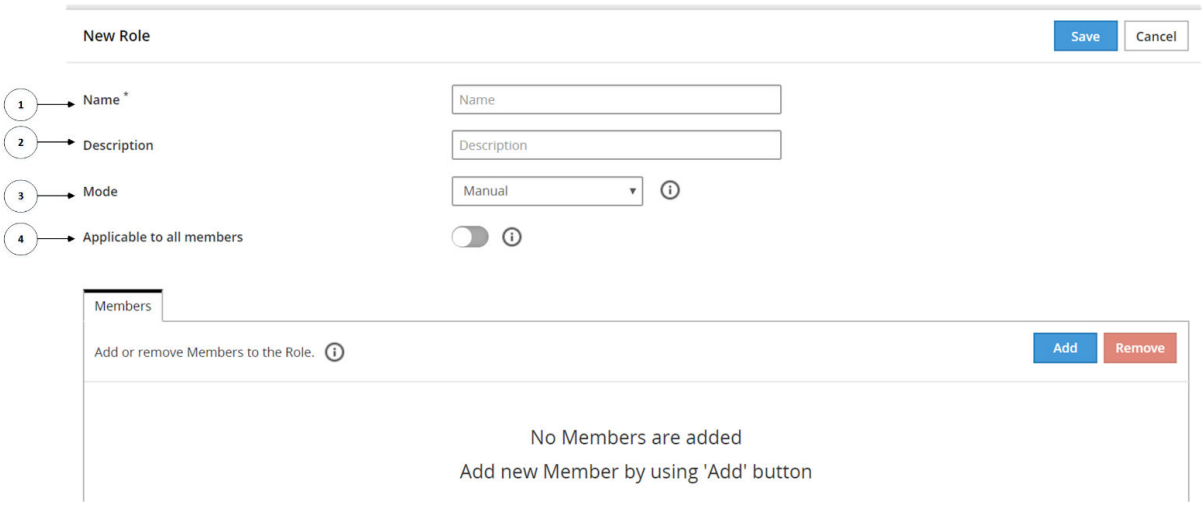


Figure 5-10: New Role Screen

The following table provides the description for each element available on the of the Web UI.

Table 5-12: Roles Fields

Callout	UI Element	Description
1	Name	The unique name of the role.
2	Description	The description of the role.
3	Mode	The refresh mode for that role. For more information about refresh mode, refer to section *Mode Types for a Role*.
4	Applicable to all members	If enabled, the specific role will be applied to any member that does not belong to any other role.

5.6.1 Creating a Role

This section describes the steps to create a role.

To create a role:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Source** > **Roles**.
2. Click **Add New Role**.
   The **New Role** screen appears.
3. Enter a unique name for the role in the **Name** textbox.

   > **Note:** Ensure that the length of the role name does not exceed 55 characters.

4. Enter the required description for the role in the **Description** textbox.
5. In the **Mode** drop-down, select a refresh mode.
   For more information about about mode types for a role, refer to section *Mode Types for a Role*.
6. If you want to apply this role to all members in all the member sources, click **Applicable to all members**. If enabled, the role is applied to all members in users or groups that do not belong to any other role.
7. Click **Save**.

> **Note:**
> When a Teradata Member Source (MBS) service is defined and member source roles are not defined in the DBC.ROLEMEMBERS table — results in a successful connection between the MBS service and the ESA. However, the roles table indicator is displayed in red, while all other section indicators appear in green.

5.6.2 Mode Types for a Role

The mode types for a role defines how roles are synchronized and then updated in a security policy. The users are refreshed in the policy as per the mode settings.

The modes that are available are Automatic, Semi-automatic, and Manual.

The synchronization of members can be described as follows. :

- **Synchronization between Hub Controller and Member Source:** The Member Source component is responsible for synchronization of the latest changes made in the external sources, such as LDAP, AD, file, or database. In the ESA, the HubController synchronizes with the Member Source to update the policy with any changes detected in roles once in an hour.

Automatic Mode

In automatic mode, groups from the member sources are synchronized periodically without user intervention. The synchronization happens every one hour. The updated policy is deployed automatically after the synchronization.

Semi-Automatic Mode

Semi-Automatic mode is similar to the automatic mode with the exception that you must synchronize the groups manually. The updated policy is deployed automatically after the manual synchronization.

For a new member added to a group, you can manually synchronize the changes by setting the mode to semi-automatic and by using the **Synchronize Members** button from the **Members** tab of a **Role** screen.

Manual Mode

The roles with mode type as Manual can accept both groups and users. You must manually synchronize the groups. After manual synchronization of members, you must set the policy as **Ready to Deploy** followed by deploying the policy manually.

For a new member added to a group, you can manually synchronize the changes by clicking the **Synchronize Members** button from the **Members** tab of a **Role** screen.

5.6.3 Adding Members to a Role

This section describes the steps to add members to a role.

To add members to a role:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Source** > **Roles**.
2. Click on the role name link to which you want to add members.
   The selected role screen appears.
3. In the **Members** tab, click **Add**.
   The **Add Members** screen appears.

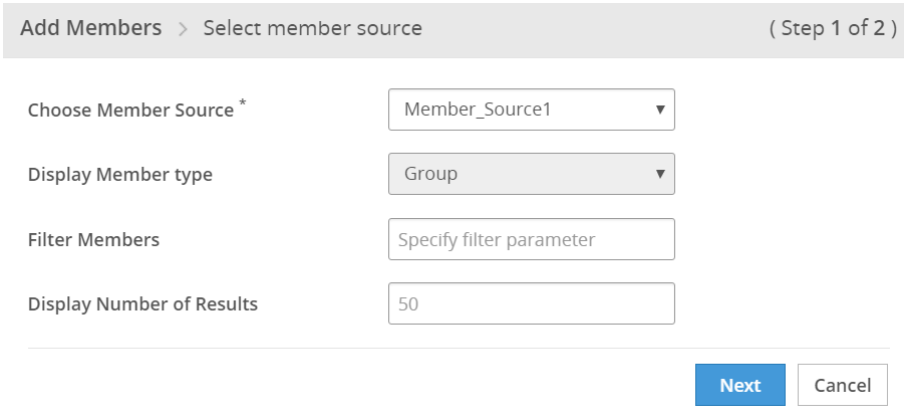


Figure 5-11: Add Members Screen

4. In the **Choose Member Source** drop-down, select the **Member Source**.
5. In the **Display Member Type** drop-down, select the member type.
   For **Automatic** or **Semi-Automatic** mode, it causes the removal of members of type Users from the role. The **Display Member Type** drop-down is disabled in this case with default Group member type.
6. Enter the filter parameter in the **Filter Members** text box.
   It accepts characters such as '*' to display all results or word search to search with a word.

   For more information about filtering members from AD and LDAP member sources, refer to the sections *Filtering Members from AD and LDAP Member Sources* and *Filtering Members from Azure AD Member Source*.
7. Select the number of display results in the **Display Number of Results** spin box.
8. Click **Next**.
   The step 2 of Add Members dialog box appears.

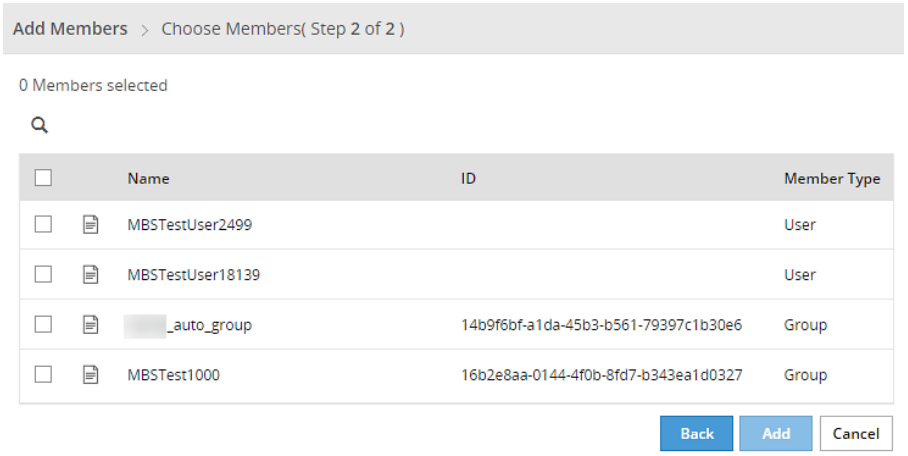
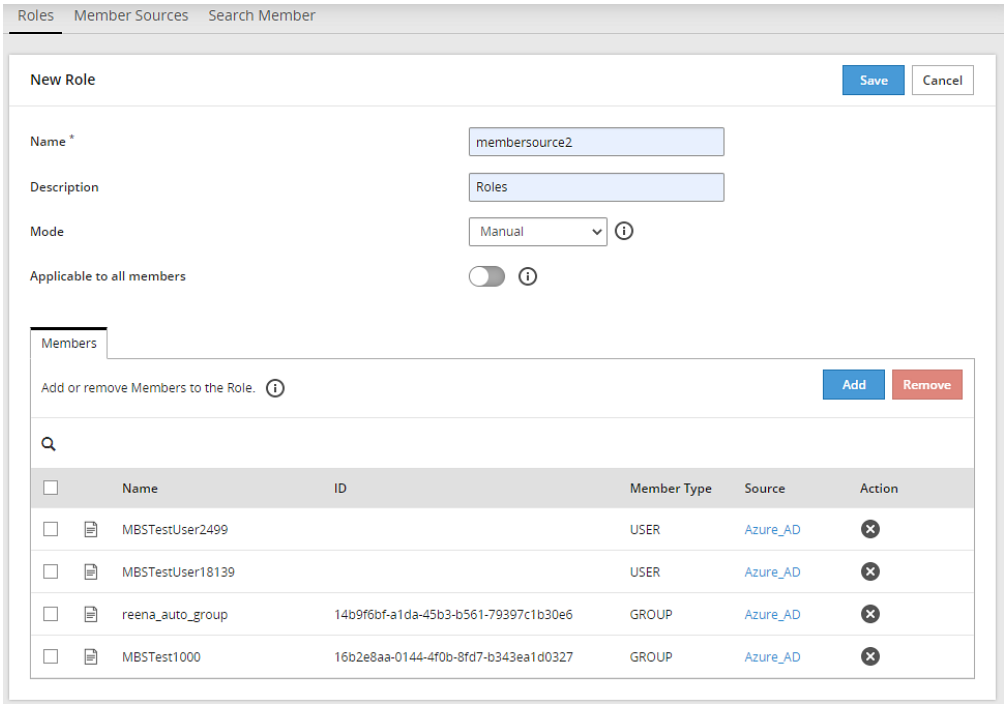


Figure 5-12: Choose Members

> **Note:** The **ID** column displays the unique identifier for the Azure AD, Posix LDAP and Active Directory member sources.

9. Select the check box next to each member you want to add.
10. Click **Add**.
    The selected members are added to the role.



> **Note:** The **ID** column displays the unique identifier for the Azure AD, Posix LDAP and Active Directory member sources.

Figure 5-13: Roles Screen

In addition to the **Members** tab, you can find:

- **Policies:** It displays all the policies that are linked to this role.
- **Data Stores:** It displays all the data stores that are linked to this role.

5.6.3.1 Filtering Members from AD and LDAP Member Sources

When adding members to a role, you can filter members from the member sources, such as, AD, LDAP, or POSIX LDAP. The filtering mechanism uses search filters based on the criteria for filtering the members from AD or LDAP. The search filters help you to query the member sources to fetch the exact results that you are looking for.

The following table lists some examples using different AD and LDAP search criteria to filter the members.

Table 5-13: Search Criteria

Search Criteria	Description
*	Retrieves all users and groups
Character or word search	Retrieves the results that contain the specified character or word
(cn=*protegrity*)	Retrieves all common names that contain the term *protegrity* in it
(sn=abc*)	Retrieves all surnames that starts with *abc*
(objectClass=*)	Retrieves all the results
(&(objectClass=user)(!(cn=protegrity)))	Retrieves all the users without the common name as *protegrity*
(&(cn=protegrity)(objectClass=user)(email=*))	Retrieves all the users with an email attribute and with common name as *protegrity*
(!(email=*))	Retrieves all the users without an email attribute
(&(objectClass=user)(| (cn=protegrity*)(cn=admin*)))	Retrieves all the users with common name that starts with *protegrity* or *admin*

If the input in the search filter includes special characters, then you must use the escape sequence in place of the special character to make it a valid input in the search filters.

The following table lists the escape sequence for each of the special characters.

Table 5-14: Usage of Special Characters in Search Filters

ASCII Character	Escape Sequence
(	\28
)	\29
*	\2A
\	\5C

The following table lists some examples of search filters with the usage of escape sequences to include special characters in the search input.

Table 5-15: Examples for Escaping Special Characters

Input with Special Character	Input with Escape Sequence	Description
(cn=protegrity*))	(cn=protegrity\2A\29)	The search filter retrieves the values that contain *protegrity*)* In this case, the parenthesis requires an escape sequence because it is unmatched.
(cn= abc (xyz) abc)		The search filter retrieves the values that contain *abc (xyz) abc* In this case, the escape sequence is not required as the parenthesis are matched.

5.6.3.2 Filtering Members from Azure AD Member Source

When adding members to a role, you can filter members from the Azure AD member source. The filtering mechanism uses search filters based on the criteria for filtering the members from the Azure AD. The search filters help you to query the member source to fetch the exact results that are required.

The following table lists an example for the Azure AD search criteria to filter the members.

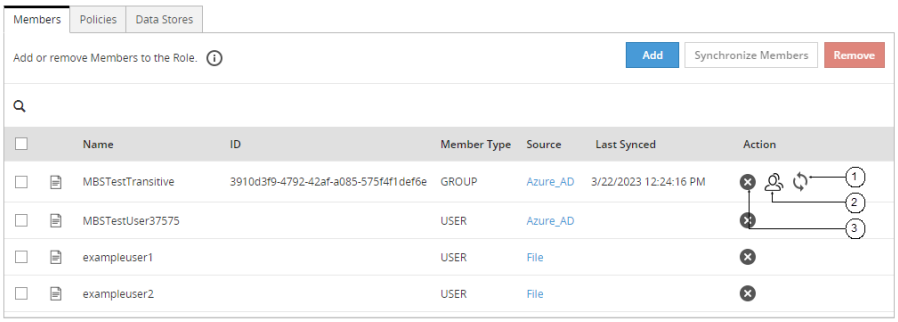
Table 5-16: Search Criteria

Search Criteria	Description
startsWith(displayname,'xyz')	Retrieves all groups and users that start with *xyz* **Note:** For more information and examples about the filter criteria for the Azure AD member source, search for the text *Advanced query capabilities on Azure AD* on Microsoft's Technical Documentation site at: *https://learn.microsoft.com/en-us/docs/*

5.6.4 Synchronizing, Listing, or Removing Members in a Role

When you add or delete members in a group, you need to synchronize the members in a role to reflect the updates done to the group.

The following figure explains the steps to synchronize, list or remove members in a role.



Note: The **ID** column displays the unique identifier for the Azure AD, Posix LDAP and Active Directory member sources.

Figure 5-14: Members Tab

The following table provides the description for each element available on the of the Web UI.

Table 5-17: Member Icon

Callout	Task Name	Steps
1	Synchronize Members	1. On the ESA Web UI, navigate to **Policy Management> Roles & Member Sources> Roles**. 2. Click **Synchronize Members** ( ). A status message appears.
2	List Group Members	1. On the ESA Web UI, navigate to **Policy Management> Roles & Member Sources> Roles**. 2. Click **List Group Members** ( ).

Callout	Task Name	Steps
		The dialog box appears with the list of all members in the group.
3	Remove Members	1. On the ESA Web UI, navigate to **Policy Management> Roles & Member Sources> Roles**. 2. Click **Remove**. A confirmation dialog box appears. 3. Click **Ok**.

5.6.5 Searching User

This section provides information on how to search user.

The Search User screen from the Roles & Member Sources screen provides a way to search the users with the associated roles. It also provides additional details like user added time, role and member source to which it belongs to.

For example, if you want to check the role of a user with its member source, then the search results can provide you a way to troubleshoot or check the user-role mapping.

Search Criteria

Consider the following scenario:

1. You have created a file member source named *MemberSource1* which includes:
   - Group File named *examplegroups* with users *examplegroupuser1* and *examplegroupuser2*
   - User File named *exampleusers* with users *exampleuser1* and *exampleuser2*
2. You have created a role named *Role1*.
3. You have added all users from *MemberSource1* to *Role1*.

For the given example, the following table lists the search results with different search criteria.

Table 5-18: Search Criteria

Search Criteria	Description	Output
Wild card	Search with '*'	It displays all the members.
Character search	Character search Search with '1'	It displays *examplegroupuser1* and *exampleuser1*.
Word search	Search with 'group'	It displays *examplegroupuser1* and *examplegroupuser2*.

You can perform additional actions on the search results such as:

- Clicking on the Role or Source column values redirects you to the *Roles* or *Member Sources* page respectively.
- Members can be sorted based on *Name*, *Added Time*, *Role* or *Source* columns.
- Search results also can be filtered with another search option, which is provided in the search results.

5.6.5.1 Searching a Member

This section describes the steps to search a member.

To search a member:

1. On the ESA Web UI, navigate to **Policy Management** > **Roles & Member Source** > **Search User**.
2. Enter the search criteria in the **Member Name** textbox.

For more on valid search criteria, refer to the table *Search Criteria*.

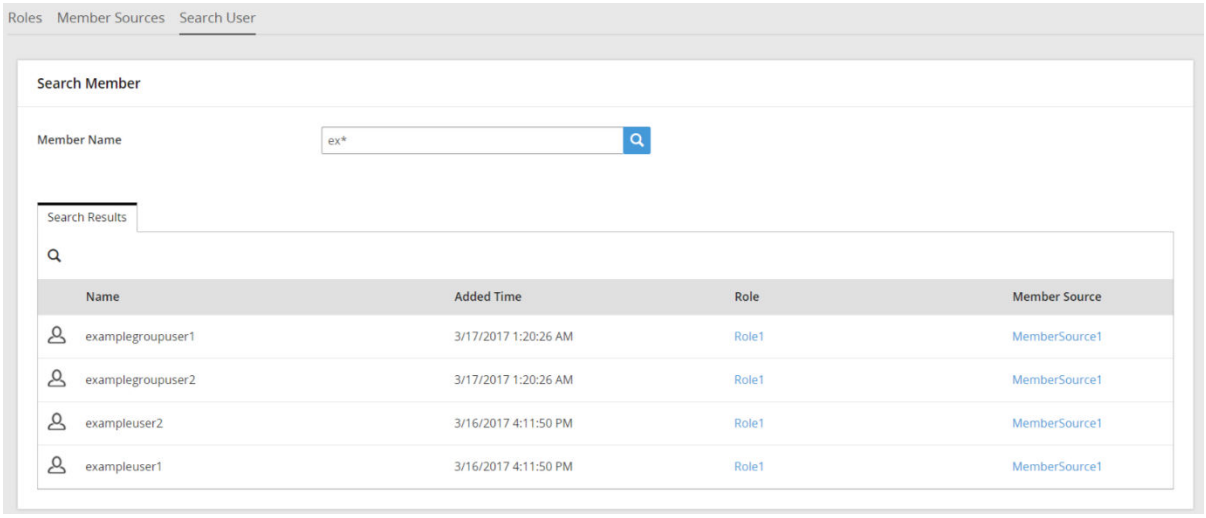


Figure 5-15: Search User Screen

3. Click **Search**.

The search results appear.

5.7 Working with Data Stores

This section discusses about the concept how data stores function.

Data stores identify a set of servers that are deployed into physical locations within your enterprise containing data that should be protected.

A data store identifies one or more PEP servers. You can add these servers individually or import a group of PEP servers at once.

5.7.1 Creating a Data Store

You create data stores to specify the locations in your enterprise to which you want to deploy policies. The addresses to these locations are described by the PEP Servers. Using the data store, you can define the list of protector nodes that can pull the policies. A data store consists information on policies, trusted applications, and nodes. You can create a default data store that deploys polices to the protections nodes that are not a part of the allowed servers list of any data store. Thus, when a new node is added that is not a part of any data store, the node inherits the policy information pertaining to the default data store.

Before you begin
You cannot create data stores with the same names or spaces in the data store name. You can create only one default data store for a single instance of ESA.

To create a data store:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Stores**.
   The list of all the data stores appear.
2. Click **Add New Data Store**.
   The **New Data Store** screen appears.

3. Enter a unique name identifying the data store in the **Name** textbox.

   > **Note:** Ensure that the length of the data store name does not exceed 55 characters.

4. Enter the required description describing the data store in the **Description** textbox.
5. Click the **Select as Default Data Store** option.

   If a default data store already exists and you are updating another data store as the default data store, then the following message appears.

   A default Data Store already exists, Please confirm to make this the new default Data Store.

6. Click **Ok**.
7. Click **Save**.

A message *Data Store has been created successfully* appears.

The following tabs are visible as per the type of data store:

- The **Nodes**, **Policies**, and **Trusted Applications** tabs are visible in case of a default data store.
- The **Allowed Server**, **Nodes**, **Policies**, and **Trusted Applications** tabs are visible in case of a non-default data store.

5.7.2 Adding Allowed Servers for the Data Store

For a data store, you can specify the allowed servers using the **Allowed Servers** tab. Allowed servers specify either the IP addresses for the range of servers or a single server IP address.

The allowed servers identify a node using the proxy IP address. If you need to restrict access to specific nodes or if the node must connect directly with the ESA, then you must set a flag in the `hubcontroller.env` file that enables the allowed servers to identify a node using the node IP address instead of the proxy IP address.

> **Note:**
> You must contact Protegrity Support/Services before editing the *hubcontroller.env* file.

The following is a snippet of the flag in the `hubcontroller.env` file located in `/opt/protegrity/hubcontroller/bin` directory:

```
ASSIGN_DATASTORE_USING_NODE_IP=false
```

The ***ASSIGN_DATASTORE_USING_NODE_IP*** configuration parameter controls the behaviour of how nodes are assigned to the data stores. The following table describes the possible values for the ***ASSIGN_DATASTORE_USING_NODE_IP*** configuration parameter.

ASSIGN_DATASTORE_USING_NODE_IP **configuration parameter value**	**Description**
false	Assign the node to the data store using the proxy IP address. This is the default setting.
true	Assign the node to the data store using the IP address of the node. If you set this flag to *true*, the ESA is configured to whitelist the PEP server by using the node IP address. With this flag set to true, you must remove the existing nodes that are linked to the data store, which is accessible from from the ESA Web

ASSIGN_DATASTORE_USING_NODE_IP configuration parameter value	Description
	UI by navigating to **Policy Management** > **Nodes**, so that the newly assigned nodes get registered with the required data store.

Note: You must restart the *HubController* service if this configuration parameter is modified.

5.7.2.1 Specifying Allowed Servers for the Data Store

This section describes the steps to specify allowed servers for a data store.

To specify allowed servers for a data store:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Stores**.
   The list of all the data stores appear.
2. From the **Allowed Servers** tab for the data store, click **Add**.
   The **Add Allowed Servers** screen appears.
3. If you want to add a single server, then select **Single Server** and specify the server IP address.
4. If you want to add a range of servers, then **Multiple Servers**. Enter the range in the **From** and **To** text boxes.
5. Click **Add**.

The servers are added to the list.

5.7.3 Adding Policies to the Data Store

You add a policy to a data store before deploying it to remote protection points.

To add policy to a data store:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Stores** .
   The list of all the data stores appear.
2. Select the required data store.
   The screen to edit the data store appears.
3. Click the **Policies** tab.
4. Click **Add**.
   The list of policies created appear.
5. Select the required policies.
6. Click **Add**.

A message *Selected Polices have been added to the Data Store successfully* appears.

Note: For more information on creating policies, refer to section *Creating and Deploying Policies*.

5.7.4 Adding Trusted Applications to the Data Store

You can add a trusted application to a data store before deploying it to remote protection points.

To add trusted application to a data store:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Stores** .
   The list of all the data stores appear.
2. Select the required data store.
   The screen to edit the data store appears.
3. Click the **Trusted Applications** tab.
4. Click **Add**.
   The list of trusted applications created appear.
5. Select the required policies.
6. Click **Add**.

A message *Selected Trusted Applications have been added to the Data Store successfully* appears.

5.8 Working with Nodes

This section provides information about how to work with nodes.

The Nodes screen displays all the nodes communicating with ESA for exchange of policy and audit information. Starting from version 7.0.1, you can view all the protector nodes with pull policy mechanism and the push policy mechanism in a single screen.

The protector nodes with the pull policy mechanism appear in the Nodes screen automatically. You can add nodes with the push policy mechanism to connect to ESA.

For more information about adding nodes with push policy mechanism, refer to section *Adding Nodes to the Data Store*.

The following table describes the icon for the nodes with pull mechanism.

No	Icon	Description
1		Protectors of v7.0.1 or higher with pull mechanism

Navigate to **Policy Management**> **Nodes**, to view the list of protector nodes communicating with the ESA. The following screen displays the nodes screen.

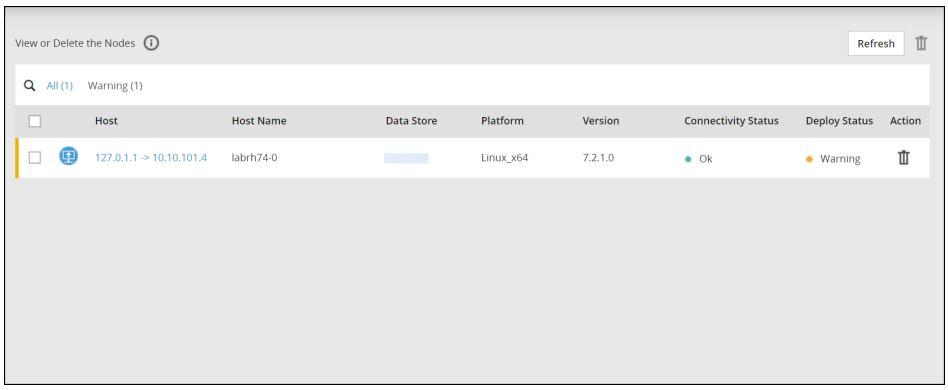


Figure 5-16: Nodes Screen

The following table describes the fields available for the nodes screen.

Table 5-19: Nodes Fields

No	Field	Description
1	IP Address	The IP address of the node.
2	Hostname	The hostname of the node.
3	Data Store	The data store deployed to the node.
4	Platform	The operating system installed on the node.
5	Version	The build version of the protector installed on the node.
6	Connectivity Status	The status of the node, whether it is running or not.
7	Deploy Status	The status of the data store deployed to the node.
8	Action	The option to delete the node.

You can delete the nodes that are not in use or not required. You would want to delete a node, for example, when the node IP address is changed and you want to delete the old node reference. When you delete a node, the registered node information is deleted from ESA.

Click the Delete ( ) icon to delete the node from the nodes list.

Note:

You can click on the icon to search a node. The search feature fetches the nodes on the basis of the hostname provided in the search box.

5.8.1 Deploy Status reported by Nodes

This section provides information about how to work with nodes.

When you navigate to **Policy Management** > **Nodes** and click on specific node IP address from the nodes list, the individual nodes screen provides **Deploy Status** tab. It provides a view of the deploy status messages reported by the node to ESA. It displays the policies that are deployed along with the policy deploy status and additional messages.

The following screen displays the **Deploy Status** tab.

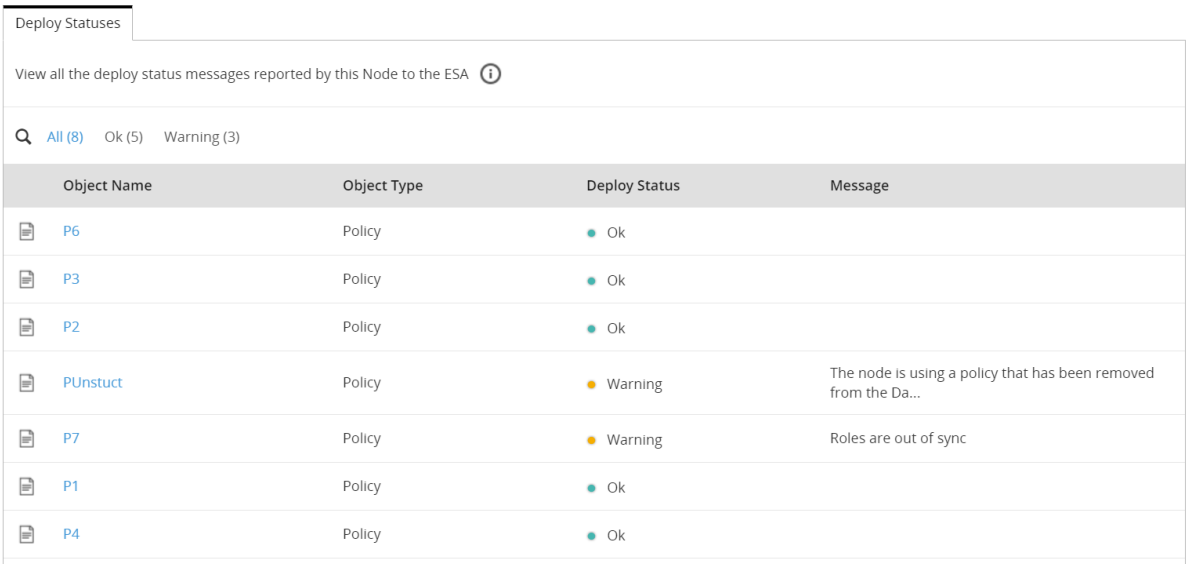


Figure 5-17: Deploy Status from Nodes

For more information on the different policy deploy status, refer to section *Policy Deploy Status*.

Chapter 6

Creating and Deploying Policies

Policies contain the detailed and comprehensive security definitions.

Policies are distributed to the locations in your enterprise where the policy is enforced. These policies contain other components that you define before you create the complete policy and deploy it.

The following figure displays a sample policy.

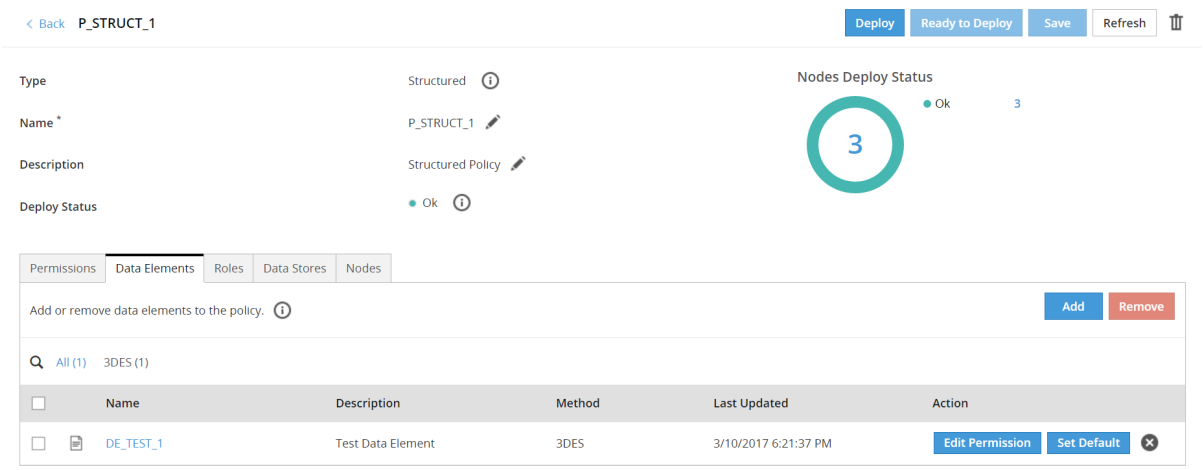


Figure 6-1: Policy Screen

You can add data elements, roles, link the policy to a data store, and deploy the policy to the protector nodes. You also set different permissions for the content, audit, and time restrictions for a policy.

> **Note:** The time restriction permission is no longer supported for the ESA version 7.1 and higher.

You can create two types of policies:

- **Structured Policy** - Policy that supports column-level database protection and integrates policies into applications using an API. This policy type contains only structured data elements.
- **Unstructured Policy** - Policy that provides support for file protection. This policy type contains only unstructured data elements.

A policy is in one of the following states:

- **Ready to Deploy** – The policy is created with the required information and ready for deployment.

- **Deployed** – The policy is deployed to the PEP servers.

> **Note:** You can modify a policy at any point in time. If a policy that is deployed is modified, then the policy returns to the *Ready to Deploy* state.

6.1 Policy Management using the Policy Management Web UI

The Policy Management Web UI is primarily used to create policies and related metadata.

6.1.1 Creating a Structured Policy

This section describes the steps to create a structured policy.

To create a structured policy:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appears.
2. Click **Add New Policy**.
   The **New Policy** screen appears.
3. Select **Structured** from **Type**.
4. Type a unique name for the policy in the **Name** textbox.

   > **Note:** Ensure that the length of the policy name does not exceed 55 characters.

5. Type the required description for the policy in the **Description** textbox.
6. Under the **Permissions** tab, select the required permissions.
   For more information about adding permissions, refer to section *Adding Permissions to Policy*.
7. Under the **Data Elements** tab, add the required data elements.
   For more information about adding data elements, refer to section *Working with Data Elements*.
8. Under the **Roles** tab, add the required roles.
   For more information about adding roles, refer to section *Working with Roles*.
9. Under the **Data Stores** tab, add the required Data Stores.
   For more information about adding data stores, refer to section *Working with Data Stores*.
10. Click **Save**.

A message *Policy has been created successfully* appears.

6.1.2 Creating an Unstructured Policy

This section describes the steps to create an unstructured policy.

To create an unstructured policy:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.

The list of all the policies appear.

2. Click **Add New Policy**.
   The **New Policy** screen appears.
3. Select **Unstructured** from **Type**.
4. Type a unique name for the policy in the **Name** textbox.

   > **Note:** Ensure that the length of the policy name does not exceed 55 characters.

5. Type the required description for the policy in the **Description** textbox.
6. Under the **Permissions** tab, select the required permissions.
   For more information about adding permissions, refer to section *Adding Permissions to Policy*.
7. Under the **Data Elements** tab, add the required data elements.
   For more information about adding data elements, refer to section *Working with Data Elements*.
8. Under the **Roles** tab, add the required roles.
   For more information about adding roles, refer to section *Working with Roles*.
9. Under the **Data Stores** tab, add the required Data Stores.
   For more information about adding data stores, refer to section *Working with Data Stores*.
10. Click **Save**.

A message *Policy has been created successfully* appears.

6.1.3 Working with Policy

This section provides information about how to work with a policy.

You can perform the following actions on the policy before marking it ready for deployment:

- Add Data Elements
- Add Roles
- Add Data Stores
- Set Permissions

6.1.3.1 Adding Permissions to Policy

Permissions are applied restrictions to access a policy.

Using the policy permissions, the system can determine what is returned to a user who wants to view protected data. If the user has the appropriate permissions, then the data gets decrypted or detokenized. If permission is denied, then a NULL value is returned by default. Depending on your data element and policy settings, the system can instead return a no-access value (such as Exception or Protected value). The permissions are always defined in the context of a roles and a data element.

You can set a no-access value, such as Exception or Protected value, through editing the permission settings for a role or a data element.

For more information about editing the permission settings of a role or data element, refer to the section *Adding Data Elements to Policy* or *Adding Roles to Policy*.

The following table describes the different permissions that you can set for a structured data.

Table 6-1: Permissions for Structured Data

Permission	Options	Permission Description
Content and Audit	Unprotect	Allow members to get protected data or audit information.
	Protect	Allow members to add and protect the data or audit information.
	Reprotect	Allow members to reprotect the protected data with a new data element.
	Delete	Allows members to delete a row in a database table. This permission cannot be applied by Application or Big Data protectors. For more information about enabling the delete permissions, refer to section *Enabling the Delete Permission*.

The following table describes the permissions that you can set for an unstructured data.

Table 6-2: Permissions for Unstructured Data

Permission	Options	Permission Description
Content and Audit	Unprotect	Allow members to get protected data.
	Protect	Allow members to add data and protect it as needed.
	Reprotect	Allow members to reprotect the protected data with a new data element.
Object and Audit	Create	Allow members to create a file or folder.
	Delete	Allow members to delete a file or folder.
Admin Permissions	Manage Protection	Allow members to add or remove protection.

6.1.3.1.1 Setting Default Permissions for a Policy

This section describes the steps to set the default permissions for a policy.

To set default permissions for a policy:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.
2. Select the required policy.
   The screen to edit the policy appears.
3. Click the **Permissions** tab.
   The following screen appears.

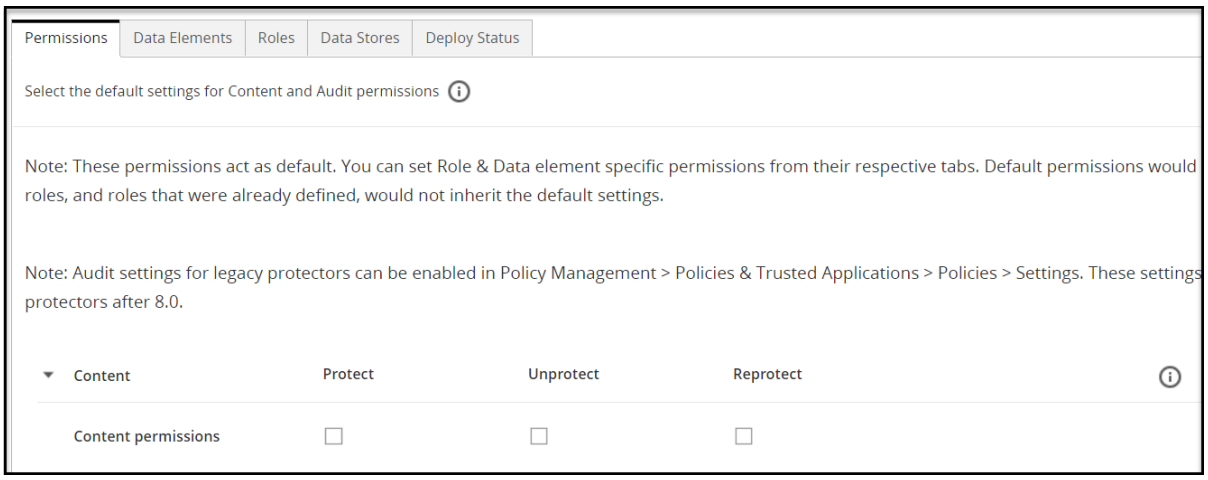


Figure 6-2: Permissions Tab

4. Select the required permissions.
   For more information about the permissions, refer to the tables *Permissions for Structured Data* and *Permissions for Unstructured Data*.
5. Click **Save**.

The permissions are set for the policy.

> **Note:** Ensure that you set the default permissions before customizing permissions for an individual role or data element.

6.1.3.2 Adding Data Elements to Policy

This section discusses about how to add data elements to policy.

6.1.3.2.1 Adding Data Elements for Structured Policies

This section describes the steps to add data elements for structured policies.

To add data elements for structured policies:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.
2. Select the required policy.
   The screen to edit the policy appears.
3. Click the **Data Elements** tab.
4. Click **Add**.

A message *Selected Data Elements have been added to the policy successfully* appears.

6.1.3.2.2 Adding Data Elements for Unstructured Policies

This section describes the steps to add data elements for unstructured policies.

To add data elements for unstructured policies:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.
2. Select the required policy.
   The screen to edit the policy appears.
3. Click the **Data Elements** tab.
4. Click **Add**.
   The list of data elements created for unstructured data appears.
5. Select the required data elements.

   > **Note:** Unstructured data elements are only visible to be added for unstructured policies.

6. Click **Add**.

A message *Selected Data Elements have been added to the policy successfully* appears.

6.1.3.2.3 Customizing Permissions for Data Element in a Policy

You can edit the permissions for an individual data element. When you edit the permissions for a data element, then you change the permissions for the roles associated with the data element.

To customize permissions for data element in a policy:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.
2. Select the required policy.
   The screen to edit the policy appears.
3. Click the **Data Elements** tab.
4. Click **Edit Permissions**.
   The screen to update the permissions for the role appears.
5. Select the required permissions.

   > **Note:** If you are using masks with any data element, then ensure that masks are created before editing permissions.

6. Click **Save**.

A message *Permissions have been updated successfully* appears.

> **Note:** The customized permissions, if any, override the default permissions for any policy.

> **Note:** For a *Monitoring* data element, the sensitive data always appears in clear irrespective of the permissions configured for the role.

> **Note:** For a *Masking* data element, the role must only be granted *Unprotect* access, if the sensitive data must be shown in clear.

> **Note:**

If the Unprotect access permission is not assigned to a user, then either the NULL value or noaccess permission, such as, Protected or Exception value is returned based on the permission settings for a role or a data element. If a user is assigned to multiple roles with different permission settings for the data element, then the resultant no-access permission on the PEP server is applicable as per the following table.

Table 6-3: No-access Permission for Users in Multiple Roles

No Access Permission 1	No Access Permission 2	Resultant Permission on the PEP server
Protected	NULL	Protected
Protected	EXCEPTION	Protected
Protected	Mask	Mask
Protected	Clear	Clear
NULL	EXCEPTION	EXCEPTION
NULL	Mask	Mask
NULL	Clear	Clear
EXCEPTION	Mask	Mask
EXCEPTION	Clear	Clear

Note:

The settings for masking output formats are applicable as per the following table:

Table 6-4: Data Element Support for Masking Output Formats

Data Element Method	Data Type	Masking Support
Tokenization	Numeric (0-9)	√
	Alpha (a-z, A-Z)	√
	Uppercase Alpha (A-Z)	√
	Uppercase Alpha-Numeric (0-9, A-Z)	√
	Printable	√
	Date (YYYY-MM-DD, DD/MM/YYYY, MM.DD.YYYY)	X
	DateTime	X
	Decimal	X
	Unicode	X
	Unicode Base64	X
	Unicode Gen2	X
	Binary	X
	Credit Card (0-9)	√
	Lower ASCII	√
	Email	√
Integer	X	
Encryption Algorithm: 3DES, AES-128, AES-256, CUSP 3DES, CUSP AES-128, CUSP AES-256		√
Format Preserving Encryption (FPE) with ASCII plaintext encoding		√
Format Preserving Encryption (FPE) with UTF-8, UTF-16LE, and UTF-16BE plaintext encodings		X
No Encryption		√

Data Element Method	Data Type	Masking Support
Masking		√

6.1.3.2.4 Setting a Data Element as Default

For data elements that are mapped to multiple roles in a policy, the **Set Default** option provides a faster alternative to assigning permissions for each role separately. The setting defined in the **Permissions** tab are automatically applied to all the new roles added to the policy.

To set a data element as default data element in a policy:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.
2. Select the required policy.
   The screen to edit the policy appears.
3. Click the **Data Elements** tab.
4. Click **Set Default**.
5. Click **Save**.

Some important points to remember:

- Once you chose to use **Set Default** option for any data element, the policy will always need a data element to be defined as a default data element.
  If a data element is set as default in a policy and you no longer want to set any data element as a default, then you must create a new policy and deploy it to the protector node.
- The settings defined in the **Permissions** tab apply to any new role added to the policy.
  If the **Set Default** option is selected after all the date elements are added to the policy, then the default settings will be applied only for subsequent new roles that are added to the policy. For older roles, you must edit the permissions manually.
- It is recommended that default permissions that you want to apply for roles that are added to the policy are defined before data elements or roles are added to the policy. In addition, define the default data element before adding other data elements to the policy.

6.1.3.3 Adding Roles to Policy

This section discusses about how to add roles to a policy and then how to customize the permissions for individual roles.

6.1.3.3.1 Adding Roles to Policies

You add roles to a policy to restrict the users who access or use the policy. The roles in the policy enforce security on the enterprise data. You can add one or more roles to a policy.

To add roles to policies:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.

2. Select the required policy.
   The screen to edit the policy appears.
3. Click the **Roles** tab.
4. Click **Add**.
   The list of roles created appears.
5. Select the required roles.
6. Click **Add**.

A message *Selected Roles have been added to the policy successfully* appears.

6.1.3.3.2 Customizing Permissions for Role in a Policy

You can edit the permissions for individual roles. When you edit the permissions for a role, then you change the permissions for the data elements associated with the role.

To customize permissions for role in a policy:

1. On the ESA Web UI, navigate to **Policy Management> Policies & Trusted Applications> Policies**.
   The list of all the policies appear.
2. Select the required policy.
   The screen to edit the policy appears.
3. Click the **Roles** tab.
4. Click **Edit Permissions**.
   The screen to update the permissions for the role appears.
5. Select the required permissions.

   Note: If you are using masks with any data element, then ensure that masks are created before editing permissions.

6. Click **Save**.

A message *Permissions have been updated successfully* appears.

Note: The customized permissions, if any, override the default permissions for any policy.

Note: For a *Monitoring* data element, the sensitive data always appears in clear irrespective of the permissions configured for the role.

Note: For a *Masking* data element, the role must only be granted *Unprotect* access, if the sensitive data must be shown in clear.

Note:
If the Unprotect access permission is not assigned to a user, then either the NULL value or noaccess permission, such as, Protected or Exception value is returned based on the permission settings for a role or a data element. If a user is assigned to multiple roles with different permission settings for the data element, then the resultant no-access permission on the PEP server is applicable as per the following table.

Table 6-5: No-access Permission for Users in Multiple Roles

No Access Permission 1	No Access Permission 2	Resultant Permission on the PEP server
Protected	NULL	Protected
Protected	EXCEPTION	Protected
Protected	Mask	Mask
Protected	Clear	Clear
NULL	EXCEPTION	EXCEPTION
NULL	Mask	Mask
NULL	Clear	Clear
EXCEPTION	Mask	Mask
EXCEPTION	Clear	Clear

Note:

The settings for masking output formats are applicable as per the following table:

Table 6-6: Data Element Support for Masking Output Formats

Data Element Method	Data Type	Masking Support
Tokenization	Numeric (0-9)	√
	Alpha (a-z, A-Z)	√
	Uppercase Alpha (A-Z)	√
	Uppercase Alpha-Numeric (0-9, A-Z)	√
	Printable	√
	Date (YYYY-MM-DD, DD/MM/YYYY, MM.DD.YYYY)	X
	DateTime	X
	Decimal	X
	Unicode	X
	Unicode Base64	X
	Unicode Gen2	X
	Binary	X
	Credit Card (0-9)	√
	Lower ASCII	√
	Email	√
Integer	X	
Encryption Algorithm: 3DES, AES-128, AES-256, CUSP 3DES, CUSP AES-128, CUSP AES-256		√
Format Preserving Encryption (FPE) with ASCII plaintext encoding		√
Format Preserving Encryption (FPE) with UTF-8, UTF-16LE, and UTF-16BE plaintext encodings		X
No Encryption		√
Masking		√

6.1.3.4 Enabling the Delete Permission

If a database supports the delete operation, then you can enable the **Show delete permissions for structured policies** setting to grant delete permissions to users in a role.

To enable the delete permission:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.
2. Click **Settings**.
   The **Settings** screen appears.
3. Click **Show delete permissions for structured policies** to enable the delete permission.
4. Click **Save**.

A message *Policy Manager Settings has been successfully updated* appears.

The delete permission column for a structured policy is visible.

6.1.3.5 Masking Rules for Users in Multiple Roles

When policy users are assigned to multiple roles with different data element permission settings, the resultant permission (access and audit settings) applicable for that user is the least restrictive permission derived from the data element - parent role association. If the mask settings, which are applied along with the permission settings, for users in multiple roles result in a conflict, then the resultant output also differs.

Consider a scenario, where user U1 with a policy P1, associated with roles R1, R2, and R3 and connected with the data element DE1 containing different masks (Left, Right) and output formats, then the resultant output is applicable as per the following table.

Sr. No.	Role	User	Data Element	Output Format	Mask Settings	Resultant Output
1	R1	U1	DE1	MASK	Left: 1, Right: 2	Left: 1, Right: 2
2	R1	U1	DE1	MASK	Left: 1, Right: 2	Left: 1, Right: 2
	R2	U1	DE1	MASK	Left: 1, Right: 2	
3	R1	U1	DE1	MASK	Left: 1, Right: 2	There is conflict in the mask settings (Left, Right) and thus, the Unprotect access is revoked with NULL as the output.
	R2	U1	DE1	MASK	Left: 0, Right: 5	
4	R1	U1	DE1	MASK	Left: 1, Right: 2 with mask character ‘*’	There is conflict in the mask character settings and thus, the Unprotect access is revoked with NULL as the output.
	R2	U1	DE1	MASK	Left: 1, Right: 2 with mask character ‘/’	
5	R1	U1	DE1	MASK	Left: 1, Right: 2	There is conflict in the mask settings (Left, Right) and thus, the Unprotect access is revoked with NULL as the output.
	R2	U1	DE1	MASK	Left: 1, Right: 2	
	R3	U1	DE1	MASK	Left: 0, Right: 5	
6	R1	U1	DE1	MASK	Left: 1, Right: 1 with masked mode	There is conflict in the mask settings and thus, the Unprotect access is revoked with NULL as the output. For example:
	R2	U1	DE1	MASK	Left: 1, Right: 1 with clear mode	

Sr. No.	Role	User	Data Element	Output Format	Mask Settings	Resultant Output
						If the value 12345 is masked with *Left: 1, Right: 1* settings in masked mode, then it results in *234*. If the value 12345 is masked with *Left: 1, Right: 1* settings in clear mode, then it results in 1***5. As the resultant values are conflicting, the Unprotect access is revoked with NULL as the output.
7	R1	U1	DE1	MASK	Left: 1, Right: 2	There is conflict in the output formats. The resultant output is most permissive, which is CLEAR.
	R2	U1	DE1	CLEAR		
8	R1	U1	DE1	MASK	Left: 1, Right: 2	There is conflict in the output formats due to conflicting MASK settings. However, with the CLEAR setting applicable in the order of access as per the role R3, the resultant output is most permissive. In this case, it is CLEAR.
	R2	U1	DE2	MASK	Left: 0, Right: 5	
	R3	U1	DE3	CLEAR		

A data element-role connection with disabled permission for unprotect operation results in a NULL value, by default, and can be set to other no-access values, such as Exception or Protected value.

The following table explains how no-access values work with different output formats for users in multiple roles.

Sr. No.	Role	User	Data Element	No Access Operation	Output Format	Mask Settings	Resultant Output
1	R1	U1	DE1		MASK	Left: 1, Right: 2	There is conflict in the output formats. If one of the roles has access, then the output format is used. The resultant output is most permissive, which is MASK.
	R2	U1	DE1	NULL			
2	R1	U1	DE1		MASK	Left: 1, Right: 2	
	R2	U1	DE1	Protected			
3	R1	U1	DE1		MASK	Left: 1, Right: 2	
	R2	U1	DE1	Exception			
4	R1	U1	DE1		CLEAR		If one of the roles has access, then the output format is used. The resultant output is most permissive, which is CLEAR.
	R2	U1	DE1	NULL			
5	R1	U1	DE1		CLEAR		
	R2	U1	DE1	Protected			
6	R1	U1	DE1		CLEAR		
	R2	U1	DE1	Exception			

6.1.3.6 Inheriting Permissions for Users in Multiple Policies and Roles

This section describes how a user in multiple policies and roles inherits permissions for a data element.

If a policy user is assigned a role that does not have a specific data element associated with the role, then the user cannot use the data element for performing security operations. If the user tries to use the data element, then an error is generated.

However, consider a policy where you have created a default role that is applicable to all the users. You associate a specific data element with this default role. In this case, the policy user, who is included in another role that is not associated with the specific

data element, inherits the permissions for this data element from the default role. This scenario is applicable only if the users are a part of the same policy or a part of multiple policies that are applied to the same data store.

> **Important:**
> The *new behavior* of policy users inheriting the permissions from the default role for the data elements is applicable to the release 9.0.0.0.

Example:

Policy 1 contains the role R1, which is assigned to the user U1. The role R1 is associated with a data element DE1, which has the permissions Unprotect, Protect, and Reprotect. The user U1 can unprotect, protect, and reprotect the data using the data element DE1.

Policy 2 contains the role R2, which is assigned to the user U2. The role R2 is associated with a data element DE2. which has the permissions Unprotect, Protect, and Reprotect. The user U2 can unprotect, protect, and reprotect the data using the data element DE2.

Policy P3 contains the role R3, which is applicable to all the users. The role R3 role is associated with two data elements DE1 and DE2. Both the data elements have the Unprotect permissions associated with it.

> **Note:**
> The ALL USERS denotes a default role which is applicable to all the users. To enable the default role, click the **Applicable to all the members** toggle button on the ESA web UI. For more information about **Applicable to all the members**, refer to the section *Working with Roles*.

Use Case 1

The Use Case 1 table demonstrates that roles R1 and R2 have an indirect relationship with data elements DE1 and DE2 that is they are part of different policies but they are deployed to the same data store, they have inherited the permission of the default role for data elements DE1 and DE2.

Table 6-7: Use Case 1

Policy structure in the ESA					**Protector side permissions after deploying the policy**					
					Old Behaviour			**New Behavior**		
P1	R1	U1	DE1	URP	U1	DE1	URP	U1	DE1	URP
						DE2	-		DE2	**U**
P2	R2	U2	DE2	URP	U2	DE1	-	U2	DE1	**U**
						DE2	URP		DE2	URP
P3	R3	ALL USERS	DE1	U	ALL USERS	DE1	U	ALL USERS	DE1	U
			DE2	U		DE2	U		DE2	U

As shown in the table, in the case of *old behaviour*, no permissions have been inherited from the role R3 that is applicable to the data elements DE1 and DE2 for all the users.

The Unprotect permissions highlighted in bold in the table for the *new behavior* column indicate the permission, that have been inherited from the role R3, that is applicable to the data elements DE1 and DE2 for all the users.

Use Case 2

The Use Case 2 table demonstrates that if roles R1 and R2 have a direct relationship with data elements DE1 and DE2, then they will not inherit the permissions of the default role. In this case, protector side permissions after deploying the policy are the same as shown in the *old behavior* and *new behaviour* columns.

Table 6-8: Use Case 2

Policy structure in the ESA					**Protector side permissions after deploying the policy**					
					Old Behavior			**New Behavior**		
P1	R1	U1	DE1	URP	U1	DE1	URP	U1	DE1	URP
			DE2	-		DE2	-		DE2	-
	R3	ALL USERS	DE1	U	U2	DE1	-	U2	DE1	-
			DE2	U		DE2	URP		DE2	URP
P2	R2	U2	DE1	-	ALL USERS	DE1	UR	ALL USERS	DE1	UR
			DE2	URP						
P3	R4	ALL USERS	DE1	R		DE2	UR		DE2	UR
			DE2	R						

Use Case 3

The Use Case 3 table demonstrates that if roles R1 and R2 have a direct relationship with data elements DE1 and DE2, then they will not inherit the permissions of the default role. In this case, protector side permissions after deploying the policy are same as shown in the *old behavior* and *new behaviour* columns.

Table 6-9: Use Case 3

Policy structure in the ESA					**Protector side permissions after deploying the policy**					
					Old Behavior			**New Behavior**		
P1	R1	U1	DE1	URP	U1	DE1	URP	U1	DE1	URP
			DE2	-		DE2	-		DE2	-
	R2	U2	DE1	-	U2	DE1	-	U2	DE1	-
			DE2	URP		DE2	URP		DE2	URP
	R3	ALL USERS	DE1	U	ALL USERS	DE1	UR	ALL USERS	DE1	UR
			DE2	U						
	R4	ALL USERS	DE1	R		DE2	UR		DE2	UR
			DE2	R						

Use Case 4

The Use Case 4 table demonstrates that as role R2 has an indirect relationship with data element DE1, it has inherited the permissions of the default role. The role R1 has a direct relationship with data element DE1, and it have not inherited the permissions of the default role.

Table 6-10: Use Case 4

Policy structure in the ESA					**Protector side permissions after deploying the policy**					
					Old Behavior			**New Behavior**		
P1	R1	U1	DE1	-	U1	DE1	-	U1	DE1	-
						DE2	-		DE2	-
	R3	ALL USERS	DE1	U	U2	DE1	-	U2	DE1	**U**
						DE2	URP		DE2	URP
P2	R2	U2	DE2	URP	ALL USERS	DE1	U	ALL USERS	DE1	U

Policy structure in the ESA					Protector side permissions after deploying the policy					
					Old Behavior			New Behavior		
						DE2	-		DE2	-

As shown in the table, in the case of *old behaviour*, no permissions have been inherited from the role R3 that is applicable to the data element DE1 for all the users.

The Unprotect permission highlighted in bold in the table for the *new behavior* column indicate the permissions that has been inherited from the role R3, that is applicable to the data element DE1 for all the users.

Use Case 5

The Use Case 5 table demonstrates that Role R1 has inherited the permissions of the default role for the data element DE2.

Table 6-11: Use Case 5

Policy structure in the ESA					Protector side permissions after deploying the policy					
					Old Behavior			New Behavior		
P1	R1	U1	DE1	URP	U1	DE1	URP	U1	DE1	URP
						DE2	-		DE2	**UP**
P2	R3	ALL USERS	DE2	U	ALL USERS	DE1	-	ALL USERS	DE1	-
P3	R4	ALL USERS	DE2	P		DE2	UP		DE2	UP

As shown in the table, in the case of *old behaviour*, no permissions have been inherited from the roles R3 and R4 that is applicable to the data element DE2 for all the users.

The resultant permissions highlighted in bold in the table for the *new behavior* column indicate the permissions that have been inherited from the roles R3 and R4, that is applicable to the data element DE2 for all the users.

Use Case 6

The Use Case 6 table demonstrates that role R1 will inherit the permissions of the default role for the data element DE2.

Table 6-12: Use Case 6

Policy structure in the ESA					Protector side permissions after deploying the policy					
					Old Behavior			New Behavior		
P1	R1	U1	DE1	U	U1	DE1	UP	U1	DE1	UP
						DE2	-		DE2	**URP**
P2	R5	U1	DE1	P	ALL USERS	DE1	-	ALL USERS	DE1	-
P3	R3	ALL USERS	DE2	URP		DE2	URP		DE2	URP

As shown in the table, in the case of *old behaviour*, no permissions have been inherited from the role R3 that is applicable to the data element DE2 for all the users.

The resultant permissions highlighted in bold in the table for *new behavior* column indicate the permissions that have been inherited from the role R3 that is applicable to the data element DE2 for all the users.

Use Case 7

The Use Case 7 table demonstrates that if role R1 is related to data element DE1 in policy P1 and and role R3 is related to data element DE1 in policy P3, then roles R1 and R3 will not inherit the permissions of the default role. In this case, protector side permissions after deploying the policy are same as shown in the *old behavior* and *new behaviour* columns.

Table 6-13: Use Case 7

Policy structure in the ESA					**Protector side permissions after deploying the policy**					
					Old Behavior			**New Behavior**		
P1	R1	U1	DE1	U	U1	DE1	U	U1	DE1	U
						DE2	-		DE2	-
P2	R1	U1	DE2	-	ALL USERS	DE1	URP	ALL USERS	DE1	URP
P3	R3	ALL USERS	DE1	URP		DE2	-		DE2	-

6.1.4 Deploying Policy

After you define the roles, data elements, data stores, and permissions for the policy, the policy is ready for deployment.

Following are the steps to deploy the policy:

- The policy should be made ready for deployment.
- Deploy the policy.

6.1.4.1 Preparing the Policy for Deployment

This section describes the steps to prepare the policy ready for deployment.

Before you begin
If all the parameters are valid, then the policy is set to the *Ready to Deploy* state.

To make the policy ready for deployment:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.
2. Select the required policy.
   The screen to edit the policy appears.
3. Click **Ready to Deploy**.

A message confirming the deployment appears. The **Ready to Deploy** is inactive and the **Deploy** is active.

Note:

- **When the ESA is offline, the PEP server is switched off and then switched on**: The PEP server fails to register with the ESA after its turned on. This registration activity continues until the PEP server successfully registers and downloads the policy.
- **When the PEP server is running and then the ESA goes offline**: The PEP server will continue to ping back the ESA, once every minute, to get the latest policy. If there is no response from the ESA, the PEP server sends a log to inform that it failed to download the index file. The policy is published as the protect operation continues.

6.1.4.2 Deploying the Policy

This section describes the steps how to deploy the policy after it has been prepared for deployment.

To deploy the policy:

1. On the ESA Web UI, navigate to **Policy Management** > **Policies & Trusted Applications** > **Policies**.
   The list of all the policies appear.
2. Select the required policy.
   The screen to edit the policy appears.
3. Click **Deploy**.

A message *Policy has been deployed successfully* appears.

> **Note:**
> Redeploy the policy only when there are changes to an existing policy.

6.2 Policy Management using the Policy API

Apart from creating and managing policy metadata through the Policy Management Web UI in ESA, policies can also be created using the Policy Management API.

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 the Policy Management APIs, refer to the section *6.3 Using the DevOps REST APIs* in the *Protegrity APIs, UDFs, Commands Reference Guide 9.1.0.5*.

Chapter 7

Deploying Data Stores to Protectors

In deployment, the data stores containing the policies are distributed to the protection points. The protector nodes pull this policy information in the data stores from the ESA to their respective policy enforcement points. Only the policies that are ready to be deployed are distributed across the protector nodes.

Before you begin

After you create a data store with the all the required components, you deploy the policy to the nodes:

For more information about Data Stores, refer to section *Working with Data Stores*.

To deploy the data store:

1. On the ESA Web UI, navigate to **Policy Management** > **Data Stores**.
   The list of all the policies appear.
2. Select the required data store.
   The screen to edit the data store appears.

   > **Note:** Click the **Nodes** tab to view the list of nodes receiving the policy information.

3. Click **Deploy**.
   A message *Data Store has been deployed successfully* appears.

When the Protector pulls the policies added to the data store, it connects to ESA to retrieve the necessary policy information such as members for each role in the policy, token elements, and so on. The PEP server then publishes the policy in the shared memory, so it can be used by the Protector.

Chapter 8

Managing Policy Components

This section provides information about how to manage policy components.

You can edit or delete the following policy components from Policy Management:

- Data Elements
- Masks
- Alphabets
- Member Sources
- Data Stores
- Trusted Applications
- Policies
- Roles

The following table describes the editable fields for each policy component.

Table 8-1: Editable Fields

Policy Component	Fields
Data Elements	• Description
Masks	• Name • Description • Mask Template • Mask Mode • Character
Alphabets	All Fields **Note:** After an alphabet entry is added to the Alphabet, the alphabet entry cannot be edited.
Roles	All fields
Policies	• Name • Description • Password • Permissions • Data Elements • Roles • Data Stores
Trusted Applications	• Name • Description

Policy Component	Fields
	• Application Name • Application User • Data Stores
Member Sources	All fields

When you click the link for name of policy component, you can edit the fields from the component edit panel. You click the Delete ( ) icon to delete the policy component.

If the policy components are already added to a policy, then you cannot delete it.

Chapter 9

Policy Deployment Feedback

The policy deployment feedback is the collective status of deployed policies, nodes and trusted applications combined with the deploy statuses by the PEP servers running on various protector nodes.

The protector nodes communicate with the ESA to exchange policy information. The PEP servers in the protector nodes pull the policy information from ESA at regular intervals. Only the protector nodes that are registered with ESA can communicate for information. The PEP servers then return the status of the policy components to the ESA in form of a feedback. This ensures that the policy components in ESA and the policy components in the protector nodes are synchronized.

The policy management dashboard from the ESA Web UI displays the deployment feedback for data stores, policies, trusted applications and nodes.

To view the Dashboard for Policy Management, navigate to **Policy Management> Dashboard**.

The following figure shows the **Dashboard** screen for Policy Management.

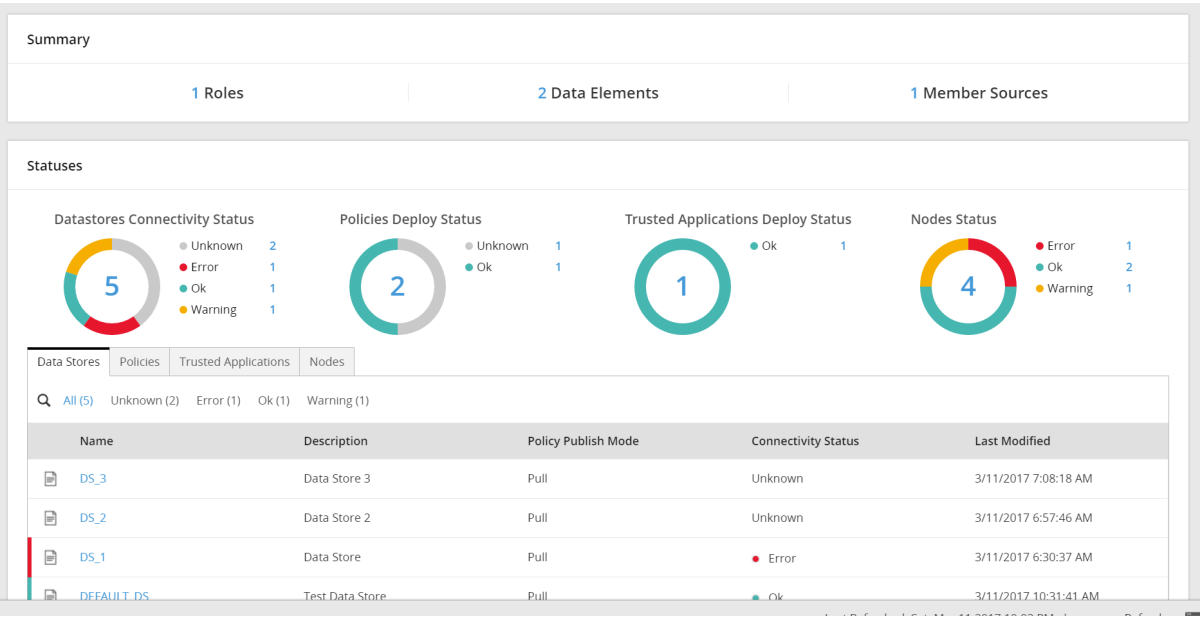


Figure 9-1: Policy Management Dashboard Screen

The Policy Management dashboard consists of the following two sections:

- *Summary*

9.1 Summary

This section provides information about the **Summary** tab in the Policy Management dashboard.

The **Summary** tab displays an overview on the number of policy components created using the Policy Management Web UI. The following policy components appear under the **Summary** tab:

- Roles
- Data Elements
- Member Sources

You can navigate to the respective policy components by clicking the corresponding number.

For example, you click **2** corresponding to *Data Elements*, to view the list of data elements.

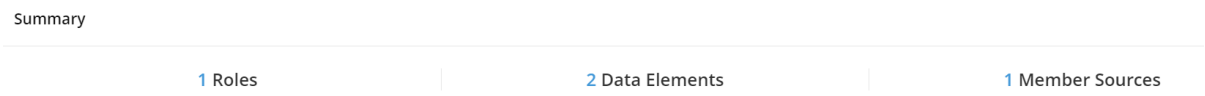


Figure 9-2: Summary tab

9.2 Status

This section provides information about the **Status** tab in the Policy Management dashboard.

The **Status** section displays the overview of the different data stores, policies, or the protector nodes connecting to ESA.

The status of the following policy components appears under the **Status** tab:

- Data Stores
- Policies deployed
- Trusted Application
- Nodes

The following figure shows the legends associated with the **Status** tab:

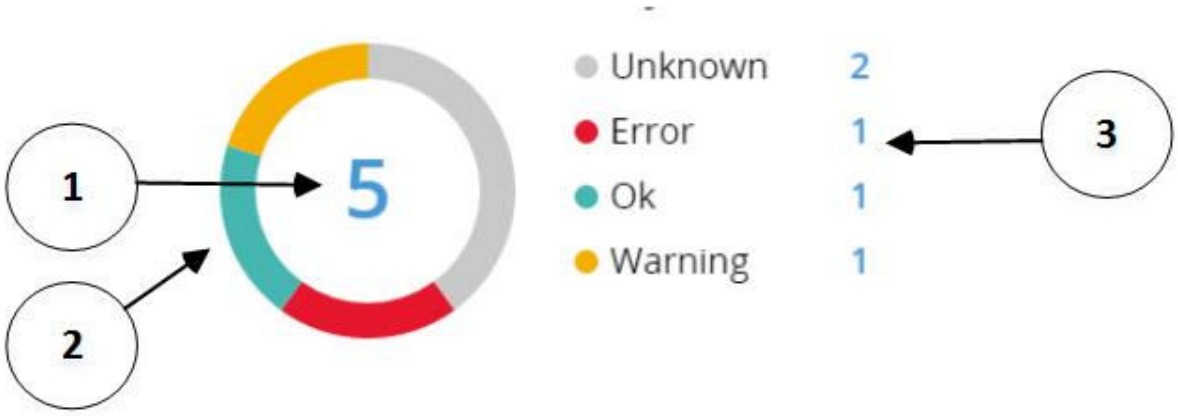


Figure 9-3: Status Callouts

Table 9-1: Status tab

Callout	Description
1	Count of the data store, policies deployed, trusted applications deployed, or protector nodes connected. Also, displays the total list of the policy components in their respective tabs.
2	Status circle displaying the distribution of policy components based on their status.
3	Link to the individual policy components based on the status.

9.2.1 Data Store Connectivity

The Data Store Connectivity shows the status of all the data stores deployed to the protector nodes.

The following table describes the different values for the data store connectivity.

Table 9-2: Data Store Status

Status	Description
Unknown	The data store is created but not deployed to any protector node.
Ok	The Data store is created and successfully deployed to the nodes. The nodes communicate with ESA for any updates in the data store.
Warning	• The nodes do not pull the updated policy information in the data store for more than ten minutes but less than 60 minutes. • The information in the data store is updated but not deployed to the protector nodes.
Error	The nodes do not pull the updated policy information in the data store for a period of more than 60 minutes.

The following columns are available for the deployed data stores under the **Data Store** tab:

- Name
- Description
- Policy Publish Mode
- Connectivity Status
- Last Modified

> **Note:** Select the data store name to view the details of that data store.

For more information on Data Stores, refer to section *Working with Data Stores*.

9.2.2 Policy Deploy Status

The Policy Deploy Status shows the status of all the polices deployed to the protector nodes.

The following table describes the different values for the deployed policies.

Table 9-3: Policy Deploy Status

Status	Description
Unknown	The policy is created but not deployed to any of the protector nodes.
Ok	The policy is created and deployed to the protector nodes.
Warning	The policy information is deployed, but the updates are not communicated to the protector nodes.

The following columns are available for the deployed data stores under the **Policies** tab:

- Name
- Description
- Deploy Status

- Last Modified

> **Note:** Select the policy name to view the details of that policy.

For more information about Policies, refer to section *Working with Policy*.

9.2.3 Trusted Application Deploy Status

The Trusted Application Deploy status displays the status of all the applications deployed to the protector nodes.

The following table describes the different values for the trusted applications.

Table 9-4: Trusted Application Status

Status	Description
Unknown	The trusted application is created but not deployed to any of the protector nodes.
Ok	The trusted application is created and deployed to the protector nodes.
Warning	The trusted application is deployed, but the updates are not communicated to the protector nodes.

The following columns are available for the deployed data stores under the **Trusted Applications** tab:

- Name
- Description
- Deploy Status
- Last Modified

> **Note:** Select the trusted application name to view the details of that trusted application.

For more information about Trusted Applications, refer to section *Working with Trusted Applications*.

9.2.4 Node Status

The Nodes Status displays the status of all the protector nodes communicating with the ESA.

It consists of the status of all the policies, trusted applications, and data store connectivity. The status of the node changes depending on the node connectivity and the deployment status of the data store for that node.

The following table describes the different values for the protector nodes.

Table 9-5: Node Status

Status	Description
Ok	• The node is functional. • Policies are successfully deployed to the nodes.
Warning	• The nodes do not pull the updated policy information in the data store for more than five minutes but less than 60 minutes. • The information in the data store is updated but not deployed to the protector nodes.
Error	• The node is not functional for more than 60 minutes. • The policy information cannot be pulled by the node.

The following columns are available for the deployed data stores under the **Nodes** tab:

- Node IP

- Host Name
- Data Store
- Platform
- Version
- Connectivity Status
- Deploy Status
- Last Seen

> **Note:** Select the Node IP address to view the details of that protector node.

For more information about Nodes, refer to section *Working with Nodes*.

Chapter 10

Appendix B: Exporting Policy for Immutable Protectors

The export policy process includes an API for exporting the policy from the ESA, a permission that must be assigned to users who want to export the policy, and the IMP service that must be installed on the ESA. The exported policy is used by the immutable protectors.

The following table provides information about each component that must be used or configured to export the policy from the ESA.

> **Important:** The exported policy can only be used with 64-bit Linux protectors.

Table 10-1: Exporting-Policy Components for Immutable Protectors

Policy Components	Description	Reference
IMP API	After the policy is configured on the ESA, the IMP API helps in exporting the policy that can be imported to the immutable protectors. For more information about how immutable policies are imported to protectors, refer to the respective Immutable Protector documentation.	For more information about the IMP API, refer to section *Appendix B: APIs for Immutable Protectors* in the *Protegrity APIs, UDFs, Commands Reference Guide 9.1.0.5*.
IMP Service	The IMP service is installed on the ESA. This service must be up and running before any resource is requested using the IMP API.	• Installing the IMP service - section *Appendix B. Installing the IMP Service for Policy Deployment on Immutable Protectors* in the *Installation Guide 9.1.0.5* • IMP service - section *4.4.1 Start and Stop Services* in the *Appliance Overview Guide 9.1.0.5*
Export IMP permission	The *Export IMP* permission must be assigned to the role that will be granted to the user exporting the policy.	For more information about the permission, refer to *5.19 Managing Roles* in the *Appliance Overview Guide 9.1.0.5*.