Enterprise Security Administrator Guide 9.1.0.5

Created on: Nov 19, 2024

Notice

Copyright

Table of Contents

Chapter 1

Protegrity ESA Appliance Introduction

Protegrity Data Security Platform provides policy management and data protection. It has as its main component the Enterprise Security Administrator (ESA). Working in combination with a Protegrity database protector, application protector, file protector, or big data protector it can be used for managing data security policy, key management, and auditing and reporting.

- **ESA**: The ESA Manager provides information on how to install specific components, work with policy management tools, manage keys and key rotation and manage switching between Soft HSM and Key Store, configuring logging repositories and using logging tools. This document contains details for all these features.
- **Audit Store**: The Audit Store is a repository for the logs generated from multiple sources, such as the kernel, policy management, member source, application logs, and protectors. The Audit Store supports clustering for scalability.
- **Protegrity Analytics**: This feature displays Forensics from the Audit Store. It provides options to query and display data from the Audit Store. Predefined graphs are available for analyzing the data from the Audit Store. It provides options for generating and saving customized queries and reports. An enhanced alerting system tracks the data in the Audit Store to monitor the systems and alert users if required. It also provides the ILM feature for archiving and importing logs.

Chapter 2

Protegrity Appliance Overview

The Protegrity Data Security Platform provides policy management and data protection and has the following appliances.

1. Enterprise Security Administrator (ESA) is the main component of the Data Security Platform. Working in combination with a Protegrity protector (Database Protector, Application Protector, File Protector, or Big Data protector), it can be used to encrypt or tokenize your data.
2. The Data Security Gateway (DSG) is a network intermediary that can be classified under Cloud Access Security Brokers (CASB) and Cloud Data Protection Gateway (CDPG). CASBs provide security administrators a central check point to ensure secure and compliant use of cloud services across multiple cloud providers. CDPG is a security policy enforcement check point that exists between cloud data consumer and cloud service provider to interject enterprise policies whenever the cloud-based resources are accessed.

All Protegrity Appliances are based on the same framework with the base operating system (OS) as hardened Linux, which provides the platform for Protegrity products. This platform includes the required OS low-level components as well as higher-level components for enhanced security manageability.

All Protegrity Appliances have two basic interfaces: CLI Manager (a console-based environment) and Web UI (web-based environment). Most of the management features are shared by all appliances. Some examples of the shared management features are network settings management, date and time settings management, logs management, and appliance configuration facilities, among others.

Chapter 3

Data Security Platform Overview

This section provides a general overview of the Protegrity Data Security Platform and the intended audience of this guide.

3.1 Protegrity Data Security Platform

The Protegrity Data Security Platform is a comprehensive source of enterprise data protection solutions. Its design is based on a hub and spoke deployment architecture.

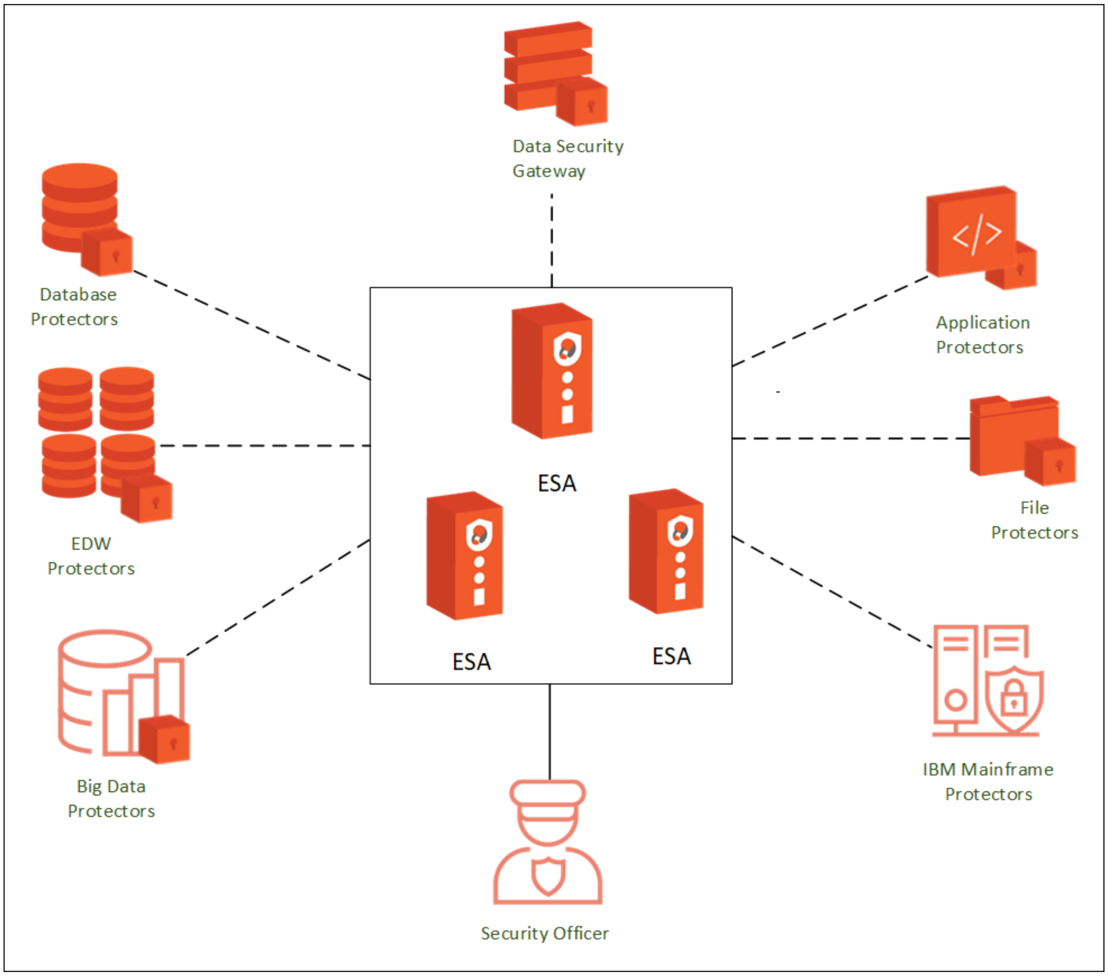
The Protegrity Data Security Platform has following components:

Enterprise Security Administrator (ESA) Handles the management of policies, keys, monitoring, auditing, and reporting of protected systems in the enterprise.

Data Protectors – Protect sensitive data in the enterprise and deploy security policy for enforcement on each installed system. A policy is deployed from ESA to the Data Protectors and Audit Logs of all activity on sensitive data is forwarded to the appliances, such as, the ESA or external logging systems.

3.2 Architecture

The following diagram shows the general architecture of the Protegrity Data Security Platform.



> **Note:** The architecture diagram shows 3 ESAs. Your architecture might also contain PSUs v9.1.0.0. If you are using the PSUs, then ensure that you keep them updated with all the available patches and fixes.

Figure 3-1: General Architecture of the Protegrity Data Security Platform

Chapter 4

Installing ESA

You can install ESA on-premise or a cloud platform such as AWS, GCP, or Azure. When you upgrade from a previous version, ESA is available as patch. The following are the different ways of installing ESA:

Installing ESA

- **ISO Installation**: This installation is performed for an on-premise environment where ESA is installed on a local system using an ESA ISO is provided by Protegrity. The installation of the ISO begins by installing the hardened version of Linux on your system, setting up the network, and configuring date/time. This is then followed by updating the location, setting up OS user accounts, and installing the ESA-related components. For more information about installing ESA using ISO, refer to the *Protegrity Installation Guide 9.1.0.5*.
- **Cloud Platforms**: On Cloud platforms such as, AWS, GCP, or Azure, ESA images for the respective cloud are generated and provided by Protegrity. In these images, ESA is installed with specific components. You must obtain the image from Protegrity and create an instance on the cloud platform. After creating the instance, you run certain steps for finalizing the installation. For more information about installing ESA on cloud platforms, refer to the *Protegrity Installation Guide 9.1.0.5*.

Upgrading ESA

If you are upgrading from a previous version, you must first install the latest version of ESA. After installing the ESA, you must migrate data and configuration from the previous version to the latest version. The process of upgrading ESA is same for both, on-premise and cloud platforms. For more information about upgrading ESA using, refer to the *Protegrity Upgrade Guide 9.1.0.5*

> **Note:** A temporary license is provided by default when you first install the Appliance and is valid for 30 days from the date of this installation. To continue using Protegrity features, you have to obtain a validated license before your temporary license expires.
>
> For more information about licensing, refer to *Protegrity Data Security Platform Licensing Guide 9.0.0.0*.

Chapter 5

Logging In to ESA

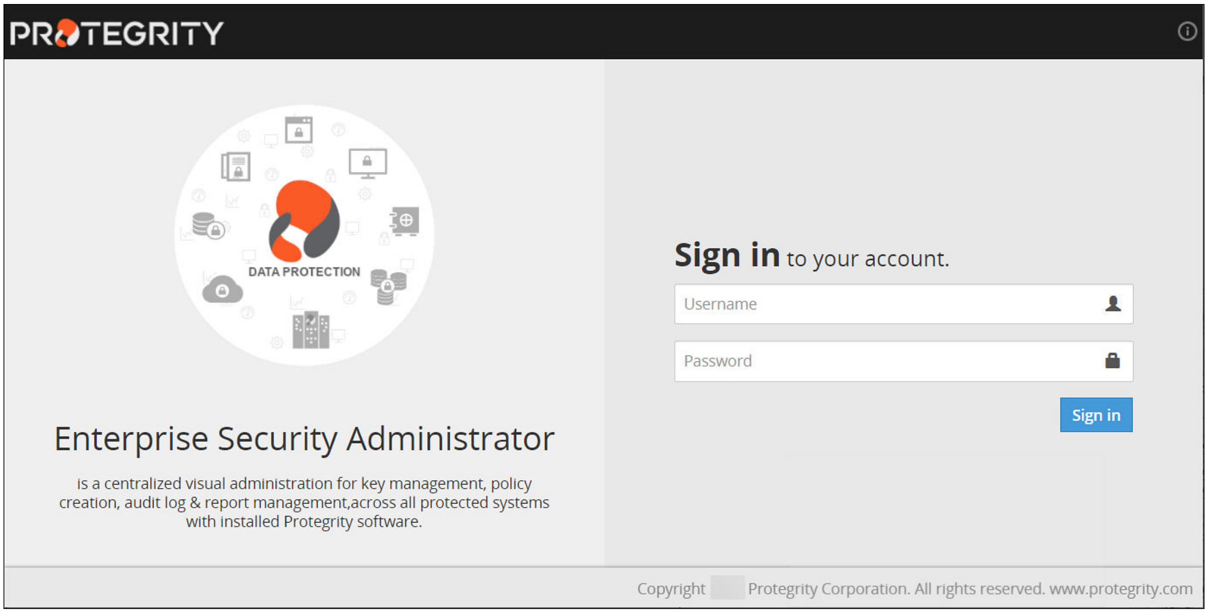
The Enterprise Security Administrator (ESA), contains several components such as, Audit Store, Analytics, Policy Management, Key Management, Certificate Management, Clustering, Backup/Restore, Networking, User Management, and so on. You must login to ESA to avail the services of these components. Log in to the CLI Manager or Web UI of ESA to secure your data using these components.

The login aspect of the appliance can be categorized into the following categories:

Simple Login

Log in to ESA from CLI or Web UI by providing valid user credentials. You can login to ESA as an appliance or LDAP user. For more information about users, refer to *ESA users*.

From your Web browser, type the domain name of the ESA HTTPS protocol, for example, *https://192.168.1.x/*. The Web Interface splash screen appearsThe following figure displays the login page of the ESA Web UI.



Enterprise Security Administrator

is a centralized visual administration for key management, policy creation, audit log & report management,across all protected systems with installed Protegrity software.

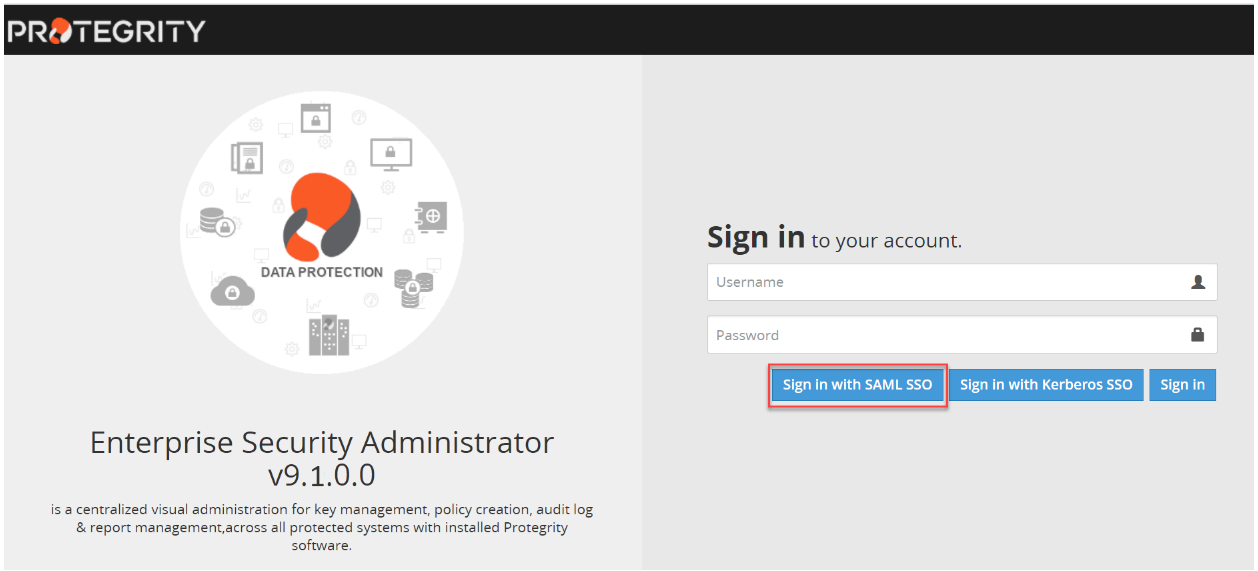
Copyright Protegrity Corporation. All rights reserved. www.protegrity.com

Figure 5-1: Web UI Login Screen

You can login to the ESA CLI Manger using an SSH session.

Single Sign-On (SSO)

Single Sign-on (SSO) is a feature that enables users to authenticate multiple applications by logging in to a system only once. On the Protegrity appliances, you can utilize the Kerberos SSO mechanism to login to the appliance. For more information about SSO, refer to *Single Sign-On*. The following figure displays the login page with SSO.



Sign in to your account.

Enterprise Security Administrator v9.1.0.0

is a centralized visual administration for key management, policy creation, audit log & report management,across all protected systems with installed Protegrity software.

Figure 5-2: Single Sign-On

Two-Factor Authentication

The two factor authentication is a verification process where two recognized factors are used to identify you before granting you access to a system or website. In addition to your password, you must correctly enter a different numeric one-time passcode or the verification code to finish the login process. This provides an extra layer of security to the traditional authentication method. For more information about two-factor authentication, refer to *Two-Factor Authentication* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

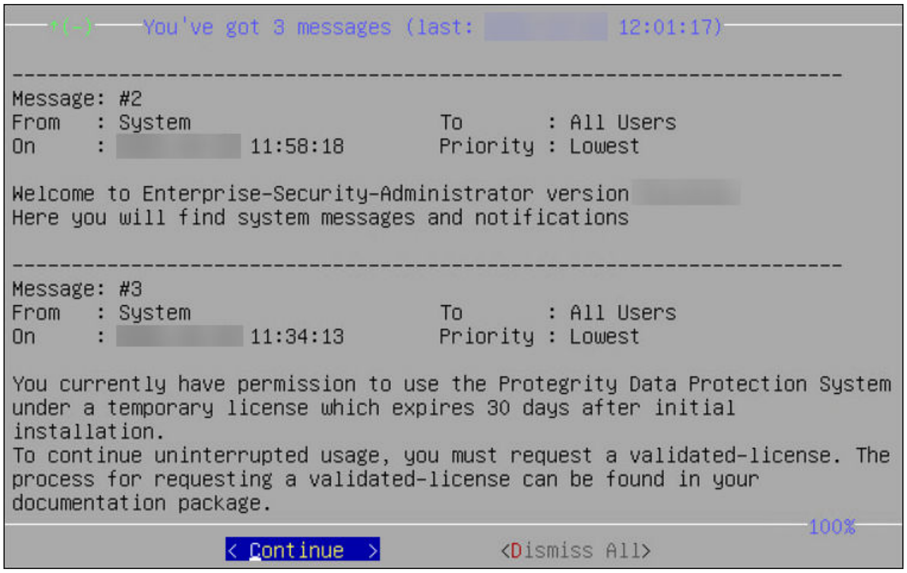
> **Note:** Protegrity supports Mozilla Firefox, Chrome, and Internet Explorer browsers for Web UI login.

Chapter 6

Working with CLI Manager

The CLI Manager is a text-based environment for monitoring status, administration, and network configuration of your appliance.

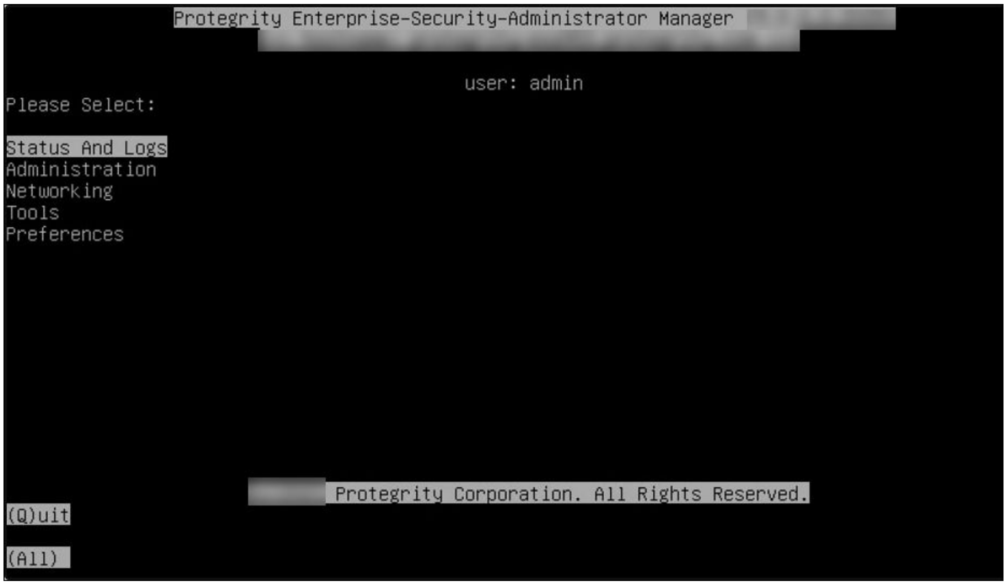
When you log in to the CLI Manager, an introductory screen with user notifications appears.



```
──↑(-)───You've got 3 messages (last: [redacted] 12:01:17)──────────

-----------------------------------------------------------------------
Message: #2
From    : System                    To       : All Users
On      : [redacted] 11:58:18       Priority : Lowest

Welcome to Enterprise-Security-Administrator version [redacted]
Here you will find system messages and notifications

-----------------------------------------------------------------------
Message: #3
From    : System                    To       : All Users
On      : [redacted] 11:34:13       Priority : Lowest

You currently have permission to use the Protegrity Data Protection System
under a temporary license which expires 30 days after initial
installation.
To continue uninterrupted usage, you must request a validated-license. The
process for requesting a validated-license can be found in your
documentation package.
──────────────────────────────────────────────────────────────100%────
                 < Continue  >          <Dismiss All>
```

Figure 6-1: CLI Introductory Message Screen

The following screen displays the main menu of the CLI Manager.



```
              Protegrity Enterprise-Security-Administrator Manager [redacted]
                     [redacted]

                                  user: admin
Please Select:

Status And Logs
Administration
Networking
Tools
Preferences




                  [redacted] Protegrity Corporation. All Rights Reserved.
(Q)uit

(All)
```

Figure 6-2: CLI Manager Main Page

The following table describes the details of options available on the main menu

Table 6-1: CLI Menu

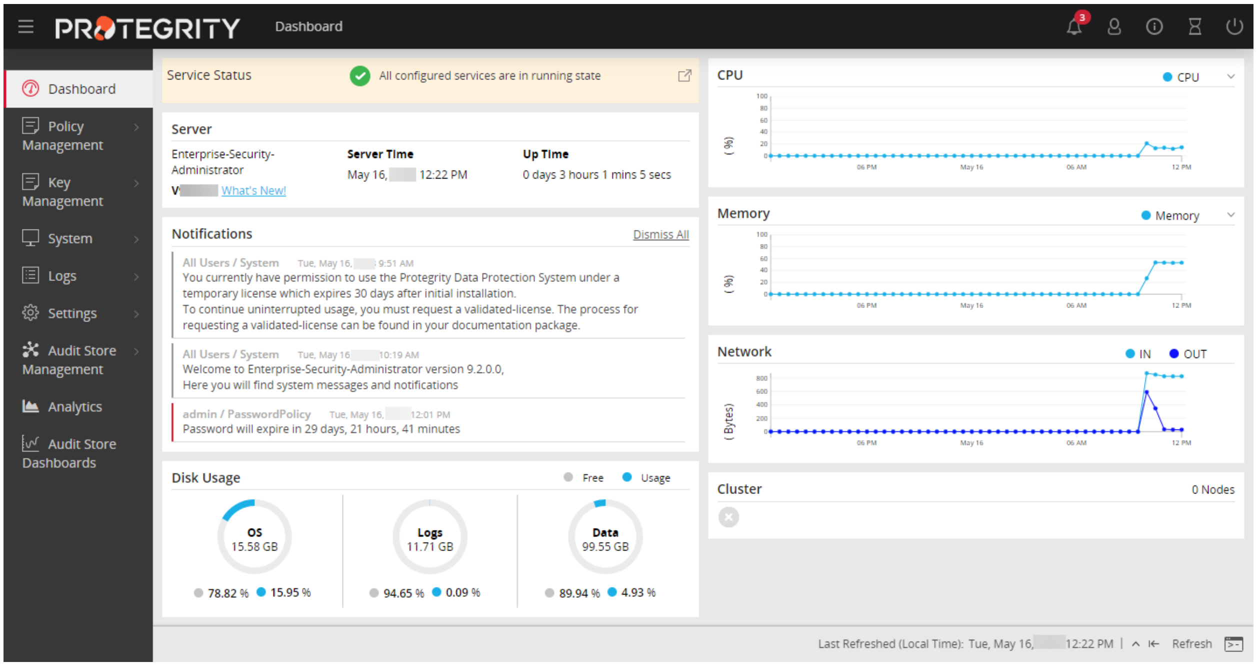
Menu	Description
Status and Logs	Enables you to monitor system performance, view all the processes, logs and user notifications
Administration	Enables you to view the services that are available in the appliance, setting date/time, backing/restoring data, setting up email, managing patches, installing/unistalling system components, setting up LDAP, and operating the OS console.
Networking	Enables you to configure the network, SNMP, firewall, and configuring port list.
Tools	Enables you to create a cluster, monitor file changes using File Integrity Monitor tool, work with the appliance antivirus, manage disk space, rotating audit store certificates, apply audit store security configurations, and run Xen Paravirtualization tools.
Preferences	Allows you to manager AppArmor, uniform response time, brute force attacks, and so on.

Chapter 7

Web User Interface (Web UI) Management

The Web UI is a web-based environment for managing status, policy, administration,networking, and so on. The options that you perform using the CLI manager can also be performed from the Web UI.

The following screen displays the ESA Web UI.



Service Status — All configured services are in running state

Server

Enterprise-Security-Administrator
V[redacted] What's New!

Server Time
May 16, [redacted] 12:22 PM

Up Time
0 days 3 hours 1 mins 5 secs

Notifications — Dismiss All

All Users / System Tue, May 16, [redacted] 9:51 AM
You currently have permission to use the Protegrity Data Protection System under a temporary license which expires 30 days after initial installation.
To continue uninterrupted usage, you must request a validated-license. The process for requesting a validated-license can be found in your documentation package.

All Users / System Tue, May 16 [redacted] 10:19 AM
Welcome to Enterprise-Security-Administrator version 9.2.0.0,
Here you will find system messages and notifications

admin / PasswordPolicy Tue, May 16, [redacted] 12:01 PM
Password will expire in 29 days, 21 hours, 41 minutes

		Free	Usage
OS	15.58 GB	78.82 %	15.95 %
Logs	11.71 GB	94.65 %	0.09 %
Data	99.55 GB	89.94 %	4.93 %

Cluster — 0 Nodes

Last Refreshed (Local Time): Tue, May 16, [redacted] 12:22 PM

Figure 7-1: ESA Dashboard

The following table describes the details of options available on the Web UI menu.

Table 7-1: Web UI

Options	**Description**
Dashboard	View user notifications, disk usage, alerts, memory/CPU/ network utilization, and cluster status
Key Management	Manage master, data. For more information about keys, refer to the *Protegrity Key Management Guide 9.1.0.5*.
Policy Management	Manage creating and deploying policies. For more information about keys, refer to the *Protegrity Policy Management Guide 9.1.0.5*.
System	Configure Trusted Appliances Cluster, set up backup and restore, view system statistics, graphs, information, and manage services.
Logs	View logs that are generated for web services.
Settings	Configure network settings, set up certificates, manage users, roles, and licenses.
Audit Store Management	Manage the repository for all audit data and logs. For more information about audit store, refer to the *Audit Store Guide 9.1.0.5*
Analytics	View dashboards that display information using graphs and charts for a quick understanding of the protect, unprotect, and reprotect transactions performed. For more information about Protegrity Analytics, refer to the *Protegrity Analytics Guide 9.1.0.5*.

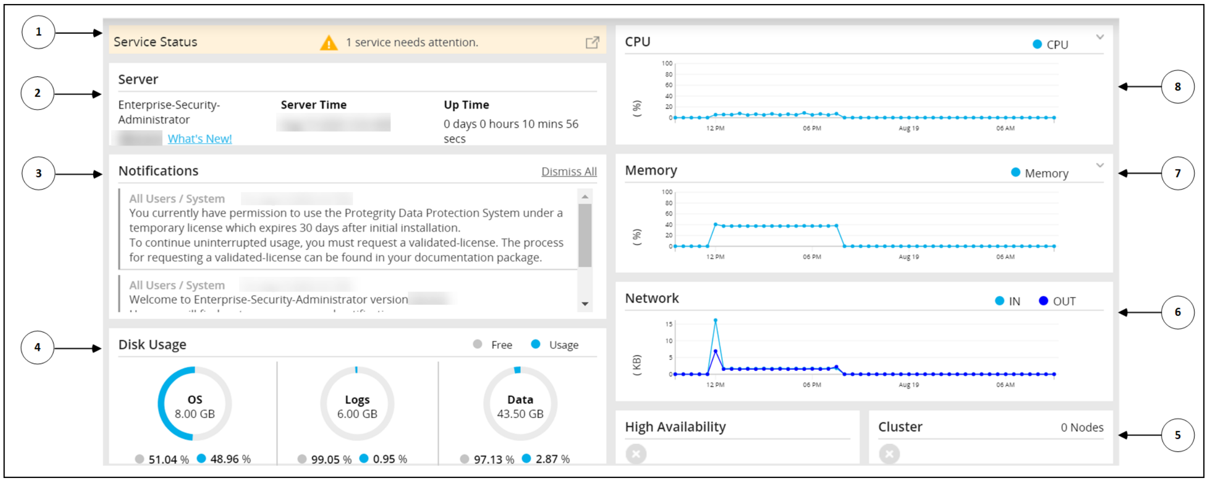
The following figure describes the icons that are visible on the ESA Web UI.

Table 7-2: Web UI Icons

Icon	**Description**
ⓘ	Download support logs and view product documentation
⌛	Extend session timeout
🔔	Notifications and alerts
👤	Edit profile or sign out of the profile
⏻	Power off or restart the system

7.1 Working with Dashboard

The Dashboard is a screen that provides a statistical view of your data in the appliance. This screen displays notifications, disk usage, graphical representation of CPU, memory, and network usage. The following figure illustrates the **Dashboard** screen.



1 service needs attention.

Enterprise-Security-Administrator

[redacted] What's New!

[redacted]

0 days 0 hours 10 mins 56 secs

All Users / System [redacted]

You currently have permission to use the Protegrity Data Protection System under a temporary license which expires 30 days after initial installation.
To continue uninterrupted usage, you must request a validated-license. The process for requesting a validated-license can be found in your documentation package.

All Users / System [redacted]

Welcome to Enterprise-Security-Administrator version [redacted]

Figure 7-2: ESA Dashboard Screen

Table 7-3: Dasbhoard Description

Callout	Description	Notes (If any)
1	Alerts the numbers of services that require attention	
2	Status of the server, type of appliance, version, and how long the appliance is running	
3	User notifications regarding, backup, restore, installation, welcome messages, and so on.	For the notifications to appear on the ESA, ensure that same set of client key pair are present on the ESA and the appliances that communicate with the ESA. For more information about certificates, refer to the *Protegrity Certificate Management Guide 9.1.0.5*
4	Free and used space for OS, Logs, and Data partitions	
5	Active, inactive and unreachable appliances in the cluster	
6	Graph about the amount of data received and sent from the appliance	
7	Graph on the memory consumption over a period of time	
8	Graph on the CPU consumption over a period of time	

7.2 Working with Services

On the **Services** screen, you can view and manage OS, logging and reporting, policy management, and other miscellaneous services. These services must be running for certain features in ESA to function. The services can be set to Automatic or Manual mode.

- **Automatic**: If the services are set to Automatic, then they are started automatically when the system restarts
- **Manual**: If the services are set to manual, then they do not start automatically on restarting the system. You must start the service when required.

The services are accessible from the CLI Manager and the Web UI.

Table 7-4: ESA Services

Type	Services	Description	Notes
OS	NTP Service	Responsible for synchronizing clocks between systems	
	Web Interface	Responsible for accessing the ESA Web UI	
	Secured Shell (SSH)	Responsible for accessing the CLI Manager	
	Firewall	Responsible for handling the firewall operations	
	Audit Service	Responsible for the auditing tool that is implemented to track certain events that can pose as a security threat	
	SNMP Service	Responsible for managing network services of ESA	
	Cluster Status	Responsible for managing Consul operations	
	Messaging System	Responsible for sending serialized data over system	
	Appliances Queues Backend	Daemon responsible for performing Remote Procedure Calls and transmitting internal messages through queues	
	Rsyslog Service	Responsible for sending logs to syslog	
	Appliance Heartbeat Server	Daemon responsible for broadcasting UDP messages with information like IP address, host name, server time, product code. and version.	
	Appliance Heartbeat Client	Daemon responsible for listening to messages broadcast by the appliance heartbeat server	
	Docker Service	Responsible for running the docker tool that deploys applications in form of containers. This service is required for running the AWS cloudwatch service.	This service can be started/ stopped/restarted only from the OS Console.
LDAP	LDAP Server	Responsible for the users and groups from the LDAP, which can take part in the policies applied on the protectors	
	Proxy Authentication Service	Responsible for integrating internal LDAP with the External LDAP	
	External Groups Sync Service	Responsible for the automatic synchronization of the external groups with the directory service	
	Name Service Cache Daemon	Caches data required for the LDAP service and improves its performance.	
Policy Management	Policy Repository	Holds all configuration, keys, roles, and definitions for security policies within the product suite.	
	Hub Controller	Responsible for interacting with the Policy management and Protection	

Type	Services	Description	Notes
		Enforcement Point, and routing the requests to the other services.	
	Member Source Service	Responsible for connecting to any external source of users that may need to be included into the data security policies.	
	DFS Cache Refresh	Enables users to enforce the access control list path for the HDFSFP protector.	
	Metering Facade	Collects the total count of successful protect, unprotect, and reprotect operations from the connected protectors. The total count is then sent at periodic intervals, which is 20 minutes as configured in the pepserver.cfg configuration file, to the Audit Store for further analysis.	• When you log in to connect to the pepserver.cfg configuration file (TCP/ STDOUT/FILE), with "output = file" setting and the default **outputfilename** setting is available in the pepserver.cfg file, connection error is displayed. • If pepserver.cfg uses the "output=file" setting, logs are not sent to stdout in Oracle database after protect/ unprotect operations.
	Log Facade	Receive audits from the protectors and send it to the Audit Store, which is then used by the Insight Analytics	If the ESA is configured with a 7.x protector or 8.x protector, then the Logfacade service is used.
	PIM Cluster	Responsible for handling Policy Management operations in the ESA	
	Soft HSM Gateway	Responsible for configuring and running Soft HSM on the ESA	
	Key Management Gateway	Responsible for configuring and running external Key Store on the ESA	
Audit Store	Audit Store Repository	Responsible for storing logs in the Audit Store	
	Audit Store Management	Responsible for managing the Audit Store	
Misc	Consul Agent	Responsible for running the Consul service used in clustering	
	Analytics	Responsible for managing Protegrity Analytics	
	td-agent	Responsible for forwarding logs to Analytics	
	walinuxagent	Service associated with the Azure Linux VM agent that interacts with the VM and Azure Fabric Controller.	This is applicable on the Azure image. If the Azure Cloud Utility is in use, do not stop this service.
	Service Dispatcher	Network layer that makes the ESA more scalable and efficient by routing the requests between various ESA components	

7.3 Working with Networks

Networking Management allows configuration of the appliance network settings such as, host name, default gateway, name servers, and so on. You can also configure SNMP settings, network bind services, NIC bonding, and network firewall. The networking management is accessible from the CLI Manager and the Web UI.

Using the Web UI, you can perform the following networking functions:

Using the CLI Manager, you can perform the following networking functions:

- Configuring hostname and IP address
- Configuring NIC Bonding
- Managing Network Interfaces
- Configuring hostname and IP address
- Configuring SNMP
- Binding Services and Address
- Network Troubleshooting
- Configuring Firewall
- Configuring Allow Portlist

For more information about networking, refer to *Working with Networks* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

7.4 Working with Antivirus

As a security compliance, it is important that your system is not prone to malicious attacks from external sources. Thus, an antivirus software is added in the appliance to scan for such threats. The AntiVirus program uses ClamAV, an open source and cross-platform antivirus engine designed to detect malicious Trojan, virus, and malware threats. A single file or directory, or the whole system can be scanned. Infected file or files are logged and can be deleted or moved to a different location. The antivirus scan can be performed from the *CLI manager* and the *Web UI*.

7.5 Working with SSH

The Secure Shell (SSH) is a network protocol that ensures an secure communication over unsecured network. A user connects to the SSH server using the SSH Client. The SSH protocol comprises of a utility suite which provides high-level authentication encryption over unsecured communication channels.

A typical SSH setup consists of a host machine and a remote machine. A key pair is required to connect to the host machine through any remote machine. A key pair consists of a Public key and a Private key. The key pair allows the host machine to securely connect to the remote machine without entering a password for authentication.

For enhancing security, a Private key is secured using a passphrase. This ensures that only the rightful recipient can have access to the decrypted data. You can either generate key pairs or work with existing key pairs.

For more information about SSH, refer to *Working with SSH using CLI Manager* and *Working with SSH using Web UI* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

7.6 Working with Logs

Based on the products installed, you can view the logs in the Logs screen. Based on the components installed in ESA, the following are the logs are generated in the following screens:

- Web Services Engine
- Service Dispatcher
- Appliance Logs

> **Note:** The information icon on the screen displays the order in which the new logs appear. If the new logs appear on top, you can scroll down through the screen the view the previously generated logs.

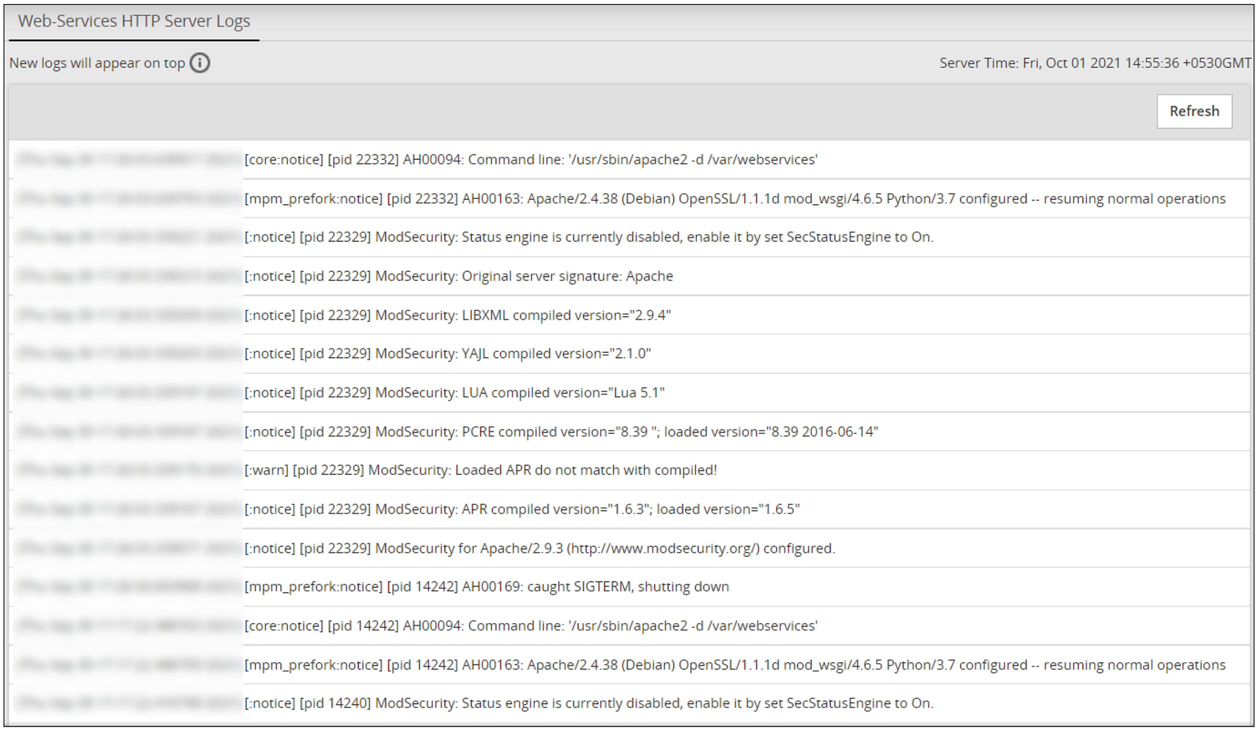
7.6.1 Viewing Web Services Engine Logs

In the Web Services screen, you can view the logs for all the Web services requests on ports, such as, 443 or 8443.

The Web Services logs are classified as follows:

- HTTP Server Logs
- SOAP Module Logs

The following figure illustrates the HTTP Server Logs.


Web-Services HTTP Server Logs
New logs will appear on top ⓘ
Server Time: Fri, Oct 01 2021 14:55:36 +0530GMT
Refresh

```
[redacted] [core:notice] [pid 22332] AH00094: Command line: '/usr/sbin/apache2 -d /var/webservices'
[redacted] [mpm_prefork:notice] [pid 22332] AH00163: Apache/2.4.38 (Debian) OpenSSL/1.1.1d mod_wsgi/4.6.5 Python/3.7 configured -- resuming normal operations
[redacted] [:notice] [pid 22329] ModSecurity: Status engine is currently disabled, enable it by set SecStatusEngine to On.
[redacted] [:notice] [pid 22329] ModSecurity: Original server signature: Apache
[redacted] [:notice] [pid 22329] ModSecurity: LIBXML compiled version="2.9.4"
[redacted] [:notice] [pid 22329] ModSecurity: YAJL compiled version="2.1.0"
[redacted] [:notice] [pid 22329] ModSecurity: LUA compiled version="Lua 5.1"
[redacted] [:notice] [pid 22329] ModSecurity: PCRE compiled version="8.39 "; loaded version="8.39 2016-06-14"
[redacted] [:warn] [pid 22329] ModSecurity: Loaded APR do not match with compiled!
[redacted] [:notice] [pid 22329] ModSecurity: APR compiled version="1.6.3"; loaded version="1.6.5"
[redacted] [:notice] [pid 22329] ModSecurity for Apache/2.9.3 (http://www.modsecurity.org/) configured.
[redacted] [mpm_prefork:notice] [pid 14242] AH00169: caught SIGTERM, shutting down
[redacted] [core:notice] [pid 14242] AH00094: Command line: '/usr/sbin/apache2 -d /var/webservices'
[redacted] [mpm_prefork:notice] [pid 14242] AH00163: Apache/2.4.38 (Debian) OpenSSL/1.1.1d mod_wsgi/4.6.5 Python/3.7 configured -- resuming normal operations
[redacted] [:notice] [pid 14240] ModSecurity: Status engine is currently disabled, enable it by set SecStatusEngine to On.
```

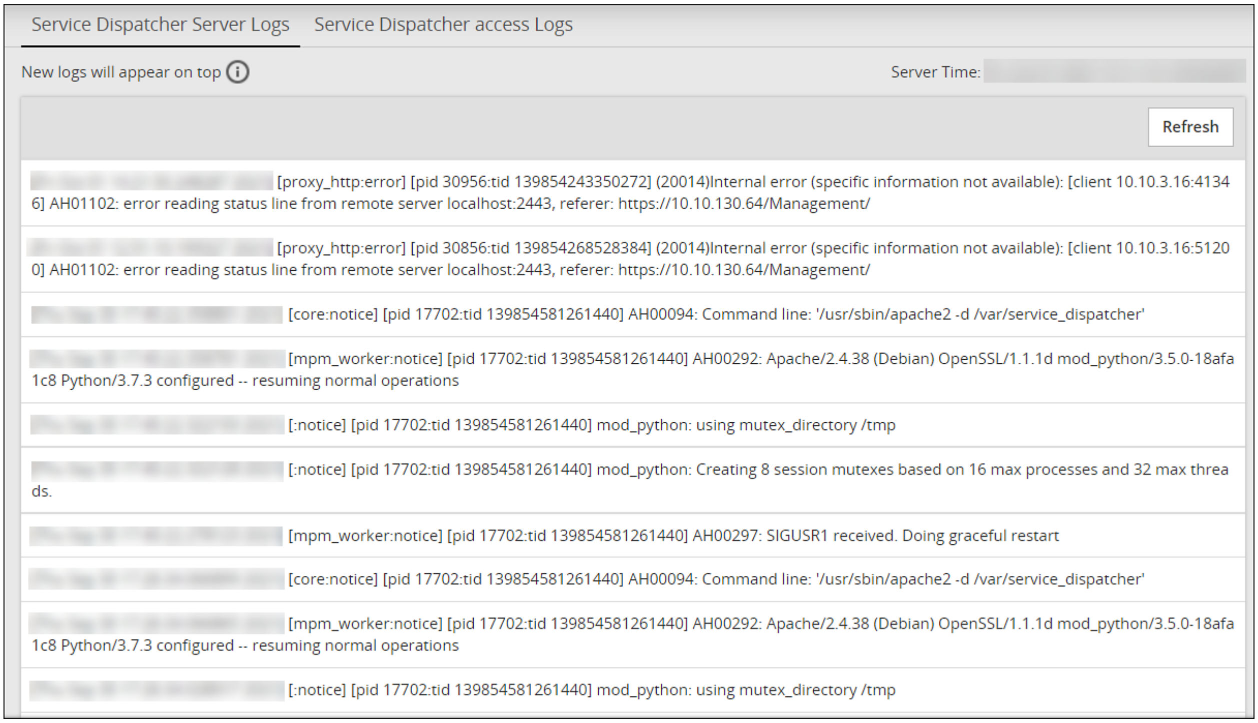
Figure 7-3: HTTP Server Logs

Navigate to **Logs** > **Web Services Engine** > **Web Services HTTP Server Logs** to view the HTTP Server logs.

7.6.2 Viewing Service Dispatcher Logs

You can view the logs for the Service Dispatcher under **Logs** > **Service Dispatcher** > **Service Dispatcher Logs**.

The following figure illustrates the service dispatcher logs.


Service Dispatcher Server Logs
Service Dispatcher access Logs
New logs will appear on top ⓘ
Server Time: [redacted]
Refresh

```
[redacted] [proxy_http:error] [pid 30956:tid 139854243350272] (20014)Internal error (specific information not available): [client 10.10.3.16:41346] AH01102: error reading status line from remote server localhost:2443, referer: https://10.10.130.64/Management/
[redacted] [proxy_http:error] [pid 30856:tid 139854268528384] (20014)Internal error (specific information not available): [client 10.10.3.16:51200] AH01102: error reading status line from remote server localhost:2443, referer: https://10.10.130.64/Management/
[redacted] [core:notice] [pid 17702:tid 139854581261440] AH00094: Command line: '/usr/sbin/apache2 -d /var/service_dispatcher'
[redacted] [mpm_worker:notice] [pid 17702:tid 139854581261440] AH00292: Apache/2.4.38 (Debian) OpenSSL/1.1.1d mod_python/3.5.0-18afa1c8 Python/3.7.3 configured -- resuming normal operations
[redacted] [:notice] [pid 17702:tid 139854581261440] mod_python: using mutex_directory /tmp
[redacted] [:notice] [pid 17702:tid 139854581261440] mod_python: Creating 8 session mutexes based on 16 max processes and 32 max threads.
[redacted] [mpm_worker:notice] [pid 17702:tid 139854581261440] AH00297: SIGUSR1 received. Doing graceful restart
[redacted] [core:notice] [pid 17702:tid 139854581261440] AH00094: Command line: '/usr/sbin/apache2 -d /var/service_dispatcher'
[redacted] [mpm_worker:notice] [pid 17702:tid 139854581261440] AH00292: Apache/2.4.38 (Debian) OpenSSL/1.1.1d mod_python/3.5.0-18afa1c8 Python/3.7.3 configured -- resuming normal operations
[redacted] [:notice] [pid 17702:tid 139854581261440] mod_python: using mutex_directory /tmp
```

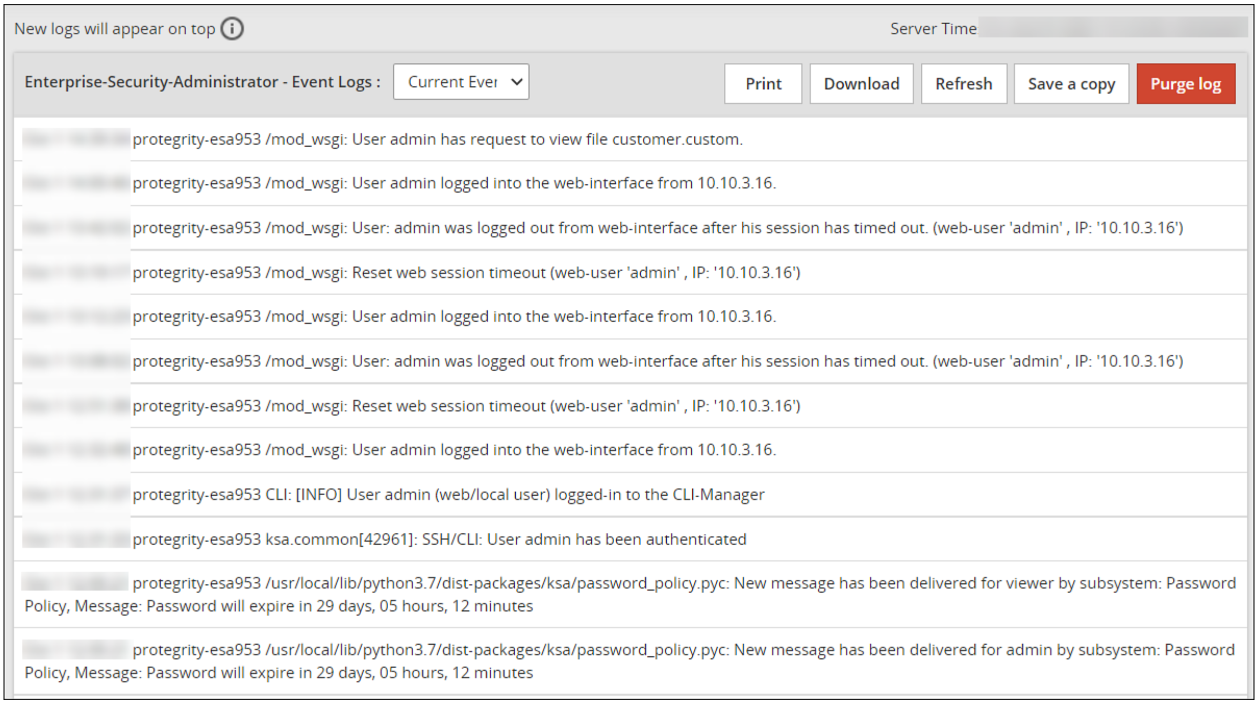
Figure 7-4: Service Dispatcher Logs

7.6.3 Viewing Appliance Logs

You can view logs of the events occurring in the appliance under **Logs** > **Appliance**. The Appliance Logs page lists events for each log and provides options for managing the logs. The logs files (.log extension) that are in the `/var/log` directory appear on the appliance logs screen. The logs can be categorized as all appliance component logs, installation logs, patch logs, kernel logs, and so on.

Current Event Logs are the most informative appliance logs and are displayed by default when you proceed to the Appliance Logs page. Depending on the logging level configuration (set in the appropriate configuration files of the appliance components), the Current Event Logs display the events in accordance with the selected level of severity (No logging, SEVERE, WARNING, INFO, CONFIG, ALL).

The following figures illustrate the appliance logs.


New logs will appear on top ⓘ
Server Time [redacted]
Enterprise-Security-Administrator - Event Logs :
Current Ever
Print
Download
Refresh
Save a copy
Purge log

```
[redacted] protegrity-esa953 /mod_wsgi: User admin has request to view file customer.custom.
[redacted] protegrity-esa953 /mod_wsgi: User admin logged into the web-interface from 10.10.3.16.
[redacted] protegrity-esa953 /mod_wsgi: User: admin was logged out from web-interface after his session has timed out. (web-user 'admin' , IP: '10.10.3.16')
[redacted] protegrity-esa953 /mod_wsgi: Reset web session timeout (web-user 'admin' , IP: '10.10.3.16')
[redacted] protegrity-esa953 /mod_wsgi: User admin logged into the web-interface from 10.10.3.16.
[redacted] protegrity-esa953 /mod_wsgi: User: admin was logged out from web-interface after his session has timed out. (web-user 'admin' , IP: '10.10.3.16')
[redacted] protegrity-esa953 /mod_wsgi: Reset web session timeout (web-user 'admin' , IP: '10.10.3.16')
[redacted] protegrity-esa953 /mod_wsgi: User admin logged into the web-interface from 10.10.3.16.
[redacted] protegrity-esa953 CLI: [INFO] User admin (web/local user) logged-in to the CLI-Manager
[redacted] protegrity-esa953 ksa.common[42961]: SSH/CLI: User admin has been authenticated
[redacted] protegrity-esa953 /usr/local/lib/python3.7/dist-packages/ksa/password_policy.pyc: New message has been delivered for viewer by subsystem: Password
Policy, Message: Password will expire in 29 days, 05 hours, 12 minutes
[redacted] protegrity-esa953 /usr/local/lib/python3.7/dist-packages/ksa/password_policy.pyc: New message has been delivered for admin by subsystem: Password
Policy, Message: Password will expire in 29 days, 05 hours, 12 minutes
```

Figure 7-5: Appliance Logs

The following table describes the actions you can perform on the appliance logs.

Table 7-5: Appliance Logs Actions

Action	Description
Print	Print the logs
Download	Download the logs to a specific directory
Refresh	Refresh the logs
Save a copy	Save a copy of the current log with a timestamp
Purge Log	Clear the logs

If the logs are rotated, a following message appears.

Logs has been rotated. Do you want to continue with new logs?

Select **OK** to view the new logs generated.

For more information about log rotation, refer to section *Configuring Log Rotation and Log Retention* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

Note:

If the new logging/fluentd component is initialized in the appliance, logs are sent to the Audit Store. If the new logging/fluentd component is not initialized in the appliance, logs are stored in /*audits_from_rsyslog.log* file under */var/log/pap* directory.

Note: Based on the configuration set for the logs, they are rotated periodically.

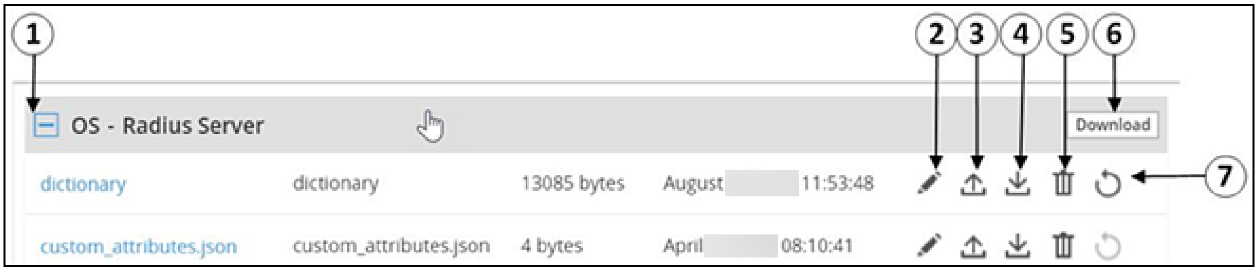
7.6.4 Working with Product Files

The *Product Files* screen displays the configuration files of all the products that are installed in ESA. You can view, modify, delete, upload, or download the configuration files from this screen. In the ESA Web UI, navigate to **System** > **Settings** > **Files** to view the configuration files.

The following table describes the different products and their respective configuration files that are available in ESA.

Product	Configuration Files	Description
OS – Radius Server	dictionary	Contains the dictionary translations for analyzing requests and generating responses for RADIUS server.
	custom_attributes.json	Contains the configuration settings of the header data for the RADIUS server.
OS –Export/Import	customer.custom	Lists the custom files that can be exported or imported. For more information about custom files refer to section *Exporting Custom Files* in the *Protegrity Appliances Overview Guide 9.1.0.5*.
Policy Management – Member Source Service User Files	exampleusers.txt	Lists the users that can be used in policy. For more information about policy users, refer to the *Protegrity Policy Management Guide 9.1.0.5*.
Policy Management – Member Source Service Group Files	examplegroups.txt	Lists the user groups that can be used in policy. For more information about policy user groups, refer to the *Protegrity Policy Management Guide 9.1.0.5*.
Downloads –Other Files	contractual.htm	Lists all the third-party software licenses that are utilized in ESA. **Note:** You cannot modify the file.
Distributed Filesystem File Protector – Configuration Files	dfscacherefresh.cfg	Contains the DFSFP configuration settings such as, logging, SSL, Security, and so on. For more information about the *dfscacherefresh.cfg* file, refer to the *Protegrity Big Data Protector Guide 9.1.0.0* .
Cloud Gateway –Settings	gateway.json	Lists the log level settings for Data Security Gateway. For more information about the *gateway.json* file, refer to the *Protegrity Data Security Gateway User Guide 3.1.0.5*.
	alliance.conf	Configuration file to direct syslog events between servers over TCP or UDP.

The following figure illustrates various actions that you can perform on the **Product Files** screen.



OS - Radius Server

dictionary	dictionary	13085 bytes	August [redacted] 11:53:48	
custom_attributes.json	custom_attributes.json	4 bytes	April [redacted] 08:10:41	

Callout	Description	Action
1	Collapse/Expand	Collapse or expand to view the configuration files
2	Edit	Edit the configuration file
3	Upload	Upload a configuration file **Note:** When you upload a file, it replaces the existing file in the system.
4	Download	Download the file to your local system
5	Delete	Delete the file from the system
6	Download	Download all the files of the product to your local system
7	Reset	Reset the configuration to the previously saved settings.

For more information about performing different operations on the files, refer to section *Working with Files* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

7.7 Working with Graphs

The graphs allow you to view performance graphs and real-time graphs in addition to statistics. In the Performance tab you can view a graphical representation of performance statistics from the past 24 hours for these items. On the ESA Web UI, navigate to **System** > **Graphs**, to view the performance graphs. The following figure illustrates the **Graphs** screen.

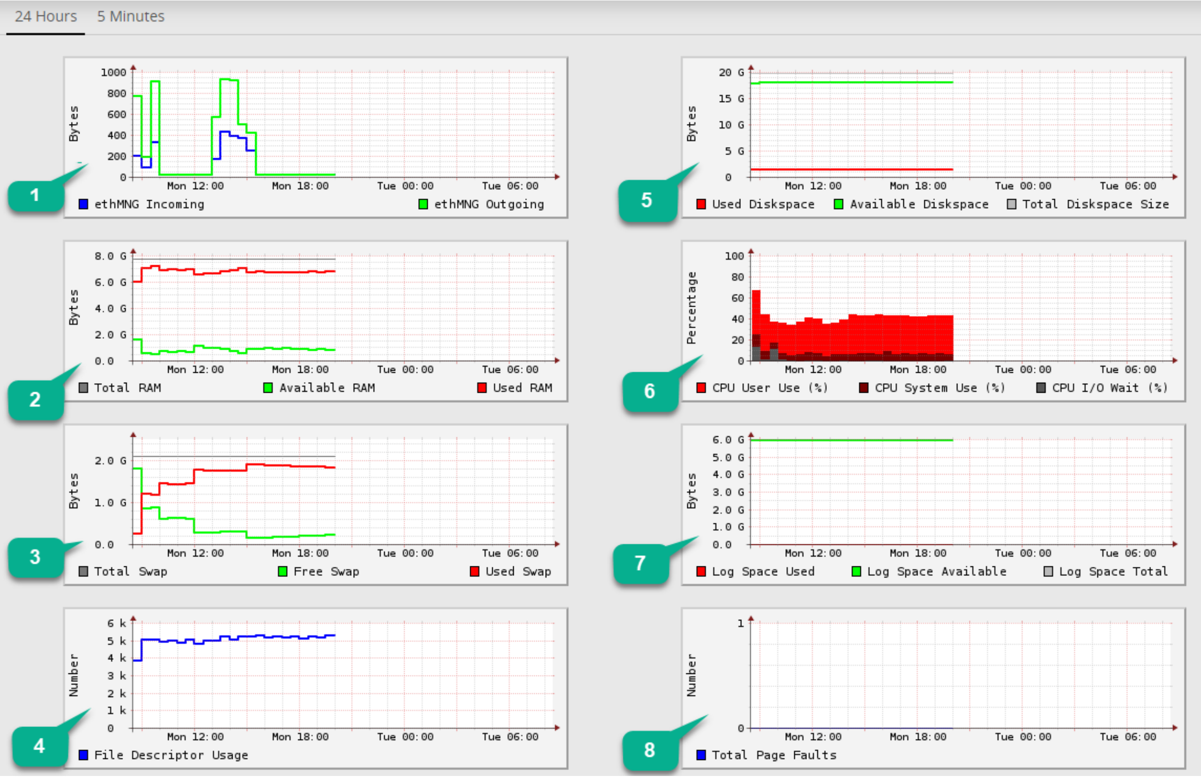
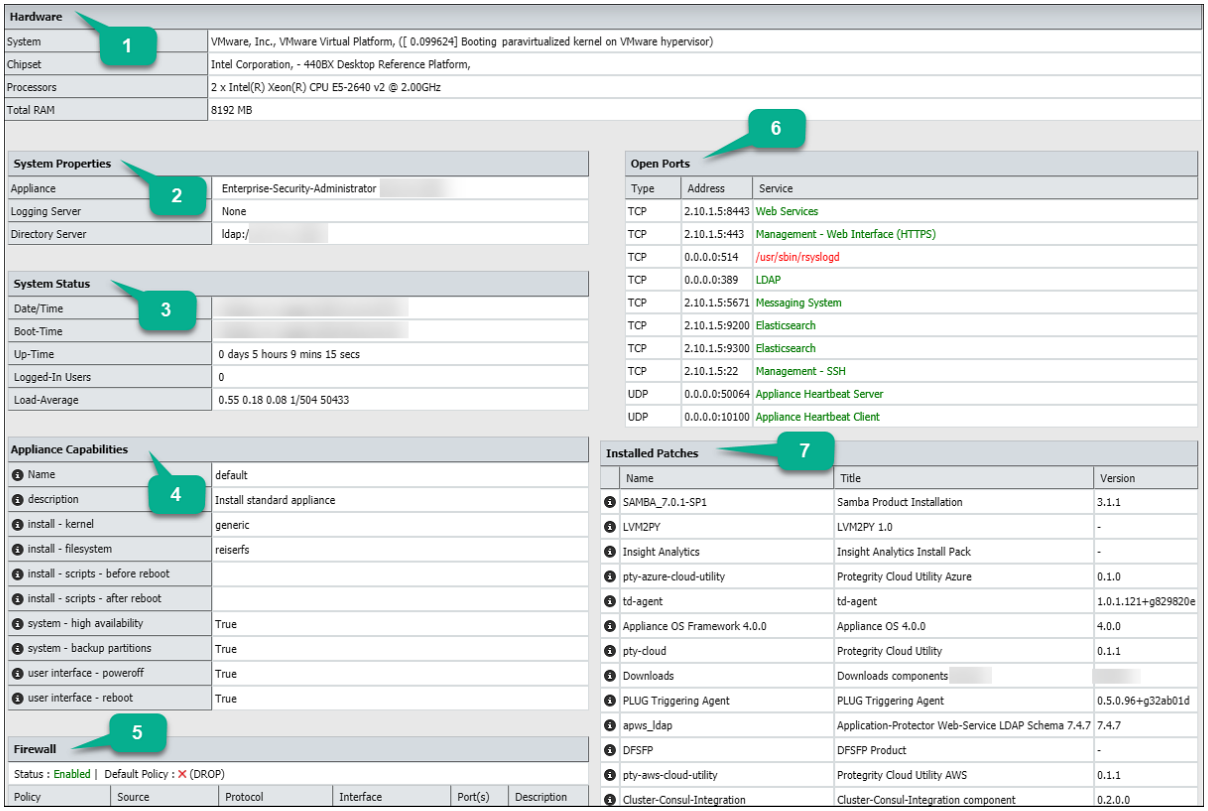


Figure 7-6: Performance Graphs

Callout	Description
1	Displays information the management NICs.
2	Displays information on total RAM, used RAM, and available RAM.
3	Displays information on total swap, used swap, and available swap.
4	Displays information about the usage of files.
5	Displays information on total disk space, used disk space, and available disk space.
6	Displays information on CPU used by the user, CPU used by the system, and CPU I/O wait.
7	Displays information on total log space, used log space, and available log space.
8	Displays information about the total page faults.

7.8 Working with Information

The Information screen is a screen that provides a tabular view for the details of the appliance. This screen All hardware information, system properties, system statuses, open ports, and firewall rules are listed in the Information tab. On the ESA Web UI, navigate to **System** > **Information**, to view the details about the appliances. The following figure illustrates the **Information** screen.



Hardware	
System	VMware, Inc., VMware Virtual Platform, ([0.099624] Booting paravirtualized kernel on VMware hypervisor)
Chipset	Intel Corporation, - 440BX Desktop Reference Platform,
Processors	2 x Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz
Total RAM	8192 MB

System Properties	
Appliance	Enterprise-Security-Administrator [redacted]
Logging Server	None
Directory Server	ldap:/[redacted]

System Status	
Date/Time	[redacted]
Boot-Time	[redacted]
Up-Time	0 days 5 hours 9 mins 15 secs
Logged-In Users	0
Load-Average	0.55 0.18 0.08 1/504 50433

Appliance Capabilities	
Name	default
description	Install standard appliance
install - kernel	generic
install - filesystem	reiserfs
install - scripts - before reboot	
install - scripts - after reboot	
system - high availability	True
system - backup partitions	True
user interface - poweroff	True
user interface - reboot	True

Firewall

Status : Enabled | Default Policy : ✗ (DROP)

Policy	Source	Protocol	Interface	Port(s)	Description

Open Ports

Type	Address	Service
TCP	2.10.1.5:8443	Web Services
TCP	2.10.1.5:443	Management - Web Interface (HTTPS)
TCP	0.0.0.0:514	/usr/sbin/rsyslogd
TCP	0.0.0.0:389	LDAP
TCP	2.10.1.5:5671	Messaging System
TCP	2.10.1.5:9200	Elasticsearch
TCP	2.10.1.5:9300	Elasticsearch
TCP	2.10.1.5:22	Management - SSH
UDP	0.0.0.0:50064	Appliance Heartbeat Server
UDP	0.0.0.0:10100	Appliance Heartbeat Client

Installed Patches

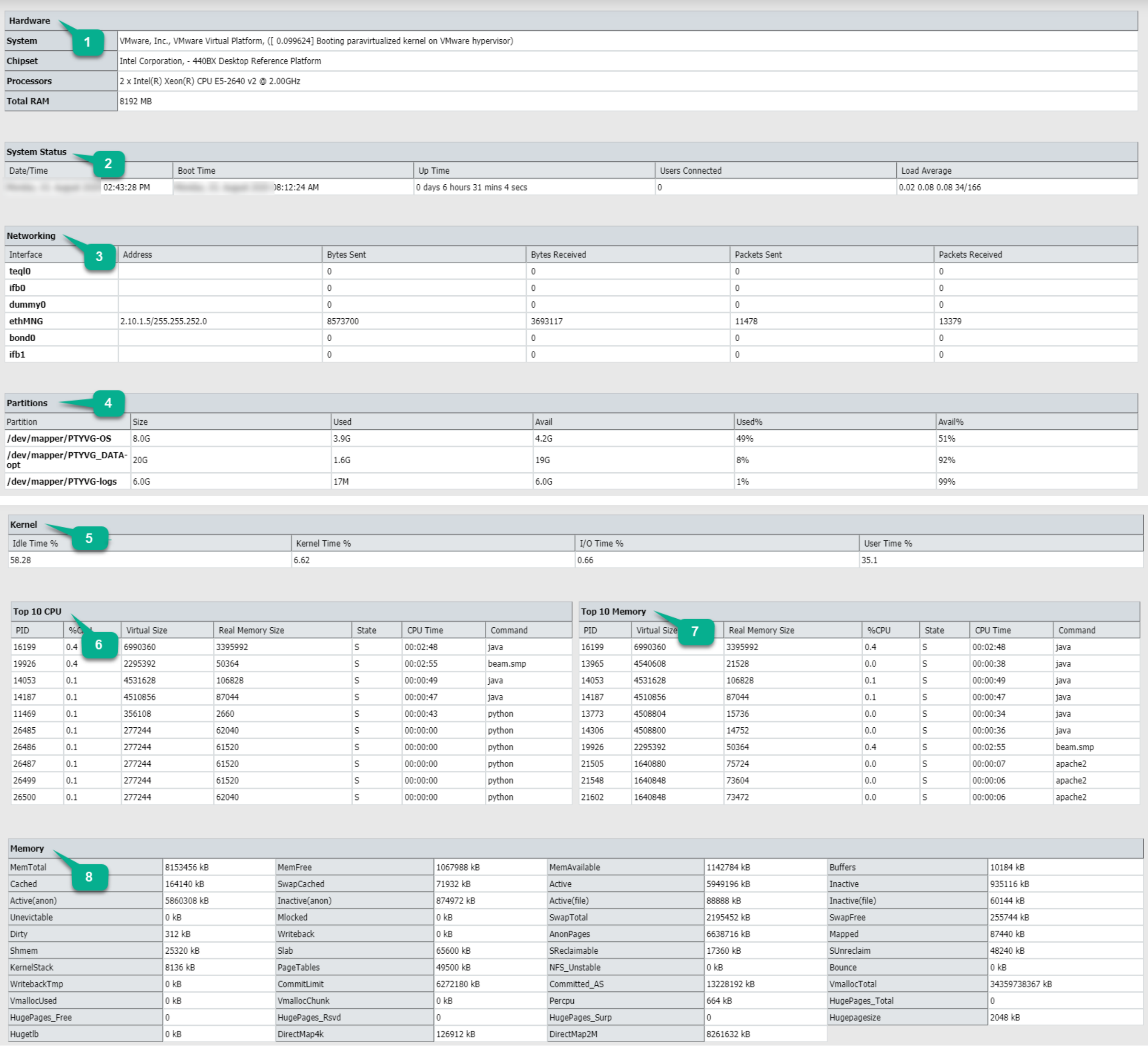
Name	Title	Version
SAMBA_7.0.1-SP1	Samba Product Installation	3.1.1
LVM2PY	LVM2PY 1.0	-
Insight Analytics	Insight Analytics Install Pack	-
pty-azure-cloud-utility	Protegrity Cloud Utility Azure	0.1.0
td-agent	td-agent	1.0.1.121+g829820e
Appliance OS Framework 4.0.0	Appliance OS 4.0.0	4.0.0
pty-cloud	Protegrity Cloud Utility	0.1.1
Downloads	Downloads components [redacted]	[redacted]
PLUG Triggering Agent	PLUG Triggering Agent	0.5.0.96+g32ab01d
apws_ldap	Application-Protector Web-Service LDAP Schema 7.4.7	7.4.7
DFSFP	DFSFP Product	-
pty-aws-cloud-utility	Protegrity Cloud Utility AWS	0.1.1
Cluster-Consul-Integration	Cluster-Consul-Integration component	0.2.0.0

Figure 7-7: Information Screen

Callout	Description
1	**Hardware** section includes information on system, chipset, processors, and number of total RAM.
2	**System Properties** section includes information on current Appliance, logging server, and directory server.
3	**System Status** section lists properties such as data and time, boot time, up time, number of logged in users, and average load.
4	**Appliance Capabilities** section includes information about the current capabilities of the appliance such as installed kernel, system -high availability, etc.
5	**Firewall** section lists all Firewall rules, Firewall status (enabled/disabled), and the default policy
6	**Open Ports** section lists types, addresses and names of services that are running
7	**Installed Patches** section lists all the patches that are installed on the system.

7.9 Working with System Statistics

The System Statistics allow you to view the system statistics to assess system usage and efficiency. On the ESA Web UI, navigate to **System** > **System Statistics**, to view the statistics.The following figure illustrates the **System Statistics** screen.



Hardware	
System	VMware, Inc., VMware Virtual Platform, ([0.099624] Booting paravirtualized kernel on VMware hypervisor)
Chipset	Intel Corporation, - 440BX Desktop Reference Platform
Processors	2 x Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz
Total RAM	8192 MB

System Status

Date/Time	Boot Time	Up Time	Users Connected	Load Average
[redacted] 02:43:28 PM	[redacted]8:12:24 AM	0 days 6 hours 31 mins 4 secs	0	0.02 0.08 0.08 34/166

Networking

Interface	Address	Bytes Sent	Bytes Received	Packets Sent	Packets Received
teql0		0	0	0	0
ifb0		0	0	0	0
dummy0		0	0	0	0
ethMNG	2.10.1.5/255.255.252.0	8573700	3693117	11478	13379
bond0		0	0	0	0
ifb1		0	0	0	0

Partitions

Partition	Size	Used	Avail	Used%	Avail%
/dev/mapper/PTYVG-OS	8.0G	3.9G	4.2G	49%	51%
/dev/mapper/PTYVG_DATA-opt	20G	1.6G	19G	8%	92%
/dev/mapper/PTYVG-logs	6.0G	17M	6.0G	1%	99%

Kernel

Idle Time %	Kernel Time %	I/O Time %	User Time %
58.28	6.62	0.66	35.1

Top 10 CPU

PID	%CPU	Virtual Size	Real Memory Size	State	CPU Time	Command
16199	0.4	6990360	3395992	S	00:02:48	java
19926	0.4	2295392	50364	S	00:02:55	beam.smp
14053	0.1	4531628	106828	S	00:00:49	java
14187	0.1	4510856	87044	S	00:00:47	java
11469	0.1	356108	2660	S	00:00:43	python
26485	0.1	277244	62040	S	00:00:00	python
26486	0.1	277244	61520	S	00:00:00	python
26487	0.1	277244	61520	S	00:00:00	python
26499	0.1	277244	61520	S	00:00:00	python
26500	0.1	277244	62040	S	00:00:00	python

Top 10 Memory

PID	Virtual Size	Real Memory Size	%CPU	State	CPU Time	Command
16199	6990360	3395992	0.4	S	00:02:48	java
13965	4540608	21528	0.0	S	00:00:38	java
14053	4531628	106828	0.1	S	00:00:49	java
14187	4510856	87044	0.1	S	00:00:47	java
13773	4508804	15736	0.0	S	00:00:34	java
14306	4508800	14752	0.0	S	00:00:36	java
19926	2295392	50364	0.4	S	00:02:55	beam.smp
21505	1640880	75724	0.0	S	00:00:07	apache2
21548	1640848	73604	0.0	S	00:00:06	apache2
21602	1640848	73472	0.0	S	00:00:06	apache2

Memory

MemTotal	8153456 kB	MemFree	1067988 kB	MemAvailable	1142784 kB	Buffers	10184 kB
Cached	164140 kB	SwapCached	71932 kB	Active	5949196 kB	Inactive	935116 kB
Active(anon)	5860308 kB	Inactive(anon)	874972 kB	Active(file)	88888 kB	Inactive(file)	60144 kB
Unevictable	0 kB	Mlocked	0 kB	SwapTotal	2195452 kB	SwapFree	255744 kB
Dirty	312 kB	Writeback	0 kB	AnonPages	6638716 kB	Mapped	87440 kB
Shmem	25320 kB	Slab	65600 kB	SReclaimable	17360 kB	SUnreclaim	48240 kB
KernelStack	8136 kB	PageTables	49500 kB	NFS_Unstable	0 kB	Bounce	0 kB
WritebackTmp	0 kB	CommitLimit	6272180 kB	Committed_AS	13228192 kB	VmallocTotal	34359738367 kB
VmallocUsed	0 kB	VmallocChunk	0 kB	Percpu	664 kB	HugePages_Total	0
HugePages_Free	0	HugePages_Rsvd	0	HugePages_Surp	0	Hugepagesize	2048 kB
Hugetlb	0 kB	DirectMap4k	126912 kB	DirectMap2M	8261632 kB		

Figure 7-8: System Statistics

Callout	Description
1	**Hardware** section includes information on system, chipset, processors, and number of total RAM.
2	**System Status** section includes information on date/time, boot time, up-time, users connected, and load average.
3	**Networking** section includes information on interface, address, bytes sent/received, and packets sent/received.
4	**Partitions** section includes information on partition name and size, used, and available partition space.
5	**Kernel** section includes information on idle time, kernel time, I/O time, and user time.
6	**Top 10 CPU** section includes information on the CPU utilization, virtual size, real memory size, state, CPU time, and command.
7	**Top 10 Memory** section includes information on the memory utilization, virtual size, real memory size, percentage memory utilized for each CPU, state, CPU time, and command.
8	**Memory** section includes information on total memory, swap cached, and inactive, among others.

Chapter 8

Working with Trusted Appliances Cluster

Network clustering is a process, where a group of computers are organized in a manner that they function as a single system. The systems in the cluster connect with each other for information exchange. Clustering supports disaster recovery, where a failure of one system does not affect business continuity and performance of the resources is maintained.

In Protegrity appliances, clustering is used as a disaster recovery mechanism, where data between the appliances is replicated. Appliances such as, ESA or DSG, are connected to each other for backing up or retrieving information. A trusted channel is created to transfer data between the appliances, thus creating a Trusted Appliances Cluster (TAC). You can also run remote commands, synchronize files and configurations across multiple sites, or import/export configurations between appliances that are directly connected to each other.

In a TAC, all the systems in the cluster are in active state. The request for security operations are handled across the active appliances in the cluster. Thus, in case of a failure of an appliance, the requests are balanced across other appliances in the cluster.

The following screen displays the TAC setup of multiple appliances.

8.1 TAC Topology

In a TAC, every appliance communicates with each other for passing information. The Consul networking solution is implemented in the cluster for communication. Based on solution, the appliances are classified as follows:

- Server: Maintains information about all the appliances in the cluster, performs regular health checks, and responds to queries from the clients
- Client: Stateless agent that requests information from a server

A server can be further classified as a leader or a follower. The leader is responsible for maintaining the status of cluster and replicating cluster-related information among other servers in the cluster. The first appliance that is added the cluster is the leader. The other appliances added to the cluster are followers. If a cluster contains multiple appliances that can perform a role of the server, a poll is conducted amongst them to elect a leader. For more information about Consul, click *here*.

It is important to maintain the number of servers to keep the cluster available. For a cluster to be functional, the number of servers available must be (N/2) + 1, where N is the number of servers in the cluster. Thus, it is recommended to have a minimum of three servers in your cluster for fault tolerance.

8.2 Deploying Appliances in a Cluster

You can deploy the appliances in a cluster, it takes up the role of a server or a client. This deployment of an appliance in a cluster is based on values that you set in the configuration files. These parameters in the files determine the role of an appliance and maximum numbers of servers in the cluster.

Before adding an appliance to the cluster, the parameters in the following configuration files must be checked:

- *agent.json*: Specifies the role of an appliance in the cluster. It is available in the */opt/cluster-consul-integration/configure* directory.
- *auto_agent.json*: Specifies the maximum number of servers allowed in a cluster. Additionally, you can also specify which appliances can be added to the cluster as servers. It is available in the */opt/cluster-consul-integration/configure* directory.
- *config.json*: Contains the cluster-related information for an appliance, such as, data center, ports, Consul certificates, bind address, and so on. It is available in the */opt/consul/configure* directory.

The following table describes the parameters of the configuration files and the required pointers that must be taken into consideration.

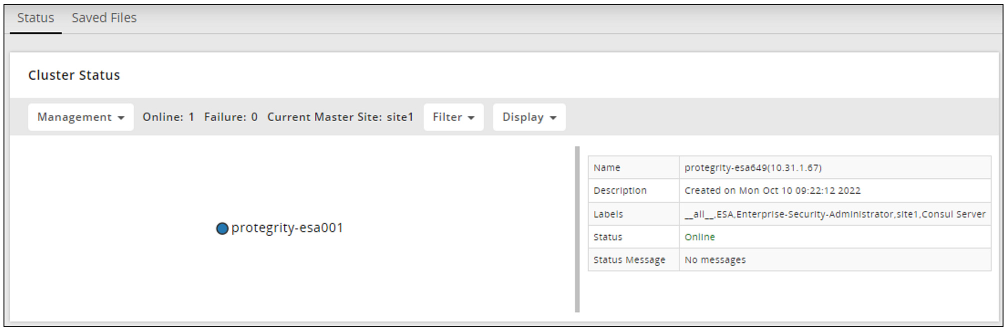
Table 8-1: Parameters of the Configuration Files

Parameter	File	Description	Value
type	*agent.json*	Set role of the appliance in the cluster	• auto (default) – Role of the appliance is determined based on state of the TAC and the parameters of the `auto_agent.json` file. • client – Appliance is added to cluster as a client • server– Appliance is added to cluster as a server
PAP_eligible_servers	*auto_agent.json*	Set maximum number of servers that can be deployed in a cluster	5 (default) **Note:** • It is recommended to set the attribute value as 3 or 5. • If the attribute value is 0, then all the appliances are added to the cluster as servers.
maximum_servers	*auto_agent.json*	Code of appliance that must deployed as servers.	• ESA (default) - ESA appliance • CG – DSG appliance

Scenario 1

Consider an ESA appliance, ESA001, on which you create a cluster. As this is the first appliance on the cluster, ESA001 is becomes the leader of the cluster. The following are the values of the default attributes of the `agent.json` and `auto_agent.json` files on ESA001.

- *type: auto*
- *maximum_servers: 5*
- *PAP_eligible_servers: ESA*



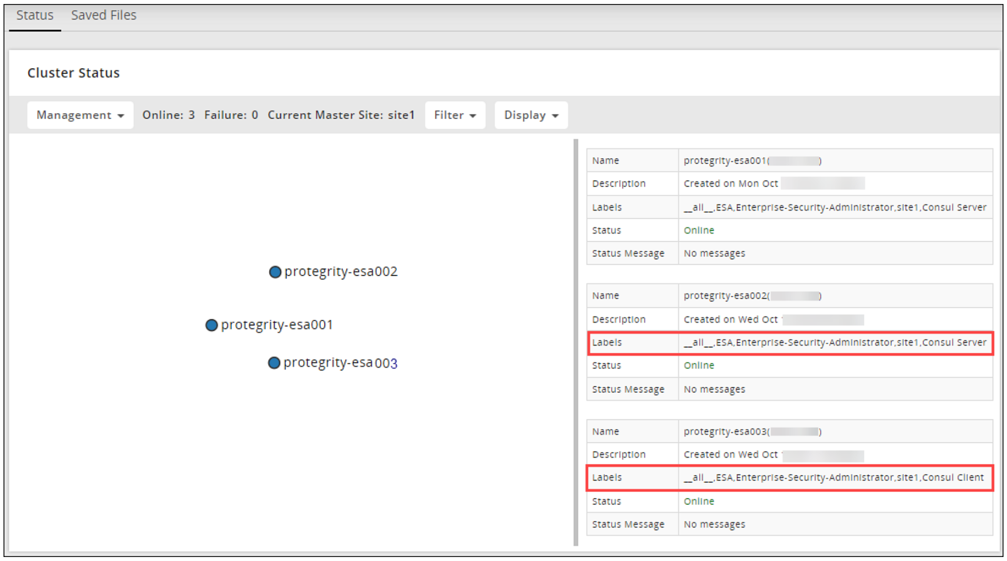
Name	protegrity-esa649(10.31.1.67)
Description	Created on Mon Oct 10 09:22:12 2022
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Scenario 2

Consider an ESA appliance on which a cluster is created. If you want to add another appliance to this cluster as a server, ensure that the type is set as server. For example, if you want to add ESA002 to a cluster created by ESA001, ensure that *type* attribute in the `agent.json` file is set as *server*.

If you want to add another ESA appliance ESA003 to this cluster as a client, you must ensure that the *type* attribute in the `agent.json` file of ESA003 is set as *client*.

The following figure illustrates the cluster comprising of nodes ESA001, ESA002, and ESA003.



Name	protegrity-esa001([redacted])
Description	Created on Mon Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa002([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa003([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Client
Status	Online
Status Message	No messages

Now, you add another ESA appliance, ESA004, to this cluster with the following attributes:

- *type: auto*
- *maximum_servers: 5*
- *PAP_eligible_servers: ESA*

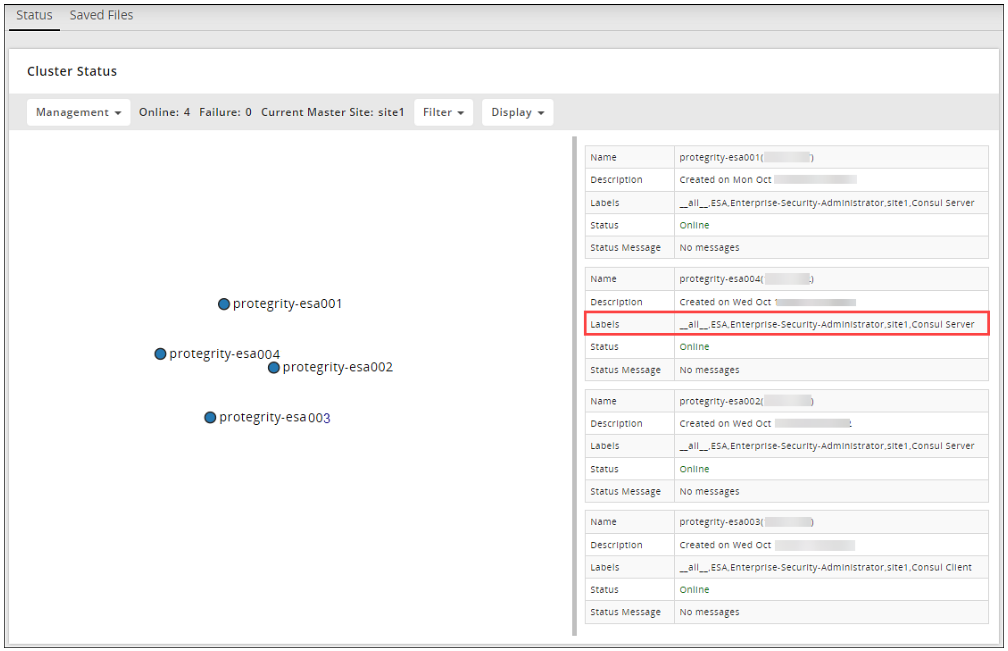
In this case, the following checks are performed:

1. Is the value of *maximum_servers* greater than zero? Yes.
2. Is the number of servers in the cluster exceeding the *maximum_servers*? No

3. Is the appliance code of ESA004 in the *PAP_eligible_servers* list? Yes.

> **Note:** You can view the appliance code of the appliance in the *Appliance_code* file in the `/etc` directory.

As the limit of the number of servers on the cluster is not exceeded and the appliance is a part of the server list, ESA004 is added as a server as shown in the following figure.



Name	protegrity-esa001([redacted])
Description	Created on Mon Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa004([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa002([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa003([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Client
Status	Online
Status Message	No messages

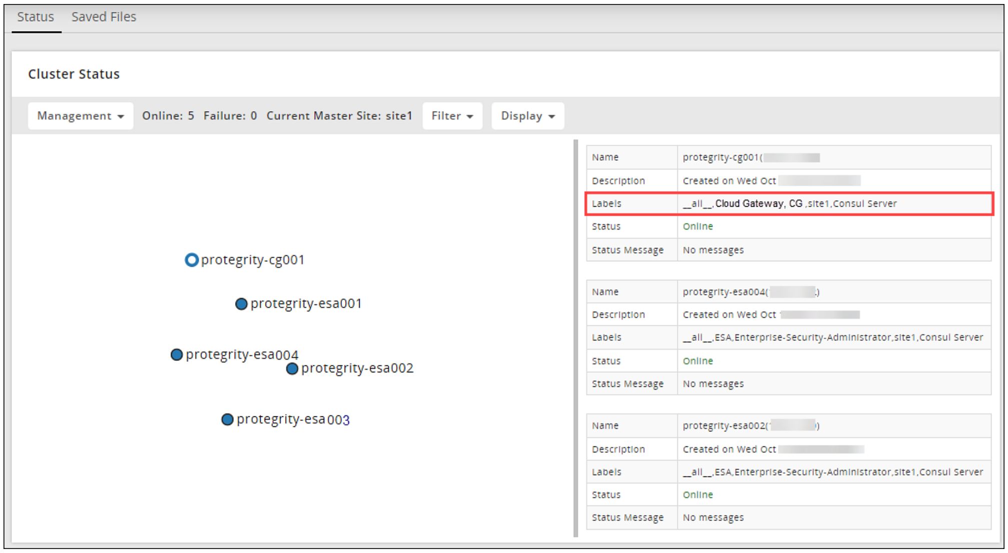
Now, add another DSG appliance, CG001, to this cluster with the following attributes:

- *type: auto*
- *maximum_servers: 5*
- *PAP_eligible_servers: CG*

In this case, the following checks are performed:

1. Is the *maximum_servers* greater than zero? Yes.
2. Is the number of servers in the cluster exceeding the *maximum_servers*? No.
3. Is the appliance code of CG001 in the *PAP_eligible_servers* list? Yes.

Thus, DSG1 is added to the cluster as a server.

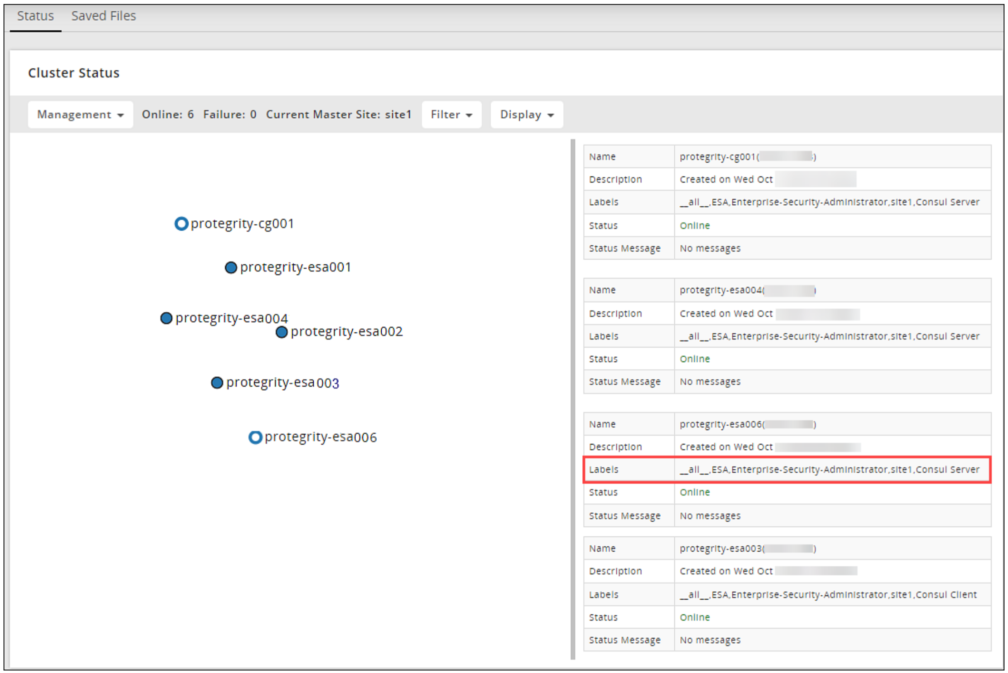


Name	protegrity-cg001([redacted]
Description	Created on Wed Oct [redacted]
Labels	__all__,Cloud Gateway, CG ,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa004([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa002([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Now, consider the cluster with five servers, ESA001, ESA002, ESA003, ESA004, and ESA006 as shown in the following figure.



Name	protegrity-cg001([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa004([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa006([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa003([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Client
Status	Online
Status Message	No messages

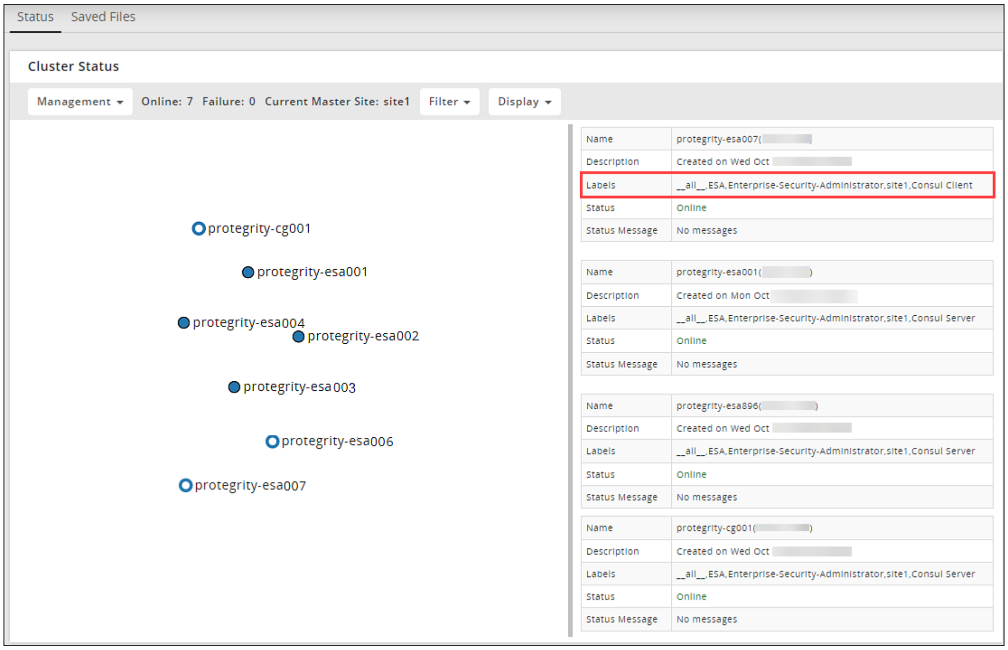
You now add another ESA appliance, ESA007 to this cluster, with the following attributes:

- *type: auto*
- *maximum_servers: 5*
- *PAP_eligible_servers: ESA*

In this case, the following checks are performed:

1. Is the *maximum_servers* greater than zero? Yes.
2. Is the number of servers in the cluster exceeding the *maximum_servers*? Yes
3. Is the appliance code of ESA007 in the *PAP_eligible_servers* list? Yes

Thus, as the limit of the number of servers in a cluster is exceeded, ESA007 is added as a client.



Cluster Status

Online: 7 Failure: 0 Current Master Site: site1

Name	protegrity-esa007([redacted]
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Client
Status	Online
Status Message	No messages

Name	protegrity-esa001([redacted])
Description	Created on Mon Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa896([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-cg001([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

8.3 Deploying Appliances in a Cluster - Flowchart

Based on the appliance and the configurations defined, the following flowchart illustrates how an appliance is deployed in a cluster.

The following table describes the parameters of the configuration files and the required pointers that must be taken into consideration.

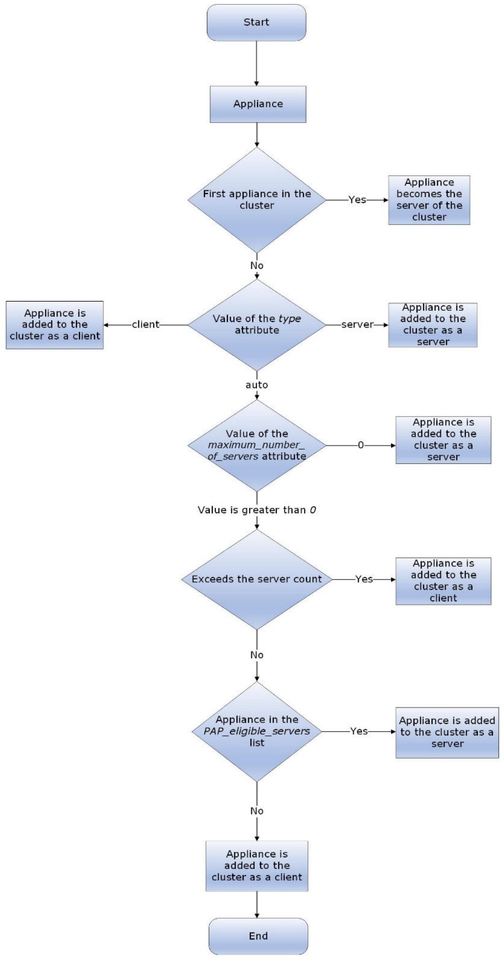

Start
Appliance
First appliance in the cluster
Yes
Appliance becomes the server of the cluster
No
Value of the *type* attribute
client
Appliance is added to the cluster as a client
server
Appliance is added to the cluster as a server
auto
Value of the *maximum_number_of_servers* attribute
0
Appliance is added to the cluster as a server
Value is greater than *0*
Exceeds the server count
Yes
Appliance is added to the cluster as a client
No
Appliance in the *PAP_eligible_servers* list
Yes
Appliance is added to the cluster as a server
No
Appliance is added to the cluster as a client
End

Figure 8-1: Flowchart for Deploying Appliances in a Cluster

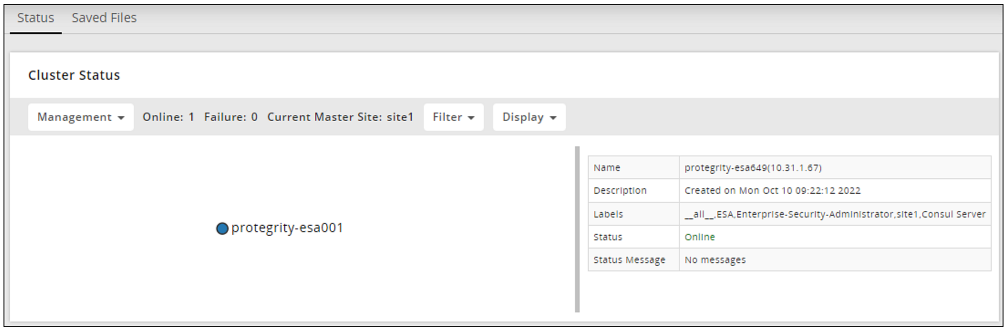
8.4 Deploying Appliances in a Cluster - Scenarios

This section describes the different scenarios for deploying appliances in a cluster.

Scenario 1

Consider an ESA appliance, ESA001, on which you create a cluster. As this is the first appliance on the cluster, ESA001 is becomes the leader of the cluster. The following are the values of the default attributes of the *agent.json* and *auto_agent.json* files on ESA001.

- *type: auto*
- *maximum_servers: 5*
- *PAP_eligible_servers: ESA*



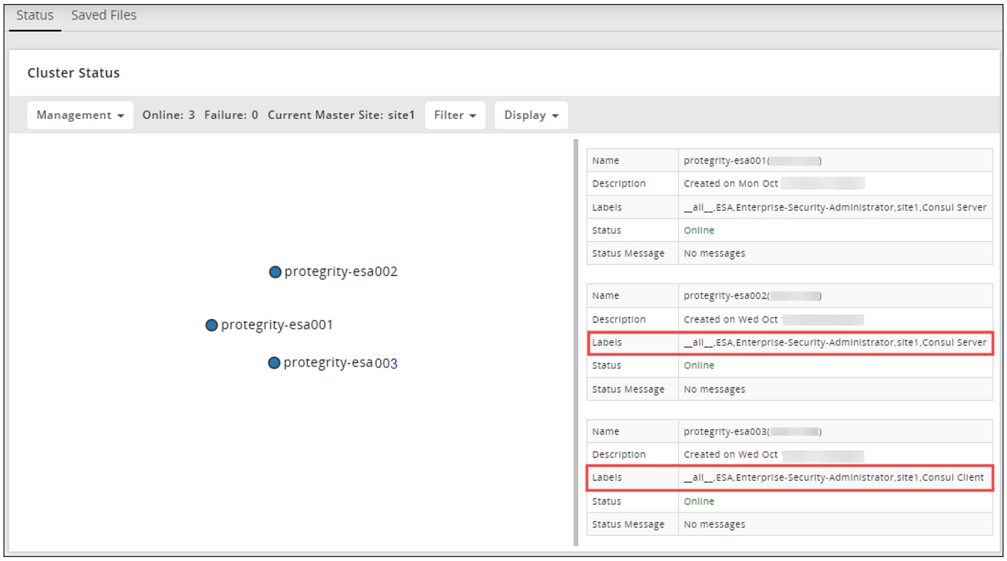
Name	protegrity-esa649(10.31.1.67)
Description	Created on Mon Oct 10 09:22:12 2022
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Scenario 2

Consider an ESA appliance on which a cluster is created. If you want to add another appliance to this cluster as a server, ensure that the type is set as server. For example, if you want to add ESA002 to a cluster created by ESA001, ensure that *type* attribute in the `agent.json` file is set as *server*.

If you want to add another ESA appliance ESA003 to this cluster as a client, you must ensure that the *type* attribute in the `agent.json` file of ESA003 is set as *client*.

The following figure illustrates the cluster comprising of nodes ESA001, ESA002, and ESA003.



Name	protegrity-esa001([redacted])
Description	Created on Mon Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa002([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa003([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Client
Status	Online
Status Message	No messages

Scenario 3

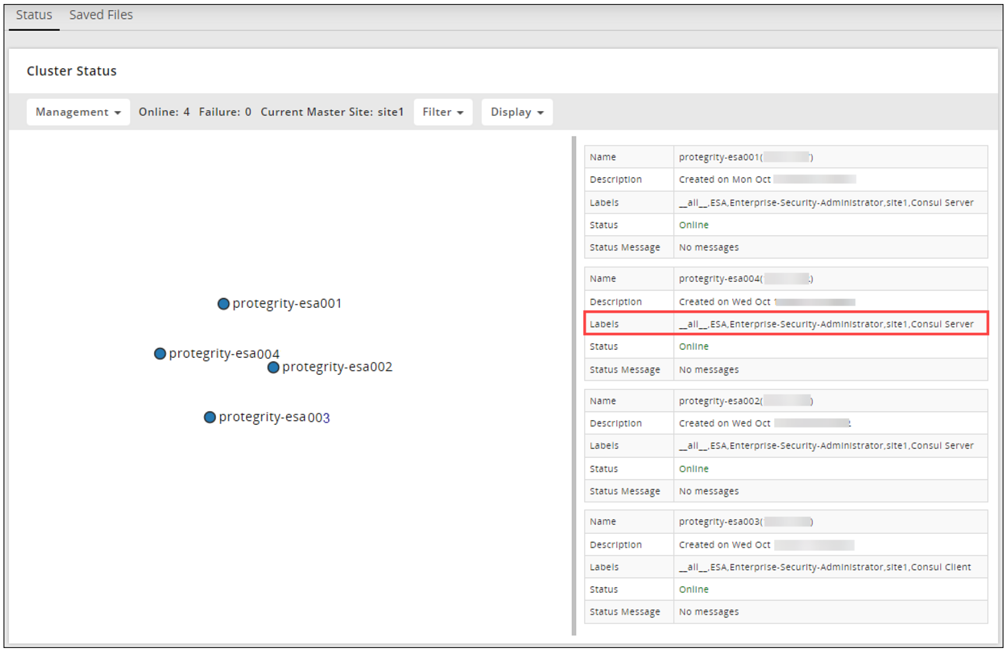
Consider appliances ESA001, ESA002, and ESA003 in a cluster. Appliances ESA001 and ESA002 are added as servers to the cluster. You add another ESA appliance, ESA004, to this cluster with the following attributes:

- *type: auto*
- *maximum_servers: 5*
- *PAP_eligible_servers: ESA*

In this case, the following checks are performed:

1. Is the value of *maximum_servers* greater than zero? Yes.
2. Is the number of servers in the cluster exceeding the *maximum_servers*? No
3. Is the appliance code of ESA004 in the *PAP_eligible_servers* list? Yes.

As the limit of the number of servers on the cluster is not exceeded and the appliance is a part of the server list, ESA004 is added as a server as shown in the following figure.



Name	protegrity-esa001([redacted])
Description	Created on Mon Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa004([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa002([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa003([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Client
Status	Online
Status Message	No messages

Scenario 4

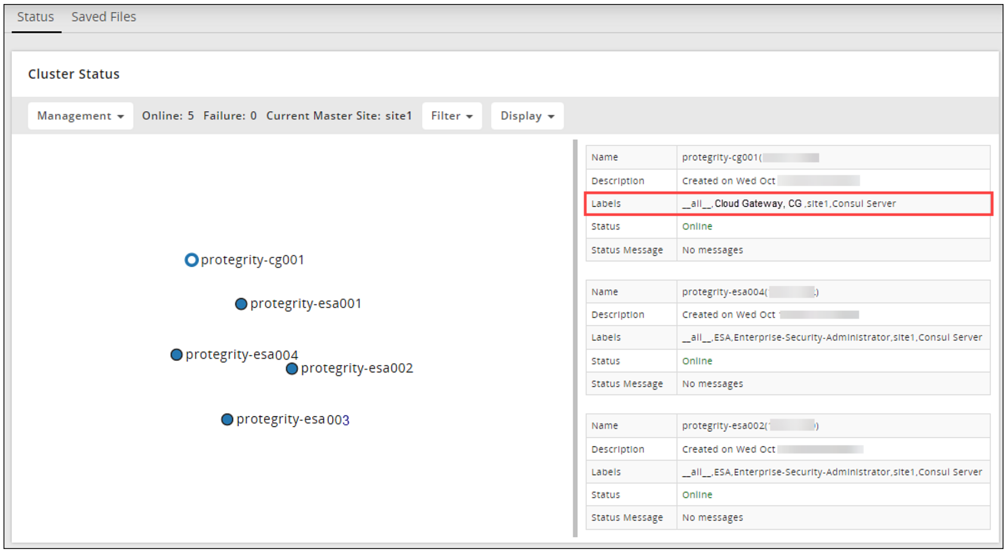
Consider appliances ESA001, ESA002, ESA003 and ESA004 in a cluster. All the appliances are added as servers to the cluster. You add a DSG appliance, CG001, to this cluster with the following attributes:

- *type: auto*
- *maximum_servers: 5*
- *PAP_eligible_servers: CG*

In this case, the following checks are performed:

1. Is the *maximum_servers* greater than zero? Yes.
2. Is the number of servers in the cluster exceeding the *maximum_servers*? No.
3. Is the appliance code of CG001 in the *PAP_eligible_servers* list? Yes.

Thus, DSG1 is added to the cluster as a server.



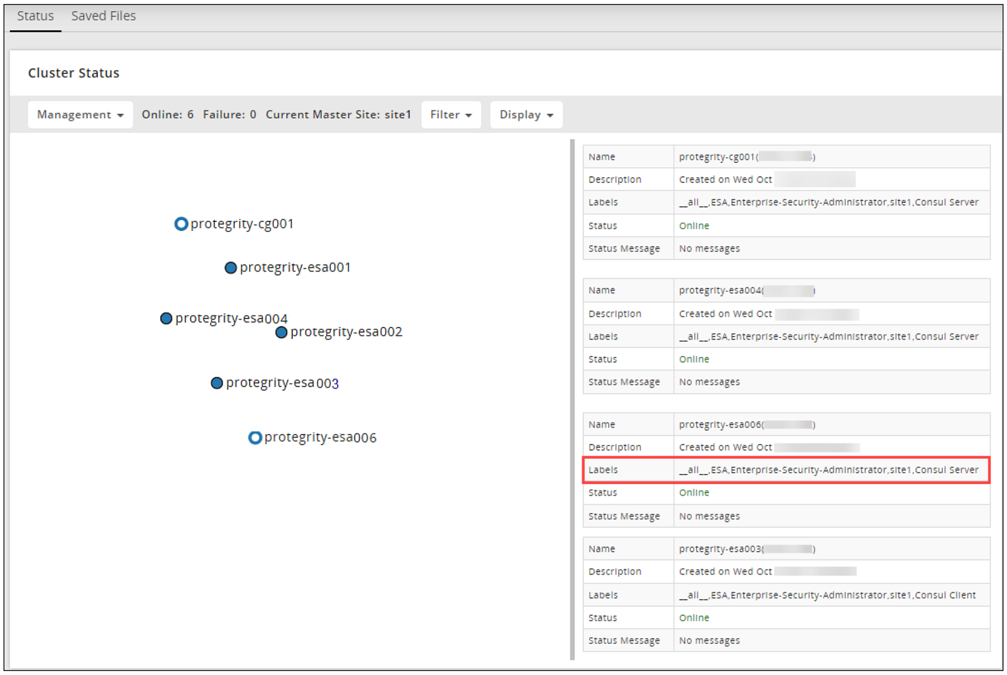
Name	protegrity-cg001([redacted]
Description	Created on Wed Oct [redacted]
Labels	__all__,Cloud Gateway, CG ,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa004([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa002([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Scenario 5

Consider the cluster with five servers, ESA001, ESA002, ESA003, ESA004, and ESA006 as shown in the following figure.



Name	protegrity-cg001([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa004([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa006([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa003([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Client
Status	Online
Status Message	No messages

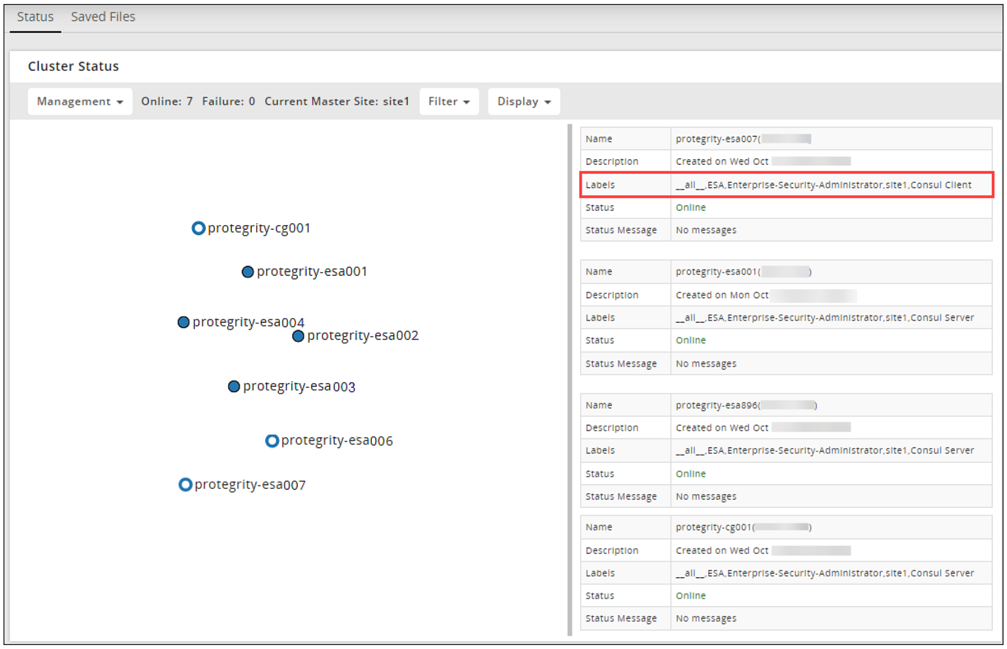
You add another ESA appliance, ESA007 to this cluster, with the following attributes:

- *type: auto*
- *maximum_servers: 5*
- *PAP_eligible_servers: ESA*

In this case, the following checks are performed:

1. Is the *maximum_servers* greater than zero? Yes.
2. Is the number of servers in the cluster exceeding the *maximum_servers*? Yes
3. Is the appliance code of ESA007 in the *PAP_eligible_servers* list? Yes

Thus, as the limit of the number of servers in a cluster is exceeded, ESA007 is added as a client.



Name	protegrity-esa007([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Client
Status	Online
Status Message	No messages

Name	protegrity-esa001([redacted])
Description	Created on Mon Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa896([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-cg001([redacted])
Description	Created on Wed Oct [redacted]
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

> **Note:** You can view the appliance code of the appliance in the *Appliance_code* file in the `/etc` directory.

8.5 Operating the Cluster

After performing the required configurations and meeting the prerequisites, you can work on the cluster. The cluster involves different operations such as creating a cluster, managing nodes, executing commands, managing sites, and so on. The following sections describe the different operations that you can perform on a TAC.

8.5.1 Creating a Cluster

The first step in setting up the TAC is the Create a Cluster operation. In this process you set up a base that allows other appliances to be added or invited to the cluster. You can create a cluster from the *CLI* or from the *Web UI*.

Creating a cluster involves defining communication methods for the appliance. Every appliance in a network is identified using a unique identifier. A communication method is a qualifier for the remote appliances in the network to communicate with the local appliance. The process of setting up communication methods is generally performed while creating the cluster. After the cluster is created, you can *edit the communication method* of the appliance from the CLI Manager.

For more information about creating a cluster, refer to *Creating a cluster* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

8.5.2 Joining a Cluster

If a TAC is already set up, you can use the Join a Cluster operation to add it to the cluster. You can join a cluster from the *CLI Manager* or from the *Web UI*. This operation can be classified into two ways:

- Adding an appliance to the cluster
- Inviting a appliance to the cluster

Similar to the creating a cluster operation, you can set the communication method that identifies the appliance in the cluster.

For more information about joining a cluster, refer to *Joining a cluster* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

> **Note:**
>
> After joining an appliance to the cluster, ensure that you delete the Consul certificates that appear on the Certificate Management screen. Navigate to **Settings** > **Network** > **Certificate Repository**. Click the delete icon next to **Server certificate and key for Consul**.

8.5.3 Managing Sites

Sites in ESA can be a geographical location or a virtual location that contain multiple appliances and protectors operating in it. You can create a TAC between appliances in a site or TAC of appliances based in multiple sites. The sites can act as disaster recovery mechanism, where failure of one site causes the traffic to be directed to other active sites. You can manage a site from the CLI Manager.

For more information about managing sites, refer to *Managing a Site* in the *Protegrity Appliances Overview Guide 9.1.0.5*

8.5.4 Managing Nodes

Using the Node Management screen, you can update the cluster information of an appliance is a TAC. Here, you can view the status of every appliance in the cluster and update appliance information, such as, name of the appliance on the cluster, labels, and description. You can also configure the communication methods that describe how the appliance communicates with other appliances in a cluster.

For more information about managing a node, refer to *CLI Manager* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

Chapter 9

Working with Backup and Restore

An essential component for any system, the backup and restore is a process that helps retain vital information. In this process multiple copies of the original data are periodically archived in a separate location. The original data is recovered in an event of data corruption, loss, human error, disaster, or security attack. Thus, organizations can recover their earlier operations in case of a temporary glitch to the system.

In the Protegrity Appliances, the Backup and Recovery process provides a medium to archive system data and configurations. You can back up and restore configurations from the Backup & Restore tab. It is recommended to back up of all system and OS configurations. The Backup/Restore page includes the **Export**, **Import**, **OS Full**, and **Log Files** tabs.

The following table describes the different appliance-related configurations that you can export or import from another appliance.

Table 9-1: Appliance Components for Backup and Restore

Configuration	Description
Appliance Configuration	Export OS configurations, such as, network settings, passwords, Web settings, SSH settings, appliance certificates, firewall settings, JWT settings, SSO configuration settings, NTP settings, FIM policies, and OS Services status. **Note:** In the appliance configuration, the certificates component is classified as follows: • **Certificates** that include Consul-related certificates, Audit Store certificates, and certificates of Protegrity products installed on the appliance. • **Management and Web Service Certificates** that are used by the Management and Web Services engine for authenticating client and server.
Directory Server and Settings	Export LDAP server-related settings
Consul Configuration and Data	Export Consul configuration files
Gateway Configuration Files	Export DSG-related configuration files
Cloud Utility AWS	Export AWS Cloudwatch-related configuration files
Backup Policy Management	Backup All Policy-Management configuration files, keys, and certificates **Note:**

Configuration	Description
	Do not use this with Backup Policy-Management Trusted Appliances Cluster.
Backup All Policy-Management for Trusted Appliance Cluster	Backup All Policy-Management configuration files, keys, and certificates for a TAC
Policy Manager for Web UI Settings	Export policy manager settings for the Web UI
DFSFP Export	Export DFS configuration settings

Note:

When you import files or configurations on an appliance from another appliance, different settings such as, firewall, SSH, or OS are imported. During this import, the settings on the target appliance might change. This might cause a product or component on the target appliance to stop functioning. Thus, after an import of the file or settings is completed, ensure that the settings, such as, ports, SSH, and firewall on the target machine are compatible with the latest features and components.

For example, new features, such as, Consul are added to v7.1 MR2. When you import the settings from the previous versions, the settings in v7.1 MR2, such as, firewall or ports are overridden. So, you must ensure that the rules are added for the functioning of the new features.

Note:

When you import files or configurations, ensure that each component is selected individually.

Important:

The Reporting Server and DMS Components are deprecated in the ESA version 8.0.0.0. Ensure that you do not export/import the **Audit Store** and **Reports** components.

9.1 Backing Up Data

In Protegrity appliances, the backup process can be classified into the following categories:

- Backing up appliance configurations
- Backing up the system
- Backing up on Cloud Platforms

9.1.1 Backing Up Configuration and Data

In the appliance, you can create a backup of the ESA-related configuration files and settings. The backup process involves exporting the settings of the appliance to a local file or another appliance. The backup settings is applicable for cloud and on-premise installations. The settings appear based on the components that are installed in your ESA. The backing up of configuration settings and data using any of the following methods:

- Exporting appliance-related files and configuration settings to a local file
- Exporting appliance-related files and configuration settings to an appliance in a cluster
- Exporting customized files

Exporting appliance-related files and configuration settings to a local file

When you back up data on a local file, the settings are contained in a file that is protected with a password. The file is stored in the directory. You can export the settings from the CLI Manager and Web UI.

- On the CLI Manager, navigate to **Administration** > **Backup/Restore** > **Export data/configuations to a local file** to export the settings to a file.
- On the ESA Web UI, navigate to **System** > **Backup & Restore** > **Export** to restore the system.

Exporting appliance-related files and configuration settings to an appliance in a cluster

In case of backing up data on an appliance in a cluster, a wizard is displayed that guides you through export process. In this wizard, you select the target appliance and the settings to be exported. After the settings are configured, a task is created in the **Task Scheduler** screen.

You can export the settings from the CLI Manager and Web UI,

- On the CLI Manager, **Administration** > **Backup/Restore** > **Export data/configuations to remote appliances(s)** to export the settings to a cluster.
- On the Web UI, navigate to **System** > **Backup & Restore** > **Export** to export the settings to a cluster.

Exporting customized files

You can export or import the files that cannot be exported using the cluster export task. These custom set of files include configuration files, library files, directories containing files, and any other files. On the ESA Web UI, navigate to **Settings** > **System** > **Files** to view the *customer.custom* file that contains the list of files that you want to export and import.

9.1.2 Backing Up the System

Backing your operating system is one of the safest approaches against a hardware of software failure. This process involves backing up the OS installation, settings, and system-specific essential data. For on-premise installations of ESA, the **OS Backup** option allows to back up your entire system. It is recommended to perform the full OS back up before any important system changes, such as appliance upgrade or creating a cluster.

You can initiate the backup of the system from the CLI Manager or Web UI as follows:

- On the CLI Manager, navigate to **Administration** > **Backup/Restore Center** > **Backup all to a local backup partition** to backup the system.
- On the ESA Web UI, navigate to **System** > **Backup & Restore** > **OS Full** to backup the system.

The time to complete the backup process depends upon the volume of data and different transactions that are conducted in your appliance. You can view the ESA Dashboard for notifications about the backup initialization and completion.

> **Note:**
> The OS Backup option is not available for appliances that are initialized from cloud platforms, such as, AWS, Azure, or GCP.

It is recommended to perform the full OS back up before performing tasks such as, creating a cluster, joining a cluster, upgrading the appliance, and so on.

9.1.3 Backing Up on Cloud Platforms

A backup on a cloud platform involves backing up your application and services on a remote server. Backing up data on cloud platforms such as, AWS, Azure, or GCP involves creating snapshots that capture the state of a system at a particular point in time. Using these snapshots, you can re-create the entire system in case of any failure. The process of creating snapshots varies from one cloud platform to another.

For more information about backing up in AWS, GCP or Azure, refer to the *Protegrity Appliances Overview Guide 9.1.0.5*.

9.2 Restoring Data

The restore is a process of retrieving backed up data to the original location. In Protegrity appliances, restoring the backed up data is classified as follows: Using the **Import** tab, you can restore the settings that were create a backup of the product configurations files and settings. In an appliance, you perform a backup by exporting the settings. Backing up a file or configuration can be classified as follows:

- Restoring appliance-related configurations
- Restoring OS
- Restoring data on Cloud platforms

9.2.1 Restoring Configurations

In the appliance, you can restore the appliance-related configuration files and settings. The settings that were exported to a file are retrieved by uploading the file in the appliance. You must use this procedure only when a specific component requires to be retrieved. For example, if the **Directory Server and Settings** requires a restore, then only select this component when you import it from the file.

In case of exporting across a cluster or customized files, the settings are automatically applied on the target appliances. Thus, a separate process to restore data is not required.

This procedure must be used only

You can restore the settings from the CLI Manager and the Web UI as follows:

- On the CLI Manager, navigate to **Adminstration** > **Backup/Restore Center** > **Import data configurations from file** to import settings to a file.
- On the ESA Web UI, navigate to **System** > **Backup & Restore** > **Import** to import settings to a file.

> **Note:**
>
> Before importing the configuration files, ensure that the required products are installed in the appliance. For example, if you are importing files related to DSG, ensure that the **Data Security Gateway** product is installed in the appliance

9.2.2 Restoring the System

In the appliance, restoring the OS reinstates the appliance to the state when the backup was initiated. After the restore is completed, the system restarts for the changes to be effective.

You can restore the settings from the CLI Manager and the Web UI as follows:

- On the CLI Manager, navigate to **Administration** > **Backup/Restore Center** > **Restore from backup partition** to restore the system.
- On the ESA Web UI, navigate to **System** > **Backup & Restore** > **OS Full** to restore the OS.

9.2.3 Restoring Data on Cloud Platforms

On Cloud Platforms such as, AWS, Azure, and GCP, the restore process is based on the cloud-native solutions. The snapshots that are created for an instance form the recovery point of restoring data. The process of recovering data from snapshots varies from one cloud platform to another.

9.3 Viewing Export/Import Logs

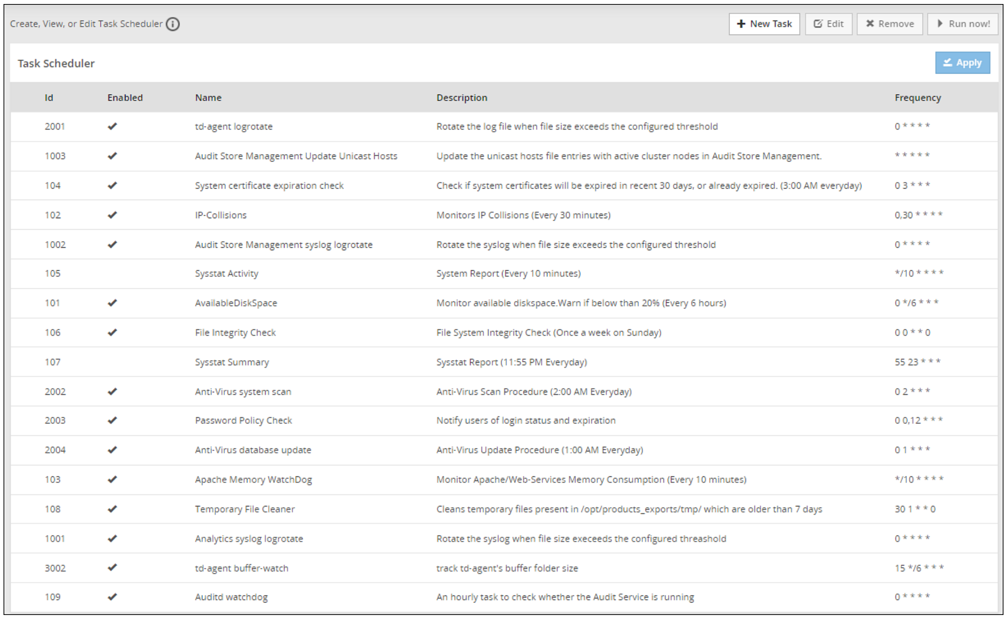
When you export or import files using the CLI Manager, the details of the files are logged. When you export or import files using the Web UI, the operation log is saved automatically. These log files are displayed in **Log Files** tab. You can view, delete, or download the log files.

Chapter 10

Working with Task Scheduler

The Task Scheduler is a option/utility on the Web UI, where scheduled tasks that run at specified intervals in an appliance are created. In a scheduled task, you specify the parameters for the task to be executed. The Task Scheduler monitors the criteria specified and triggers an event criteria is met.

The following figure illustrates the different scheduled tasks that are available when ESA is installed on your system.



Task Scheduler

Id	Enabled	Name	Description	Frequency
2001	✓	td-agent logrotate	Rotate the log file when file size exceeds the configured threshold	0 * * * *
1003	✓	Audit Store Management Update Unicast Hosts	Update the unicast hosts file entries with active cluster nodes in Audit Store Management.	* * * * *
104	✓	System certificate expiration check	Check if system certificates will be expired in recent 30 days, or already expired. (3:00 AM everyday)	0 3 * * *
102	✓	IP-Collisions	Monitors IP Collisions (Every 30 minutes)	0,30 * * * *
1002	✓	Audit Store Management syslog logrotate	Rotate the syslog when file size exceeds the configured threshold	0 * * * *
105		Sysstat Activity	System Report (Every 10 minutes)	*/10 * * * *
101	✓	AvailableDiskSpace	Monitor available diskspace.Warn if below than 20% (Every 6 hours)	0 */6 * * *
106	✓	File Integrity Check	File System Integrity Check (Once a week on Sunday)	0 0 * * 0
107		Sysstat Summary	Sysstat Report (11:55 PM Everyday)	55 23 * * *
2002	✓	Anti-Virus system scan	Anti-Virus Scan Procedure (2:00 AM Everyday)	0 2 * * *
2003	✓	Password Policy Check	Notify users of login status and expiration	0 0,12 * * *
2004	✓	Anti-Virus database update	Anti-Virus Update Procedure (1:00 AM Everyday)	0 1 * * *
103	✓	Apache Memory WatchDog	Monitor Apache/Web-Services Memory Consumption (Every 10 minutes)	*/10 * * * *
108	✓	Temporary File Cleaner	Cleans temporary files present in /opt/products_exports/tmp/ which are older than 7 days	30 1 * * 0
1001	✓	Analytics syslog logrotate	Rotate the syslog when file size execeeds the configured threashold	0 * * * *
3002	✓	td-agent buffer-watch	track td-agent's buffer folder size	15 */6 * * *
109	✓	Auditd watchdog	An hourly task to check whether the Audit Service is running	0 * * * *

Figure 10-1: Scheduler page

The following table describes the different actions that you can perform for a scheduled task.

Table 10-1: Actions on Task Scheduler

Pointer	Description
1	Create a scheduled task
2	Edit a scheduled task
3	Delete a scheduled task
4	Run the scheduled task
5	Apply the changes performed to a scheduled task

Pointer	Description
6	Internal Id assigned to a scheduled task
7	Status of the scheduled task, enabled or disabled

A scheduled task in an appliance contains the following sections as described in the table.

Table 10-2: Scheduled Tasks Options

Sections	Description
Basic Properties	Details about the scheduler task, such as, name, description, and type of task (cluster task or a scheduled task)
Frequency	Frequency of executing the scheduled task
Command	Command that the scheduled task must run
Restrictions	Specify whether task should run on the primary site or secondary sites in a cluster

10.1 Creating a Scheduled Task

Consider a task that you want to create a task to run the Antivirus scan every hour on a daily basis. You can create the task by performing the following steps.

Before you begin
Ensure that the the permissions for the scheduled task is added to the AppArmor profiles. For more information about creating a profile, refer to *Creating a profile* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

➤ To create a scheduled task:

1. On the ESA Web UI, navigate to **System** > **Task Scheduler**.
2. Click **New Task**.
   The **New Task** screen appears.
3. Enter the required information in the **Basic Properties** such as, **Name** and **Description**.
4. In the **Frequency** drop-down list, enter **Every hour**.
5. In the Command section, enter the following command.

```
/etc/opt/AntiVirus/AntiVirus --scan --user admin
```

6. In the **Logging** section, select Log Server.
   a. Choose Critical Severity in the Success Severity drop-down list.
   b. Choose High Severity in the Fail Severity drop-down list.
7. Click **Save**.
   A new scheduled task is created.
8. Click **Apply** to apply the modifications to the task.
   A dialog box to enter the root user password appears.
9. Enter the root password and click **OK**.

   The scheduled task to run an Antivirus scan every hour is now operational.

10.2 Creating a Cluster Scheduled Task

Consider a task that you want to create a task to run the Antivirus scan every hour on a daily basis. You can create the task by performing the following steps.

Before you begin
Ensure that the the permissions for the scheduled task is added to the AppArmor profiles. For more information about creating a profile, refer to *Creating a profile* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

➤ To create a scheduled task:

1. On the ESA Web UI, navigate to **System** > **Task Scheduler**.
2. Click **New Task**.
   The **New Task** screen appears.
3. Enter the required information in the **Basic Properties** such as, **Name** and **Description**.
4. Select **Cluster task**.
5. In the **Frequency** drop-down list, enter **Every hour**.
6. In the Command section, enter the following command.

   ```
   /etc/opt/AntiVirus/AntiVirus --scan --user admin
   ```
7. In the **Logging** section, select Log Server.
   a. Choose Critical Severity in the Success Severity drop-down list.
   b. Choose High Severity in the Fail Severity drop-down list.
8. Click **Save**.
   A new scheduled task is created.
9. Click **Apply** to apply the modifications to the task.
   A dialog box to enter the root user password appears.
10. Enter the root password and click **OK**.

    The scheduled task to run an Antivirus scan every hour is now operational.

10.3 Disabling a Cluster Scheduled Task

Perform the following steps to disable a cluster schedule task.

➤ To disable a scheduled task:

1. On the ESA Web UI, navigate to **System** > **Task Scheduler**.
2. Select the cluster scheduler task which you want to disable.
3. Select **Edit**.
4. Disable the **Cluster task** check box.
5. Click **Save**.
6. Click **Apply** to apply the modifications to the task.
   A dialog box to enter the root user password appears.
7. Enter the root password and click **OK**.

Chapter 11

Managing Users

You require users in every system to run the business application. The foremost step in any system involves setting up users that operate on different faces of the application.

In ESA, setting up a user involves operations such, as assigning roles, setting up password policies, setting up Active Directories (ADs) and so on. This section describes the various activities that constitute the user management for ESA. In ESA, you can add the following users:

- **OS Users**: Users for for managing and debugging OS related operations.
- **Appliance users**: User for performing various operations based on the roles assigned to them. Created or imported from other directory services too.

11.1 Understanding ESA Users

In any given environment, users are entities that consume services provided by a system. Only authorized users can access the system. In the Protegrity appliances, users are created to manage ESA for various purposes. These users are system users and LDAP administrative users.

On ESA, the users navigate to **Settings** > **Users** > **User Management** to view the list of the users that are available in the appliance.

In ESA, users can be categorized as follows:

Internal Appliance Users

These are users created by default when the ESA is installed. These users are used to perform various operations on the Web UI, such as managing cluster, managing LDAP, and so on. On ESA Web UI, navigate to **Settings** > **Users** > **User Management** to view the list of the users that are available in the appliance.

The following is the list of users that are created when ESA is installed.

User Name	Description	Role
admin	Administrator account with access to the Web UI and CLI Manager options.	Security Administrator
viewer	User with view only access to the Web UI and CLI Manager options.	Security Administrator Viewer

User Name	Description	Role
ldap_bind_user	Created when local LDAP is installed	N/A
samba_admin_user	Access folders shared by CIFS service running on File Protector Vault.	N/A
PolicyUser	Perform security operations on the protector node.	Policy User
ProxyUser	Perform security operations on behalf of other policy users.	ProxyUser

OS users

These users that contain access to all the CLI operations in the appliance. You can create local OS users from the CLI Manager. On CLI Manager, navigate to **Administration** > **Accounts and Passwords** > **Manage Passwords and Local Accounts** to view and manage the OS users in the appliance. For more information about managing users, refer to *Managing Accounts and Passwords* in the *Protegrity Appliances Overview Guide 9.1.0.5*

The following is the list of OS users in the appliance.

Table 11-1: OS Users in the Appliance

OS Users	Description
alliance	Handles DSG processes
root	Super user with access to all commands and files
local_admin	Local administrator that can be used when an LDAP user is not accessible
www-data	Daemon that runs the Apache, Service dispatcher, and Web services as a user
ptycluster	Handles TAC related services and communication between TAC through SSH.
service_admin and *service_viewer*	Internal service accounts used for components that do not support LDAP
clamav	Handles ClamAV antivirus
rabbitmq	Handles the RabbitMQ messaging queues
epmd	Daemon that tracks the listening address of a node
openldap	Handles the openLDAP utility
dpsdbuser	Internal repository user for managing policies

Policy Users

These users are imported from a file or an external source for managing policy operations on ESA. Policy users are used by protectors that communicate with ESA for performing security operations. For more information about policy users, refer the *Protegrity Policy Management Guide 9.1.0.5*.

External Appliance users

These are external users that are added to the appliance for performing various operations on the Web UI. The LDAP users are imported by using the External Groups or Importing Users.You can also add new users to the appliances from the **User Management** screen.

> **Note:**
>
> Ensure that the **Proxy Authentication Settings** are configured before importing the users.

11.2 Working with Roles

Roles are a set of permission that allow or restrict user to use certain features in a system. In ESA, the roles are a collection of privileges that assigned to a user.

Users in the appliance must be attached to one role or multiple roles. The capabilities of a role are defined by the permissions attached to the role. Though roles can be created, modified, or deleted from the appliance, permissions cannot be edited. On the ESA Web UI, navigate to **Settings** > **Users** > **Roles** to view the list of the that are available in the appliance.

The default roles packaged with ESA are as described in the following table.

Roles	Description	Permissions
Policy Proxy User	Allows a user to connect to DSG via SOAP/REST and access web services using Application Protector (AP)	Proxy-User
Policy User	Allows user to connect to DSG via SOAP/ REST and perform security operations using Application Protector (AP)	Policy-User
Security Administrator Viewer	Role that can view the ESA Web UI, CLI, and reports.	Security Viewer, Appliance CLI Viewer, Appliance web viewer, Reports Viewer
Shell Accounts	Role who has direct SSH access to Appliance OS shell **Note**: It is recommended that careful consideration is taken when assigning the Shell Accounts role and permission to a user. Ensure that if a user is assigned to the Shell Account role, no other role is linked to the same user. The user has no access to the Web UI or CLI, except when the user has password policy enabled and is required to change password through Web UI.	Shell (non-CLI) Access **Note**: The user can access SSH directly if the permission is tied to this role.
Security Administrator	Role who is responsible for setting up data security using ESA policy management, which includes but is not limited to creating policy, managing policy, and deploying policy.	Security Officer, Reports Manager, Appliance web manager, Appliance CLI Administrator, Export Certificates, DPS Admin, Directory Manager, Export Keys, RLP Manager

The following table describes the different permissions that are available in ESA.

Table 11-2: Roles Description

Permission	Description
AWS Admin	Allows user to access the services of AWS Cloud Utility
Appliance CLI Administrator	Allows user to perform all operations available as part of ESA CLI Manager
Appliance CLI Viewer	Allows user to view certain options on ESA CLI Manager
Appliance web manager	Allows user to perform all operations available as part of the ESA Web UI
Appliance web viewer	Allows user to only view certain screens on the ESA Web UI.
Audit Store Admin	Allows user to perform operations on Audit Store Management
Can Create JWT Token	Allows user to create a Java Web Token (JWT) for user authentication
DPS Admin	Responsible for running the DPS admin tool on the protectors
Directory Manager	Allows to manage external directory configuration
Export Certificates	Allows user to use download certificates from ESA
Export Keys	Allows user to export keys from ESA
Insight Admin	Allows to perform operations on Discover Web UI
Key Manager	Allows user to access the Key Management Web UI, rotate ERK or DSK, and modify ERK states

Permission	Description
Policy-User	Allows user to connect to Data Security Gateway (DSG) via REST and perform security operations using Application Protector (AP).
Proxy-User	Allows user to connect to DSG via REST and perform security operations using Application Protector (AP)
RLP Manager	Allows user to manage rules stored on Row-Level Security Administrator (ROLESA)
SSO Login	Allows user to login to the system using the Single Sign-On (SSO) mechanism
Security Officer	Allows user to manage policies and keys, perform functions related to policy and key management.
Security Viewer	Allows user to view the policy management issues
Shell (non-CLI) Access	Allows user to get direct access to the Appliance OS shell via SSH. It is recommended that careful consideration is taken when assigning the Shell Accounts role and permission to a user. Ensure that if a user is assigned to the Shell Account role, no other role is linked to the same user.
Deny Concurrent Login	Denies from logging in or accessing ESA simultaneously using multiple Web sessions. You can access ESA only from a single Web session.

11.3 Password Policy Configuration

Password policies ensure that a user enters strong passwords for logging into the system. These policies define a set of rules, such that a password set by a user cannot be easily compromised by attackers. Password policies often form a part of an organizations regulation to secure its system. In ESA, password policies are defined and can be configured by a user with administrative privileges.

11.3.1 Strengthening Password Policy

Passwords are a common way of maintaining a security of a user account. The strength and complexity of a password are some of the primary requirements of an enterprise to prevent security vulnerability. A weak password increases chances of a security breach. Thus, to ensure a strong password, different password policies are set to enhance the security of an account.

The password policies are rules that enforce validation checks to provide a strong password. You can set your password policy based on the enterprise ordinance. Some requirements of a strong password policy might include use of numerals, characters, special characters, password length, and so on.

The default requirements of a strong password policy for an appliance OS user are as follows.

- The password must have at least 8 characters.
- All the printable ASCII characters are allowed.
- The password must contain at least one character each from any of the two groups from the following.
  - Numeric: Includes numbers from 0-9.
  - Alphabets: Includes capitals [A-Z] and small [a-z] alphabets.
  - Special characters: Includes ! # $ % & ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

You can enforce password policy rules for the LDAP and OS users by editing the check_password.py file. This file contains a Python function that validates a user password. The check_password.py file is run before you set a password for a user. The password for the user is applied only after it is validated using this Python function.

For more information about password policy for LDAP users, refer to section *Password Policy for the LDAP Users*.

11.3.2 Password Policy for the LDAP Users

The password policy applies to all LDAP users.

The LDAP user password should:

1. Be at least 8 characters long
2. Contain at least two of the following three character groups:
    - Numeric [0-9]
    - Alphabetic [a-z, A-Z]
    - Special symbols, such as: ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ? ` - = [ ] \ ; ' , . /

Thus, your password should look like one of the following examples:

- Protegrity123 (alphabetic and numeric)
- Protegrity!@#$ (alphabetic and special symbols)
- 123!@#$ (numeric and special symbols)

> **Note:** In the z/OS Protector, supporting various special symbols in the password, depends on the codepage selected on the protector. The recommended codepage is 1047.

The strength of the password is validated by default. This strength validation can also be customized by creating a script file to meet the requirements of your organization.

From the CLI, press **Administration** > **Accounts and Passwords** > **Manage Passwords and Local-Accounts**. Select the correct Change option and update the password.

You can enforce organization rules for password validity from the Web UI, from **Settings** > **Users** > **User Management**, where the following can be configured:

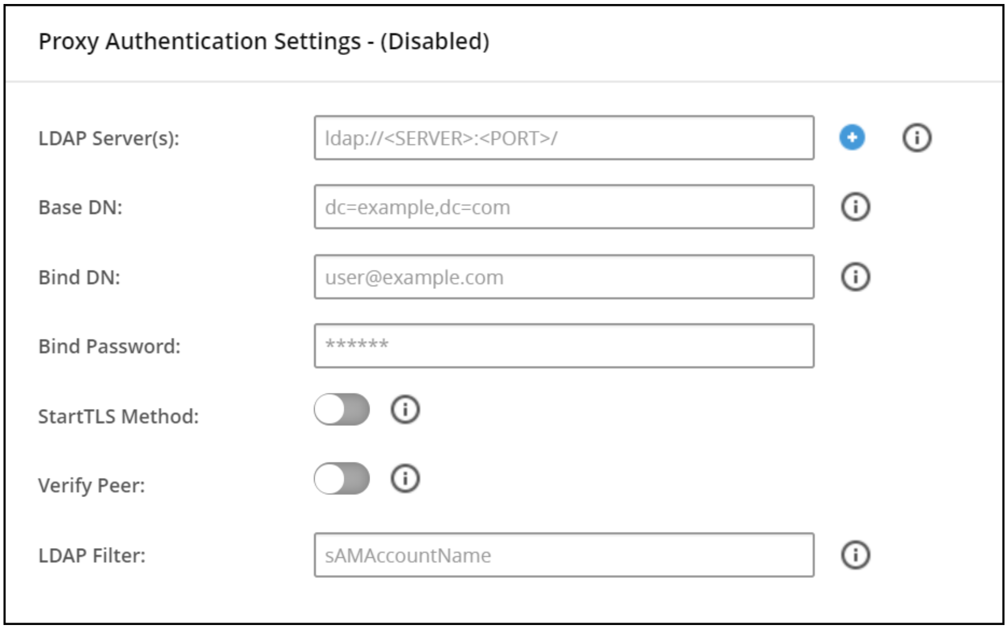
- Minimum period for changeover
- Password expiry
- Lock on maximum failures
- Password history

For more information about configuring the password policy, refer to section *Password Policy Configuration*.

11.4 Working with Proxy Authentication

Proxy Authentication enables ESA to separate authentication and authorization of users. The implementation is such that when users are imported, a user with the same name is recreated in the internal LDAP. When the user accesses the data security platform, ESA authorizes the user and communicates with the external LDAP for authenticating the user. This implementation ensures that organizations are not forced to modify their LDAP configuration to accommodate the data security platform. Proxy authentication can be configured from the CLI Manager and Web UI.

The following screen displays the Proxy Authentication screen on the ESA Web UI.



Proxy Authentication Settings - (Disabled)

LDAP Server(s): ldap://<SERVER>:<PORT>/

Base DN: dc=example,dc=com

Bind DN: user@example.com

Bind Password: ******

StartTLS Method:

Verify Peer:

LDAP Filter: sAMAccountName

Figure 11-1: Proxy Authentication

In this screen, the Base DN, Bind DN, Bind Password, and LDAP Filter text boxes contain the information about the external directory server that you are connecting to. The parameters are described as follows.

LDAP Server

The IP address or hostname of the AD server preceded by *ldap* or *ldaps*

For example, *ldap://192.1.10.256:389* or *ldaps://192.1.10.256:389*

It is recommended to use LDAP over SSL, *ldaps*, to establish a secure LDAP communication over TLS between ESA and the external directory server.

> **Note:**
> A secure communication is established by the exchange of certificates.

Base DN

The Base Distinguished name of the external directory server. For example, *dc=sherwood,dc=com*.

Bind DN

Distinguished name of the Bind User. For example, *bdnuser@protegrity.com*. It is recommended that this user is granted viewer permissions.

Bind Password

The password of the specified Bind User.

StartTLS Method

Enable this setting for a secure TLS communication between ESA and the external directory server. If the IP address of the external directory server is preceded by *ldaps*, it is not required to enable this setting.

Verify Peer

Enable this setting to validate the external directory server communicating with ESA. If **Verify Peer** is enabled, ensure that CA certificate to validate the server certificate of the external directory server is uploaded on the **Certificate Management** screen.

For more information about uploading certificates, refer to the *Protegrity Certificate Management Guide 9.1.0.5*.

LDAP Filter

Provide the attribute to be used for filtering users in the external LDAP. For example, you can use the default attribute, *sAMAccountName*, to authenticate users in a single AD.

It is recommended to enable the **Verify Peer** setting and the **StartTLS** method, to establish a secure communication between ESA and the external directory server.

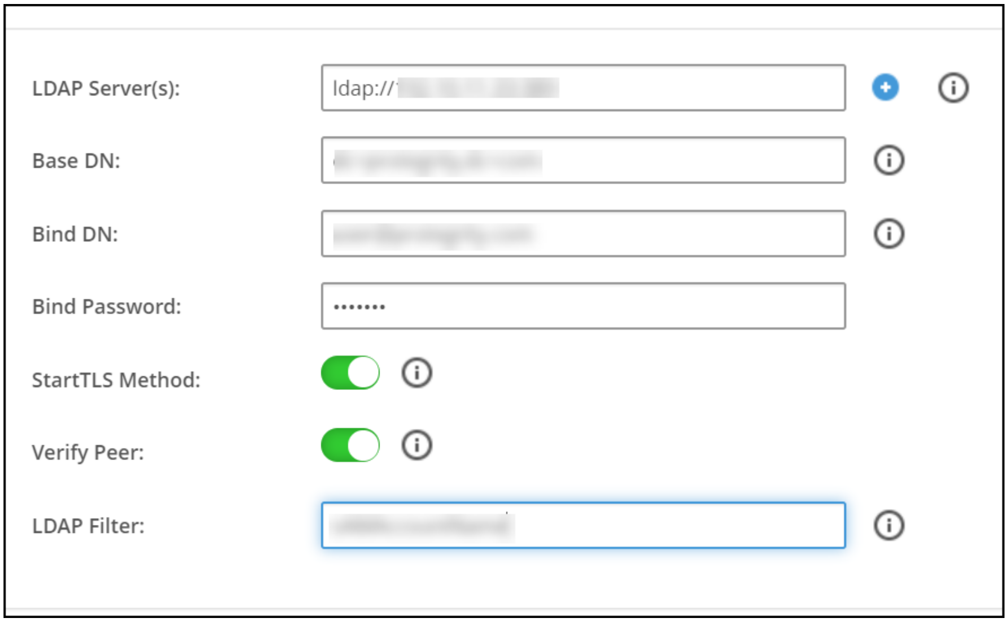
While setting the Proxy Authentication, the LDAP Server text box must be configured based on the **Verify Peer** and the **StartTLS** setting. The following table describes the ports and server address that you must enter while the **Verify Peer** and **StartTLS** settings are enabled or disabled.

Table 11-3: Proxy Authentication

StartTLS	Verify Peer	LDAP Server	Example
Enabled	Enabled	• Specify the hostname of the external directory server • Port number can either be *389* or *636*	The external directory server is set as, *ldap://ADServer-01:389* or *ldap://ADServer-01:636*
Enabled	Disabled	• Specify the hostname or IP address of the external directory server • Port number can either be *389* or *636*	The external directory server can be set as, *ldap://ADServer-01:389* or *ldap://192.115.100.10:636*
Disabled	Enabled	• Specify the hostname of the external directory server • Only *389* must be specified as port number	The external directory server is set as, *ldaps://ADServer-01:389*
Disabled	Disabled	• Specify the hostname or IP address the external directory server • Only *389* must be specified as port number	The external directory server is set as, *ldaps://ADServer-01:389* or *ldaps://192.115.100.10:389*

> **Note:**
> Ensure that External Directory server and ESA machine are configured with the same DHCP configuration.

The following figure shows a recommended configuration for the **Proxy Authentication Settings**.



LDAP Server(s): ldap://[redacted]

Base DN: [redacted]

Bind DN: [redacted]

Bind Password: •••••••

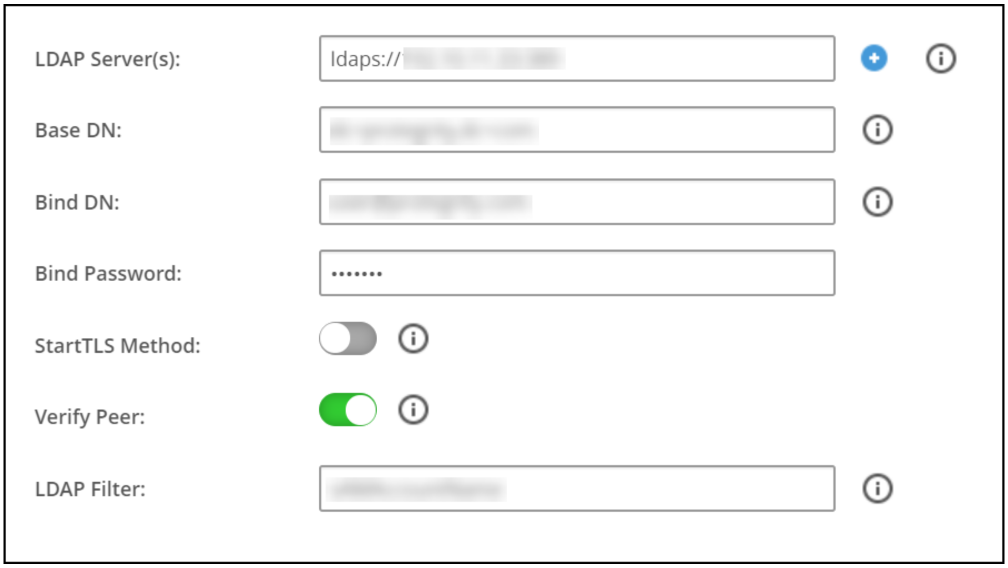
StartTLS Method: ●

Verify Peer: ●

LDAP Filter: [redacted]

Figure 11-2: Proxy Authentication Settings

or



LDAP Server(s): ldaps://[redacted]

Base DN: [redacted]

Bind DN: [redacted]

Bind Password: •••••••

StartTLS Method: ○

Verify Peer: ●

LDAP Filter: [redacted]

Figure 11-3: Proxy Authentication Settings

In appliances, the external directory servers such as, Active Directory (AD) or Oracle Directory Server Enterprise Edition (ODSEE) use the OpenLDAP protocol to authenticate users. The following sections illustrate a sample AD and ODSEE configurations.

11.4.1 Sample AD configuration

The following example describes the parameters for setting up an AD connection.

LDAP Uri: `ldap://192.257.50.10:389`

Base DN: `dc=sherwood,dc=com`

Bind DN: `administrator@sherwood.com`

Bind Password: <Password for the Bind User>

StartTLS Method: *Yes*

Verify Peer: *Yes*

LDAP Filter: `sAMAccountName`

> **Note:**
> In case of same usernames across multiple ADs, it is recommended to use LDAP Filter such as *UserPrincipalName* to authenticate users.

11.4.2 Sample ODSEE configuration

The following example describes the parameters for setting up an ODSEE connection.

> **Note:**
> Protegrity appliances support ODSEE v11.1.1.7.0.

LDAP Uri: `ldap://192.257.50.10:389`

Base DN: `dc=sherwood,dc=com`

Bind DN: `cn=Directory Manager` or `cn=admin,cn=Administrators,cn=config`

Bind Password: <Password for the Bind User>

StartTLS Method: Yes

Verify Peer: Yes

LDAP Filter: User attributes such as, `uid`, `cn`, `sn,` and so on.

11.4.3 Sample SAML Configuration

The following example describes the parameters for setting up a SAML connection.

SAML Single Sign-On:

Enable: *Yes*

Access User Management Screen: *No*

Service Provider(SP) Settings:

FQDN: `appliancefqdn.com`

Entity ID: *`e595ce43-c50a-4fd2-a3ef-5a4d93a602ae`*

Identity Provider(IdP) Settings:

Metadata Settings: *Metadata URL*

SAML Sample URL: *`https://login.microsoftonline.com/4b1c35a8-5a82-4cb4-9b03-7b818fa58cfc/federationmetadata/2007-06/federationmetadata.xml?appid=e595ce43-c50a-4fd2-a3ef-5a4d93a602ae`*

Sample SAML File: *`FQDN_EntityID_Metadata_user_credentials 1.csv`*

Sample Content of the SAML File:

11.4.4 Sample Kerberos Configuration

The following example describes the parameters for setting up a Kerberos connection.

Kerberos for Single Sign-On using (Spnego):

Enable: *Yes*

Service Principal Name: *`HTTP/<username>.esatestad.com@ESATESTAD.COM`*

Sample Keytab File: *`<username> 1.keytab`*

11.4.5 Sample Azure AD Configuration

The following example describes the parameters for setting up an Azure AD connection.

Azure AD Settings - (Enabled):

Tenant ID: *`3d45143b-6c92-446a-814b-ead9ab5c5e0b`*

Client ID: *`a1204385-00eb-44d4-b352-e4db25a55c52`*

Auth Type: *`Secret`*

Client Secret: *`xxxx`*

11.5 Working with External Groups

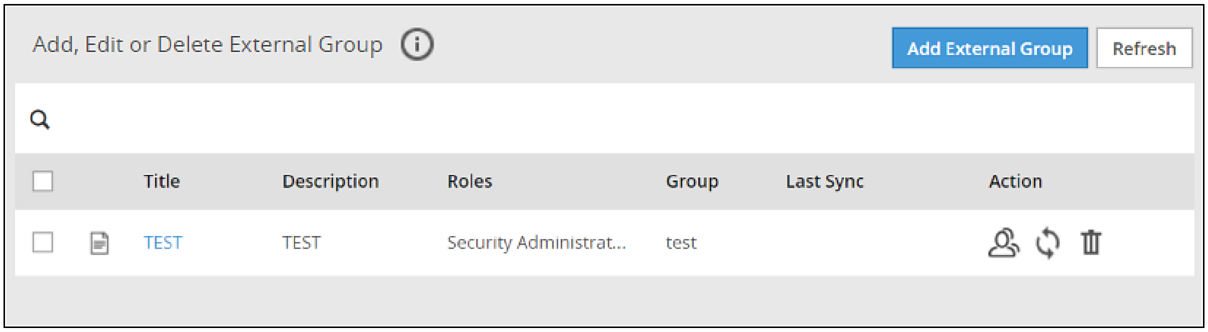
The directory service providers, such as, Active Directory (AD) or Oracle Directory Server Enterprise Edition (ODSEE), are an identity management systems that contain information about the enterprise users. You can map the users in the directory service providers to the various roles defined in the Appliances. The External Groups feature enables you to associate users or groups to the roles.

You can import users from a directory service to assign roles for performing various security and administrative operations in the appliances. Using External Groups, you connect to an external source, import the required users or groups, and assign the Appliance-specific roles to them. The appliances automatically synchronize with the directory service provider at regular time intervals to update user information. If any user or group in source directory service is updated, it is reflected across the users in the external groups. The updates made to the local LDAP do not affect the source directory service provider.

If any changes occur to the roles or users in the external groups, an audit event is triggered.

> **Note:** Ensure that **Proxy Authentication** is enabled to use an external group.

The following screen displays the **External Groups** screen.



□		Title	Description	Roles	Group	Last Sync	Action
□		TEST	TEST	Security Administrat...	test		👤 🔄 🗑

Figure 11-4: External Groups Screen

> **Note:** Only users with **Directory Manager** role can configure the **External Groups** screen.

The following table describes the actions you can perform on the **External Groups** screen.

Table 11-4: External Groups Icons

Icon	Description
👤	List the users present for the external group
🔄	Synchronize with the external group to update the users
🗑	Delete the external group

The following describes the fields required for creating an External Group.

Title

Name designated to the External Group

Description

Additional text describing the External Group

Group DN

Distinguished name where groups can be found in the directory

Query by

To pull users from the directory server to the appliance, you must query the directory server using required parameters. This can be achieved using one of the following two methods:

Query By User

Query by User allows to add specific set of users from a directory server.

Group Properties

In the Group Properties, the search is based on the values entered in the **Group DN** and **Member Attribute Name** text boxes. Consider an example, where the values in the **Group DN** and **Member Attribute Name** are *cn=esa,ou=groups,dc=sherwood,dc=com* and *memberOf* respectively. In this case, the search is performed on every user that is available in the directory server. The *memberOf* value of the users are matched with the specified **Group DN**. Only those users whose *memberOf* value matches the **Group DN** values are returned.

Search Filter

This field facilitates to search multiple users using regex patterns. Consider an example, where the values in the **Search Filter** for the user is *cn=S**. In this case all the users beginning with *cn=S* in the directory server are retrieved.

Query By Group

Using this method, you can search and add users of a group in the directory server. All the users belonging to the group are retrieved in the search process.

Group Properties

In the **Group Properties**, the search is based on the values entered in the **Group DN** and **Member Attribute Name** text boxes. Consider an example, where the values in the **Group DN** and **Member Attribute Name** are *cn=hr,ou=groups,dc=sherwood,dc=com* and *member* respectively. The search is performed in the directory server for the group mentioned in the Group DN text box.
If the group is available, then all the users of that group containing value of *member* attribute as *cn=hr,ou=groups,dc=sherwood,dc=com* are retrieved.

Search Filter

This field facilitates to search multiple groups across the directory server. The users are retrieved based on the values provided in the **Search Filter** and **Member Attribute Name** text boxes. A search is performed on the group mentioned in **Search Filter** and the value mentioned in the **Member Attribute Name** attribute of the group is fetched. Consider an example, where the values in the **Search Filter** for the group is *cn=accounts* and the value in the **Member Attribute Name** value is *member*. All the groups that match with *cn=accounts* are searched. The value that is available in the *member* attribute of those groups are retrieved as the search result.

11.6 Working with Azure AD

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. It allows access to external (Azure portal) and internal resources (corporate appliances). Azure AD manages your cloud and on-premise applications and protects user identities and credentials.

When you subscribe to Azure AD, it automatically creates an Azure AD tenant. After the Azure AD tenant is created, register your application in the **App Registrations** module. This acts like an end-point for the appliance to connect to the tenant.

Using the Azure AD configuration tool, you can:

- Enable the Azure AD Authentication and manage user access to the appliance.
- Import the required users or groups to the appliance, and assign specific roles to them.

11.6.1 Configuring the Azure AD Settings

You can configure the Azure AD settings from the Web UI. Using the Web UI, you can enable the Azure AD settings to manage user access to cloud applications, import users or groups, and assign specific roles to them.

Before you begin

Before configuring Azure AD Settings on the appliance, you must have the following information that is required to connect the appliance with the Azure AD:

- Tenant ID

- Client ID
- Client Secret or Thumbprint

> **Note:** For more information about the Tenant ID, Client ID, Authentication Type, and Client Secret/Thumbprint, search for the text *Register an app with Azure Active Directory* on Microsoft's Technical Documentation site at:
>
> *https://learn.microsoft.com/en-us/docs/*

The following are the list of the **API permissions** that must be granted and associated with the listed **Type**.

API/Permission Name	Type
Group.Read.All	Application
GroupMember.Read.All	Application
User.Read	Delegated
User.Read.All	Application
User.ReadBasic.All	Delegated

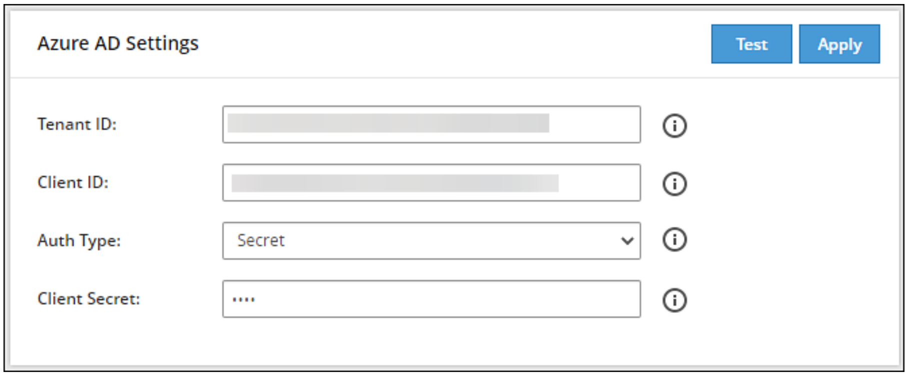
> **Note:** For more information about configuring the application permissions in the Azure AD, please refer *https://learn.microsoft.com/en-us/graph/auth-v2-service?tabs=http*

> **Note:** Ensure that the **Allow public client flows** setting is *Enabled*. To enable the **Allow public client flows** setting, navigate to **Authentication** > **Advanced settings**, click the toggle button, and select **Yes**.

To configure Azure AD settings:

1. On the Web UI, navigate to **Settings** > **Users** > **Azure AD**.

   The following figure shows an example of Azure AD configuration.



Tenant ID: [redacted]

Client ID: [redacted]

Auth Type: Secret

Client Secret: ····

Figure 11-5: Azure AD configuration

2. Enter the data in the fields as shown in the following table:

Table 11-5: Azure AD Settings

Setting	Description
Tenant ID	Unique identifier of the Azure AD instance

Setting	Description
Client ID	Unique identifier of an application created in Azure AD
Auth Type	Select one of the Auth Type: • *SECRET* indicates a password-based authentication. In this authentication type, the secrets are symmetric keys, which the client and the server must know. • *CERT* indicates a certificate-based authentication. In this authentication type, the certificates are the private keys, which the client uses. The server validates this certificate using the public key **Note:** If you use the Elliptic Curve Cryptographic (ECC) certificate to configure the Azure AD settings, then the authentication will fail. This is a limitation. Therefore, it is recommended to use the client secret authentication.
Client Secret/ Thumbprint	The client secret/thumbprint is the password of the Azure AD application. • If the Auth Type selected is **SECRET**, then enter **Client Secret**. • If the Auth type selected is **CERT**, then enter Client **Thumbprint**.

> **Note:** For more information about the Tenant ID, Client ID, Authentication Type, and Client Secret/Thumbprint, search for the text *Register an app with Azure Active Directory* on Microsoft's Technical Documentation site at:
>
> *https://learn.microsoft.com/en-us/docs/*

3. Click **Test** to test the provided configuration.
   The Azure AD settings are authenticated successfully. To save the changes, click 'Apply' message appears.
4. Click **Apply** to apply and save the configuration settings.
   The Azure AD settings are saved successfully message appears.

Chapter 12

Working with Keys

The Protegrity Data Security platform uses many keys to protect your sensitive data. The Protegrity Key Management solution manages these keys and this system is embedded into the fabric of the Protegrity Data Security Platform. For example, the creation of a cryptographic or data protection key is a part of the process of how you define the way sensitive data is to be protected. There is not a specific user visible function to create a data protection key.

With key management as a part of the platform's core infrastructure, the security team can focus on protecting data and not the low-level mechanics of key management. This platform infrastructure-based key management technique eliminates the need for any human to be a custodian of keys. This holds true for any of the functions included in key management.

The keys that are part of the Protegrity Key Management solution are:

- **Key Encryption Key (KEK):** The cryptographic key used to protect other keys. The KEKs are categorized as follows:
  - **Master Key -** It protects the Data Store Keys and Repository Key. In the ESA, only one active Master Key is present at a time.
  - **Repository Key** - It protects policy information in the ESA. In the ESA, only one active Repository Key is present at a time.
  - **Data Store Key -** It encrypts the audit logs on the protection endpoint. In the ESA, multiple active Data Store Keys can be present at a time. This key applies only to v8.0.0.0 and earlier protector versions.
- **Signing Key**: The protector utilizes the Signing Key to sign the audit logs for each data protection operation. The signed audit log records are then sent to the ESA, which authenticates and displays the signature details received for the log records.

  For more information about the signature details for the log records, refer to the *Protegrity Log Forwarding Guide 9.1.0.5*.
- **Data Encryption Key (DEK):** The cryptographic key used to encrypt the sensitive data for the customers.
- **Codebooks:** The lookup tables used to tokenize the sensitive data.

For more information about managing keys, refer to the *Protegrity Key Management Guide 9.1.0.5*.

Chapter 13

Working with Certificates

Digital certificates are used to encrypt online communication and authentication between two entities. For two entities exchanging sensitive information, the one that initiates the request for exchange can be called the client and the one that receives the request and constitutes the other entity can be called the server.

The authentication of both the client and the server involves the use of digital certificates issued by the trusted Certificate Authorities(CAs). The client authenticates itself to a server using its client certificate. Similarly, the server also authenticates itself to the client using the server certificate. Thus, certificate-based communication and authentication involves a client certificate, server certificate, and a certifying authority that authenticates the client and server certificates.

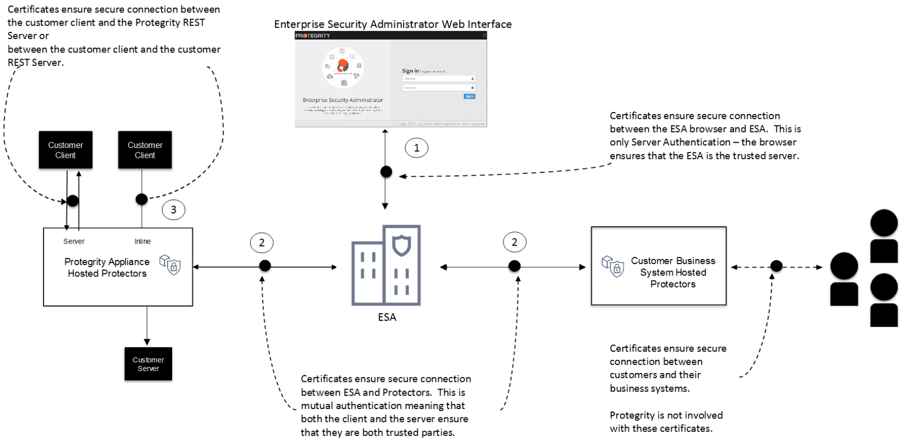
Protegrity client and server certificates are self-signed by Protegrity. However, you can replace them by certificates signed by a trusted and commercial CA. These certificates are used for communication between various components in ESA.

The certificate support in Protegrity involves the following:

- ESA supports the upload of certificates with strength equal to 4096 bits. You can upload a certificate with strength less than 4096 bits but the system will show you a warning message.
- The ability to replace the self-signed Protegrity certificates with the CA based certificates.
- The retrieval of username from client certificates for authentication of user information during policy enforcement.
- The ability to download the server’s CA certificate and upload it to a certificate trust store to trust the server certificate for communication with ESA.

The various components within the Protegrity Data Security Platform that communicate with and authenticate each other through digital certificates are:

- ESA Web UI and ESA
- ESA and Protectors
- Protegrity Appliances and external REST clients


Certificates ensure secure connection between the customer client and the Protegrity REST Server or between the customer client and the customer REST Server.

Certificates ensure secure connection between the ESA browser and ESA. This is only Server Authentication – the browser ensures that the ESA is the trusted server.

Certificates ensure secure connection between ESA and Protectors. This is mutual authentication meaning that both the client and the server ensure that they are both trusted parties.

Certificates ensure secure connection between customers and their business systems.

Protegrity is not involved with these certificates.

Enterprise Security Administrator Web Interface
PROTEGRITY
Enterprise Security Administrator
Sign in
Customer Client
Customer Client
Server
Inline
Protegrity Appliance Hosted Protectors
Customer Server
1
2
2
3
ESA
Customer Business System Hosted Protectors

Figure 13-1: Using Certificates with Protegrity

As illustrated in the figure, the use of certificates within the Protegrity systems involves the following:

1. Communication between ESA Web UI and ESA

   In case of a communication between the ESA Web UI and ESA, ESA provides its server certificate to the browser. In this case, it is only server authentication that takes place in which the browser ensures that ESA is the trusted server.

2. Communication between ESA and Protectors

   In case of a communication between ESA and Protectors, certificates are used to mutually authenticate both the entities. The server and the client i.e. ESA and the Protector respectively ensure that both are trusted entities. The Protectors could be hosted on customer business systems or it could be a Protegrity Appliance.

3. Communication between Protegrity Appliances and external REST clients

   Certificates ensure the secure communication between the customer client and Protegrity REST server or between the customer client and the customer REST server.

Chapter 14

Managing Policies

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.

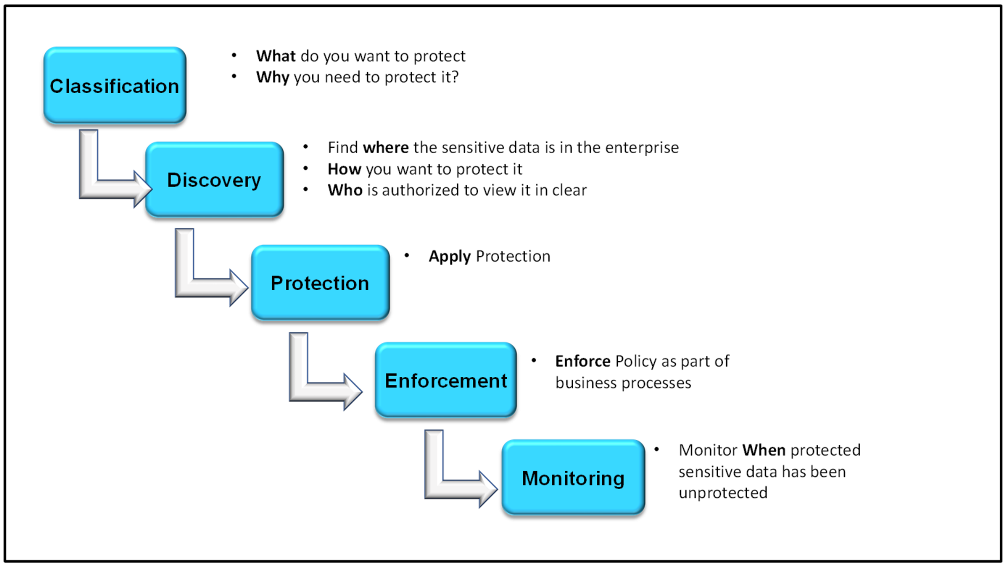

Classification
• **What** do you want to protect
• **Why** you need to protect it?
Discovery
• Find **where** the sensitive data is in the enterprise
• **How** you want to protect it
• **Who** is authorized to view it in clear
Protection
• **Apply** Protection
Enforcement
• **Enforce** Policy as part of business processes
Monitoring
• Monitor **When** protected sensitive data has been unprotected

Figure 14-1: Protegrity Data Security Methodology

14.1 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.

14.2 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.

14.3 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.

14.4 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.

14.5 Monitoring

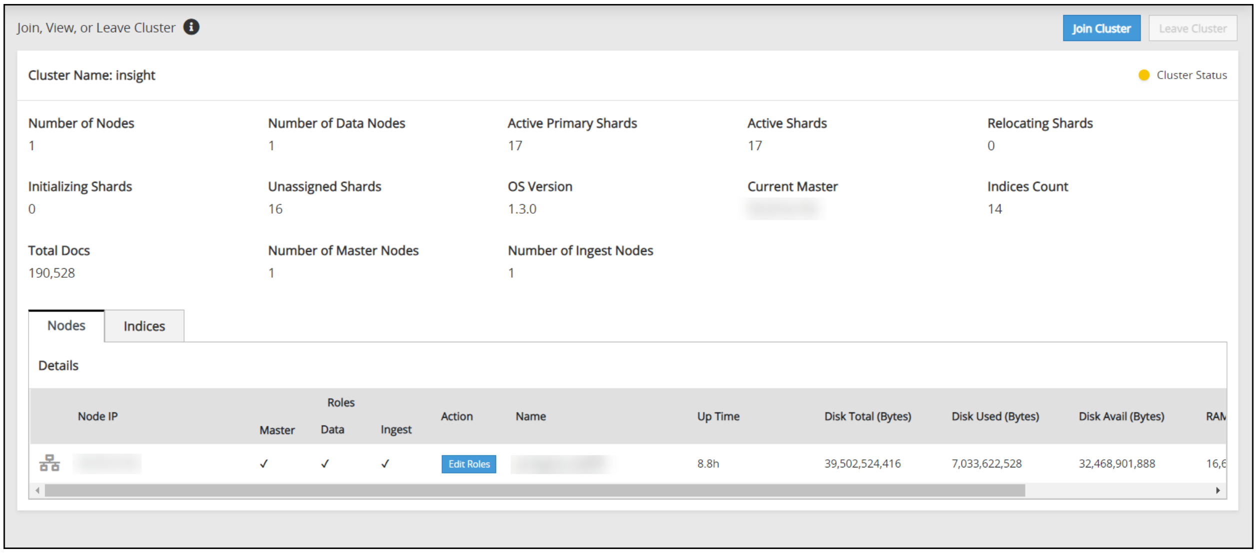
As a policy is enforced, the Protegrity Protectors collects audit logs in their systems and reports back to ESA. Audit logs helps you to capture authorized and unauthorized attempts to access sensitive data at all protection points. It also captures logs on all changes made to policies. You can specify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

Chapter 15

Audit Store Management

The Audit Store is a repository for all data. The Audit Store is built to support multiple nodes making it scalable. Thus, you can add nodes to the Audit Store Management cluster as per your requirements.

You can add, view, and remove nodes from the Audit Store cluster from Audit Store Management. In addition to nodes, this interface shows the node and shard health.



Cluster Name: insight

Number of Nodes: 1
Number of Data Nodes: 1
Active Primary Shards: 17
Active Shards: 17
Relocating Shards: 0
Initializing Shards: 0
Unassigned Shards: 16
OS Version: 1.3.0
Current Master: [redacted]
Indices Count: 14
Total Docs: 190,528
Number of Master Nodes: 1
Number of Ingest Nodes: 1

Details

	Node IP	Roles			Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
		Master	Data	Ingest							
	[redacted]	✓	✓	✓	Edit Roles	[redacted]	8.8h	39,502,524,416	7,033,622,528	32,468,901,888	16,6

Figure 15-1: Audit Store Management Page

For more information about the Audit Store, refer to the *Audit Store Guide 9.1.0.5*.

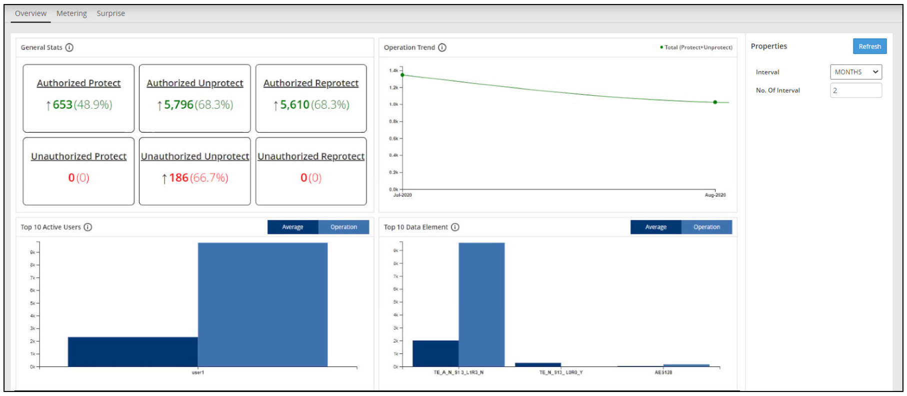
Chapter 16

Protegrity Analytics

Protegrity Analytics provides a set of tools for analyzing the data in the Audit Store. The Protegrity Analytics product provides various reports, graphs, and tables for viewing the Audit Store data. The data is used and displayed in dashboards, alerts, monitors, triggers, actions, destinations, reports, ILM, signature verification jobs, and the scheduler on different tabs in Analytics.

Analytics contain Forensics which is useful for obtaining audit data and which might be necessary for fulfilling compliance requirements.

The tools for viewing and working with logging and alerting that that earlier existed in the ESA is found in this section. You need to re-create alerts, reports, and scheduled tasks that were in the ESA in Analytics.



Authorized Protect ↑653(48.9%)

Authorized Unprotect ↑5,796(68.3%)

Authorized Reprotect ↑5,610(68.3%)

Unauthorized Protect 0(0)

Unauthorized Unprotect ↑186(66.7%)

Unauthorized Reprotect 0(0)

Interval: MONTHS

No. Of Interval: 2

Figure 16-1: Analytics Page

For more information about Analytics, refer to the *Protegrity Analytics Guide 9.1.0.5*.

Chapter 17

Open Listening Ports

The ports in a network are communication channels through which information flows from one system to another. This section provides the list of ports that must be configured in your environment to access the features and services on the Protegrity appliances.

The following are the list of ports that must configured for the system users to access ESA.

Table 17-1: Ports for Users

Port Number	Protocol	Source	Destination	NIC	Description
22	TCP	System User	ESA	Management NIC (ethMNG)	Access to CLI Manager
443	TCP	System User	ESA	Management NIC (ethMNG)	Access to Web UI for Security Officer or ESA administrator

The following are the list of ports that must configured for the system users to access Insight.

Table 17-2: Ports for Insight Users

Port Number	Protocol	Source	Destination	NIC	Description
22	TCP	System User	Insight	Management NIC (ethMNG)	Access to CLI Manager
443	TCP	System User	Insight	Management NIC (ethMNG)	Access to Web UI for Security Officer or Insight administrator

The following are the list of ports that must be configured between the ESA and the non-appliance based protectors such as, Big Data Protector (BDP), Application Protector (AP), and so on.

Table 17-3: Ports for Non-appliance-based Protectors

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
8443	TCP	Non-appliance-based Protectors such as, Big Data Protector (BDP), Application Protector (AP), z/OS and so on.	ESA	Management NIC (ethMNG)	• Downloading certificates and policies from ESA • Sending audit logs from the protectors to ESA	

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
6379	TCP	ESA	BDP Lead Node	Management NIC (ethMNG)	Communication between ESA and BDP lead node.	If HDFSFP is used, this port must be opened. **Note:** Starting from the Big Data Protector 7.2.0 release, the HDFS File Protector (HDFSFP) is deprecated. The HDFSFP-related sections are retained to ensure coverage for using an older version of Big Data Protector with the ESA 7.2.0. **Note:** If a port other than 6379 is configured while installing BDP, ensure that the configured port is open.
9200	TCP	Log Forwarder	Elastic search instance	Management NIC (ethMNG) of ESA	To send audit logs received from the Log Server and forward it to the ESA/Elastic search instance.	

The following are the list of ports that must be configured for the ESA appliances in a Trusted Appliances Cluster (TAC).

Table 17-4: Ports for ESA on TAC

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
22	TCP	ESA Master	ESA Slave	Management NIC (ethMNG)	Communication in TAC	
22	TCP	ESA Slave	ESA Master	Management NIC (ethMNG)	Communication in TAC	
443	TCP	ESA Master	ESA Slave	Management NIC (ethMNG)	Communication in TAC	
443	TCP	ESA Slave	ESA Master	Management NIC (ethMNG)	Communication in TAC	
443	TCPing	ESA Master	ESA Slave	Management NIC (ethMNG)	Communication in TAC	Used for joining a cluster
443	TCPing	ESA Slave	ESA Master	Management NIC (ethMNG)	Communication in TAC	Used for joining a cluster
10100	UDP	ESA Master	ESA Slave	Management NIC (ethMNG)	Communication in TAC	This port is optional. If the appliance heartbeat

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
						services are stopped, this port can be disabled.
10100	UDP	ESA Slave	ESA Master	Management NIC (ethMNG)	Communication in TAC	This port is optional. If the appliance heartbeat services are stopped, this port can be disabled.
8300	TCP	ESA Master	ESA Slave	Management NIC (ethMNG)	Used by servers to handle incoming request.	This is used by servers to handle incoming requests from other agents
8300	TCP	ESA Slave	ESA Master	Management NIC (ethMNG)	Handle incoming requests	This is used by servers to handle incoming requests from other agents
8301	TCP and UDP	ESA Master	ESA Slave	Management NIC (ethMNG)	Gossip on LAN.	This is used to handle gossip in the LAN. Required by all agents
8301	TCP and UDP	ESA Slave	ESA Master	Management NIC (ethMNG)	Gossip on LAN.	This is used to handle gossip in the LAN. Required by all agents
8302	TCP and UDP	ESA Master	ESA Slave	Management NIC (ethMNG)	Gossip on WAN.	This is used by servers to gossip over the WAN, to other servers. As of Consul 0.8 the WAN join flooding feature requires the Serf WAN port (TCP/ UDP) to be listening on both WAN and LAN interfaces.
8302	TCP and UDP	ESA Slave	ESA Master	Management NIC (ethMNG)	Gossip on WAN.	This is used by servers to gossip over the WAN, to other servers. As of Consul 0.8 the WAN join flooding feature requires the Serf WAN port (TCP/ UDP) to be listening on both WAN and LAN interfaces.
8600	TCP and UDP	ESA	DSG	Management NIC (ethMNG)	Listens to the DNS server port.	Used to resolve DNS queries
8600	TCP and UDP	DSG	ESA	Management NIC (ethMNG)	Listens to the DNS server port.	Used to resolve DNS queries
9000	TCP and UDP	ESA	DSG	Management NIC (ethMNG)	Checks local certificates.	If your TAC utilizes Consul services, you must enable this port.
9000	TCP and UDP	DSG	ESA	Management NIC (ethMNG)	Checks local certificates.	If your TAC utilizes Consul services, you must enable this port.

Based on the firewall rules and network infrastructure of your organization, you must open ports for the services listed in the following table.

Table 17-5: Additional Ports

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
123	UDP	ESA	Time servers	Management NIC (ethMNG) of ESA	NTP Time Sync Port	This port can be configured based on the enterprise network policies or according to your use case.
389	TCP	ESA	Active Directory server	Management NIC (ethMNG) of ESA	Authentication for External AD and synchronization with External Groups	This port can be configured based on the enterprise network policies or according to your use case.
389	TCP	ESA	Active Directory server	Management NIC (ethMNG) of ESA	Synchronization with External AD Groups for policy users	This port can be configured based on the enterprise network policies or according to your use case.
636	TCP	ESA	Active Directory server	Management NIC (ethMNG) of ESA	Authentication for External AD and synchronization with External Groups	This port is for LDAPS. It can be configured based on the enterprise network policies or according to your use case.
636	TCP	ESA	Active Directory server	Management NIC (ethMNG) of ESA	Synchronization with External AD Groups for policy users	This port is for LDAPS. It can be configured based on the enterprise network policies or according to your use case.
1812	TCP	ESA	RADIUS server	Management NIC (ethMNG) of ESA	Authentication with RADIUS server	This port can be configured based on the enterprise network policies or according to your use case.
514	UDP	ESA	Syslog servers	Management NIC (ethMNG) of ESA	Storing logs	This port can be configured based on the enterprise network policies or according to your use case.
FutureX (9111)	TCP	ESA	HSM server	Management NIC (ethMNG) of ESA	HSM communication	This port can be configured based on the enterprise network policies or according to your use case.
Safenet (1792)	TCP	ESA	HSM server	Management NIC (ethMNG) of ESA	HSM communication	This port must be opened and configured based on the enterprise network policies or according to your use case.
nCipher non-privileged port (8000)	TCP	ESA	HSM sever	Management NIC (ethMNG) of ESA	HSM communication	This port must be opened and configured based on the enterprise network policies or according to your use case.
nCipher privileged port (8001)	TCP	ESA	HSM sever	Management NIC (ethMNG) of ESA	HSM communication	This port must be opened and configured based on the enterprise network policies

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
						or according to your use case.
Utimaco (288)	TCP	ESA	HSM sever	Management NIC (ethMNG) of ESA	HSM communication	This port must be opened and configured based on the enterprise network policies or according to your use case.

If you are utilizing the DSG appliance, the following ports must be configured in your environment.

Table 17-6: Ports for Users

Port Number	Protocol	Source	Destination	NIC	Description
22	TCP	System User	DSG	Management NIC (ethMNG)	Access to CLI Manager
443	TCP	System User	DSG	Management NIC (ethMNG)	Access to Web UI

The following are the list of ports that must be configured for communication between DSG and ESA.

Table 17-7: Ports for Communication with ESA

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
22	TCP	ESA	DSG	Management NIC (ethMNG)	• Replication or Rulesets from DSG to ESA • DSG Patching from ESA	
443	TCP	ESA	DSG	Management NIC (ethMNG)	Communication in TAC	
443	TCP	DSG	ESA and Virtual IP address of ESA	Management NIC (ethMNG)	Downloading certificates from ESA	
8443	TCP	DSG	ESA and Virtual IP address of ESA	Management NIC (ethMNG)	• Establishing communication with ESA • Retrieving policy from ESA • Sending audit logs to ESA	
389	TCP	DSG	Virtual IP address of ESA	Management NIC (ethMNG)	Authentication and authorization by ESA	
5671	TCP	DSG	ESA	Management NIC (ethMNG)	Messages sent from DSG to ESA	This port is required to support backward compatibility, where ESA v7.2.1 communicates with

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
						the earlier versions of appliances other than ESA. For example, port *5671* is required for user notifications from a DSG system to appear on the ESA v7.2.1 Dashboard.
10100	UDP	DSG	ESA	Management NIC (ethMNG)	• Establishing communication with ESA • Communication in TAC	This port is optional. If the appliance heartbeat services are stopped, this port can be disabled.

The following are the list of ports that must also be configured when DSG is configured in a TAC.

Table 17-8: DSG Ports for Communication in TAC

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
22	TCP	DSG	ESA	Management NIC (ethMNG)	Communication in TAC	
8585	TCP	ESA	DSG	Management NIC (ethMNG)	Cloud Gateway cluster	
443	TCP	ESA	DSG	Management NIC (ethMNG)	Communication in TAC	
10100	UDP	ESA	DSG	Management NIC (ethMNG)	Communication in TAC	This port is optional. If the Appliance Heartbeat services are stopped, this port can be disabled.
10100	UDP	DSG	ESA	Management NIC (ethMNG)	• Establishing communication with ESA • Communication in TAC	This port is optional. If the Appliance Heartbeat services are stopped, this port can be disabled.
10100	UDP	DSG	DSG	Management NIC (ethMNG)	Communication in TAC	This port is optional.
8300	TCP	ESA	DSG	Management NIC (ethMNG)	Used by servers to handle incoming request.	This is used by servers to handle incoming requests from other agents
8300	TCP	DSG	ESA	Management NIC (ethMNG)	Handle incoming requests	This is used by servers to handle incoming requests from other agents.

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
8300	TCP	DSG	DSG	Management NIC (ethMNG)	Handle incoming requests	This is used by servers to handle incoming requests from other agents
8301	TCP and UDP	ESA	DSG	Management NIC (ethMNG)	Gossip on LAN.	This is used to handle gossip in the LAN. Required by all agents.
8301	TCP and UDP	DSG	ESA	Management NIC (ethMNG)	Gossip on LAN.	This is used to handle gossip in the LAN. Required by all agents.
8301	TCP and UDP	DSG	DSG	Management NIC (ethMNG)	Gossip on LAN.	This is used to handle gossip in the LAN. Required by all agents.
8302	TCP and UDP	ESA	DSG	Management NIC (ethMNG)	Gossip on WAN.	This is used by servers to gossip over the WAN, to other servers. As of Consul 0.8 the WAN join flooding feature requires the Serf WAN port (TCP/UDP) to be listening on both WAN and LAN interfaces.
8302	TCP and UDP	DSG	ESA	Management NIC (ethMNG)	Gossip on WAN.	This is used by servers to gossip over the WAN, to other servers. As of Consul 0.8 the WAN join flooding feature requires the Serf WAN port (TCP/UDP) to be listening on both WAN and LAN interfaces.
8302	TCP and UDP	DSG	DSG	Management NIC (ethMNG)	Gossip on WAN.	This is used by servers to gossip over the WAN, to other servers. As of Consul 0.8 the WAN join flooding feature requires the Serf WAN port (TCP/UDP) to be listening on both WAN and LAN interfaces.

Based on the firewall rules and network infrastructure of your organization, you must open ports for the services listed in the following table.

Table 17-9: Additional Ports for DSG

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
123	UDP	DSG	Time servers	Management NIC (ethMNG) of ESA	NTP Time Sync Port	This port can be configured based on the enterprise network policies or according to your use case.
514	UDP	DSG	Syslog servers	Management NIC (ethMNG) of ESA	Storing logs	This port can be configured based on the enterprise network policies or according to your use case.
N/A*	N/A*	DSG	Applications/Systems	Service NIC (ethSRV) of DSG	Enabling communication for DSG with different applications in the organization	This port can be configured based on the enterprise network policies or according to your use case.
N/A*	N/A*	Applications/ System	DSG	Service NIC (ethSRV) of DSG	Enabling communication for DSG with different applications in the organization	This port can be configured based on the enterprise network policies or according to your use case.

Note: In DSG, service NICs are not assigned a specific port number. You can configure a port number as per your requirements.

The following ports must be configured on ESA for communication with the Internet.

Table 17-10: Ports for the Internet

Port Number	Protocol	Source	Destination	NIC	Description
80	TCP	ESA	ClamAV Database	Management NIC (ethMNG) of ESA	Updating the Antivirus database on ESA

The following ports are recommended for strengthening the firewall configurations.

Table 17-11: Recommended Ports for Strengthening Firewall Rules

Port Number	Protocol	Source	Destination	NIC	Description
67	UDP	Appliance/System	DHCP server	Management NIC (ethMNG)	Allows server requests from the DHCP server
68	UDP	Appliance/System	DHCP server	Management NIC (ethMNG)	Allows client requests on the DHCP server
161	UDP	ESA/DSG	SNMP	Management NIC (ethMNG)	Allows SNMP requests
10161	TCP and UDP	ESA/DSG	SNMP	Management NIC (ethMNG)	Allows SNMP requests over DTLS

The following ports must be configured for communication between the ESA and the Audit Store.

Table 17-12: Audit Store Ports

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
9200	TCP	ESA	ESA	Management NIC (ethMNG) of ESA	Audit Store REST communication	This port can be configured based on the enterprise network policies or according to your use case.
9300	TCP	ESA	ESA	Management NIC (ethMNG) of ESA	Internode communication between the Audit Store nodes	This port can be configured based on the enterprise network policies or according to your use case.
24224	UDP	ESA	ESA	Management NIC (ethMNG) of ESA	Communication between *td-agent* and the Audit Store	This port can be configured according to your use case when forwarding logs to an external Security information and event management (SIEM).
24284	TCP	Protector	ESA	Management NIC (ethMNG) of ESA	Communication between Protector and *td-agent*	This port can be configured according to your use case when forwarding logs to an external Security information and event management (SIEM).

Chapter 18

Accessing Appliances using Single Sign-On (SSO)

What is SSO

Consider an enterprise user having access to multiple applications that offer a variety of services. The applications might require user authentication, where one provides usernames and passwords to access them. Each time the user accesses any of the applications, the ask to provide the credentials increases. It is required that a user remember multiple user credentials for the applications. Thus, to avoid the confusion for the users, the Single Sign-On (SSO) mechanism can be used to facilitate access to multiple applications by logging in to the system only once.

Single Sign-on (SSO) is a feature that enables users to authenticate multiple applications by logging to a system only once. It provides federated access, where a ticket or token is trusted across multiple applications in a system. Users log in using their credentials. They are authenticated through authentication servers such as Active Directory (AD) or LDAP that validate the credentials. After successful authentication, a ticket is generated for accessing different services.

For more information about Kerberos, refer to *https://web.mit.edu/kerberos/*

18.1 What is Kerberos

About Kerberos

One of the protocols that SSO uses for authentication is Kerberos. Kerberos is an authentication protocol that uses secret key cryptography for secure communication over untrusted networks. Kerberos is a protocol used in a client-server architecture, where the client and server verify each other’s identities. The messages sent between the client and server are encrypted, thus preventing attackers from snooping.

Key Entities in Kerberos

There are few key entities that are involved in a Kerberos communication:

- **Key Distribution Center (KDC)**: Third-party system or service that distributes tickets
- **Authentication Server (AS)**: Server that validates the user logging into a system
- **Ticket Granting Server (TGS)**: Server that grants clients a ticket to access the services
- **Encrypted Keys**: Symmetric keys that are shared between the entities such as, authentication server, TGS, and the main server.
- **Simple and Protected GSS-API Negotiation (SPNEGO)**: The Kerberos SPNEGO mechanism is used in a client-server architecture for negotiating an authentication protocol in an HTTP communication. This mechanism is utilized when the client and the server want to authenticate each other, but are not sure about the authentication protocols that are supported by each of them.

- **Service Principal Name (SPN)**: SPN represents a service on a network. Every service must be defined in the Kerberos database.
- **Keytab File**: It is an entity that contains an Active Directory account and the keys for decrypting Kerberos tickets. Using the keytab file, you can authenticate remote systems without entering a password.

For implementing Kerberos SSO, ensure that the following prerequisites are considered:

- The appliances, such as, the ESA, or DSG are up and running
- The AD is configured and running
- The IP addresses of the appliances are resolved to a Fully Qualified Domain Name (FQDN).

18.1.1 Implementing Kerberos SSO for Protegrity Appliances

In the Protegrity appliances, you can utilize the Kerberos SSO mechanism to login to the appliance. The user logs in to the system with his domain credentials for accessing the appliances such as, the ESA or DSG. The appliance validates the user and on successful validation, allows the user access to the appliance. For utilizing the SSO mechanism, you must configure certain settings on different entities, such as, AD, Web browser, and the ESA appliance. The following sections describe a step-by-step approach for setting up SSO.

> **Note:**
> For Protegrity appliances, only Microsoft AD is supported.

18.1.1.1 Prerequisites

For implementing Kerberos SSO, ensure that the following prerequisites are considered:

- The appliances, such as, the ESA, or DSG are up and running
- The AD is configured and running
- The IP addresses of the appliances are resolved to a Fully Qualified Domain Name (FQDN).

18.1.1.2 Setting up Kerberos SSO

This section describes about the different tasks that an administrative user must perform for enabling the Kerberos SSO feature on the Protegrity appliances.

Table 18-1: Setting up SSO

Order	Platform	Step	Reference
1	Appliance Web UI	On the appliance Web UI, import the domain users from the AD to the internal LDAP of the appliance and assign **SSO Login** permissions to the required user role	*Importing Users and assigning role*
2	Active Directory	On the AD, map the Kerberos SPN to a user account.	*Configuring SPN*
3	Active Directory	On the AD, generate a keytab file.	*Generating keytab file*
4	Appliance Web UI	On the appliance Web UI, upload the generated keytab file.	*Uploading keytab file*

Order	Platform	Step	Reference
5	Web Browser	On the user's machine, configure the Web browsers to handle SPNEGO negotiation.	*Configuring browsers*

18.1.1.2.1 Importing Users and Assigning Role

In the initial steps for setting up Kerberos SSO, a user with administrative privileges must import users from an AD to the appliance and assign the required permissions to the users for logging with SSO.

To import users and assign roles:

1. On the appliance Web UI, navigate to **Settings** > **Users** > **Proxy Authentication**.
2. Enter the required parameters for connecting to the AD.

   For more information about setting AD parameters, refer to section *Configuring the Proxy Authentication Settings* in the *Protegrity Appliances Overview Guide 9.1.0.5*.
3. Navigate to the **Roles** tab.
4. Create a role or modify an existing role.
5. Select the **SSO Login** permission check box for the role and click **Save**.

   > **Note:** If you are configuring SSO on the DSG, then ensure the user is also granted the required cloud gateway permissions.
6. Navigate to the **User Management** tab.
7. Click **Import Users** to import the required users to the internal LDAP.

   For more information about importing users, refer to section *Importing Users to Internal LDAP* in the *Protegrity Appliances Overview Guide 9.1.0.5*.
8. Assign the role with the SSO Login permissions to the required users.

18.1.1.2.2 Creating Service Principal Name (SPN)

A Service Principal Name (SPN) is an entity that represents a service mapped to an instance on a network. For a Kerberos-based authentication, the SPN must be configured in the Active Directory (AD). The SPN is registered with the AD. In this configuration, a service associates itself with the AD for the purpose of authentication requests.

For Protegrity, the instance is represented by appliances, such as, the ESA or DSG. It uses the SPNEGO authentication for authenticating users for SSO. The SPNEGO uses the *HTTP* service for authenticating users. The SPN is configured for the appliances in the following format.

service/instance@domain

> **Note:**
>
> For Protegrity appliances, only Microsoft AD is supported.

Consider an appliance with host name *esa1.protegrity.com* on the domain *protegrity.com*. The SPN must be set in the AD as *HTTP/esa1.protegrity.com@protegrity.com*.

The SPN of the appliance can be configured in the AD using the **`setspn`** command. Thus, to create the SPN for *esa1.protegrity.com*, run the following command.

```
setspn -A HTTP/esa1.protegrity.com@protegrity.com
```

> **Note:**
> Ensure that the SPN is created for every ESA appliance that is involved in the Kerberos SSO implementation.

18.1.1.2.3 Creating the Keytab File

The keytab is an encrypted file that contains the Kerberos principals and keys. It allows an entity to use a Kerberos service without being prompted a password on every access. The keytab file decrypts every Kerberos service request and authenticates it based on the password.

For Protegrity appliances, an SSO authentication request of a user from appliance to the AD passes through the keytab file. In this file, you map the appliance user's credentials to the SPN of the appliance. The keytab file is created using the **`ktpass`** command. The following is the syntax for this command:

```
ktpass -out <Location where to generate the keytab file> -princ HTTP/<SPN of the appliance>
-mapUser <username> -mapOp set -pass <Password> -crypto All -pType KRB5_NT_PRINCIPAL
```

The following sample snippet describes the **`ktpass`** for mapping a user in the keytab file. Consider an ESA appliance with host name *esa1.protegrity.com* on the domain *protegrity.com*. The SPN for the appliance is set as *HTTP/esa1.protegrity.com@protegrity.com*. Thus, to create a keytab file and map a user *Tom*, run the following command.

```
ktpass -out C:\esa1.keytab -princ HTTP/esa1.protegrity.com@protegrity.com -mapUser
Tom@protegrity.com -mapOp set -pass Test@1234 -crypto All -pType KRB5_NT_PRINCIPAL
```

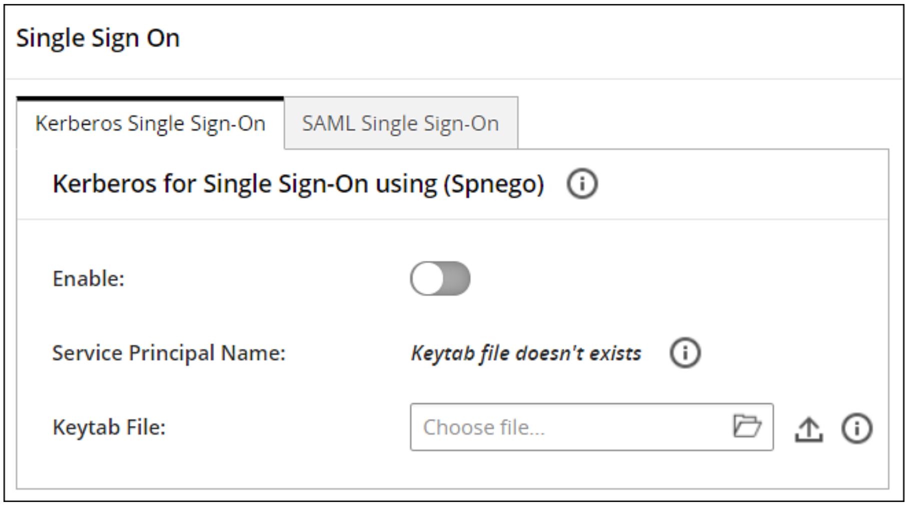
18.1.1.2.4 Uploading Keytab File

After creating the keytab file from the AD, you must upload it on the appliance.

> **Note:**
> You must upload the keytab file before enabling the Kerberos SSO.

➤ To upload the keytab file:

1. On the Appliance Web UI, navigate to **Settings** > **Users** > **Proxy Authentication**.
   The **Proxy Authentication Settings** screen appears.
2. From the **Keytab File** field, upload the keytab file generated.


Single Sign On

Kerberos Single Sign-On | SAML Single Sign-On

Kerberos for Single Sign-On using (Spnego)

Enable:

Service Principal Name: *Keytab file doesn't exists*

Keytab File: Choose file...

Figure 18-1: Uploading Keytab

3. Click the **Upload Keytab** icon.
   A confirmation message appears.
4. Select **Ok**.

> **Note:**
> Click the **Delete** icon to delete the keytab file. You can delete the keytab file only when the **Kerberos for single sign-on (Spnego)** option is disabled.

5. Under the **Kerberos for single sign-on (Spnego)** tab, click the **Enable** toggle switch to enable Kerberos SSO.
   A confirmation message appears.
6. Select **Ok**.
   A message `Kerberos SSO was enabled successfully` appears.

18.1.1.2.5 Configuring SPNEGO Authentication on the Web Browser

Before implementing Kerberos SSO for Protegrity appliances, you must ensure that the Web browsers are configured to perform SPNEGO authentication. The tasks in this section describe the configurations that must be performed on the Web Browsers. The recommended Web browsers and their versions are as follows:

- Google Chrome version 123.0.6312.123 (64-bit)
- Mozilla Firefox version 124.0.2 (64-bit) or higher
- Microsoft Edge version 123.0.2420.81 (64-bit)

The following sections describe the configurations on the Web browsers.

18.1.1.2.5.1 Configuring SPNEGO Authentication on Firefox

The following steps describe the configurations on Mozilla Firefox.

➤ To configure on the Firefox Web browser:

1. Open Firefox on the system.
2. Enter *about:config* in the URL.

3. Type *negotiate* in the **Search** bar.
4. Double click on *network.negotiate-auth.trusted-uris* parameter.
5. Enter the FQDN of the appliance and exit the browser.

18.1.1.2.5.2 Configuring SPNEGO Authentication on Internet Explorer

The following steps describe the configurations on Internet Explorer 11.

➤ To configure on the Internet Explorer Web browser:

1. Open Internet Explorer on the machine
2. Navigate to **Tools** > **Internet options** > **Security** .
3. Select **Local intranet**.
4. Enter the FQDN of the appliance under sites that are included in the local intranet zone.
5. Select **Ok**.

18.1.1.2.5.3 Configuring SPNEGO Authentication on Chrome

With Google Chrome, you must set the white list servers that Chrome will negotiate with. If you are using a Windows machine to log in to the appliances, then the configurations entered in other browsers are shared with Chrome. You need not add a separate configuration.

18.1.1.3 Logging to the Appliance

After configuring the required SSO settings, you can login to the appliance using Kerberos SSO.

➤ To login to the appliance using SSO:

1. Open the Web browser and enter the FQDN of the ESA or DSG in the URL.
2. Click **Sign in with Kerberos SSO**.
   The Dashboard of the ESA/DSG appliance appears.

18.1.1.4 Scenarios for Implementing Kerberos SSO

This section describes the different scenarios for implementing Kerberos SSO.

18.1.1.4.1 Implementing Kerberos SSO on an Appliance Connected to an AD

This section describes the process of implementing Kerberos SSO when an appliance utilizes authentication services of the local LDAP.

> **Note:**
> You can also login to the appliance without SSO by providing valid user credentials.

Steps to configure Kerberos SSO with a Local LDAP

Consider an appliance for which you are configuring SSO. Ensure that you perform the following steps to implement it.

1. *Import users from an external directory* and assign SSO permissions.
2. *Configure SPN* for the appliance.
3. *Create* and *upload* the keytab file on the appliance.
4. *Configure the browser* to support SSO.

Logging in with Kerberos SSO

After configuring the required settings, user enters the appliance domain name on the Web browser and clicks **Sign in with SSO** to access appliance. On successful authentication, the Dashboard of the appliance appears.

Process

The following figure illustrates the SSO process for appliances that utilize the local LDAP.

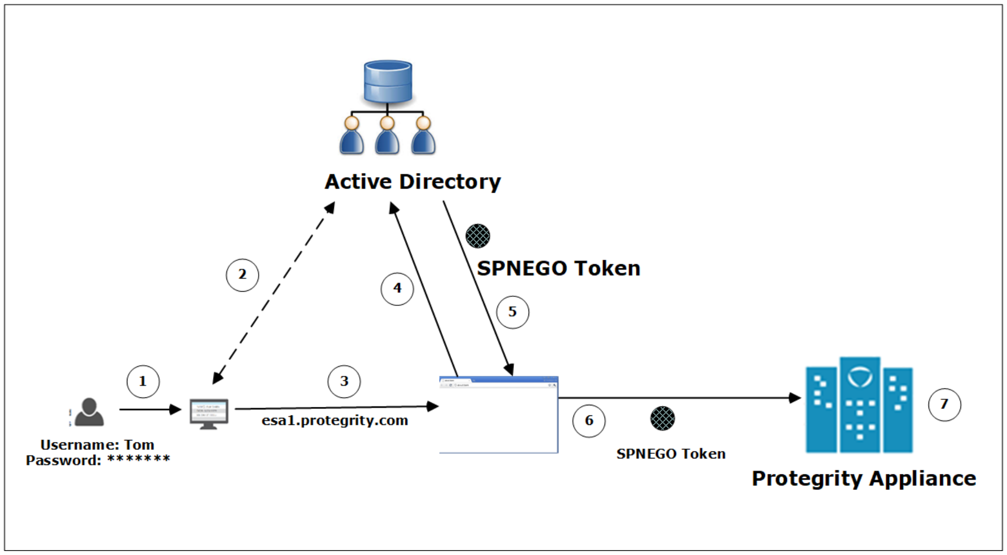


Figure 18-2: SSO Implementation

1. The user logs in to the domain with their credentials.

   For example, a user, Tom, logs in to the domain *abc.com* as *tom@abc.com* and password *********.

2. Tom is authenticated on the AD. On successful authentication, he is logged in to the system.
3. For accessing the appliance, the user enters the FQDN of the appliance on the Web browser.

   For example, *esa1.protegrity.com*.

4. If Tom wants to access the appliance using SSO, then he clicks **Sign in with SSO** on the Web browser.

   A message is sent to the AD requesting a token for Tom to access the appliance.

5. The AD generates a SPNEGO token and provides it to Tom.
6. This SPNEGO token is then provided to the appliance to authenticate Tom.
7. The appliance performs the following checks.
   a. It receives the token and decrypts it. If the decryption is successful, then the token is valid.
   b. Retrieves the username from the token.
   c. Validates Tom with the internal LDAP.
   d. Retrieves the role for Tom and verifies that the role has the **SSO Login** permissions.

After successfully validating the token and the role permissions, Tom can access the appliance.

18.1.1.4.2 Implementing Kerberos SSO on other Appliances Communicating with ESA

This section describes the process of implementing Kerberos SSO when an appliance utilizes authentication services of another appliance. Typically, the DSG depends on ESA for user management and LDAP connectivity. This section explains the steps that must be performed to implement SSO on the DSG.

18.1.1.4.2.1 Implementing Kerberos SSO on DSG

This section explains the process of SSO authentication between the ESA and the DSG. It also includes information about the order of set up to enable SSO authentication on the DSG.

The DSG depends on the ESA for user and access management. The DSG can leverage the users and user permissions that are defined in the ESA only if the DSG is set to communicate with the ESA.

The following figure illustrates the SSO process for appliances that utilize the LDAP of another appliance.

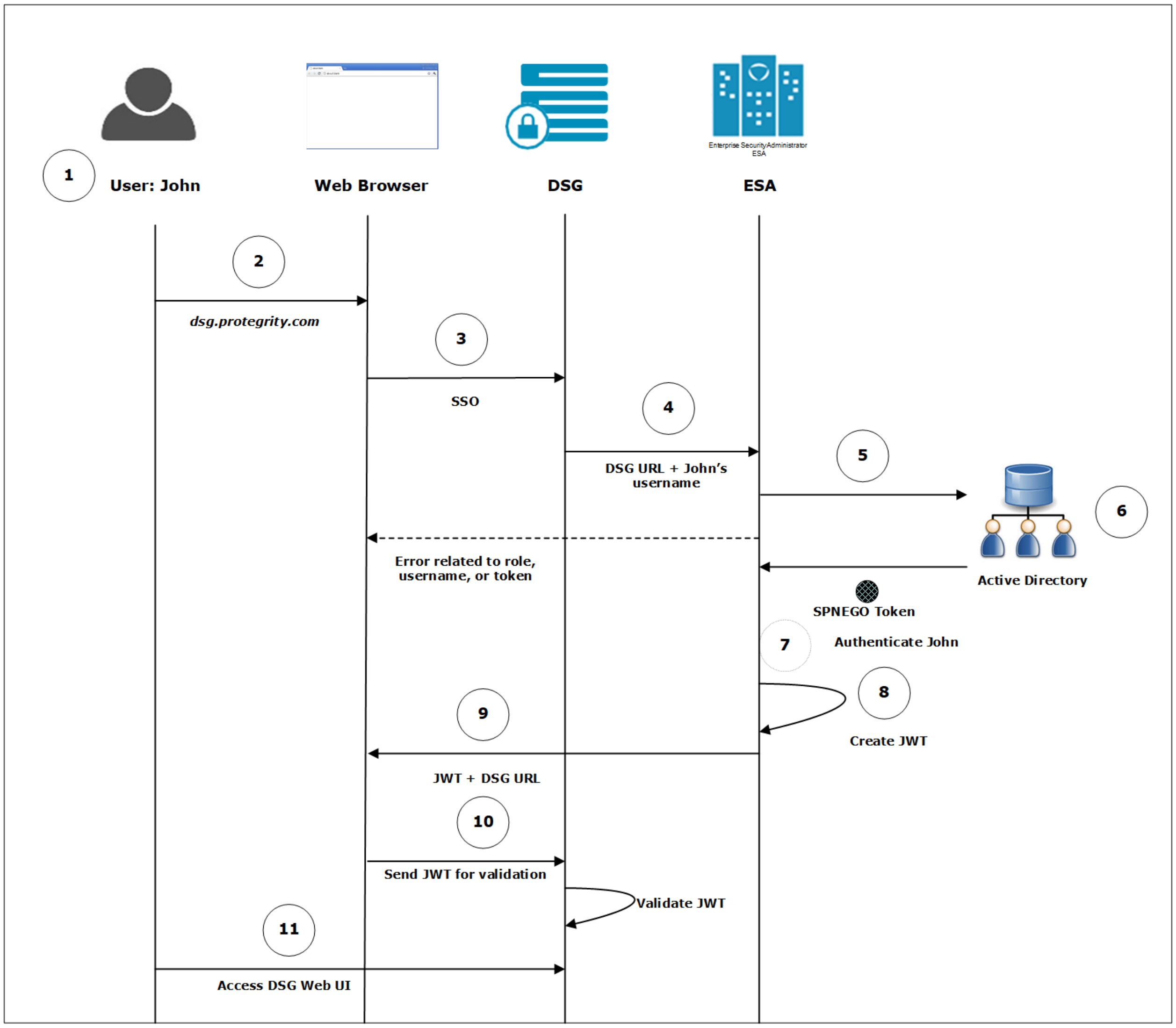


Figure 18-3: SSO with External LDAP

1. The user logs in to the system with their credentials.

For example, John logs in to the domain *abc.com* as *john@abc.com* and password *********. The user is authenticated on the AD. On successful authentication the user is logged in to the system.

2. For accessing the DSG Web UI John enters the FQDN of the DSG on the Web browser.

   For example, *dsg.protegrity.com*.

3. If John wants to access the DSG Web UI using SSO, he clicks **Sign in with SSO** on the Web browser.
4. The username of John and the URL of the*DSG* is forwarded to the ESA.
5. The ESA sends the request to the AD for generating a SPNEGO token.
6. The AD generates a SPNEGO token to authenticate John and sends it to the ESA.
7. The ESA performs the following steps to validate John.
   a. Receives the token and decrypts it. If the decryption is successful, then the token is valid.
   b. Retrieves the username from the token.
   c. Validates John with the internal LDAP.
   d. Retrieves the role for John and verifies that the role has SSO Login .

> **Note:**
>
> If the ESA encounters any error related to the role, username, or token, an error is displayed on the Web UI. For more information about the errors, refer to section *Troubleshooting*.

8. On successful authentication, the ESA generates a service JWT.
9. The ESA sends this service JWT and the URL of to the Web browser.
10. The Web browser presents this JWT to the DSG for validation.
11. The *DSG* validates the JWT based on the secret key shared with ESA. On successful validation, John can login to the DSG Web UI.

Before You Begin:

Ensure that you complete the following steps to implement SSO on the *DSG*.

This section describes the process of implementing SSO on the DSG.

1. Ensure that the *Set ESA Communication* process is performed on the DSG for establishing communication with the ESA.

   For more information about setting ESA communication, refer to section *Setting up ESA Communication* in the *Protegrity Data Security Gateway User Guide 3.1.0.5*.

2. *Import users from an external directory* on the ESA and assign SSO and cloud gateway permissions.
3. *Configure SPN* for the ESA.
4. *Create* and *upload* the keytab file on the ESA.
5. *Enable Single Sign-on* on the ESA.
6. *Export the JWT settings* to all the DSG nodes in the cluster.

Next Steps:

After ensuring that the prerequisites for SSO in the DSG implementation are completed, you must complete the configuration on the DSG Web UI.

For more information about completing the configuration, refer to section *LDAP and SSO Configurations* in the *Protegrity Data Security Gateway User Guide 3.1.0.5*.

18.1.1.4.2.1.1 Exporting the JWT Settings to the DSG Nodes in the Cluster

As part of SSO implementation for the DSG, the JWT settings must be exported to all the DSG nodes that will be configured to use SSO authentication.

Before you begin

Ensure that the ESA, where SSO is enabled, and the DSG nodes are in a cluster.

➤ To export the JWT settings:

1. Log in to the ESA Web UI.
2. Navigate to **System** > **Backup & Restore**.
3. On the **Export**, select the **Cluster Export** option, and click **Start Wizard**.
4. On the **Data to import** tab, select **Appliance JWT Configuration**, and click **Next**.

> **Note:**
> Ensure that only **Appliance JWT Configuration** check box is selected.

5. On the **Source Cluster Nodes** tab, select **Create and Run a task now**, and click **Next**.
6. On the **Target Cluster Nodes** tab, select all the DSG nodes where you want to export the JWT settings, and click **Execute**.

18.1.1.4.3 Implementing Kerberos SSO with a Load Balancer Setup

This section describes the process of implementing SSO with a Load Balancer that is setup between the appliances.

Steps to configure SSO in a load balancer setup

Consider two appliances, *L1* and *L2*, that are configured behind a load balancer. Ensure that you perform the following steps to implement it.

1. *Import users from an external directory* on the *L1* and *L2* and assign SSO login permissions.
2. Ensure that the FQDN is resolved to the IP address of the load balancer.
3. *Configure SPN* for the load balancer.
4. *Create* and *upload* the keytab file on *L1* and *L2*.
5. *Configure the browser* to support SSO.

Logging in with SSO

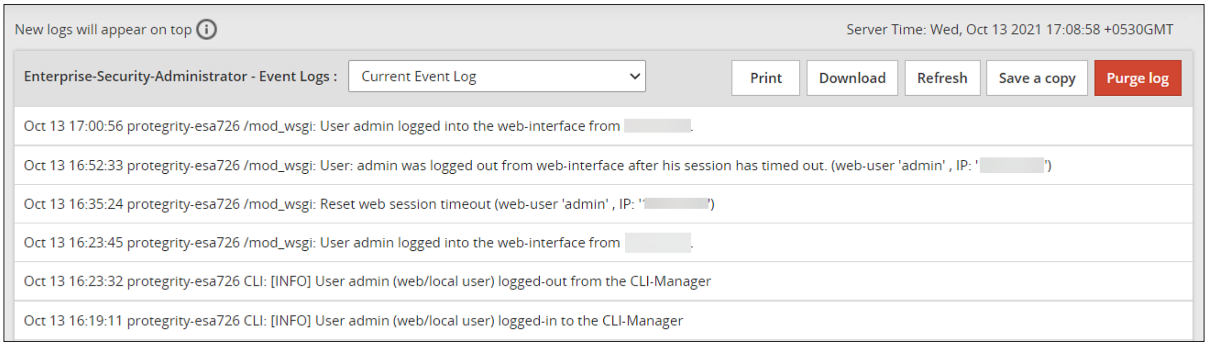
After configuring the required settings, the user enters the FQDN of load balancer on the Web browser and clicks **Sign in with Kerberos SSO** to access it. On successful authentication, the Dashboard of the appliance appears.

18.1.1.5 Viewing Logs

You can view the logs that are generated for when the Kerberos SSO mechanism is utilized. The logs are are generated for the following events:

- Uploading keytab file on the appliance
- Deleting the keytab file on the appliance
- User logging to the appliance through SSO
- Enabling or disabling SSO

Navigate to **Logs** > **Appliance Logs** to view the logs. The following figure displays the logs for SSO.


New logs will appear on top
Server Time: Wed, Oct 13 2021 17:08:58 +0530GMT
Enterprise-Security-Administrator - Event Logs :
Current Event Log
Print
Download
Refresh
Save a copy
Purge log

```
Oct 13 17:00:56 protegrity-esa726 /mod_wsgi: User admin logged into the web-interface from [redacted].
Oct 13 16:52:33 protegrity-esa726 /mod_wsgi: User: admin was logged out from web-interface after his session has timed out. (web-user 'admin' , IP: '[redacted]')
Oct 13 16:35:24 protegrity-esa726 /mod_wsgi: Reset web session timeout (web-user 'admin' , IP: '[redacted]')
Oct 13 16:23:45 protegrity-esa726 /mod_wsgi: User admin logged into the web-interface from [redacted].
Oct 13 16:23:32 protegrity-esa726 CLI: [INFO] User admin (web/local user) logged-out from the CLI-Manager
Oct 13 16:19:11 protegrity-esa726 CLI: [INFO] User admin (web/local user) logged-in to the CLI-Manager
```

Figure 18-4: Appliance Logs

You can also navigate on the **Insight Analytics** screen to view the logs.

18.1.1.6 Feature Limitations

This section covers some known limitations of the Kerberos SSO feature.

Trusted Appliances Cluster

The keytab file is specific for an SPN. A keytab file assigned for one appliance is not applicable for another appliance. Thus, if your appliance is in a TAC, it is recommended not to replicate the keytab file between different appliances.

18.1.1.7 Troubleshooting

This section describes the issues and their solutions while utilizing the Kerberos SSO mechanism.

Table 18-2: Kerberos SSO Troubleshooting

Issue	Reason	Solution
The following message appears while logging in with SSO. `Login Failure: SPNEGO authentication is not supported on this client.`	The browser is not configure to handle SPNEGO authentication	Configure the browser to perform SPNEGO authentication. For more information about configuring the browser settings, refer to section *Configuring browsers*.
The following message appears while logging in with SSO. `Login Failure: Unauthorized to SSO Login.`	- Username is not present in the internal LDAP - Username does not have roles assigned to it - Role that is assigned to the user does not have SSO Login permissions	Ensure that the following points are considered: - The user is imported to the internal LDAP. - Role assigned to the user has **SSO Login** permission enabled. For more information about configuring user role, refer to section *Importing Users and assigning role*.
The following error appears while logging in with SSO. `Login Failure: Please contact System Administrator`	The JWT secret key is not the same between the appliances.	If an appliance is using an LDAP of another appliance for user authentication, then ensure that the JWT secret is shared between them.

Issue	Reason	Solution
The following error appears while logging in with SSO. `Login Failure: SSO authentication disabled`	This error might occur when you are using LDAP of another appliance for authentication. If SSO in the appliance that contains the LDAP information is disabled, the error message appears.	On the ESA Web UI, navigate to **System** > **Settings** > **Users** > **Advanced** and check **Enable SSO** check box.
When you are using an LDAP of another appliance for authentication and logging in using SSO, a `Service not available` message appears on the Web browser.	• Active Directory is not reachable • Appliance on which the LDAP services are utilized is not reachable	Ensure the following points are considered: • The active directory is up and running. • The appliance on which the LDAP services are utilized is up and running.

18.2 What is SAML

About SAML

Security Assertion Markup Language (SAML) is an open standard for communication between an identity provider (IdP) and an application. It is a way to authenticate users in an IdP to access the application.

SAML SSO leverages SAML for seamless user authentication. It uses XML format to transfer authentication data between the IdP and the application. Once users log in to the IdP, they can access multiple applications without providing their user credentials every time. For SAML SSO to be functioning, the IdP and the application must support the SAML standard.

Key Entities in SAML

There are few key entities that are involved in a Kerberos communication:

- **Identity Provider (IdP)**: A service that manages user identities.
- **Service Provider (SP)**: An entity connecting to the IdP for authenticating users
- **Metadata**: An file containing information for connecting an SP to an IdP

18.2.1 Implementing SAML SSO for Protegrity Appliances

In the Protegrity appliances, you can utilize the SAML SSO mechanism to login to the appliance. To use this feature, you log in to an IdP, such as, AWS, Azure, or GCP. After you are logged in to the IdP, you can access appliances such as, the ESA or the DSG. The appliance validates the user and on successful validation, allows the user access to the appliance. The following sections describe a step-by-step approach for setting up SAML SSO.

18.2.2 Prerequisites

For implementing SAML SSO, ensure that the following prerequisites are met:

- The SPs, such as, the ESA or the DSG are up and running
- The users are available in IdPs, such as, AWS, Azure, or GCP.
- The IdP contains a SAML application for your appliance.
- The users that will leverage the SAML SSO feature are added to the appliance from the **User Management** screen
- The IP addresses of the appliances are resolved to a Fully Qualified Domain Name (FQDN)

18.2.3 Setting up SAML SSO

This section describes the different tasks that an administrative user must perform for enabling the SAML SSO feature on the Protegrity appliances.

Table 18-3: Setting up SSO

Order	Platform	Step	Reference
1	Appliance Web UI	Add the users that require SAML SSO. Assign **SSO Login** permissions to the required user role. Ensure that the password of the users are changed after the first login to the appliance.	• Adding Users • Adding Roles **Note:** For more information, refer to section *Adding Users to Internal LDAP* and *Managing Roles* in the *Protegrity Appliances Overview Guide 9.1.0.5*.
2	Appliance Web UI	Provide the FQDN and entity ID. This is retrieved from the IdP in which a SAML enterprise application is created for your appliance.	*Importing Users and Assigning Role*
3	Appliance Web UI	Provide the metadata information that is generated on the IdP.	*Importing Users and Assigning Role*

18.2.3.1 Configuring Service Provider (SP) Settings

Before enabling SAML SSO on the appliance, you must provide the following values that are required to connect the appliance with the IdP.

Fully Qualified Domain Name (FQDN)

The FQDN is an address using which the Web UI of the appliance is accessed from the Web browser. While configuring SSO on the IdP, you are required to provide a URL that maps your application on the IdP. Ensure that the URL specified in the IdP matches the FQDN specified on the appliance Web UI. Also, ensure that the IP address of your appliance is resolved to a reachable domain name.

Entity ID

The entity ID is a unique value that identifies your SAML application on the IdP. This value is assigned/generated on the IdP after registering your SAML enterprise application on it.

> **Note:**
>
> The nomenclature of the entity ID might vary between IdPs.

➤ To enter the SP settings:

1. On the appliance Web UI, navigate to **Settings** > **Users** > **Single Sign-On** > **SAML SSO**.
2. Under the **SP Settings** section, enter the FQDN that is resolved to the IP address of the appliance in the **FQDN** text box.
3. Enter the unique value that is assigned to the SAML enterprise application on the IdP in the **Entity ID** text box.
4. If you want to allow access to User Management screen, enable the **Access User Management screen** option.

> **Note:**

> User Management screens require users to provide local user password while performing any operation on it. Enabling this option will require users to remember and provide the password created for the user on the appliance.

5. Click **Save**.
   The SP settings are configured.

18.2.3.2 Configuring IdP Settings

After configuring the the SP settings, you provide the metadata that acts as an important parameter in SAML SSO. The metadata is the chain that links the appliance to the IdP. It is an XML structure that contains information, such as, keys, certificates, and entity ID URL. This information is required for communication between the appliance and IdP. The metadata can be provided in either of the following ways:

- Metadata URL: Provide the URL of the metadata that is retrieved from the IdP.
- Metadata File: Provide the metadata file that is downloaded from the IdP and stored on your system. If you edit the metadata file, then ensure that the information in the metadata is correct before uploading it on the appliance.

➤ To enter the metadata settings:

1. On the appliance Web UI, navigate to **Settings** > **Users** > **Single Sign-On** > **SAML SSO**.
2. Click **Enable** to enable SAML SSO.
3. If the metadata URL is available, under **IdP Settings** section, then select **Metadata URL** from the **Metadata Settings** drop-down list. Enter the URL of the metadata.
4. If the metadata file is downloaded, under **IdP Settings** section, then select **Metadata File** from the **Metadata Settings** drop-down list. Upload the metadata file.
5. If you want to allow access to User Management screen, enable the **Access User Management screen** option.

   > **Note:**
   >
   > User Management screens require users to provide local user password while performing any operation on it. Enabling this option will require users to remember and provide the password created for the user on the appliance.

6. Click **Save**.
   The metadata settings are configured.

   > **Note:**
   >
   > If you upload a new metadata file over the existing file, the changes are overridden by the new file.

18.2.4 Workflow of SAML SSO on an Appliance

After entering all the required data, you are ready to log in to the appliance with SAML SSO. Before explaining the procedure to log in, the general flow of information is illustrated in the following figure.

> **Note:**
>
> You can also login to the appliance without SSO by providing valid user credentials.

Process

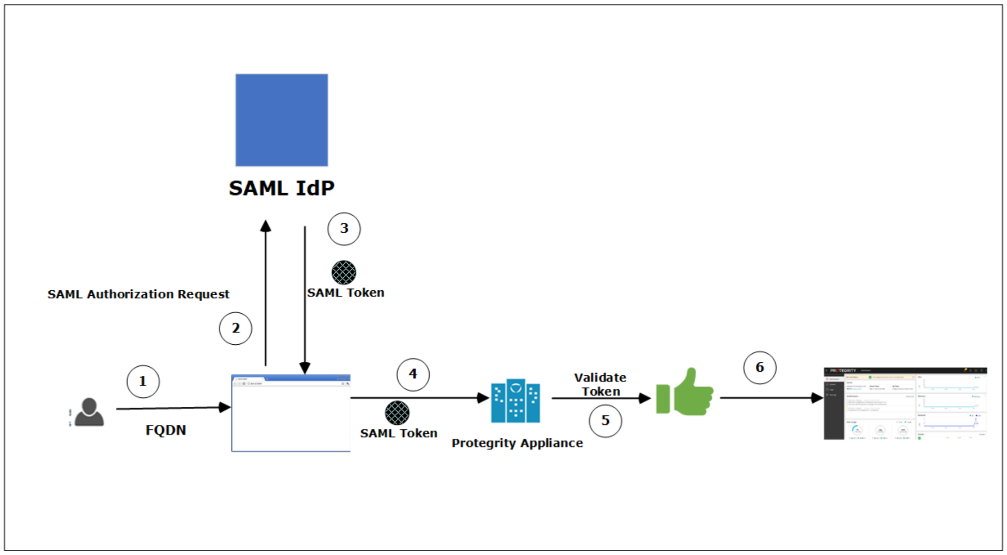


Figure 18-5: SAML SSO Workflow

1. The user provides the FQDN of the appliance on the Web browser.

   For example, the user enters *esa.protegrity.com* and clicks **SAML Single Sign-On**.

   > **Note:**
   >
   > Ensure that the user session on the IdP is active. If the session is idle or inactive, then a screen to enter the IdP credentials will appear.

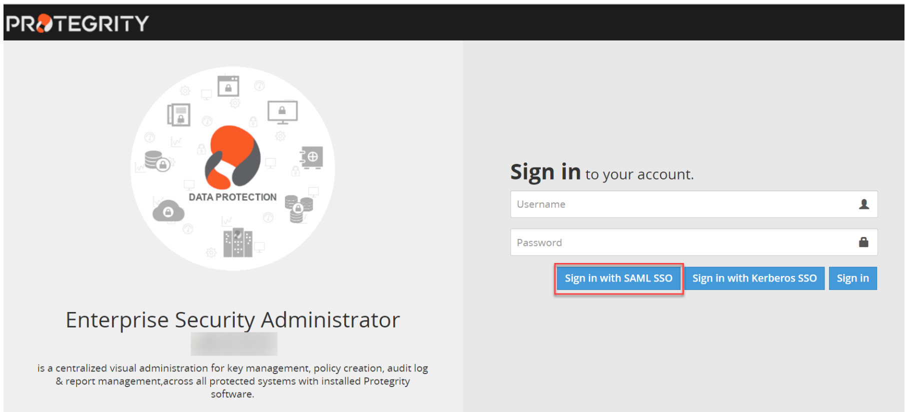
2. The browser generates an authorization request and sends it to the IdP for verification.
3. If user is authorized, then the IdP generates a SAML token and returns it to the Web browser.
4. This SAML token is then provided to the appliance to authenticate the user.
5. The appliance receives the token. If the token is valid, then the permissions of the user are checked.
6. Once these are validated, Web UI of the appliance appears.

18.2.5 Logging on to the Appliance

After configuring the required SSO settings, you can login to the appliance using SSO.

➤ To login to the appliance using SSO:

1. Open the Web browser and enter the FQDN of the ESA or the DSG in the URL.
   The following screen appears.



Enterprise Security Administrator

is a centralized visual administration for key management, policy creation, audit log & report management,across all protected systems with installed Protegrity software.

Figure 18-6: Login Screen

2. Click **Sign in with SAML SSO**.
   The Dashboard of the ESA/DSG appliance appears.

> **Note:**
>
> Ensure that the user session on the IdP is active. If the session is idle or inactive, then a screen to enter the IdP credentials will appear.

18.2.6 Implementing SAML SSO on Azure IdP - An Example

This section provides you a step-by-step sample scenario for implementing SAML SSO on the ESA with the Azure IdP.

Prerequisites

- An ESA v9.1.0.0 is up and running.
- Ensure that the IP address of ESA is resolved to a reachable FQDN.

  For example, resolve the IP address of ESA to *esa.protegrity.com*.
- On the Azure IdP, perform the following steps to retrieve the entity ID and metadata.
  1. Log in to the Azure Portal. Navigate to **Azure Active Directory**. Select the tenant for your organization. Add the enterprise application in the Azure IdP. Note the value of **Application Id** for your enterprise application.

     For more information about creating an enterprise application, refer to *https://docs.microsoft.com/*.
  2. Select **Single sign-on** > **SAML**. Edit the **Basic SAML configuration** and enter the **Reply URL (Assertion Consumer Service URL)**. The format for this text box is *https://<FQDN of the appliance>/Management/Login/SSO/SAML/ACS*.

     For example, the value in the **Reply URL (Assertion Consumer Service URL)** is, *https://esa.protegrity.com/Management/Login/SSO/SAML/ACS*
  3. Under the **SAML Signing Certificate** section, copy the Metadata URL or download the Metadata XML file.
- Users leveraging the SAML SSO feature are available in the Azure IdP tenant.

Steps

1. Log in to ESA as an administrative user. Add all the users for which you want to enable SAML SSO. Assign the roles to the users with the **SSO Login** permission.

   For example, add the user *Sam* from the **User Management** screen on the ESA Web UI. Assign a **Security Administrator** role with **SSO Login** permission to *Sam*.

   > **Note:**

> Ensure that the user *Sam* is present in the Azure AD.

2. Navigate to **Settings** > **Users** > **Single Sign-On** > **SAML Single Sign-On**. In the **Service Provider (SP) settings** section, enter *esa.protegrity.com* and the Appliance ID in the **FQDN** and **Entity ID** text boxes respectively. Click **Save**.
3. In the **Identity Provider (IdP) Settings** section, enter the Metadata URL in the **Metadata Settings** text box. If the Metadata XML file is downloaded on your system, then upload it. Click **Save**.
4. Select the **Enable** option to enable SAML SSO.
5. If you want to allow access to User Management screen, enable the **Access User Management screen** option.
6. Log out from ESA.
7. Open a new Web browser session. Log in to the Azure portal as *Sam* with the IdP credentials.
8. Open another session on the Web browser and enter the FQDN of ESA. For example, *esa.protegrity.com*.

> **Note:**
>
> Ensure that the user session on the IdP is active. If the session is idle or inactive, then a screen to enter the IdP credentials will appear.

9. Click **Sign in with SAML SSO**. You are automatically directed to the **ESA Dashboard** without providing the user credentials.

18.2.7 Implementing SSO with a Load Balancer Setup

This section describes the process of implementing SSO with a Load Balancer that is setup between the appliances.

Steps to configure SSO in a Load Balancer setup

Consider two appliances, *L1* and *L2*, that are configured behind a load balancer. Ensure that you perform the following steps to implement it.

1. Add the users to the internal LDAP and assign SSO login permissions.
2. Ensure that the FQDN is resolved to the IP address of the load balancer.

Logging in with SSO

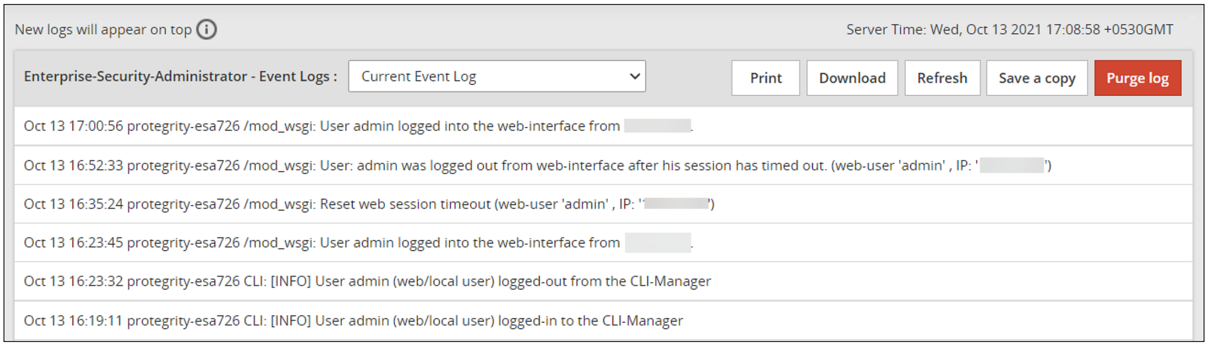
After configuring the required settings, the user enters the FQDN of load balancer on the Web browser and clicks **Sign in with SAML SSO** to access it. On successful authentication, the appliance Dashboard appears.

18.2.8 Viewing Logs

You can view the logs that are generated for when the SAML SSO mechanism is utilized. The logs are generated for the following events:

- Uploading the metadata
- User logging to the appliance through SAML SSO
- Enabling or disabling SAML SSO
- Configuring the Service Provider and IdP settings

Navigate to **Logs** > **Appliance Logs** to view the logs. The following figure displays the logs for SAML SSO.


New logs will appear on top
Server Time: Wed, Oct 13 2021 17:08:58 +0530GMT
Enterprise-Security-Administrator - Event Logs :
Current Event Log
Print
Download
Refresh
Save a copy
Purge log

```
Oct 13 17:00:56 protegrity-esa726 /mod_wsgi: User admin logged into the web-interface from [redacted].
Oct 13 16:52:33 protegrity-esa726 /mod_wsgi: User: admin was logged out from web-interface after his session has timed out. (web-user 'admin' , IP: '[redacted]')
Oct 13 16:35:24 protegrity-esa726 /mod_wsgi: Reset web session timeout (web-user 'admin' , IP: '[redacted]')
Oct 13 16:23:45 protegrity-esa726 /mod_wsgi: User admin logged into the web-interface from [redacted].
Oct 13 16:23:32 protegrity-esa726 CLI: [INFO] User admin (web/local user) logged-out from the CLI-Manager
Oct 13 16:19:11 protegrity-esa726 CLI: [INFO] User admin (web/local user) logged-in to the CLI-Manager
```

Figure 18-7: Appliance Logs

You can also navigate on the **Insight Analytics** screen to view the logs.

18.2.9 Feature Limitations

This section covers some known limitations of the SAML SSO feature.

- The *Configuration export to Cluster Tasks* and *Export data configuration to remote appliance* of the SAML SSO settings are not supported. The SAML SSO settings include the hostname, so importing the SAML settings on another machine will replace the hostname.

> **Note:**
>
> For more information, refer to section *Configuration export to Cluster Tasks* and *Export data configuration to remote appliance* in the *Protegrity Appliances Overview Guide 9.1.0.5*.

- After logging in to the appliance through SAML SSO, if you have the **Directory Manager** permissions, you can access the User Management screen. A prompt to enter the user password appears after a user management operation is performed on it. In this case, you must enter the password that you have set on the appliance. The password that is set on the IdP is not applicable here.

18.2.10 Troubleshooting

This section describes the issues and their solutions while utilizing the SAML SSO mechanism.

Table 18-4: SAML SSO Troubleshooting

Issue	Reason	Solution
The following message appears while logging in with SSO. `Login Failure: Unauthorized to SSO Login.`	• Username is not present in the internal LDAP • Username does not have roles assigned to it • Role that is assigned to the user does not have **SSO Login** permission .	Ensure that the following points are considered: • The user is imported to the internal LDAP. • Th role assigned to the user has **SSO Login** permission enabled. For more information about configuring user role, refer to section *Importing Users and assigning role*.