



Protegrity Appliances Overview Guide 9.1.0.5

Created on: Nov 19, 2024

Copyright

Copyright © 2004-2024 Protegry Corporation. All rights reserved.

Protegry products are protected by and subject to patent protections;

Patent: <https://www.protegry.com/patents>.

Protegry logo is the trademark of Protegry Corporation.

NOTICE TO ALL PERSONS RECEIVING THIS DOCUMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Utimaco Safeware AG is a member of the Sophos Group.

Xen, XenServer, and Xen Source are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

VMware, the VMware “boxes” logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Amazon Web Services (AWS) and AWS Marks are the registered trademarks of Amazon.com, Inc. in the United States and other countries.

HP is a registered trademark of the Hewlett-Packard Company.

HPE Ezmeral Data Fabric is the trademark of Hewlett Packard Enterprise in the United States and other countries.

Dell is a registered trademark of Dell Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

POSIX is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc.

Mozilla and Firefox are registered trademarks of Mozilla foundation.

Chrome and Google Cloud Platform (GCP) are registered trademarks of Google Inc.

Table of Contents

Copyright.....	2
Chapter 1 Introduction to this Guide.....	12
1.1 Sections contained in this Guide.....	12
1.2 Accessing the Protegity documentation suite.....	13
1.2.1 Viewing product documentation.....	13
1.2.2 Downloading product documentation.....	14
Chapter 2 Protegity Appliance Overview.....	15
Chapter 3 Command-Line Interface (CLI) Manager.....	16
3.1 Accessing the CLI Manager.....	16
3.2 CLI Manager Structure Overview.....	17
3.2.1 CLI Manager Main Screen.....	19
3.2.2 CLI Manager Navigation.....	19
3.3 Working with Status and Logs.....	20
3.3.1 Monitoring System Statistics.....	21
3.3.2 Viewing the Top Processes.....	21
3.3.3 Working with System Statistics (SYSSTAT).....	21
3.3.4 Auditing Service.....	22
3.3.5 Viewing Appliance Logs.....	24
3.3.6 Viewing User Notifications.....	25
3.4 Working with Administration.....	26
3.4.1 Working with Services.....	27
3.4.2 Setting Date and Time.....	28
3.4.3 Managing Accounts and Passwords	30
3.4.3.1 OS Users in Appliances.....	30
3.4.3.2 Strengthening Password Policy.....	30
3.4.3.3 Changing Current Password.....	32
3.4.3.4 Resetting Directory Account Passwords.....	33
3.4.3.5 Changing the Root User Password.....	33
3.4.3.6 Changing the Local Admin Account Password.....	33
3.4.3.7 Changing the Local Admin Account Permission.....	34
3.4.3.8 Changing Service Accounts Passwords.....	34
3.4.3.9 Managing Local OS Users.....	35
3.4.4 Working with Backup and Restore.....	36
3.4.4.1 Exporting Data Configuration to Local File.....	37
3.4.4.2 Exporting Data or Configuration to Remote Appliance.....	40
3.4.4.3 Importing Data/Configurations from a File.....	41
3.4.4.4 Reviewing Exported Files and Logs.....	41
3.4.4.5 Deleting Exported Files and Logs.....	42
3.4.4.6 Backing Up/Restoring Local Backup Partition.....	42
3.4.5 Setting Up the Email Server.....	45
3.4.6 Working with Azure AD.....	46
3.4.6.1 Configuring Azure AD Settings.....	46
3.4.6.2 Enabling/Disabling Azure AD.....	48
3.4.7 Accessing REST API Resources.....	48
3.4.7.1 Using Basic Authentication.....	49
3.4.7.2 Using Client Certificates.....	49
3.4.7.3 Using JSON Web Token (JWT).....	50
3.4.8 Securing the GRand Unified Bootloader (GRUB).....	53
3.4.8.1 Enabling the Credentials for the GRUB Menu.....	53
3.4.8.2 Disabling the GRUB Credentials.....	55
3.4.9 Working with Installations and Patches.....	55
3.4.9.1 Add/Remove Services.....	55



3.4.9.2 Uninstalling Products.....	57
3.4.9.3 Managing Patches.....	57
3.4.10 Managing LDAP	59
3.4.10.1 Working with the Protegity LDAP Server.....	59
3.4.10.2 Changing the Bind User Password.....	61
3.4.10.3 Working with Proxy Authentication.....	63
3.4.10.4 Configuring Local LDAP Settings.....	65
3.4.10.5 Monitoring Local LDAP.....	66
3.4.10.6 Optimizing Local LDAP Settings.....	66
3.4.11 Rebooting and Shutting down.....	67
3.4.12 Accessing the OS Console.....	67
3.5 Working with Networking.....	67
3.5.1 Configuring Network Settings.....	68
3.5.1.1 Changing Hostname.....	69
3.5.1.2 Configuring Management IP Address.....	69
3.5.1.3 Configuring Default Route.....	70
3.5.1.4 Configuring Domain Name.....	70
3.5.1.5 Configuring Search Domain.....	70
3.5.1.6 Configuring Name Server.....	70
3.5.1.7 Assigning a Default Gateway to the NIC.....	71
3.5.1.8 Selecting Management NIC.....	71
3.5.1.9 Changing the management IP on ethMNG.....	71
3.5.1.10 Identifying an Interface.....	72
3.5.1.11 Adding a service interface address.....	72
3.5.2 Configuring SNMP.....	73
3.5.2.1 Configuring SNMPv3 as a USM Model.....	75
3.5.2.2 Configuring SNMPv3 as a TSM Model.....	76
3.5.3 Working with Bind Services and Addresses.....	76
3.5.3.1 Binding Interface for Management.....	77
3.5.3.2 Binding Interface for Services.....	78
3.5.4 Using Network Troubleshooting Tools.....	78
3.5.5 Managing Firewall Settings.....	79
3.5.5.1 Adding a New Rule with Predefined List of Functionality.....	81
3.5.6 Using the Management Interface Settings.....	82
3.5.7 Ports Allowlist.....	82
3.6 Working with Tools.....	83
3.6.1 Configuring the SSH.....	84
3.6.1.1 Specifying SSH Mode.....	85
3.6.1.2 Setting Up Advanced SSH Configuration.....	85
3.6.1.3 Managing SSH Known Hosts.....	86
3.6.1.4 Managing Authorized Keys.....	86
3.6.1.5 Managing Identities.....	86
3.6.1.6 Generating SSH Keys.....	86
3.6.1.7 Configuring the SSH.....	86
3.6.1.8 Customizing the SSH Configurations.....	88
3.6.1.9 Exporting/Importing the SSH Settings.....	88
3.6.1.10 Securing SSH Communication.....	89
3.6.2 Clustering Tool.....	90
3.6.2.1 Creating a TAC using the CLI Manager.....	90
3.6.2.2 Joining an Existing Cluster using the CLI Manager.....	91
3.6.2.3 Cluster Operations.....	92
3.6.2.4 Managing a Site.....	94
3.6.2.5 Node Management.....	96
3.6.2.6 Trusted Appliances Cluster.....	103
3.6.3 Working with Xen Paravirtualization Tool.....	105
3.6.4 Working with the File Integrity Monitor Tool.....	105
3.6.5 Rotating Appliance OS Keys.....	105
3.6.6 Managing Removable Drives.....	108



3.6.6.1 Disabling CD or DVD drive.....	108
3.6.6.2 Disabling USB Flash Drive.....	108
3.6.6.3 Enabling CD or DVD Drive.....	109
3.6.6.4 Enabling USB Flash Drive.....	109
3.6.7 Tuning the Web Services.....	109
3.6.8 Tuning the Service Dispatcher	110
3.6.9 Working with Antivirus.....	111
3.6.9.1 Customizing Antivirus Scan Options from the CLI.....	111
3.7 Working with Preferences.....	112
3.7.1 Viewing System Monitor on OS Console.....	113
3.7.2 Setting Password Requirements for CLI System Tools.....	113
3.7.3 Viewing user notifications on CLI load.....	113
3.7.4 Minimizing the Timing Differences.....	113
3.7.5 Setting a Uniform Response Time.....	113
3.7.6 Limiting Incorrect <i>root</i> Login.....	114
3.7.7 Enabling Mandatory Access Control.....	114
Chapter 4 Web User Interface (Web UI) Management.....	115
4.1 Working with the Web UI.....	116
4.2 Logging Out of Appliance Web UI.....	117
4.3 Shutting down the Appliance.....	118
4.4 Description of Appliance Web UI.....	119
4.4.1 Support.....	121
4.4.2 Extending Timeout from Appliance.....	122
4.5 Viewing User Notifications.....	123
4.6 Web Interface Auto-Refresh Mode.....	123
4.7 Working with System.....	123
4.7.1 Working with Services.....	124
4.7.1.1 Logfacade Services.....	124
4.7.1.2 Meteringfacade Service.....	124
4.7.2 Viewing System Information.....	125
4.7.3 Viewing System Statistics.....	126
4.7.4 Viewing Performance Graphs.....	126
4.7.5 Working with Trusted Appliances Cluster.....	127
4.7.6 Working with System Backup and Restore.....	128
4.7.6.1 Backing Up Data.....	128
4.7.6.2 Exporting Configuration to Cluster.....	130
4.7.6.3 Scheduling Configuration Export to Cluster Tasks.....	131
4.7.6.4 Exporting Custom Files.....	131
4.7.6.5 Restoring Configurations.....	139
4.7.6.6 Working with OS Full Backup and Restore.....	139
4.7.6.7 Viewing Export/Import Logs.....	140
4.7.7 Scheduling Appliance Tasks.....	140
4.7.7.1 Creating a Scheduled Task.....	141
4.7.7.2 Basic Properties.....	141
4.7.7.3 Customizing Frequency.....	142
4.7.7.4 Execution.....	143
4.7.7.5 Restrictions.....	144
4.7.7.6 Logging.....	144
4.8 Working with Logs.....	144
4.8.1 Viewing Web Services Engine Logs.....	144
4.8.2 Viewing Service Dispatcher Logs.....	145
4.8.3 Viewing Appliance Logs.....	146
4.9 Working with Settings.....	148
4.9.1 Working with Antivirus.....	148
4.9.1.1 Customizing Antivirus Scan Options.....	148
4.9.1.2 Scheduling AntiVirus Scan.....	148
4.9.1.3 Updating the Antivirus Database.....	149



4.9.1.4 Viewing AntiVirus Logs.....	150
4.9.2 Configuring Appliance Two Factor Authentication.....	151
4.9.2.1 Configuring Two Factor Authentication with Automatic Per User Shared Secret.....	152
4.9.2.2 Configuring Two Factor Authentication with Host-Based Shared-Secret.....	154
4.9.2.3 Working with Remote Authentication Dial-up Service (RADIUS) Authentication.....	155
4.9.2.4 Working with Shared-Secret Lifecycle.....	158
4.9.2.5 Logging in Using Appliance Two Factor Authentication.....	159
4.9.2.6 Disabling Appliance Two Factor Authentication.....	160
4.9.3 Working with File Integrity.....	160
4.9.4 Working with Files.....	161
4.9.4.1 Viewing a Configuration File.....	163
4.9.4.2 Uploading a Configuration File.....	164
4.9.4.3 Modifying a Configuration File.....	164
4.9.4.4 Deleting a Configuration File.....	164
4.9.4.5 Resetting a File.....	165
4.9.5 Managing Upload Files.....	165
4.9.6 Configuring Date and Time.....	166
4.9.7 Configuring Email.....	167
4.9.8 Configuring Network Settings.....	169
4.9.8.1 Managing Network Interfaces.....	169
4.9.8.2 NIC Bonding.....	170
4.9.9 Configuring Web Settings.....	174
4.9.9.1 General Settings.....	174
4.9.9.2 Session Management.....	175
4.9.9.3 Fixing the Session Timeout.....	176
4.9.9.4 Shell In A Box Settings.....	177
4.9.9.5 SSL Cipher Settings.....	178
4.9.9.6 Updating a Protocol from the ESA Web UI.....	178
4.9.10 Working with Secure Shell (SSH) Keys.....	179
4.9.10.1 Configuring the SSH Key.....	181
4.10 Managing Appliance Users.....	190
4.11 Password Policy for the LDAP Users.....	191
4.11.1 Managing Users.....	191
4.11.1.1 Adding Users to Internal LDAP.....	194
4.11.1.2 Importing Users to Internal LDAP.....	195
4.11.1.3 Password Policy Configuration.....	196
4.11.1.4 Editing Users.....	198
4.11.2 Managing Roles.....	199
4.11.2.1 Adding a Role.....	201
4.11.3 Configuring the Proxy Authentication Settings.....	202
4.11.4 Working with External Groups.....	204
4.11.4.1 Adding an External Group.....	206
4.11.4.2 Editing an External Group.....	208
4.11.4.3 Deleting an External Group.....	208
4.11.4.4 Synchronizing the External Group.....	209
4.11.5 Configuring the Azure AD Settings.....	210
4.11.5.1 Importing Azure Users.....	211
4.11.5.2 Working with External Azure Groups.....	213
Chapter 5 Trusted Appliances Cluster (TAC).....	216
5.1 TAC Topology.....	216
5.2 Cluster Configuration Files.....	217
5.3 Deploying Appliances in a Cluster.....	218
5.4 Cluster Security.....	222
5.5 Reinstalling Cluster Services.....	224
5.6 Uninstalling Cluster Services.....	224
5.7 FAQs on TAC.....	225
5.8 Creating a TAC using the Web UI.....	226



5.9 Joining an Existing Cluster using the Web UI.....	227
5.10 Connection Settings.....	229
5.10.1 Connection Settings for Nodes.....	229
5.11 Managing Communication Methods for Local Node.....	230
5.11.1 Adding a Communication Method from the Web UI.....	231
5.11.2 Editing a Communication Method from the Web UI.....	231
5.11.3 Deleting a Communication Method from the Web UI.....	231
5.12 Viewing Cluster Information.....	232
5.13 Removing a Node from the Cluster using the Web UI.....	232
Chapter 6 Appliance Virtualization.....	234
6.1 Xen Paravirtualization Setup.....	234
6.1.1 Pre-Conversion Tasks.....	235
6.1.1.1 System Check.....	235
6.1.1.2 Interface Check.....	235
6.1.1.3 System Backup.....	235
6.1.1.4 Backup and Restore.....	237
6.1.2 Paravirtualization Process.....	237
6.1.2.1 Starting Appliance Paravirtualization Support Tool.....	237
6.1.2.2 Enabling Paravirtualization.....	238
6.1.2.3 Configuring Host for PVM.....	238
6.1.2.4 Rebooting Appliance for PVM.....	240
6.1.2.5 Disabling Paravirtualization.....	241
6.2 Xen Server Configuration.....	241
6.2.1 Appliance Configuration Files for PVM.....	241
6.2.2 Xen Server Parameters for PVM.....	242
6.2.3 Manual Configuration of Xen Server.....	242
6.2.3.1 Converting HVM to PVM.....	242
6.2.3.2 Converting PVM to HVM.....	242
6.3 Installing Xen Tools.....	243
6.4 Xen Source – Xen Community Version.....	243
6.4.1 HVM Configuration.....	244
6.4.2 PVM Configuration.....	244
6.4.3 Virtual Appliance.....	244
6.4.4 Paravirtualization FAQ and Troubleshooting.....	245
Chapter 7 Appliance Hardening.....	246
7.1 Linux Kernel.....	246
7.2 Restricted Logins.....	247
7.3 Enhanced Logging.....	248
7.4 Open Listening Ports.....	248
7.5 Configuring User Limits.....	256
7.6 Packages and Services.....	257
Chapter 8 VMware Tools in Appliances.....	258
Chapter 9 System Requirements.....	259
Chapter 10 Increasing the Appliance Disk Size.....	260
10.1 Configuration of Appliance for Adding More Disks.....	260
10.2 Installation of Additional Hard Disks.....	260
10.3 Rolling Back Addition of New Hard Disks.....	261
Chapter 11 Extending the Size of the OS Partition.....	262

11.1 Starting in Single User Mode.....	264
11.2 Creating a Partition.....	265
11.3 Extending the OS and the Backup Volume.....	267
11.4 Extending the Logs Volume.....	268
Chapter 12 Mandatory Access Control (MAC).....	269
12.1 Viewing Status of Profiles.....	270
12.2 Creating a Profile.....	271
12.3 Setting a Profile on Complain Mode.....	273
12.4 Setting a Profile on Enforce Mode.....	273
12.5 Analyzing Events.....	274
12.6 Modifying an Existing Profile.....	275
12.7 AppArmor Permissions.....	276
12.8 Troubleshooting for AppArmor.....	277
Chapter 13 Accessing Appliances using Single Sign-On (SSO).....	279
13.1 What is Kerberos.....	279
13.1.1 Implementing Kerberos SSO for Protegity Appliances.....	280
13.1.1.1 Prerequisites.....	280
13.1.1.2 Setting up Kerberos SSO.....	280
13.1.1.3 Logging to the Appliance.....	284
13.1.1.4 Scenarios for Implementing Kerberos SSO.....	284
13.1.1.5 Viewing Logs.....	288
13.1.1.6 Feature Limitations.....	289
13.1.1.7 Troubleshooting.....	289
13.1.2 What is SAML.....	289
13.2.1 Implementing SAML SSO for Protegity Appliances.....	290
13.2.2 Prerequisites.....	290
13.2.3 Setting up SAML SSO.....	290
13.2.3.1 Configuring Service Provider (SP) Settings.....	291
13.2.3.2 Configuring IdP Settings.....	291
13.2.4 Workflow of SAML SSO on an Appliance.....	292
13.2.5 Logging on to the Appliance.....	293
13.2.6 Implementing SAML SSO on Azure IdP - An Example.....	293
13.2.7 Implementing SSO with a Load Balancer Setup.....	294
13.2.8 Viewing Logs.....	295
13.2.9 Feature Limitations.....	295
13.2.10 Troubleshooting.....	295
Chapter 14 Appendix: Sample External Directory Configurations.....	297
14.1 Sample AD configuration.....	297
14.2 Sample ODSEE configuration.....	298
14.3 Sample SAML Configuration.....	298
14.4 Sample Kerberos Configuration.....	299
14.5 Sample Azure AD Configuration.....	299
Chapter 15 Installing Protegity Appliances on Cloud Platforms.....	300
Appendix 15.1 Installing Protegity Appliances on Amazon Web Services (AWS).....	301
15.1.1 Verifying Prerequisites	302
15.1.1.1 Prerequisites.....	302
15.1.1.2 Hardware Requirements.....	302
15.1.1.3 Network Requirements.....	302
15.1.1.3.1 Accessing the Internet.....	302
15.1.1.3.2 Accessing a Corporate Network.....	303



15.1.2 Obtaining the AMI.....	303
15.1.3 Loading the Protegity Appliance from an Amazon Machine Image (AMI).....	306
15.1.3.1 Creating an Instance of the Protegity Appliance from the AMI.....	306
15.1.3.2 Configuring the Virtual Private Cloud (VPC).....	308
15.1.3.3 Adding a Subnet to the Virtual Private Cloud (VPC).....	309
15.1.3.4 Finalizing the Installation of Protegity Appliance on the Instance.....	309
15.1.3.4.1 Logging in and Finalising the AWS Instance using the SSH Client.....	310
15.1.3.5 Connecting to an ESA instance (for DSG deployment).....	312
15.1.3.5.1 Deploying the Instance of the Protegity Appliance with the Protectors.....	312
15.1.4 Backing up and Restoring Data on AWS.....	312
15.1.4.1 Creating a Snapshot of a Volume on AWS.....	312
15.1.4.2 Restoring a Snapshot on AWS.....	313
15.1.5 Increasing Disk Space on the Appliance.....	314
15.1.6 Best Practices for Using Protegity Appliances on AWS.....	315
15.1.7 Running the Appliance-Rotation-Tool.....	315
15.1.8 Working with Cloud-based Applications.....	317
15.1.8.1 Prerequisites.....	317
15.1.8.2 Configuring Access for AWS Resources.....	318
15.1.8.2.1 AWS Configure.....	319
15.1.8.2.2 Configuring AWS Services.....	319
15.1.8.3 Working with CloudWatch Console.....	321
15.1.8.3.1 Prerequisites.....	321
15.1.8.3.2 Integrating CloudWatch with Protegity Appliance.....	322
15.1.8.3.3 Configuring Custom Logs on AWS CloudWatch Console.....	323
15.1.8.3.4 Toggling the CloudWatch Service.....	325
15.1.8.3.5 Reloading the AWS CloudWatch Integration.....	326
15.1.8.3.6 Viewing Logs on AWS CloudWatch Console.....	326
15.1.8.3.7 Working with AWS CloudWatch Metrics.....	327
15.1.8.3.8 Viewing Metrics on AWS CloudWatch Console.....	327
15.1.8.3.9 Disabling AWS CloudWatch Integration.....	328
15.1.8.4 Working with the AWS Cloud Utility.....	329
15.1.8.4.1 Storing Backup Files on the AWS S3 Bucket.....	329
15.1.8.4.2 Set Metrics Based Alarms Using the AWS Management Console.....	332
15.1.8.5 FAQs for AWS Cloud Utility.....	337
15.1.8.6 Working with AWS Systems Manager.....	339
15.1.8.6.1 Prerequisites.....	339
15.1.8.6.2 Setting up AWS Systems Manager.....	339
15.1.8.6.3 FAQs on AWS Systems Manager.....	341
15.1.8.7 Troubleshooting for the AWS Cloud Utility.....	341

Appendix 15.2 Installing Protegity Appliances on Azure.....	344
15.2.1 Prerequisites.....	345
15.2.1.1 Hardware Requirements.....	345
15.2.1.2 Network Requirements.....	345
15.2.2 Azure Cloud Utility.....	345
15.2.3 Setting up Azure Virtual Network.....	346
15.2.4 Creating a Resource Group.....	346
15.2.5 Creating a Storage Account.....	346
15.2.6 Creating a Container.....	346
15.2.7 Obtaining the Azure BLOB.....	347
15.2.8 Creating Image from the Azure BLOB.....	349
15.2.9 Creating a VM from the Image.....	350
15.2.10 Accessing the Appliance.....	351
15.2.11 Finalizing the Installation of Protegity Appliance on the Instance.....	351
15.2.11.1 Finalizing ESA Installation.....	351
15.2.12 Accelerated Networking.....	353
15.2.12.1 Prerequisites.....	355
15.2.12.2 Supported Instance Sizes for Accelerated Networking.....	356



15.2.12.3 Creating a Virtual Machine with Accelerated Networking Enabled.....	356
15.2.12.4 Enabling Accelerated Networking.....	357
15.2.12.5 Disabling Accelerated Networking.....	357
15.2.12.6 Troubleshooting and FAQs for Azure Accelerated Networking.....	358
15.2.13 Backing up and Restoring VMs on Azure.....	360
15.2.13.1 Backing up and Restoring using Snapshots of Disks.....	360
15.2.13.1.1 Creating a Snapshot of a Virtual Machine on Azure.....	360
15.2.13.1.2 Restoring from a Snapshot on Azure.....	361
15.2.13.2 Backing up and Restoring using Recovery Services Vaults.....	362
15.2.13.2.1 Creating Recovery Services Vaults.....	362
15.2.13.2.2 Backing up Virtual Machine using Recovery Services Vault.....	363
15.2.13.2.3 Restoring a Virtual Machine using Recovery Services Vaults.....	363
15.2.14 Connecting to an ESA Instance.....	365
15.2.15 Deploying the Protegity Appliance Instance with the Protectors.....	365

Appendix 15.3 Installing Protegity Appliances on Google Cloud Platform (GCP)..... 366

15.3.1 Verifying Prerequisites	366
15.3.1.1 Prerequisites.....	367
15.3.1.2 Hardware Requirements.....	367
15.3.1.3 Network Requirements.....	367
15.3.2 Configuring the Virtual Private Cloud (VPC).....	367
15.3.2.1 Adding a Subnet to the Virtual Private Cloud (VPC).....	368
15.3.3 Obtaining the GCP Image.....	369
15.3.4 Converting the Raw Disk to a GCP Image.....	371
15.3.5 Loading the Protegity Appliance from a GCP Image.....	372
15.3.5.1 Creating a VM Instance from an Image.....	372
15.3.5.2 Creating a VM Instance from a Disk.....	373
15.3.5.2.1 Creating a Disk from the GCP Image.....	373
15.3.5.2.2 Creating a VM Instance from a Disk.....	374
15.3.5.3 Accessing the Appliance.....	375
15.3.6 Finalizing the Installation of Protegity Appliance on the Instance.....	375
15.3.6.1 Finalizing ESA Installation.....	375
15.3.7 Connecting to an ESA instance (for DSG deployment).....	377
15.3.8 Deploying the Instance of the Protegity Appliance with the Protectors.....	378
15.3.9 Backing up and Restoring Data on GCP.....	378
15.3.9.1 Creating a Snapshot of a Disk on GCP.....	378
15.3.9.2 Restoring from a snapshot on GCP.....	379
15.3.10 Increasing Disk Space on the Appliance.....	379

Chapter 1

Introduction to this Guide

1.1 Sections contained in this Guide

1.2 Accessing the Protegility documentation suite

This guide provides an overview of the Protegility Appliances and the common features in the Appliances.

The Appliance is a software provided to the user. The package includes the Linux OS, that is used to run the Protegility Appliance, and the Appliance itself. The major role of the Appliance is that of maintaining secure policies and certificates that in turn help secure user data.

The following four guides provide the details of features specific to each Appliance:

- *Protegility Enterprise Security Administrator Guide 9.1.0.5*
- *Protegility Data Security Gateway User Guide 3.1.0.5*

If you are new to working with Protegility appliances, then we recommend you read the preceding documents first.

New users should go through the *Master Index Document 9.1.0.5* for more information on how the documents are designed and the information contained in each document.

1.1 Sections contained in this Guide

The guide is broadly divided into the following sections:

- *Section 1 Introduction to this Guide* defines the purpose and scope for this Guide. In addition, it explains how information is organized in this Guide.
- *Section 2 Protegility Appliance Overview* introduces the four Protegility Appliances.
- *Section 3 CLI Manager* describes the Appliance CLI. Detailed steps for performing tasks such as, the maintenance and logs/status features, and monitoring the system statistics, and so on, are provided. The CLI duplicates many features available in the Web UI of the Appliance.
- *Section 4 Web User Interface (Web UI) Management* familiarizes you with the regular login procedures, Policy Management (in ESA), configuring High Availability and SSH, among others.
- *Section 5 Trusted Appliances Cluster* explains how to configure the trusted appliance feature in your system.
- *Section 6 Appliance Virtualization* deals with the details of appliance virtualization.
- *Section 7 Appliance Hardening* describes the concept of how the kernels, logins and TCP ports are tweaked to make the Appliances secure.
- *Section 8 VMware Tools in Appliances* provides the information for VMware tools on appliances.
- *Section 9 System Requirements* describes the hardware requirements for the appliances.
- *Section 10 Increasing the Appliance Disk Size* includes details about how additional disk space can be added and provisioned, as required in a deployed ESA.

- [Section 11 Extending the Size of the OS Partition](#) describes how to extend the root partition.
- [Section 12 Mandatory Access Control MAC](#)
- [Section 13 Accessing Appliances using Single Sign-On \(SSO\)](#)
- [Section 14 Appendix: Sample External Directory Configurations](#) describes the parameters that you must configure to connect with an external directory.
- [Section 15 Installing Protegility Appliances on Cloud Platforms](#) explains how to install appliances on cloud platforms.

1.2 Accessing the Protegility documentation suite

This section describes the methods to access the *Protegility Documentation Suite* using the [My.Protegility](#) portal.

1.2.1 Viewing product documentation

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

1. Log in to the [My.Protegility](#) portal.
2. Click **Resources > Product Documentation**.
3. Click a product version.
The documentation appears.

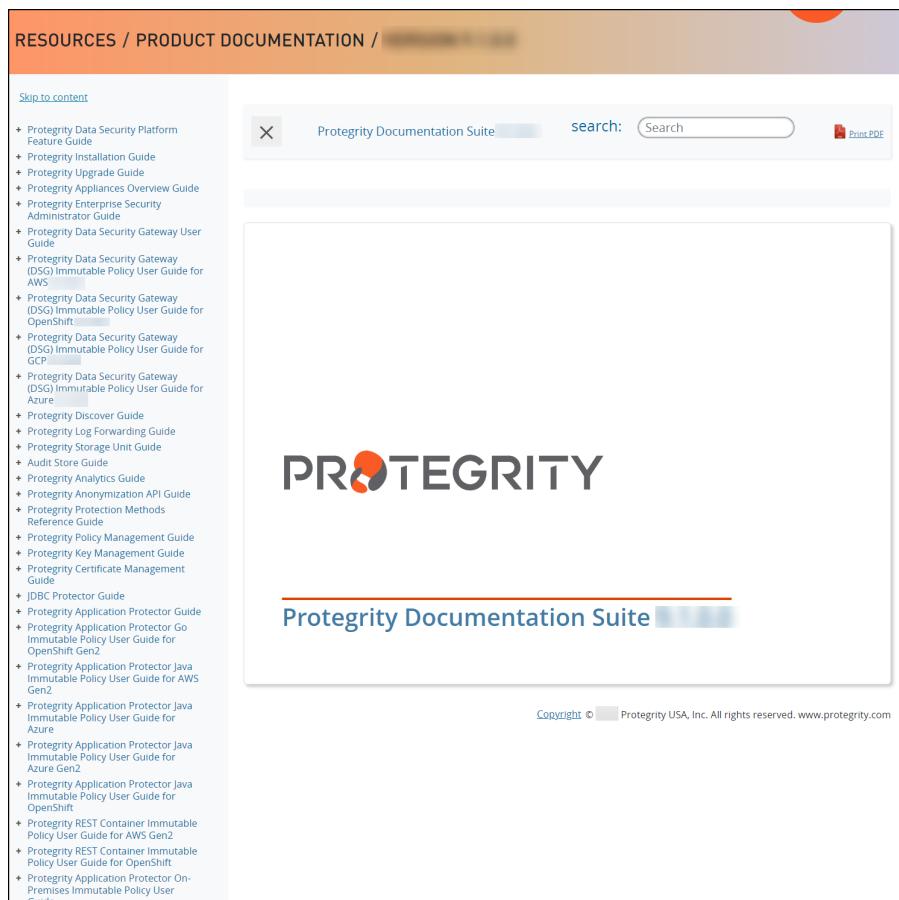


Figure 1-1: Documentation

4. Expand and click the link for the required documentation.
5. If required, then enter text in the **Search** field to search for keywords in the documentation.

The search is dynamic, and filters results while you type the text.

6. Click the **Print PDF** icon from the upper-right corner of the page.
The page with links for viewing and downloading the guides appears. You can view and print the guides that you require.

1.2.2 Downloading product documentation

This section explains the procedure to download the product documentation from the [*My.Protegity*](#) portal.

1. Click **Product Management > Explore Products**.

2. Select **Product Documentation**.

The **Explore Products** page is displayed. You can view the product documentation of various Protegity products as per their releases, containing an overview and other guidelines to use these products at ease.

3. Click **View Products** to advance to the product listing screen.

4. Click the **View** icon (ⓘ) from the **Action** column for the row marked **On-Prem** in the **Target Platform Details** column.

If you want to filter the list, then use the filters for: **OS**, **Target Platform**, and **Search** fields.

5. Click the icon for the action that you want to perform.

Chapter 2

Protegility Appliance Overview

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

All Protegility 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.

The following guides provide the details of features specific to each Appliance:

- Protegility Enterprise Security Administrator Guide
- Data Security Gateway User Guide

An organization can use a mix of these mandatory and may-use methods to secure data.

Chapter 3

Command-Line Interface (CLI) Manager

- [3.1 Accessing the CLI Manager](#)
- [3.2 CLI Manager Structure Overview](#)
- [3.3 Working with Status and Logs](#)
- [3.4 Working with Administration](#)
- [3.5 Working with Networking](#)
- [3.6 Working with Tools](#)
- [3.7 Working with Preferences](#)

Command-Line Interface (CLI) Manager is a Protegility Platform tool for managing Protegility appliances. CLI Manager is a text-based environment for managing status, administration, configuration, preferences, and networking of your appliance. This section describes how to login to CLI Manager, and its many features.

Note: The File Protector(FP) are certified for version 6.6.4.

3.1 Accessing the CLI Manager

You log onto the CLI Manager to manage the appliance settings and monitor your appliance. The CLI Manager is available using any of the following text consoles:

- Direct connection using local keyboard and video
- Serial connection using an RS232 console cable
- Network connection using a Secure Shell (SSH port 22) connection to the appliance management IP address.

► To log on to the CLI Manager:

1. From the Web UI pane, click the window that appears at the bottom right.
A new CLI window opens.
2. At the prompt, type the admin login credentials set during appliance installation.
3. Press ENTER.

The CLI Manager main screen appears.

Note: When you login through the CLI or the Web UI for the first time, with the password policy enabled, the *Update Password* screen appears. It is recommended that you change the password since the administrator sets the initial password.

Note:

If you are a user associated to Shell Accounts role with Shell(non-CLI) Access permissions, you cannot access the Web UI or CLI, except when you have the password policy enabled and are required to change the password through Web UI.

For more information about configuring the password policy, refer to section [Password Policy Configuration](#).

3.2 CLI Manager Structure Overview

There are five main system menus in the CLI Manager which are common for Protegity appliances:

- Status and Logs
- Administration
- Networking
- Tools
- Preferences

Status and Logs

Status and Logs menu includes four options that make the analysis of logs easier.

- System Monitor tool with real-life information on the CPU, network, and disk usage.
- Top Processes view having a list of 10 top memory and CPU users. The information is updated periodically.
- Appliance Logs tool, divided into subcategories. These can be appliance common logs and appliance specific logs. Thus, you can view system event logs that relate to, for example, syslog, installation, kernel and pepdispatcher logs, and web services engine logs which are common for all four Protegity appliances.
- PEP Server logs are DSG-specific. Logging and Reporting, and Policy Management logs are ESA specific. Distributed Filesystem File Protector Logs are specific to FP in HDFS.
- User Notifications tool include all the messages for a user. The latest notifications are also displayed on the screen after login.

For more information about status and logs, refer to section [Working with Status and Logs](#).

Administration

Administration menu is the same for all three appliances. Using this menu, you can perform most of the standard server administration tasks:

- Start/stop/restart services
- Change time/time zone/date/NTP server
- Change passwords for admin/viewer/root user/LDAP users and unlock locked users
- Backup/restore OS, appliance configuration
- Set up email (SMTP)
- Install/uninstall services and patches
- Set up communication with a directory server (Local/external LDAP, Active Directory) and monitor the LDAP
- Reboot and shut down
- Access appliance OS console



For more information about appliance administration, refer to section [*Working with Administration*](#).

Networking

Networking menu is the same for all four appliances. Using the Networking menu, you can configure the network settings as per your requirements.

- Change host name, appliance address, gateway, domain information
- Configure SNMP – refresh/start/set service or show/set string
- Specify management interface for Web UI and Web Services
- Configure network interface settings and assign services to multiple IP addresses
- Troubleshoot the network
- Manage Firewall settings

For more information about appliance networking, refer to section [*Working with Networking*](#).

Tools

Tools menu is different for all the four appliances. However, most of the tools are common. Using this menu, you can perform the following tasks.

- Configure SSH mode to include known hosts/authorized keys/identities, and generate new server key
- Set up High Availability cluster with active/passive nodes, trusted appliances cluster
- Set up XEN paravirtualization
- View status of external hard drives
- Run antivirus and update signature file
- Configure Web services settings
- Backup/restore logs
- Manage Distributed File System ACL

For more information about common appliance tools, refer to section [*Working with Tools*](#).

If you are using DSG, then you have additional tools for configuring ESA communication (refer to the appropriate Appliance guide for details).

The additional tools for logging and reporting and policy management mentioned in the list are specifically for configuring ESA appliance.

Preferences

Preferences menu is common for all four appliances. Using this menu, you can perform the following tasks:

- Set up local console settings
- Specify if root password is required for CLI system tools
- Display the system monitor in OS console

For more information about appliance preferences, refer to section [*Working with Preferences*](#).

3.2.1 CLI Manager Main Screen

The CLI Manager main screen appears when you successfully logon to CLI Manager. This screen appears with the messages that relate to the user who has logged in and also mentions the priority of each message. Note here that % to the bottom-right of the screen indicates the information available for viewing on the screen.

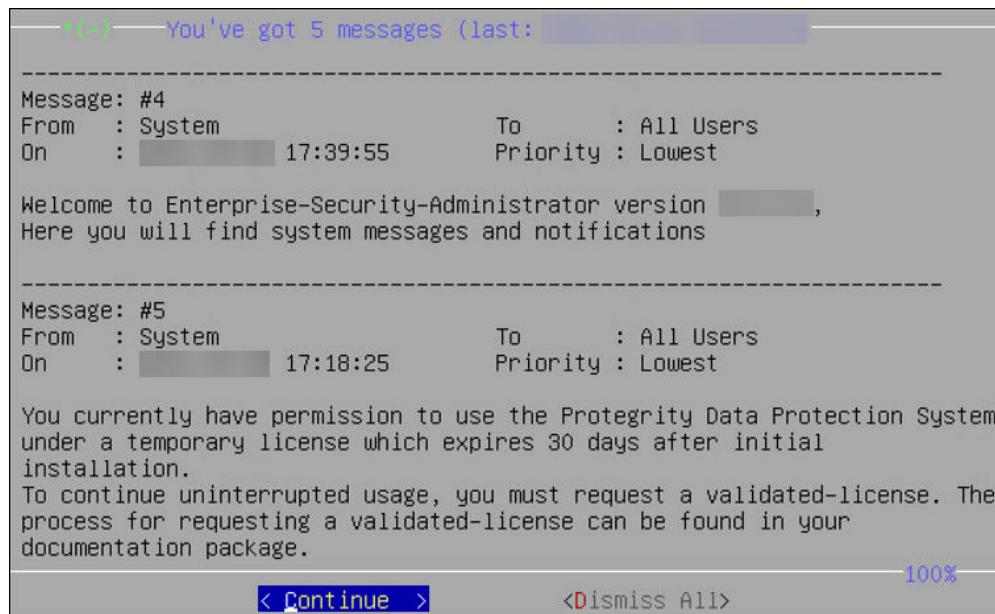


Figure 3-1: Introductory Splash Screen

If you click **Continue**, then the main menu screen appears.

For example, the following figure illustrates the ESA main screen.



Figure 3-2: CLI Manager Main Options Screen (ESA)

3.2.2 CLI Manager Navigation

There are many common keystrokes that help you to navigate the CLI Manager. The following table describes the navigation keys.

Table 3-1: Navigation Keys

Key	Description
UP ARROW	Navigates up and down menu options
DOWN ARROW	
ENTER	Selects an option or continues process
Q	Quits the CLI Manager
T	Goes to the top of the current menu
U	Moves up one level
H	Displays key settings and instructions
TAB	Moves between multiple fields
Page Up	Scroll Up
Page Down	Scroll Down

In the following sections, each of the five choices are explained in detail.

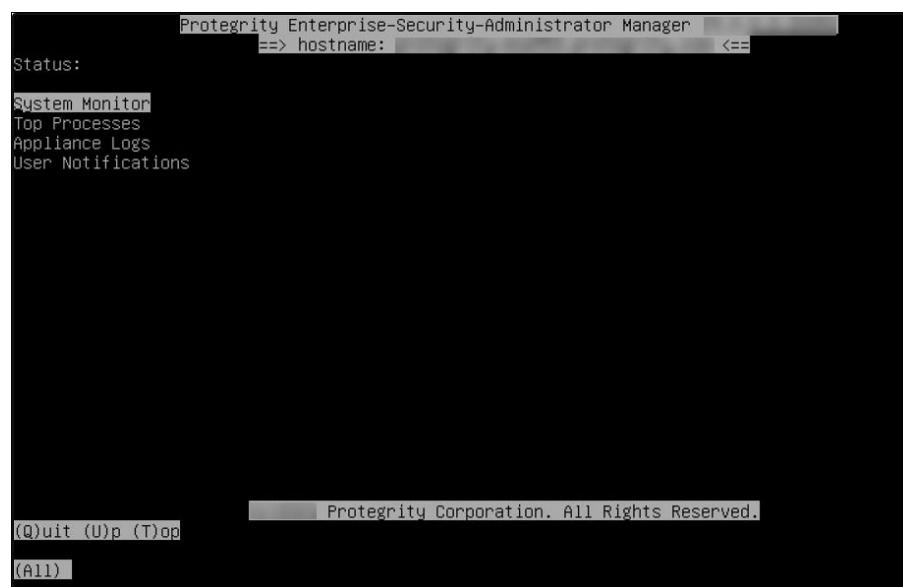
3.3 Working with Status and Logs

Using the Status and Logs screen, you can access system monitor information, examine top memory and CPU usage, and view appliance logs. You can access it from the CLI Manager main screen. This screen shows the Host to which you are attached and allows you to view and manage your audit logs.

In addition to the existing logs, the following additional security logs are generated:

- Appliance's own LDAP when users are added and removed
- SUDO commands are issued from the shell
- There are failed attempts to log in from SSH or Web UI
- All shell commands: This is a PCI-DSS requirement for the user with admin privileges.

The following figure shows the Status and Logs screen.

*Figure 3-3: Status and Logs Screen*

3.3.1 Monitoring System Statistics

Using **System Monitor**, you can view the system statistics. This screen shows information such as CPU usage, RAM and disk space free or in use, the reason for the Appliance working the way it is, and if more hard disks are required, among others.

```
protegility-es953 ( ) / Enterprise-Security-Administrator
CPU Idle : 49.0% Mem Total : 8GB Swap Total : 8GB
System : 5.6% Used : 7GB ( 90.3%) Used : 206MB ( 2.5%)
User : 45.5% Free : 773MB ( 9.7%) Free : 8GB ( 97.5%)
Load : 0.34,0.32,0.57 on 2 CPUs
Running : 1 days 0 hours 39 mins 42 secs (11:29:04)

NIC bytesIn bytesOut Packets Errors Collisions
ethMNG 0 0 0/0 - -
ethSRVx 0 0 0/0 - -

Mount Size Used Free
/ 7.8GB 4.6GB (58.3%) 3.3GB (41.7%)
/ 7.8GB 4.6GB (63.6%) 2.8GB (36.4%)
/opt 16.3GB 1.9GB (17.0%) 13.5GB (83.0%)
/var/log 5.8GB 87.7MB (6.9%) 5.4GB (93.1%)

Disk R/W : -/24KB Swap In/Out : -/8
```

Figure 3-4: System Monitor Screen

To view system information, navigate to **Status and Logs> System Monitor**.

3.3.2 Viewing the Top Processes

Using **Top Processes**, you can examine in real-time, the processes using up memory or CPU.

Top Processes Mem/CPU					
Top Memory			Top CPU		
PID	VSZ	RSS %CPU COMMAND	PID	%CPU VSZ	COMMAND
8107	7005804	4828984 0.4 java	4223	1.7 2368180	beam.smp
6831	4723544	192508 0.1 java	3654	1.0 77164	python3
6792	4692664	173264 0.1 java	8107	0.4 7005804	java
7255	4656800	240100 0.1 java	4642	0.4 1469936	dockerd
7322	4654744	121940 0.1 java	4688	0.2 1344996	containerd
7169	4652696	158584 0.1 java	6831	0.1 4723544	java
7500	4650648	108276 0.1 java	6792	0.1 4692664	java
4223	2368180	95184 1.7 beam.smp	7255	0.1 4656800	java
6973	1484596	62392 0.0 apache2	7322	0.1 4654744	java

Figure 3-5: Top Processes Memory/CPU Screen

3.3.3 Working with System Statistics (SYSSTAT)

The System Statistics (SYSSTAT) is a tool to monitor system resources and their performance on LINUX/UNIX systems. It is a contains utilities that collect system information, report CPU statistics, report input-output statistics, and so on. The SYSSTAT tool provides an extensive and detailed data for all the activities in your system.

The SYSSTAT contains the following utilities for analyzing your system:

- *sar*
- *iostat*
- *mpstat*
- *pidstat*



- *nfsiostat*
- *cisfiosstat*

These utilities collect, report, and save system activity information. Using the reports generated, you can check the performance of your system.

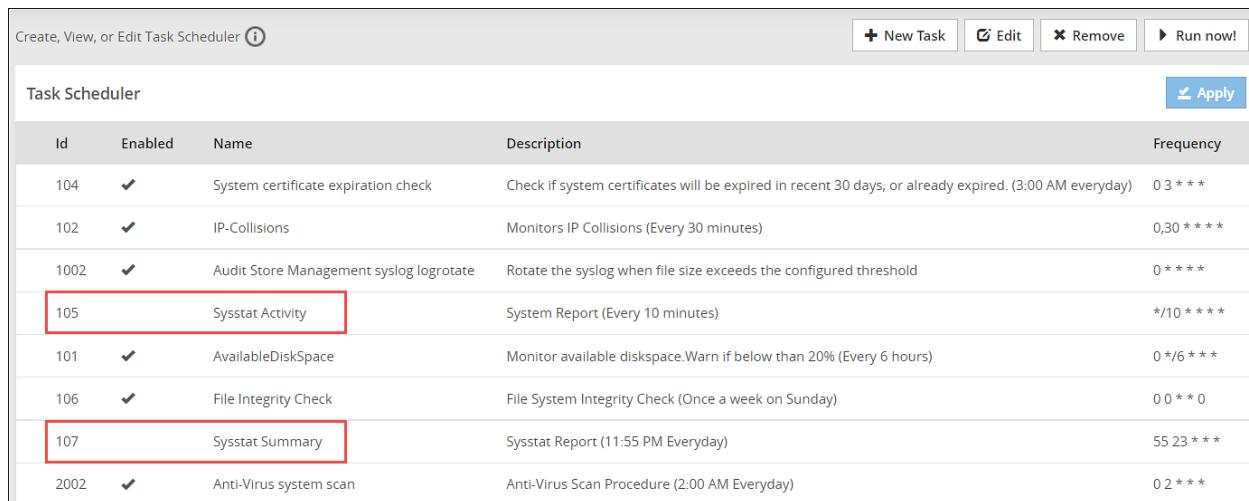
Note:

The SYSSTAT tool is available when you install the appliance.

On the ESA Web UI, navigate to **System > Task Scheduler** to view the SYSSTAT tasks. You must run the following tasks to collect the system information:

- **Sysstat Activity Report** to collect information at short intervals
- **Sysstat Activity Summary** to collect information at a specific time daily

The following figure displays the SYSSTAT tasks on the Web UI.



The screenshot shows the 'Task Scheduler' page with the following details:

Task Scheduler				
Id	Enabled	Name	Description	Frequency
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 * * *

Figure 3-6: SYSSTAT Task Scheduler

The logs are stored in the `/var/logs/sysstat` directory.

Note:

The tasks are disabled by default. You must enable the tasks from the **Task Scheduler** for collecting system information.

3.3.4 Auditing Service

The Linux Auditing System is a tool/utility that allows to monitor events occurring in a system. It is integrated with the kernel to watch the system operations. The events that must be monitored are added as rules and defined to which extent that the event must be tracked. If the event is triggered, then a detailed audit log is generated. Based on this log, you can track any violations to the system and improve security measures to prevent them.

In Protegility appliances, the auditing tool is implemented to track certain events that can pose as a security threat. The **Audit Service** is installed and running in the appliance for this purpose. On the Web UI, navigate to **System > Services** to view the status of the service. The **Audit Service** runs to check the following events:

- Update timezone
- Update AppArmor profiles
- Manage OS users and their passwords

If any of these events occur, then a low severity log is generated and stored in the logs. The logs are available in the `/var/log/audit/audit.log` directory. The logs that are generated by the auditing tool, contain detailed information about modifications triggered by the events that are listed in the audit rules. This helps to differentiate between a simple log and an audit log generated by the auditing tool for monitoring potential risks to the appliance.

For example, consider a scenario where an OS user is added to the appliance. If the **Audit Service** is stopped, then details of the user addition are not displayed and logs contain entries as illustrated in the following figure.

```
May 18 19:53:02 protegity-esa895 /usr/local/lib/python2.7/dist-packages/ksa/acl.py: Adding user debian
```

Figure 3-7: Logs

If the **Audit Service** is running, then the same event triggers a detailed audit log describing the user addition. The logs are illustrated in the following figure.

```

May 18 19:41:44 protegity-esa895 /etc/init.d/appliance-queues-server: {"origin": {"time_utc": 1589811104, "ip": "2.10.1.8", "hostname": "protegity-esa895"}, "level": "Low", "process": {"version": "8.0.0.1837", "name": "BSAPAP"}, "logtype": "System", "client": {"ip": "2.10.1.8"}, "additional_info": {"description": "2020-05-18T19:41:43.739926+05:30 protegity-esa895 audispd: node=protegity-esa895 type=USER_CHAUTHOK msg=audit(1589811103.690:8320); pid=18125 uid=0 auid=33 ses=27 subj=unconfined msg=op=PAM:chauthok acct=<ubuntu> exe=</usr/sbin/chpasswd> hostname=? addr=? terminal=? res=success", "title": "Appliance Warning:2020-05-18T19:41:43.739926+05:30 protegity-esa895 audispd: node=protegity-esa895 type=USER_CHAUTHOK msg..."}}
```

```

May 18 19:41:44 protegity-esa895 /etc/init.d/appliance-queues-server: {"origin": {"time_utc": 1589811104, "ip": "2.10.1.8", "hostname": "protegity-esa895"}, "level": "Low", "process": {"version": "8.0.0.1837", "name": "BSAPAP"}, "logtype": "System", "client": {"ip": "2.10.1.8"}, "additional_info": {"description": "2020-05-18T19:41:43.739915+05:30 protegity-esa895 audispd: node=protegity-esa895 type=EOE msg=audit(1589811103.690:8319)", "title": "Appliance Warning:2020-05-18T19:41:43.739915+05:30 protegity-esa895 audispd: node=protegity-esa895 type=EOE msg=audit(1589811103.690:8319)"}}
```

```

May 18 19:41:44 protegity-esa895 /etc/init.d/appliance-queues-server: {"origin": {"time_utc": 1589811104, "ip": "2.10.1.8", "hostname": "protegity-esa895"}, "level": "Low", "process": {"version": "8.0.0.1837", "name": "BSAPAP"}, "logtype": "System", "client": {"ip": "2.10.1.8"}, "additional_info": {"description": "2020-05-18T19:41:43.739903+05:30 protegity-esa895 audispd: node=protegity-esa895 type=PROCTITLE msg=audit(1589811103.690:8319); procfile=</usr/sbin/chpasswd>", "title": "Appliance Warning:2020-05-18T19:41:43.739903+05:30 protegity-esa895 audispd: node=protegity-esa895 type=PROCTITLE msg=audit(1589811103.690:8319)"}}
```

```

May 18 19:41:44 protegity-esa895 /etc/init.d/appliance-queues-server: {"origin": {"time_utc": 1589811104, "ip": "2.10.1.8", "hostname": "protegity-esa895"}, "level": "Low", "process": {"version": "8.0.0.1837", "name": "BSAPAP"}, "logtype": "System", "client": {"ip": "2.10.1.8"}, "additional_info": {"description": "Running /etc/opt/scripts/on-pwd-set/on-pwd-delete-webession.sh - Password was changed for user: ubuntu. Closing all web sessions if exists forcing logout.", "title": "Appliance Warning: Running /etc/opt/scripts/on-pwd-set/on-pwd-delete-webession.sh - Password was changed for user: ubuntu. ..."}, "type": "PATH"}}
```

```

May 18 19:41:44 protegity-esa895 /etc/init.d/appliance-queues-server: {"origin": {"time_utc": 1589811104, "ip": "2.10.1.8", "hostname": "protegity-esa895"}, "level": "Low", "process": {"version": "8.0.0.1837", "name": "BSAPAP"}, "logtype": "System", "client": {"ip": "2.10.1.8"}, "additional_info": {"description": "2020-05-18T19:41:43.739875+05:30 protegity-esa895 audispd: node=protegity-esa895 type=PATH msg=audit(1589811103.690:8319); item=4 name=</etc/shadow> inode=43779 dev=f:02 mode=0100400 uid=0 ogid=42 rdev=0:00 nametype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0", "title": "Appliance Warning:2020-05-18T19:41:43.739875+05:30 protegity-esa895 audispd: node=protegity-esa895 type=PATH msg=audit(1589811103.690:8319)"}}
```

Figure 3-8: Audit Logs with Auditing Service

As illustrated in the figure, the following are some audits that are triggered for the event:

- **USER_CHAUTHOK:** User attribute is modified.
- **EOE:** Multiple record event ended
- **PATH:** Recorded a path file name

Thus, based on the details provided in the `type` attribute, a potential threat to the system can be monitored.

For more information about the audit types, refer to the following link:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-audit_record_types

Note:

On the Web UI, an **Audit Service Watchdog** scheduled task is added to ensure that the **Audit Service** is running. This task is executed once every hour.

Caution:

It is recommended to not stop the **Audit Service** for security purposes.

3.3.5 Viewing Appliance Logs

Using **Appliance Logs**, you can view all logs that are gathered by the appliance.

These logs are listed in the following table:

Table 3-2: Appliance Logs

Logs	Logs Types	Description	Appliances Specific	
			ESA	DSG
System Event Logs	Syslog	All appliance logs.	✓	✓
	Installation	Installation logs contain all of the information gathered during the installation procedure. These logs include all errors during installation and information on all the processes, resources, and settings used for installation.	✓	✓
	Patches	Patches installed on appliance	✓	✓
	Patch_SASL	Proxy Authentication (SASL) related logs		
	Authentication	Authentication logs, such as user logins.	✓	✓
	Web Services	Logs generated by the Web Services modules.	✓	✓
	Web Management	Logs generated by the Appliance Web UI engine	✓	✓
	Current Event	Current event logs contain all the operations performed on the appliance. It gathers all information from different services and appliance components.	✓	✓
	Kernel	System kernel logs.	✓	✓
	Web Services Server	Web Services Apache logs	✓	✓



Logs	Logs Types	Description	Appliances Specific	
			ESA	DSG
	Patch_Logging	Logging server related logs such as installation log: logging server and so on.	✓	✓
Web Services Engine	Web Services HTTP-Server logs	Appliance Web UI related logs.	✓	✓
Service Dispatcher	Access Logs	Service Dispatcher Access Logs	✓	✓
	Server Logs	Service Dispatcher Server Logs	✓	✓
Logging	Startup	ESA logging and reporting mechanism specific logs.	✓	
	WatchDog		✓	
	Database Access Layer		✓	
	Database Engine		✓	
PEP Server		Logs received from PEP Server that is located on the FPV and DSG.		✓
Cluster Logs	Export Import Cluster			✓
DSG Patch Installation	Cluster	Log all operations performed during installation of the DSG patch		✓

You can delete the desired logs using **Purge** button and view them in real time using **Real-Time View** button. When you finish viewing logs, press **Done** to exit.

3.3.6 Viewing User Notifications

All the messages that display when you log in to either to ESA Web UI or CLI can be viewed here as well.

```

* (-) You've got 4 messages (last: [REDACTED] 12:00:24)
Message: #1
From : PasswordPolicy           To : admin
On   : [REDACTED] 12:00:24       Priority : Critical
Password will expire in 25 days, 05 hours, 12 minutes

-----
Message: #2
From : AntiVirus                To : admin
On   : [REDACTED] 01:01:05       Priority : Normal
Database update is done. (from version 26305 to 26308)

-----
Message: #3
From : System                     To : All Users
On   : [REDACTED] 17:39:55       Priority : Lowest
Welcome to Enterprise-Security-Administrator version [REDACTED],
Here you will find system messages and notifications
* (+) < Continue > <Dismiss All> 59%

```

Figure 3-9: Messages for User

3.4 Working with Administration

Appliance administration is the most important part of the appliance framework. Most of the administrative tools and administrative tasks can be performed using the Administration menu of the Appliance CLI Manager.

The following screen illustrates the Administration screen on the CLI Manager.

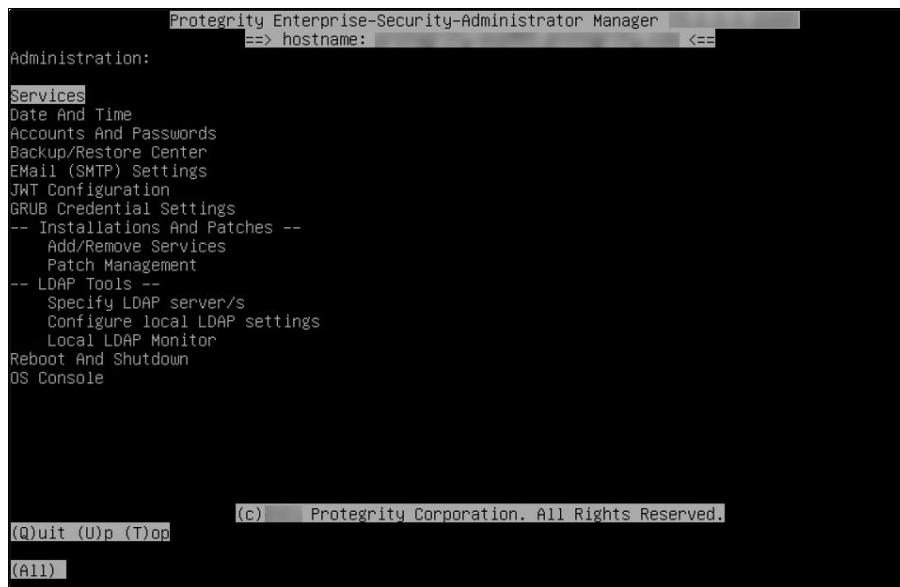


Figure 3-10: Administration Menu

Note: Most of the administration tasks can be performed using Web UI. Some of the administration tasks, such as creating clustered environment or setting up the virtualization can be done only in the CLI Manager by selecting Administration menu.

3.4.1 Working with Services

You can manually start and stop appliance services. In the CLI Manger, you can view all appliance services and their statuses by navigating to **Administration> Services**.

Caution:

Before stopping/restarting a particular service, make sure that no important actions are being performed by the other users using the service that you want to stop/restart.

In the Services dialog box, you can start/stop/restart the following services:

Table 3-3: Appliance Services

Services	ESA	DSG
OS	✓	✓
Web UI, Secure Shell (SSH), Firewall, Real-time Graphs, SNMP Service, NTP Service, Cluster Status, Appliance Heartbeat Server, Appliance Heartbeat Client, Log Filter Server, Messaging System, Appliance Queues Backend, Docker		
LDAP	✓	✓
LDAP Server		
Web Services Engine	✓	✓
Web Services Engine		
Service Dispatcher	✓	✓
Service Dispatcher		
Logging	✓	
Management Server, Management Server Database, Reports Repository, Reporting Engine		
Policy Management	✓	
Policy Repository, HubController, PIM Cluster, Soft HSM Gateway, Key Management Gateway, Member Source Service, Meteringfacade, DevOps, Logfacade, Logfacade Legacy		
For more information about the Meteringfacade and Logfacade services, refer to the section Services .		
Reporting Server	✓	
Reports repository and reporting engine		
Distributed Filesystem File Protector	✓	
DFS Cache Refresh		
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.		
PEP Server		✓
PEP Server Service		
Storage and Share		
NFS Server, iSCSI Target, CIFS Server, FTP Server WebDav module, Storage		
ETL Toolkit		



Services	ESA	DSG
ETL Server		
Cloud Gateway		✓
Cloud Gateway Cluster		
td-agent	✓	✓
td-agent		
Audit Store		✓
Audit Store Repository		
Audit Store Management		
Analytics		✓
Analytics		
IMP	✓	
IMPS		

You can change the status of any service when you select it from the list and choose **Select**. In the screen that follows the Service Management screen, select stop, start, or restart a service, as required.

When you apply any action on a particular service, the status message appears with the action applied. Press **ENTER** again to continue.

Note: You can also use the Web UI to start or stop services. In the Web UI Services, you have additional options for stopping/starting services, such as Enable/Disable Auto-start for most of the services.

Important:

Although the services can be started or stopped from the Web UI, the start/stop/restart action is restricted for some services. These services can be operated from the OS Console. Run the following command to start/stop/restart a service.

```
/etc/init.d/<service_name> stop/start/restart
```

For example, to start the docker service, run the following command.

```
/etc/init.d/docker start
```

3.4.2 Setting Date and Time

You can adjust the date and time settings of your appliance using **Administration > Date and Time**. You may need to do so if this information was entered incorrectly during initialization.

You can synchronize time with NTP Server using **Time Server (NTP)** option (explained in the following paragraph), change time zone using **Set Time Zone** option, change date using **Set Date** option, or change time using **Set Time** option. The information selected during installation is available beside each option.



Use Up Arrow or Down Arrow keys to change the values in the editable fields, such as Month/Year. Use any arrow key to navigate the calendar. Use the Tab key to navigate between the editable fields.

Caution: Date and time modifications may affect licenses and certificates. It is recommended to have time synchronized between Appliances and Protectors.

Note:

You can set the time and date using the Web UI as well.

For more information about setting the appliance time and date, refer to section [Configuring Date and Time](#).

Configure NTP Time Server

You can access the Configure Server NTP Time Server screen using **Administration > Date and Time > Time Server** option.

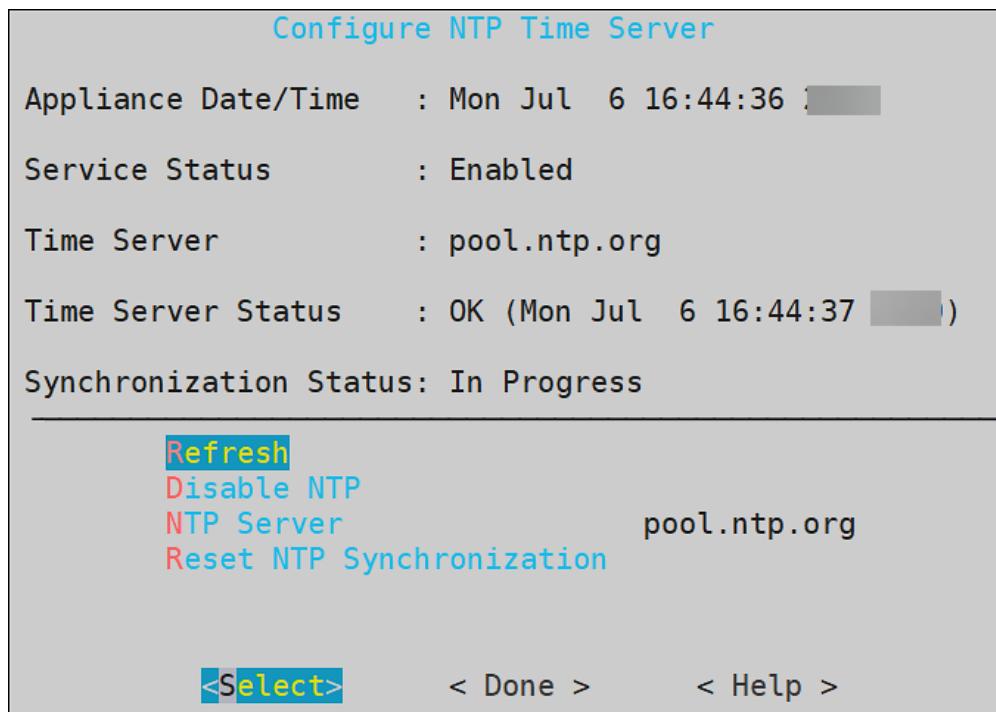


Figure 3-11: Configure NTP Time Server

To enable NTP synchronization, you need to specify the NTP Server first and then enable NTP. Once an NTP Server is specified, the new time will be applied immediately.

The NTP synchronization may take some time and while it is in progress, the Synchronization Status displays *In Progress*. When it is over, the Synchronization Status displays *Time Synchronized*.

Important:

You must enable/disable the NTP settings only from the CLI Manager or the Web UI.

3.4.3 Managing Accounts and Passwords

The Appliance CLI Manager includes options to change password and permissions for multiple users through the CLI interface. The options available are listed as follows:

- Change My Password
- Manage Password and Local-Accounts
 - Reset directory user password
 - Change OS *root* account password
 - Change OS *local_admin* account password
 - Change OS *local_admin* account permissions
 - Manage internal *Service-Accounts*
 - Manage local OS users

3.4.3.1 OS Users in Appliances

When you install an appliance, some users are installed to run specific services for the products. The following table describes the OS users that are available in your appliance.

Table 3-4: OS Users in the Appliance

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

Caution:

Ensure that you do not add the OS users as policy users.

3.4.3.2 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](#).

3.4.3.2.1 Enforcing Password Policy

The following section describes how to enforce your policy restrictions for the OS and LDAP user accounts.

► To enforce password policy:

1. On the CLI Manager, navigate to **Administration > OS Console**.

2. Run the following command to edit the `check_password.py` file.

`vi /etc/ksa/check_password.py`

3. Define the password rules as per your organizational requirements.

For more information about the password policy examples, refer to section [Examples](#).

4. Save the file.

The password rules for the users in ESA are updated.

3.4.3.2.2 Examples

The following section describes a few scenarios about enforcing validation checks for the LDAP and OS users.

The `check_password.py` file contains the `def check_password(password)` Python function. In this function you can define your validations for the user password. This function returns a status code and a status message. In case of successful validation, the status code is zero and the status message is empty. In case of validation failure, the status code is non-zero and the status message contains the appropriate error message.

Scenario 1:

An enterprise wants to implement the following password rules:

- Length of the password should contain atleast 15 characters
- Password should contain digits

You must add the following snippet in the `def check_password(password)` function:

```
# Password length check
if len(password)<15: return (1,"Password should contain at least 15 characters")
# Password digits check
password_set=set(password)
digits=set(string.digits)
if ( password_set.intersection(digits) == set([]) ): return (2,"Password must contain digit")
```

Scenario 2:

An enterprise wants to implement the following password rule:

- Password should not contain 1234.

You must add the following snippet in the `def check_password(password)` function:

```
if password==1234:
    return (1,"Password must not contain 1234")
    return (0,None)
```

Scenario 3:

An enterprise wants to implement the following password rules:

- Password should contain a combination of uppercase, lowercase, and numbers.

You must add the following snippet in the `def check_password(password)` function:

```
digits=set(string.digits)
if ( password_set.intersection(digits) == set([]) ): return (2,"Password must contain
numbers, upper, and lower case characters.")
# Force lowercase
lower_letters=set(string.ascii_lowercase)
if ( password_set.intersection(lower_letters) == set([]) ): return (2,"Password must contain
numbers, upper, and lower case characters.")
# Force uppercase
upper_letters=set(string.ascii_uppercase)
if ( password_set.intersection(upper_letters) == set([]) ): return (2,"Password must contain
numbers, upper ,and lower case characters.")
```

3.4.3.3 Changing Current Password

In situations where you need to change your current password due to suspicious activity or reasons other than password expiration, you can use the following steps.

For more information about appliance users, refer to section [Managing Appliance Users](#).

► To change the current password:

1. Navigate to **Administration > Accounts and Passwords > Change My Password**.
2. In the **Current password** field, type the current password.
3. In the **New password** field, type the new password.
4. In the **Retype password** field, retype the new password.
5. Select **OK** and press **ENTER** to save the changes.

3.4.3.4 Resetting Directory Account Passwords

You can change the password for any user existing in the internal LDAP directory. The user accounts and their security privileges as well as passwords are defined in the LDAP directory.

For more information about the internal LDAP directory, refer to section [Managing Appliance Users](#).

Note: The LDAP Administrator is an admin user or the Directory Administrator assigned by admin. Admin can define Directory Administrators in the LDAP directory.

To be able to change the password for any LDAP user, you need to provide Administrative LDAP user credentials. You can also provide the old credentials of the LDAP user.

► To change a directory account password:

1. Navigate to **Administration > Accounts and Passwords > Manage Passwords and Local-Accounts > Reset directory user-password**.
2. In the displayed dialog box, enter Administrative LDAP user name and password.

Note: You can also use the *local_admin* credentials.

3. In the Target LDAP user field, enter the LDAP user name you wish to change the password for.
4. Enter the old password for the selected LDAP user. This step is optional.
5. Enter a new password for the selected LDAP user and confirm it.
6. Select **OK** and press **ENTER** to save the changes.

3.4.3.5 Changing the Root User Password

You may want to change the root user password due to security reasons, and this can only be done using the Appliance CLI Manager.

► To change the root password:

1. In the CLI Manager, navigate to **Administration > Accounts and Passwords > Manage Passwords and Local-Accounts > Change OS ‘root’ account password**.
2. Enter the administrative user name and its valid password into the required text boxes.

Note: You can also use the *local_admin* credentials

3. Enter the old password for the *root* user in the required text box.
4. Enter the new password for the *root* user in the required text box.
5. Select **OK** and press **ENTER** to save the changes.

3.4.3.6 Changing the Local Admin Account Password

You can log into CLI Manager as a *local_admin* user if the LDAP is down or for LDAP maintenance. It is recommended that the *local_admin* account is not used for standard operations since it is primarily intended for maintenance tasks.

► To change *local_admin* account password:

1. Navigate to **Administration > Accounts and Passwords > Manage Passwords and Local-Accounts > Change OS local_admin account password**.
2. Enter the old password for the *local_admin* in the Administrative user name text box and the password into the Administrative user password field.

Note: You can also use the *Directory Server Administrator* credentials.

3. Enter New *local_admin* password and confirm it.
4. Select **OK** and press **ENTER** to save changes.

3.4.3.7 Changing the Local Admin Account Permission

By default, the *local_admin* user cannot log into CLI Manager using SSH or log into the Web UI. However, you can configure this access using the tool, which changes the *local_admin* account permissions.

► To change *local admin* account permissions:

1. Navigate to **Administration > Accounts and Passwords > Manage Passwords and Local Accounts > Change OS local_admin account permissions**.
2. In the dialog box displayed, enter the local admin password, and then select **OK**.
3. Specify the permissions for the local admin. You can allow SSH Access, Web-Interface Access, or both.
4. Select **OK** and press **ENTER** to save changes.

3.4.3.8 Changing Service Accounts Passwords

Service Account users are *service_admin* and *service_viewer*. They are used for internal operations of components that do not support LDAP, such as Management Server internal users, and Management Server Postgres database. You cannot log into the Appliance Web UI, Reports Management (for ESA), or CLI Manager using service accounts users. Since service accounts are internal OS accounts, they must be modified only in special cases.

► To change service accounts:

1. Navigate to **Administration > Accounts and Passwords > Manage Passwords and Local-Accounts > Manage internal ‘Service-Accounts’**.
2. Enter Administrative user name and password.
3. Select **OK** and press **ENTER**.
4. In the dialog box displayed, enter the new Admin Service Account password and retype to confirm the password.
5. Enter the new Viewer Service Account password and confirm.
6. Select **OK** and press **ENTER** to save changes.

Note: Click **Generate Random** to generate new passwords randomly. Select **OK** and press **ENTER** to save changes.

3.4.3.9 Managing Local OS Users

Managing local OS user option provides you the ability to create users that need direct OS shell access and are allowed to perform non-standard functions, such as schedule remote operations, backup agents, run health monitoring, etc. This option also lets you manage passwords and permissions for the *jasperdbuser*, and *dpsdbuser*, which are available by default when ESA is installed.

The password restrictions for OS users are as follows:

- For all OS users, you cannot repeat the last 10 passwords used.
- If an OS user signs in thrice using an incorrect password, the account is locked for five minutes. You can unlock the user by providing the correct credentials after five minutes. If an incorrect password is provided in the subsequent sign-in attempt, the account is again locked for five minutes.

► To manage local OS users:

1. Navigate to **Administration > Accounts and Passwords > Manage Passwords and Local-Accounts > Manage local OS users**.
2. In the dialog box displayed, enter the root password and confirm selection.
3. Add a new user or select an existing user as explained in following steps.
 - a. Select **Add** to create a new local OS user.
 - i. In the dialog box displayed, enter a User name and Password for the new user.

Note:

The **&** character is not supported in the **Username** field.

- ii. Confirm the password in the required text boxes.
 - iii. Select **OK** and press **ENTER** to save the user.
- b. Select an existing user from the list displayed.
 - i. You can select one of the following options from the displayed menu.

Table 3-5: User Options

Options	Description	Procedure
Check password	Validate entered password.	<ol style="list-style-type: none"> 1. In the dialog box displayed, enter the password for the local OS user. A <i>Validation succeeded</i> message appears.
Update password	Change password for the user.	<ol style="list-style-type: none"> 1. In the dialog box displayed, enter the Old password for the local OS user. This step is optional. 2. Enter the New Password and confirm it in the required text boxes.
Update shell	Define shell access for the user.	<ol style="list-style-type: none"> 1. In the dialog box displayed, select one of the following options. <ul style="list-style-type: none"> • No login access • Linux Shell - <i>/bin/sh</i>



Options	Description	Procedure
		<ul style="list-style-type: none"> Custom <p>Note: The default shell is set as No login access (<code>/bin/false</code>).</p>
Toggle SSH access	Set SSH access for the user.	<p>Select the Toggle SSH access option and press ENTER to set SSH access to Yes.</p> <p>Note: The default is set as No when a user is created.</p>
Delete user	Delete the local OS user and related home directory.	Select the Delete user option and confirm the selection.

4. Select **Close** to exit the option.

3.4.4 Working with Backup and Restore

Using the Backup/Restore Center tool, you can create backups of configuration files and settings. If you want to restore the files and configuration, then you can restore a stable configuration.

Note: You will be prompted to enter the root password before the Backup Center dialog box appears.

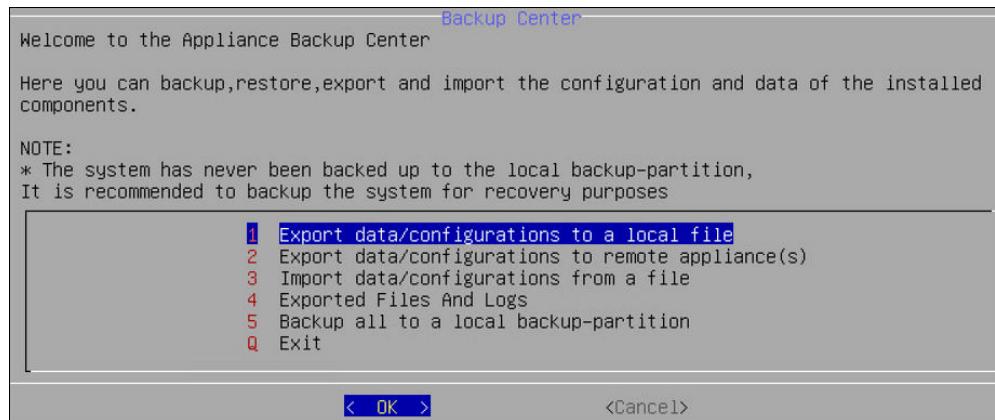


Figure 3-12: Backup Center

You can select from a list of packages to be backed up.

For more information about using backup and restore, refer to section [Working with System Backup and Restore](#).

Note:

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

3.4.4.1 Exporting Data Configuration to Local File

Select the configuration/s to export to a local file. When you select **Administration > Backup/Restore Center > Export data/configurations to a local file** (option 1) in the Backup Center screen, you will be asked to specify the packages to export:

Table 3-6: List of Appliance Specific Services

Services	Description	Appliance Specific	
		ESA	DSG
Appliance OS Configuration	<p>Export the OS configuration (networking, passwords, and others) but not the security modules data.</p> <p>Note: In the OS configuration, the certificates component is classified as follows:</p> <ul style="list-style-type: none"> • Certificates that include Consul-related certificates, Audit Store certificates, and certificates of Protegity 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 the local directory server and authentication settings.	✓	✓
Export Consul Configuration and Data	Export Consul configuration and data	✓	✓
Backup Policy-Management * ²	Export policy management configurations and data, such as, policies, data stores, data elements, roles, certificates, keys, logs, Key Store-specific files and certificates among others to a file.	✓	
Backup Policy-Management Trusted Appliances Cluster* ²	Export policy management configurations and data, such as, policies, data stores, data elements, roles, certificates, keys, logs, Key Store-specific files and certificates among others to a specific cluster node for a Trusted Appliances Cluster.	✓	
Backup Policy-Management Trusted Appliances Cluster without Key Store* ¹	<p>Export policy management configurations and data, such as, policies, data stores, data elements, roles, certificates, keys, logs among others, but excluding the Key Store-specific files and certificates to a specific cluster node for a Trusted Appliances Cluster.</p> <p>Note: It is recommended to use this option with cluster export only.</p>	✓	



Services	Description	Appliance Specific	
		ESA	DSG
	<p>This option excludes the backup of the Key Store-specific files and certificates.</p> <p>It is recommended to use this option with cluster export only.</p>		
Policy Manager Web UI Settings	Export the Policy Management Web UI settings that includes the <i>Delete</i> permissions specified for content and audit logs.	✓	
Export All PEP Server Configuration, Logs, Keys, Certs	Export the data (.db files, license, token elements, etc.), configuration files, keys, certificates and log files.		✓
Export PEP Server Configuration Files	Export all PEP Server configuration files (.cfg).		✓
Export PEP Server Log Files	Export PEP Server log files (.log and .dat).		✓
Export PEP Server Key and Certificate Files	Export PEP Server Key and Certificate files (.bin, .crt, and .key).		✓
Export PEP Server Data Files	Export all PEP Server data files (.db), license, token elements and log counter files.		✓
Application Protector Web Service	Export Application Protector Web Service configuration files.		
Export Storage and Share Configuration Files	Export all configuration files including NFS, CIFS, FTP, iSCSI, Webdav.		
Export File Protector Configuration Files	Export all File Protector configuration files.		
Export ETL Jobs	Export all ETL job configuration files.		
Export Gateway Configuration Files			✓
Export Gateway Log Files			✓
Cloud Utility AWS	Exports Cloud Utility AWS CloudWatch configuration files.	✓	✓

Note:

*¹ Ensure that only one backup-related option is selected among the options *Backup Policy-Management*, *Backup Policy-Management Trusted Appliances Cluster*, and *Backup Policy-Management Trusted Appliances Cluster without Key Store*.

Note:

The *Backup Policy-Management* option must be used to back up the data to a file. In this case, this backup file is used to restore the data to the same machine, at a later point in time.

The *Backup Policy-Management Trusted Appliances Cluster* option must be used to replicate the data to a specific cluster node in the Trusted Appliances Cluster (TAC).

Note:

This option excludes the backup of the metering data.

It is recommended to use this option with cluster export only.

If you want to exclude the Key Store-specific files during the TAC replication, then the *Backup Policy-Management Trusted Appliances Cluster without Key Store* option must be used to replicate the data, which excludes the Key Store-specific files and certificates, to a specific cluster node in the Trusted Appliances Cluster (TAC).

Note:

This option excludes the backup of the metering data and the Key Store-specific files and certificates.

It is recommended to use this option with cluster export only.

For more information about the *Backup Policy-Management Trusted Appliances Cluster* option or the *Backup Policy-Management Trusted Appliances Cluster without Key Store* option, refer to the section *Appendix C: TAC Replication of Key Store-specific Files and Certificates* in the [Protegity Key Management Guide 9.1.0.3](#).

If the OS configuration export is selected, then only the network setting and passwords, among others, are exported. The data and configuration of the security modules are not included. This data is mainly used for replication or recovery.

Before you import the data, note the OS and network settings of the target machine. Ensure that you do not import the saved OS and network settings to the target machine as this creates two machines with the same IP address in your network.

If you need to import all appliance configuration and settings, then perform a full restore for the system configuration. The following will be imported:

- OS configuration and network
- SSH and certificates
- Firewall
- High Availability
- Services status
- Authentication settings
- File Integrity Monitor Policy and settings

3.4.4.1.1 Exporting Data Configurations to Local File

► To export data configurations to a local file:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the root password.
The Backup Center dialog box appears.
3. From the menu, select option **1** to export data configurations to a local file.

4. Select the packages to export.
5. Enter the desired Export Name.
6. Specify the password for the backup file.
7. Confirm the specified password.
8. If required, then enter description for the file.
9. Click **OK**.
10. You can optionally save the logs for the export operation when the export is done:
 - a. Click **More Details** button.
The export operation log will display.
 - b. Click **Save** button to save the export log.
 - c. In the following dialog box, enter the export log file name.
 - d. Click **OK**.
 - e. Click **Done** to exit the *More Details* screen.

Note: The newly created configuration file will be saved into */products/exports*. It can be accessed from the CLI Manager, **Exported Files and Logs** menu, or from the **Import** tab available in the Backup/Restore page, available in the Appliance Web UI.

The export log file can be accessed from the from the CLI Manager, **Exported Files and Logs** menu, or from the **Log Files** tab available in the Backup/Restore page, available in the appliance Web UI.

3.4.4.2 Exporting Data or Configuration to Remote Appliance

You can export backup configurations to a remote appliance. Follow the steps in this scenario for a successful export of the backup configuration.

► To export data configurations to a remote appliance:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the *root* password.
The Backup Center dialog box appears.
3. From the menu, select option **Export data/configurations to remote appliance(s)** to export data configurations to a remote appliance.
4. From **Current (Active) Appliance Configuration**, you can select the package to export.
5. In the following dialog box, enter the password for this backup file.
6. Select the Import method.
For more information on each import method, select **Help**.
7. Type the IP address or hostname for the destination appliance.
8. Type the admin user credentials of the remote appliance and select **Add**.
9. In the information dialog box, press **OK**.
The Backup Center screen appears.

Exporting Appliance OS Configuration

When you import the appliance core configuration from the other appliance, the second machine will receive all network settings, such as, IP address, and default gateway, and so on.

Note: You should not import all network settings to another machine since it will create two machines with the same IP in your network.

It is recommended to restart the appliance receiving an appliance core configuration backup.

This dialog box shows up only when exporting to a file.

3.4.4.3 Importing Data/Configurations from a File

You can import (restore) data from a file if you need to restore a specific configuration that you have previously saved. During data configurations import, you are asked to enter the file password set during the backup file creation.

Before you begin

Note:

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

► To import data configurations from file:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the root password.
The Backup Center dialog box appears.
3. From the menu, select option **3** to import the configuration from a file.
4. In the following dialog box, select a file from the list which will be used for the configuration import.
5. Press **OK**.
6. In the following dialog box, enter the password for this backup file.
7. Select Import method.
8. Press **OK**.
9. In the information dialog box, press **OK**.

Note: Consider a scenario when importing a policy management backup that includes the external Key Store data. If the external Key Store is not working, then the HubController service does not start post the restore process.

The Backup Center screen appears.

3.4.4.4 Reviewing Exported Files and Logs

You can review the exported files and logs.

► To review exported files and logs:

1. Navigate to **Administration > Backup/Restore Center**.

2. Enter the root password.
The Backup Center dialog box appears.
3. From the menu, select option **4**.
4. In the Exported Files and logs dialog box, select **Main Log** file, to view logs.
5. Press Review.
6. To view the export files or operation logs, select it from the list of available exported files.
7. Press Review.

3.4.4.5 Deleting Exported Files and Logs

► To delete exported files and logs:

1. Navigate to **Administration > Backup/Restore Center**.
2. Enter the root password.
The Backup Center dialog box appears.
3. From the menu, select option **4**.
4. In the Exported Files and logs dialog box, select between Operations Logs and Exported Files.
5. Press **Delete**.
6. To confirm the deletion, press **Yes**.
Alternatively, to cancel the deletion, press **No**.

3.4.4.6 Backing Up/Restoring Local Backup Partition

The backup is created on the second partition of the local machine.

Note:

FOR XEN VIRTUALIZATION ONLY: If you are using virtualization, and have backed up the OS in HVM/PVM mode, then you can to restore only in the mode you backed it up (refer to section 8.1 Xen Paravirtualization Setup).

Thus, for example, if you make an OS full backup in the PVM mode (both Appliance and Xen Server are set to PVM), enable HVM mode, and then reboot the Appliance, you will not be able to boot the system in system-restore mode.

3.4.4.6.1 Backing up Appliance OS from CLI

It is recommended to perform the full OS back up before any important system changes, such as appliance upgrade or creating a cluster, among others.

► To back up the appliance OS from CLI Manager:

1. Login to the CLI Manager.
2. Proceed to **Administration > Backup/Restore Center**.
The **Backup Center** screen appears.
3. Select Backup all to a local backup-partition.
The following screen appears.

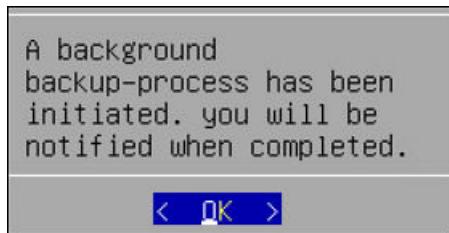


Figure 3-13: Backup Confirmation Screen

4. Press **ENTER**.
The **Backup Center** screen appears and the OS backup process is initiated.
5. Login to the Appliance Web UI.
6. Navigate to **Dashboard**.

The following message appears after the OS backup completes.

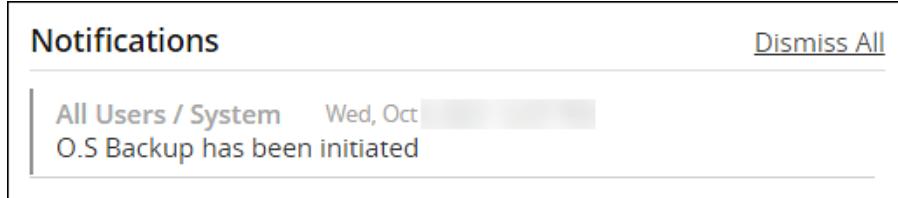


Figure 3-14: Notification Message

Caution: The **Restore from backup-partition option** appears in the **Backup Center** screen, after the OS backup is complete.

3.4.4.6.2 Restoring Appliance OS from Backup

This section describes the procedure to restore an Appliance OS from the backup either by initiating the OS-Restore procedure or by booting into the system-restore partition.

► To restore the appliance OS from backup by initiating the OS-Restore:

1. In the CLI Manager, navigate to the **Administration > Reboot and Shutdown > Reboot**.
The **Reboot** screen appears.
2. Enter the reason and select **OK**.
The appliance restarts and the following screen appears.



Figure 3-15: Console Screen

3. Select **System-Restore**.

The Welcome to **System Restore Mode** screen appears.

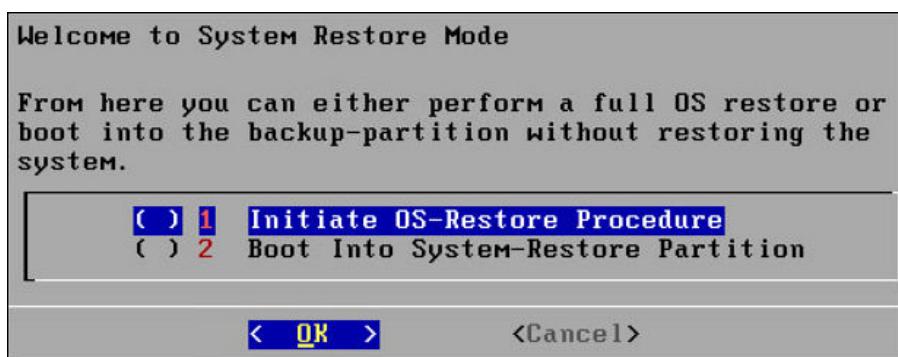


Figure 3-16: System Restore Screen

4. Select **Initiate OS-Restore Procedure**.

The OS restore procedure is initiated.

Booting into the System-Restore Partition

- To restore the appliance OS from backup by booting into the system-restore partition:

1. In the CLI Manager, navigate to the **Administration > Reboot and Shutdown > Reboot**. The **Reboot** screen appears.
2. Enter the reason and select **OK**.
The appliance restarts.
3. Select **System-Restore**.
The Welcome to **System Restore Mode** screen appears.
4. Select **Boot Into System-Restore Partition**.
The OS restore procedure is initiated.
5. Login to the Appliance Web UI.
6. Proceed to **System > Backup & Restore**.
7. Navigate to the **OS Full** tab and click **Restore**.
A message that the restore process is initiated appears.

8. Select **OK**.
The restore process starts and the system restarts after the process is completed.
9. Log in to the appliance and navigate to Appliance **Dashboard**.
A notification *OS Restore has been completed* appears.

Note:

Consider a scenario when restoring a full OS backup that includes the external Key Store data. If the external Key Store is not working, then the HubController service does not start post the restore process.

3.4.5 Setting Up the Email Server

You can set up an email server that supports the notification features in Protegility Reports. The Protegility Appliance Email Setup tool guides you through the setup. After you set up the email server, you can Protegility Reporting schedule reports to send notifications. For more information on how to schedule reports, refer to *Reports Guide 7.0*.

Keep the following information handy before the setup process:

- SMTP server details
- SMTP user credentials
- Contact email account: This email address is used by the Appliance to send user notifications.

Note: Remember to save the email settings before you exit the Email Setup tool.

► To set up the Email Server:

1. Navigate to **Administration > Email (SMTP) Settings**.
The Protegility Appliance Email Setup wizard appears.
2. Enter the root password and select **OK**.
3. In the SMTP Server Address field, type the address to the SMTP server and the port number that the mail server uses.
For SMTP Server, the default port is **25**.
4. In the SMTP Username field, type the name of the user in the mail server that the reporting engine can use.
Protegility Reporting requires a full email address in the Username.
5. In the SMTP Password text box and Confirm Password text boxes, type the password of the mail server user.
SMTP Username/Password settings are optional. If your SMTP does not require authentication, then you can leave the text boxes empty.
6. In the Contact address field, type the email recipient address.
7. In the Host identification field, type the name of the computer hosting the mail server.
8. Select **OK**.
The tool tests the connectivity and then appears the next Secured SMTP screen.
9. Specify the encryption method. Select *StartTLS* or disable encryption. *SSL/TLS* is not supported.
10. Click **OK**.
11. In the SMTP Setting screen that appears, you can:

To...	Follow these steps...
Send a test email	<ol style="list-style-type: none"> 1. Select Test. 2. At the prompt, type the recipient email address. 3. Select OK. A dialog box appears. 4. To view diagnostics while testing, follow these steps: <ol style="list-style-type: none"> a. Select Yes. A running status appears until the process completes. b. At the prompt, press ENTER. A message box appears. c. Select OK to return to the email tool. 5. To test without diagnostics, follow these steps <ol style="list-style-type: none"> a. Select No. A message box appears when the process completes. b. Select OK to return to the email tool.
Save the settings	<ol style="list-style-type: none"> 1. Select Save. A message box appears. 2. Select EXIT. 3. The Tools screen appears.
Change the settings	Select Reconfigure . The SMTP Configuration screen appears.
Exit the tool without saving	<ol style="list-style-type: none"> 1. Select Cancel. 2. At the prompt, select Yes. The Tools screen appears.

3.4.6 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.

3.4.6.1 Configuring Azure AD Settings

Before you begin

Before configuring Azure AD Settings on the appliance, you must have the following values that are 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:

- On the CLI Manager, navigate to **Administration > Azure AD Configuration**.
- Enter the *root* password and select **OK**.
The **Azure AD Configuration** dialog box appears.
- Select **Configure Azure AD Settings**.
The **Azure AD Configuration** screen appears.

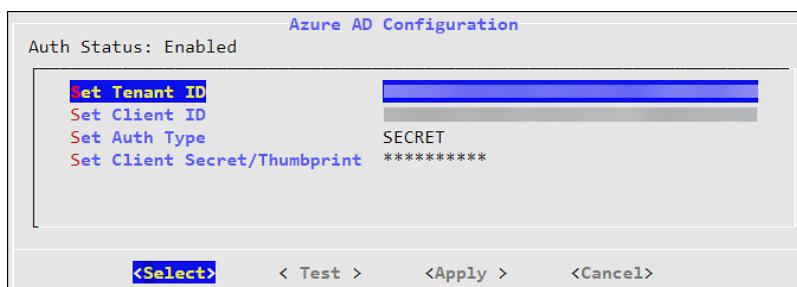


Figure 3-17: Azure AD Configuration

- Enter the information for the following fields.

Table 3-7: Azure AD Settings

Setting	Description
Set Tenant ID	Unique identifier of the Azure AD instance
Set Client ID	Unique identifier of an application created in Azure AD

Setting	Description
Set Auth Type	<p>Select one of the Auth Type:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Set Client Secret/Thumbprint	<p>The client secret/thumbprint is the password of the Azure AD application.</p> <ul style="list-style-type: none"> • If the Auth Type selected is SECRET, then enter Client Secret. • If the Auth type selected is CERT, then enter Thumbprint.

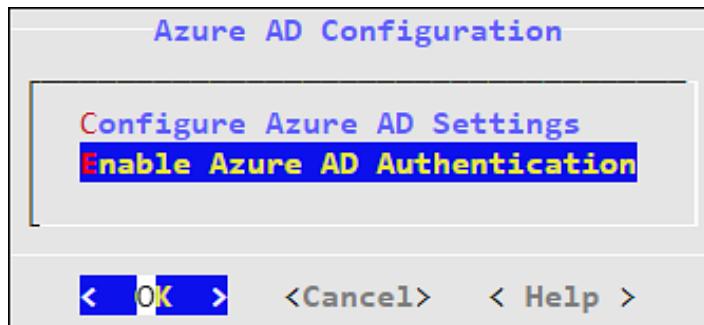
Note: For more information about the Tenant ID, Client ID, Authentication Type, and Client Secret/Thumbprint, search for the text *Register an app with Azure Active Directory* on Microsoft's Technical Documentation site at:

<https://learn.microsoft.com/en-us/docs/>

5. Click **Test** to check the configuration/settings.
The message *Successfully Done* appears.
6. Click **OK**.
7. Click **Apply** to apply and save the changes.
The message *Configuration saved successfully* appears.
8. Click **OK**.

3.4.6.2 Enabling/Disabling Azure AD

Using the Enable/Disable Azure AD option, you can enable or disable the Azure AD settings. You can import users or groups and assign roles when you enable the Azure AD settings.



3.4.7 Accessing REST API Resources

User authentication is the process of identifying someone who wants to gain access to a resource. A server contains protected resources that are only accessible to authorized users. When you want to access any resource on the server, the server uses different authentication mechanism to confirm your identity.

There are different mechanisms for authenticating and authorizing users in a system. In the ESA, REST API services are only accessible to authorized users. You can authorize or authenticate users using one of the following authentication mechanisms:

- Basic Authentication with username and password
- Client Certificates

- Tokens

3.4.7.1 Using Basic Authentication

In the Basic Authentication mechanism, you provide only the user credentials to access protected resources on the server. You provide the user credentials in an authorization header to the server. If the credentials are accurate, then the server provides the required response to access the APIs.

If you want to access the REST API services on ESA, then the IP address of ESA with the username and password must be provided. The ESA matches the credentials with the LDAP or AD. On successful authentication, the roles of the users are verified. The following conditions are checked:

- If the role of the user is **Security Officer**, then the user can run read and write operations on the REST APIs
- If the role of the user is **Security Viewer**, then the user can only run read operations on the REST APIs

The following Curl snippet provides an example to access an API on ESA.

```
curl -i -X <METHOD> "https://<ESA IP address>/<path of the API>" -d  
"loginname=<username>&password=<password>"
```

Note:

This command uses an SSL connection. If the server certificates are not configured on ESA, you can append **--insecure** to the curl command.

For example,

```
curl -i -X <METHOD> "https://<ESA IP address>/<path of the API>" -d  
"loginname=<username>&password=<password>" --insecure
```

You must provide the username and password every time you access the REST APIs on ESA.

3.4.7.2 Using Client Certificates

The Client Certificate authentication mechanism is a secure way of accessing protected resources on a server. In the authorization header, you provide the details of the client certificate. The server verifies the certificate and allows you to access the resources. When you use certificates as an authentication mechanism, then the user credentials are not stored in any location.

On ESA, the Client Certificate authentication includes the following steps:

1. In the authorization header, you must provide the details, such as, client certificate, client key, and CA certificate.
2. The ESA retrieves the name of the user from the client certificate and authenticates it with the LDAP or AD.
3. After authenticating the user, the role of that user is validated:
 - If the role of the user is **Security Officer**, then the user can run read and write operations on the REST APIs.
 - If the role of the user is **Security Viewer**, then the user can only run read operations on the REST APIs.
4. On successful authentication, you can utilize the API services.

The following Curl snippet provides an example to access an API on ESA.

```
curl -k https://<ESA IP Address>/<path of the API> -X <METHOD> --key <client.key> --  
cert <client.pem> --cacert <CA.pem> -v --insecure
```

You must provide your certificate every time you access the REST APIs on ESA.

Note:

As a security feature, it is recommended to use client certificates that are protected with a passphrase.

3.4.7.3 Using JSON Web Token (JWT)

Tokens are reliable and secure mechanisms for authorizing and authenticating users. They are stateless objects created by a server that contain information to identify a user. Using a token, you can gain access to the server without having to provide the credentials for every resource. You request a token from the server by providing valid user credentials. On successive requests to the server, you provide the token as a source of authentication instead of providing the user credentials.

There are different mechanisms for authenticating and authorizing users using tokens. Authentication using JSON Web Tokens (JWT) is one of them. The JWT is an open standard that defines a secure way of transmitting data between two entities as JSON objects.

One of the common uses of JWT is as an API authentication mechanism that allows you to access the protected API resources on your server. You present the JWT generated from the server to access the protected APIs. The JWT is signed using a secret key. Using this secret key, the server verifies the token provided by the client. Any modification to the JWT results in an authentication failure. The information about tokens are not stored on the server.

Note:

Only a privileged user can create a JWT. To create a token, ensure that the **Can Create JWT** Token permission/privilege is assigned to the user role.

The JWT consists of the following three parts:

- **Header:** The header contains the type of token and the signing algorithm, such as, HS512, HS384, or HS256.
- **Payload:** The payload contains the information about the user and additional data.
- **Signature:** Using a secret key, you create the signature to sign the encoded header and payload.

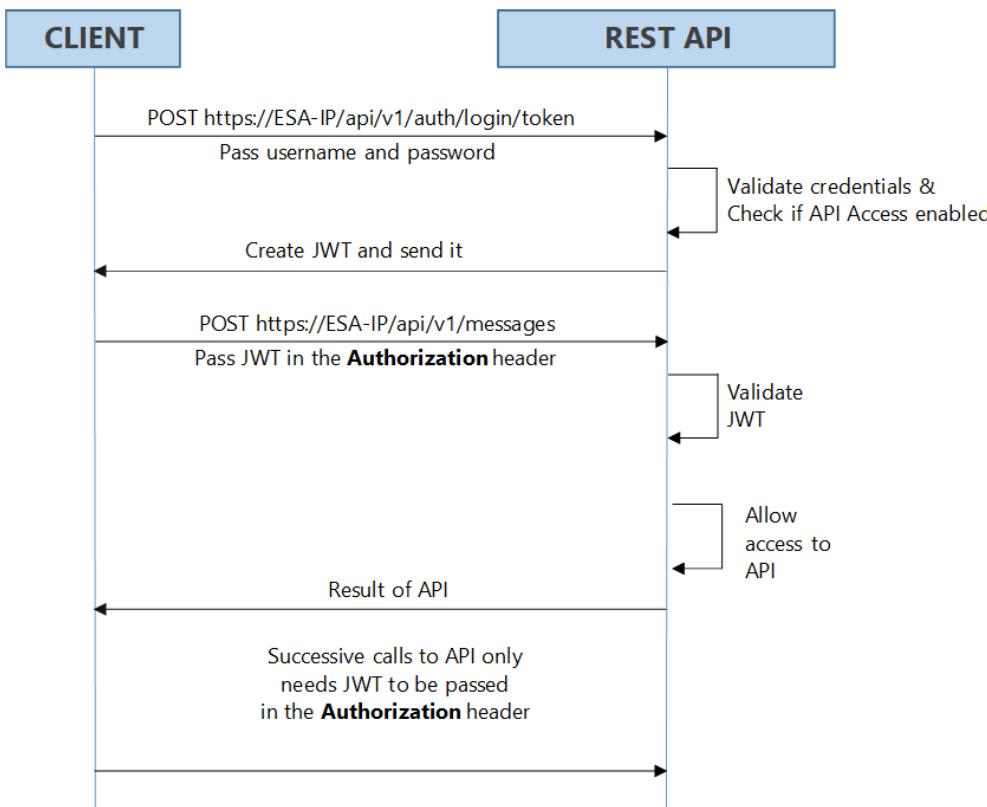
The header and payload are encoded using the *Base64Url* encoding. The following is the format of JWT:

<encoded header>. <encoded payload>. <signature>

3.4.7.3.1 Implementing JWT

On Protegility appliances, you must have the required authorization to access the REST API services. The following figure illustrates the flow of JWT on the appliances.





As shown in the figure, login with your credentials to access the API. The credentials are validated against a local or external LDAP. A verification is performed to check the API access for the username. After the credentials are validated, a JWT is created and sent to the user as an authentication mechanism. Using JWT, information can be verified and trusted as it is digitally signed. The JWTs can be signed using a secret with the HMAC algorithm or a private key pair using RSA. After you successfully login using your credentials, a JWT is returned from the server. When you want to access a protected resource on the server, you must send the JWT with the request in the headers.

3.4.7.3.2 Working with the Secret Key

The JWT is signed using a private secret key and sent to the client to ensure message is not changed during transmission. The secret key encodes that token sent to the client. The secret key is only known to the server for generating new tokens. The client presents the token to access the APIs on the server. Using the secret key, the server validates the token received by the client.

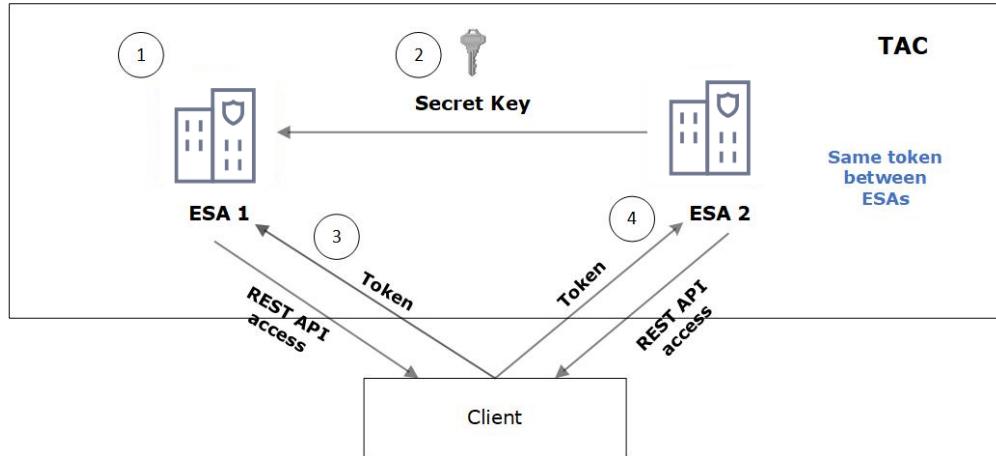
The secret key is generated when you install or upgrade your appliance. You can change the secret key from the CLI Manager. This secret key is stored in the appliance in a scrambled form.

For more information about setting the secret key, refer to section [Configuring JWT](#).

For appliances in a TAC, the secret key is shared between appliances in the cluster. Using the export-import process for a TAC, secret keys are exported and imported between the appliances.

If you want to export the JWT configuration to a file or another machine, ensure that you select the **Appliance OS Configuration** option in the **Export** screen. Similarly, if you want to import the JWT configurations between appliances in a cluster, from the **Cluster Export Wizard** screen, select the **Appliances JWT Configuration** check box under **Appliance OS Configuration**.

For example, consider ESA 1 and ESA 2 in a TAC setup.



1. JWT is created on ESA 1 for appliance using a secret key.
2. ESA 1 and ESA 2 are added to TAC. The secret key of ESA 1 is shared with ESA 2.
3. Client application requests API access from ESA 1. A JWT is generated and shared with the client application. The client accesses the APIs available in ESA 1.
4. To access the APIs of ESA 2, the same token generated by ESA1 is applicable for authentication.

3.4.7.3.3 Configuring JWT

You can configure the encoding algorithm, secret key, and JWT token expiry.

► To configure the JWT settings:

1. On the CLI Manager, navigate to **Administration > JWT Configuration**.
A screen to enter the root credentials appears.
2. Enter the root credentials.
The **JWT Settings** screen appears.
3. Select **Set JWT Algorithm** to set the algorithm for validating a token.
The **Set JWT Algorithm** screen appears.
 - a. Select the one of the following algorithms:
 - HS512
 - HS384
 - HS256
 - b. Select **OK**.
4. Select **Set JWT Secret** to set the secret key.
The **Set JWT Secret** screen appears.
 - a. Enter the secret key in the **New Secret** and **Confirm Secret** text boxes.
 - b. Select **OK**.
5. Set the token expiry period in the **Set Token Expiry** and **Set Token Expiry Unit** text boxes.
6. Select **Done**.

3.4.7.3.4 Refreshing JWT

Tokens are valid for certain period. When a token expires, you must request a new token by providing the user credentials. Instead of providing your credentials on every request, you can extend your access to the server resources by refreshing the token.

In the refresh token process, you request a new token from the server by presenting your current token instead of the username and password. The server checks the validity of the token to ensure that the current token is not expired. After the validity check is performed, a new token is issued to you for accessing the API resources.

In the Protegility appliances, you can refresh the token by executing the REST API for token refresh.

3.4.8 Securing the GRand Unified Bootloader (GRUB)

When a system is powered on, it goes through a boot process before loading the operating system, where an initial set of operations are performed for the system to function normally. The boot process consists of different stages, such as, checking the system hardware, initializing the devices, and loading the operating system.

When the system is powered on, the BIOS performs the Power-On Self-Test (POST) process to initialize the hardware devices attached to the system. It then executes the Master Boot Record (MBR) that contains information about the disks and partitions. The MBR then executes the GRand Unified Bootloader (GRUB).

The GRUB is an operation that identifies the file systems and loads boot images. The GRUB then passes control to the kernel for loading the operating system. The entries in the GRUB menu can be edited by pressing **e** or **c** to access the GRUB command-line. Some of the entries that you can modify using the GRUB are, loading kernel images, switching kernel images, logging into single user mode, recovering root password, setting default boot entries, initiating boot sequences, viewing devices and partition, and so on.

In the Protegility appliances, GRUB version 2 (GRUB 2) is used for loading the kernel. If the GRUB menu settings are modified by an unauthorized user with malicious intent, it can induce threat to the system. Additionally, as per CIS Benchmark, it is recommended to secure the boot settings. Thus, to enhance security of the Protegility appliances, the GRUB menu can be protected by setting a username and password.

Note:

- This feature available only for on-premise installations
- It is recommended to reset the credentials at regular intervals to secure the system.

The following sections describe about setting user credentials for accessing the GRUB menu on the appliance.

3.4.8.1 Enabling the Credentials for the GRUB Menu

You can set a username and password for the GRUB menu from the appliance CLI Manager.

Note:

The user created for the GRUB menu is neither a policy user nor an ESA user.

Note:

Ensure that the backup of the system is completed.

► To enable access to GRUB menu:

1. Login to the appliance CLI manager as an administrative user.
2. Navigate to **Administration > GRUB Credentials Settings**.
The screen to enter the root credentials appears.
3. Enter the root credentials and select **OK**.
The screen to **Grub Credentials** screen appears.
4. Select **Enable** and press **ENTER**.
The following screen appears.

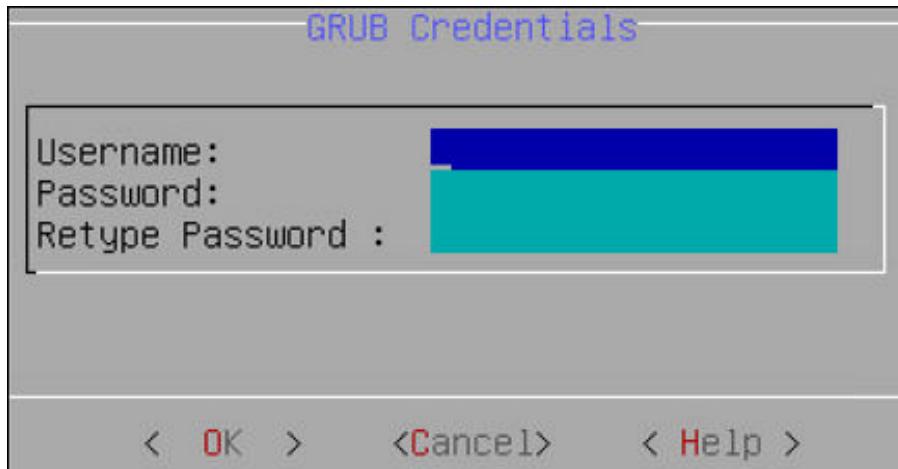


Figure 3-18: GRUB Credentials screen

5. Enter a username in the **Username** text box.

Note:

The requirements for the **Username** are as follows:

- It should contain a minimum of three and maximum of 16 characters
- It should not contain numbers and special characters

6. Enter a password in the **Password** and **Re-type Password** text boxes.

Note:

The requirements for the **Password** are as follows:

- It must contain at least eight characters
- It must contain a combination of alphabets, numbers, and printable characters

7. Select **OK** and press **ENTER**.

A message *Credentials for the GRUB menu has been set successfully* appears.

8. Restart the system.

The following screen appears.



Figure 3-19: GRUB Menu

9. Press **e** or **c**.
The screen to enter the credentials appears.
10. Enter the credentials provided in steps 4 and 5 to modify the GRUB menu.

3.4.8.2 Disabling the GRUB Credentials

You can disable the username and password that is set for accessing the GRUB menu. When you disable access to the GRUB, then the username and password that are set get deleted. You must enable the **GRUB Credentials Settings** option and set new credentials to secure the GRUB again.

► To disable access to the GRUB menu:

1. Login to the appliance CLI Manager as an administrative user.
2. Navigate to **Administration > GRUB Credentials Settings**.
The screen to enter the root credentials appears.
3. Enter the root credentials and select **OK**.
The **GRUB credentials** screen appears.
4. Select **Disable** and press **ENTER**.
A message *Credentials for the GRUB menu has been disabled* appears.

3.4.9 Working with Installations and Patches

Using the **Installations and Patches** menu, you can install or uninstall the products. You can also view and manage the patches from this menu.

3.4.9.1 Add/Remove Services

Using **Add/Remove Services** tool, you can install the necessary products or remove already installed ones.

► To install services:

1. Login to the appliance CLI Manager.
2. Navigate to **Administration > -- Installations and Patches -- > Add/Remove Services**.
3. Enter the root password to execute the install operation and click **OK**.
4. Select **Install applications** and click **OK**.

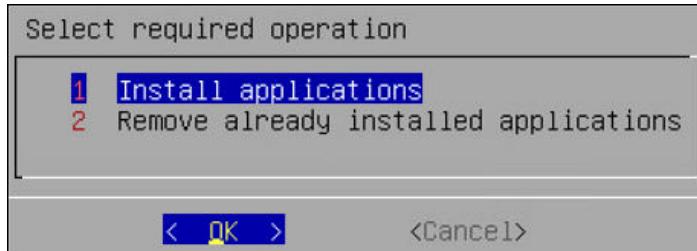


Figure 3-20: Select Install or Uninstall Screen

5. Select products to install and select **OK**.

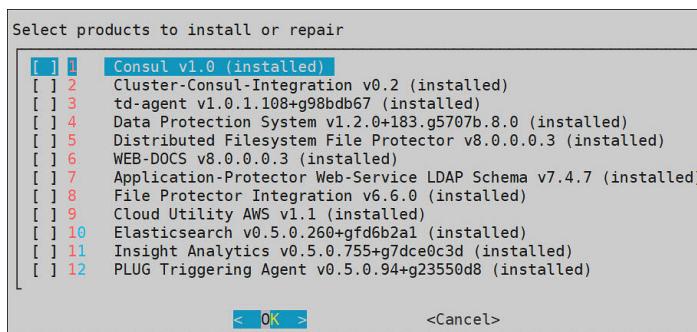


Figure 3-21: Install Products

Note:

- If a new product is selected, the installation process starts.
- If the product is already installed, then refer to step 6.

6. Select an already installed product to upgrade, uninstall, or reinstall, and click **OK**..
- a. The **Package is already installed** screen appears.

Note:

This step is not applicable for the DSG appliance.

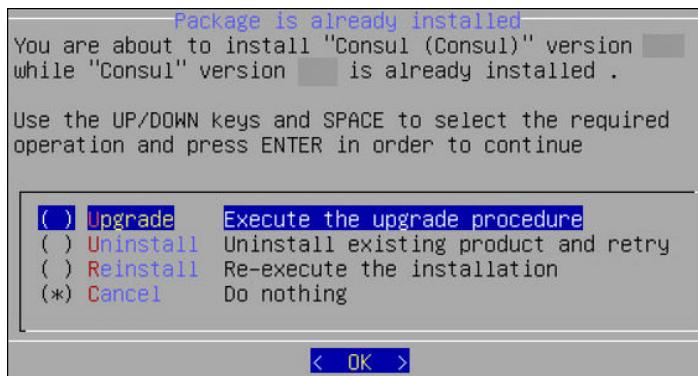


Figure 3-22: Select Upgrade or Uninstall or Reinstall Products Screen

- Select any one of the following options:

Table 3-8:

Option	Description
Upgrade	Installs a newer version of the selected product.
Uninstall	Removes the selected product.
Reinstall	Removes and installs the product again.
Cancel	Returns to the Administration menu.

- Select **OK**.

3.4.9.2 Uninstalling Products

► To uninstall products:

- Login to CLI.
- Proceed to **Administration > --Installations and Patches-- > Add or Remove Services**.
- Enter the root password to execute the uninstall operation.
- Select **Remove already installed applications** and click **OK**.
The **Select products to uninstall** screen appears.
- Select the necessary products to uninstall and click **OK**.
The selected products are uninstalled.

3.4.9.3 Managing Patches

You can install and manage your patches from the Patch Management screen.

It allows you to perform the following tasks.

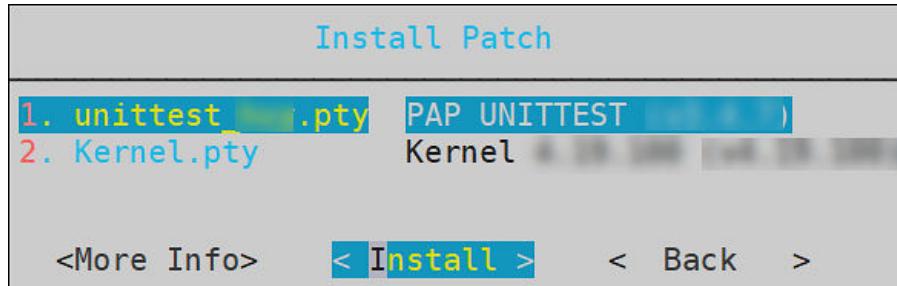
Option	Description
List installed patches	Displays the list of all the patches which are installed in the system.
Install a patch	Allows you to install the patches
Display log	Displays the list of logs for the patches.

3.4.9.3.1 Installing Patches

► To install a patch:

1. Login to the CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Choose **Install a patch** and select **OK**.

The screen *Install Patch* appears.



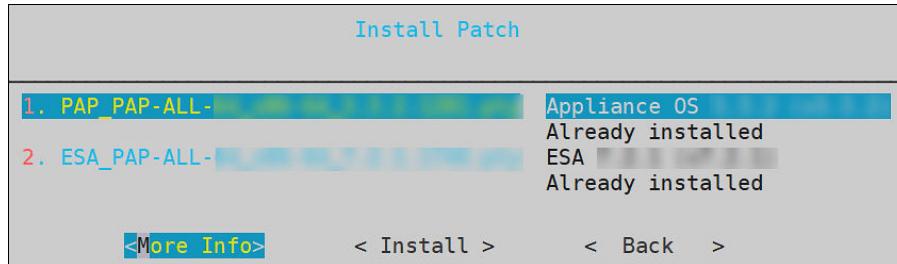
5. Choose the required patch and select **Install**.

3.4.9.3.2 Viewing Patch Information

► To view information of a patch:

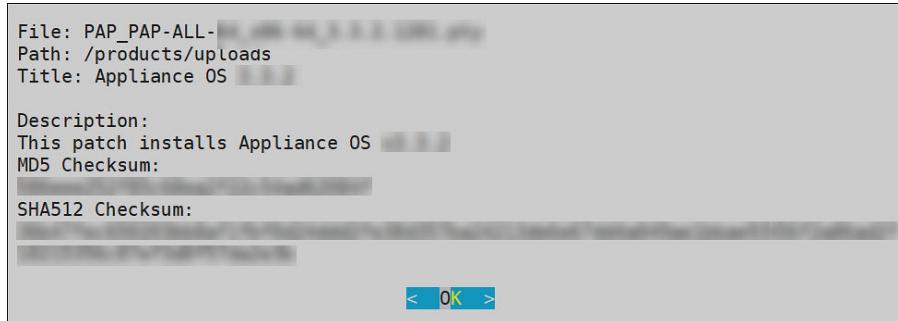
1. Login to the CLI Manager.
2. Navigate to **Administration > Patch Management**.
3. Enter the *root* password.
4. Choose **Install a patch** and select **OK**.

The screen *Install Patch* appears.



5. Choose the required patch and select **More Info**.

The information for the selected patch appears.



3.4.10 Managing LDAP

LDAP is an open industry standard application protocol that is used to access and manage directory information over IP. You can consider it as a central repository of username and passwords, thus providing applications and services the flexibility to validate users by connecting with the LDAP.

The security system of the Appliance distinguishes between two types of users:

- End users with specific access or no access to sensitive data. These users are managed through the User Management screen in the Web UI. For more information about user management, refer to [Managing Users](#).
- Administrative users who manage the security policies, for example, ‘Admin’ users who grant or deny access to end users

In this section, the focus is on managing administrative users. The Administrative users connect to the management interfaces in Web UI or CLI, while the end users connect to the specific security modules they have been allowed access to. For example, a database table may need to be accessed by the end users, while the security policies for access to the table are specified by the Administrative users.

LDAP Tools available in the Administration menu include three tools explained in the following table.

Table 3-9: LDAP Tools

Tool	Description
Specify LDAP Server	<p>Reconfigure all client-side components to use a specific LDAP. To authenticate users, the data security platform supports three modes for integration with directory services: Protegity LDAP Server, Proxy Authentication, and Local LDAP Server.</p> <ul style="list-style-type: none"> • Protegity LDAP: In this mode, all administrative operations such as policy management, key management, etc. are handled by users that are part of the Protegity LDAP. This mode can be used to configure or authenticate with either local or remote appliance product. • Proxy Authentication: In this mode, you can import users from an external LDAP to ESA. ESA is responsible for authorization of users, while the external LDAP is responsible for authentication of users. • Reset LDAP Server Settings: In this mode, administrative users can reset the configuration to the default configuration using admin credentials.
Configure Local LDAP settings	Configure your LDAP to be accessed from the other machines.
Local LDAP Monitor	Examine how many LDAP operations per second are running.

3.4.10.1 Working with the Protegity LDAP Server

Every appliance includes an internal directory service. This service can be utilized by other appliances for user authentication.

For example, a DSG instance might utilize the ESA LDAP for user authentication. In such cases, you can configure the LDAP settings of the DSG in the **Protegity LDAP Server** screen. In this screen, you can specify the IP address of the ESA with which you want to connect.

You can add IP addresses of multiple appliances to enable fault tolerance. In this case, if connection to the first appliance fails, connection is transferred to next appliance in the list.

Note:

If you are adding multiple appliances in the **LDAP URI**, ensure that the values of the **Bind DN**, **Bind Password**, and **Base DN** is same for all the appliances in the list.

► To specify Protegity LDAP server:

1. Login to CLI Manager using the admin credentials.
2. Navigate to **Administration > Specify LDAP Server**.
3. In the LDAP Server Type screen, select **Protegity LDAP Server**.
The following screen appears.

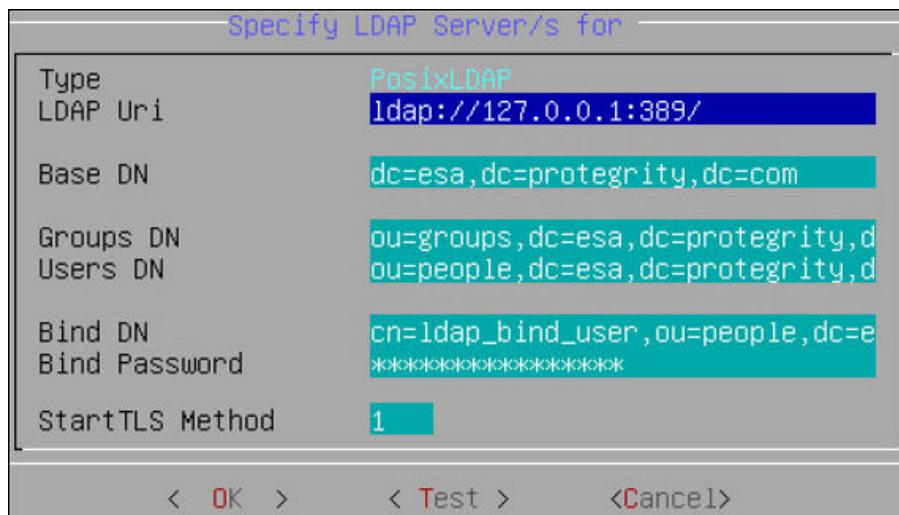


Figure 3-23: Specify LDAP Server

4. Enter information for the following fields.

Table 3-10: LDAP Server Settings

Setting	Description
LDAP URI	<p>Specify the IP address of the LDAP server you want to connect to in the following format. <i>ldap://host:port</i>. You can configure to connect Protegity Appliance LDAP. For example, <i>ldap://192.168.3.179:389</i>.</p> <p>For local LDAP, enter the following IP address: <i>ldap://127.0.0.1:389</i>.</p> <p>If you specify multiple appliances, ensure that the IP addresses are separated by the space character.</p>

Setting	Description
	For example, <code>ldap://192.1.1.1 ldap://10.0.0.0 ldap://127.0.0.1:389</code>
Base DN	The LDAP Server Base distinguished name. For example: ESA LDAP Base DN: dc=esa,dc=protegrity,dc=com.
Group DN	Distinguished name of the LDAP Server group container. For example: ESA LDAP Group DN: <code>ou=groups,dc=esa,dc=protegrity,dc=com.</code>
Users DN	Distinguished name of the user container. For example: ESA LDAP Users DN: <code>ou=people,dc=esa,dc=protegrity,dc=com.</code>
Bind DN	Distinguished name of the LDAP Bind User. For example: ESA LDAP Bind User DN <code>cn=admin, ou=people, dc=esa, dc=protegrity, dc=com</code> .
Bind Password	<p>The password of the specified LDAP Bind User. If you modify the bind user password, ensure that you use the Specify LDAP Server tool to update the changes in the internal LDAP.</p> <p>Bind User</p> <p>The bind user account password allows you to specify the user credentials used for LDAP communication. This user should have full read access to the LDAP entries in order to obtain accounts/groups/permissions.</p> <p>If you are using the internal LDAP, and you change the bind username/password, using Change a directory account option, then you must update the actual LDAP user. Make sure that a user with the specified username/password exists. Run Specify LDAP Server tool with the new password to update all the products with the new password (refer to section Protegrity LDAP Server for details).</p>

- Click **Test** to test the connection.

If the connection is established, then a *Successfully Done* message appears.

3.4.10.2 Changing the Bind User Password

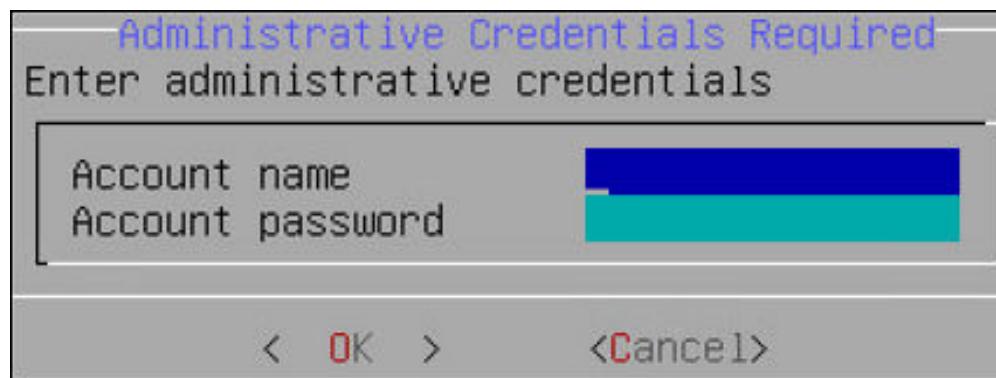
The following section describe the steps to change the password for the `ldap_bind_user` using the CLI manager.

► To change the `ldap_bind_user` passwords:

- Login to the CLI Manager using the `local admin` user.
- Navigate to **Administration > Specify LDAP server/s**.
- Enter the **root** password.

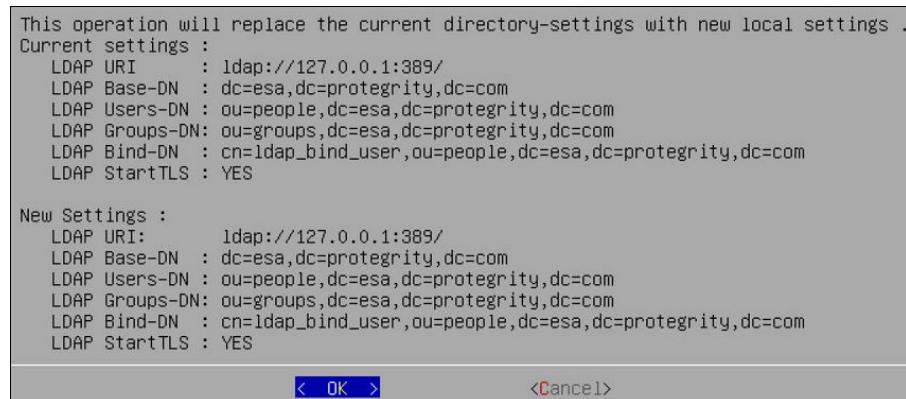
4. Select **Reset LDAP Server settings**.

The following screen appears.



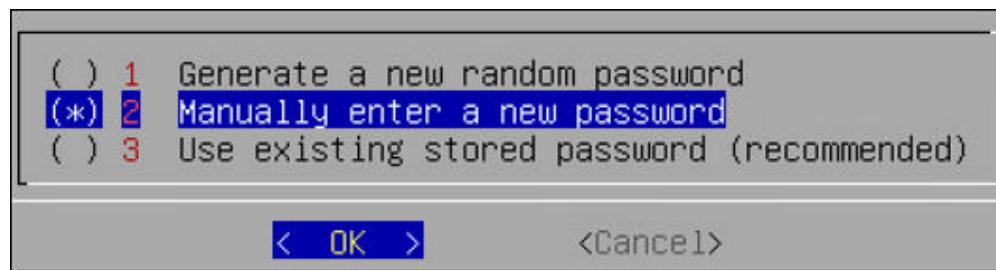
5. Enter the *admin* username and password, and then press OK.

The following screen appears.



6. Select **OK**.

The following screen appears.



7. Select **Manually enter a new password** and select **OK**.

The following screen appears.



8. Enter the new password and select **OK**.

The following screen appears.



9. Select **OK**.

The password is successfully changed.

3.4.10.3 Working with Proxy Authentication

The Simple Authentication and Security Layer (SASL) is a framework that provides authentication and data security for Internet protocols. The data security layer offers data integrity and confidentiality services. It provides a structured interface between protocols and authentication mechanisms.

SASL 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. SASL is referred to as Proxy authentication in ESA CLI and Web UI.

► To enable proxy authentication:

1. Navigate to **Administration > LDAP Tools > Specify LDAP Server**.
2. Enter the root password and select **OK**.
3. Select **Set Proxy Authentication**.
4. Specify the LDAP Server settings for proxy authentication with external LDAP as shown in the following figure.

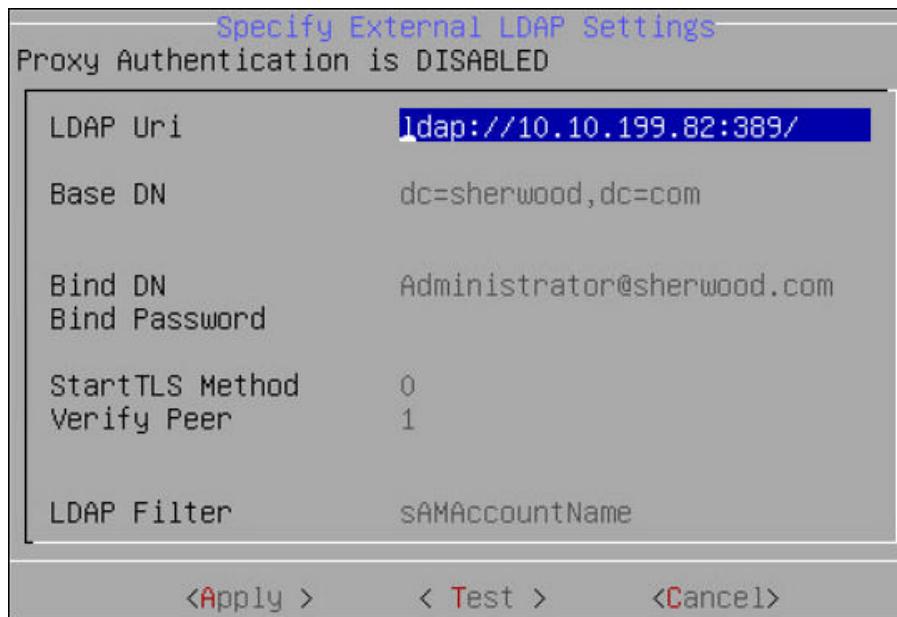


Figure 3-24: External LDAP Server

For more information about the LDAP settings, refer to *Proxy Authentication Settings*.

5. Select **Test** to test the settings provided.

Note:

When you click Test, ESA verifies if connection to external LDAP works as per the Proxy Authentication settings provided.

6. Enter the LDAP user name and password provided as the bind user.

You can provide username and password of any other user from the LDAP as long as the LDAP Filter field exists in both the bind user name and any other user.

A *Testing Proxy Authentication-Completed successfully* message appears.

7. Click **OK** in the following message screen.

The following confirmation message appears.

Proxy Authentication is set and ready.
Please choose which user will be assigned with administrator privileges.

< **OK** >

8. Select **Apply** to apply the settings.

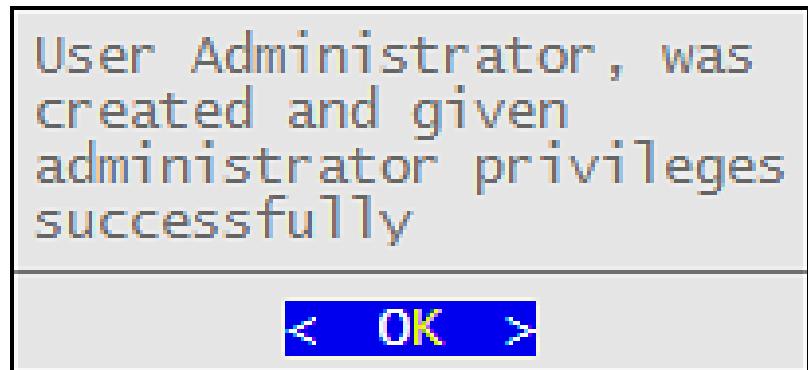
Note:

In ESA CLI, only one user is allowed to be imported. This user is granted admin privileges, such that importing users and managing users can be performed by the user in the User Management screen. The User Management web UI is used to import users from the external LDAP.

9. In the select user to grant administrative privileges screen, select a user and confirm selection.

10. In the **Setup administrator privileges** screen, enter the ESA admin user name and password, and then select **OK**.

The following message appears.



11. Navigate to **Administration > Services** to verify that the *Proxy Authentication Service* is running.

Service Management		
OS		
NTP Service		Stopped
Web Interface		Running
Secured Shell (SSH)		Running
Firewall		Running
Realtime Graphs		Running
SNMP Service		Stopped
Cluster Status		Stopped
Appliance Heartbeat Server		Running
Appliance Heartbeat Client		Running
Log Filter Server		Running
Messaging System		Running
Appliance Queues Backend		Running
LDAP		
LDAP Server		Running
Proxy Authentication Service		Running
Web Services Engine		Running
Web-Services Engine		
Service Dispatcher		
Service Dispatcher		Running
Logging		
Management Server		Running
Management Server Database		Running
Policy Management		
Policy Repository		Running
Admin-Server		Running
v(+)		76%
<Refresh> <Select > < Exit >		

3.4.10.4 Configuring Local LDAP Settings

The local LDAP settings are enabled on port 389 by default.

► To specify local LDAP server configuration:

1. Proceed to **Administration > Configure local LDAP listening addresses**.
2. Enter the *root* username and password, and then press OK.

The following screen appears.

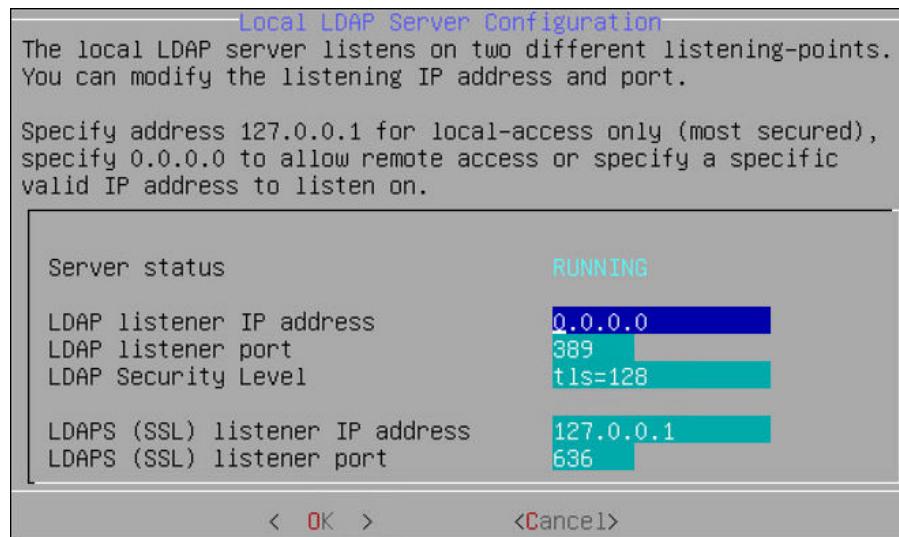


Figure 3-25: Specify LDAP Server

3. Specify **LDAP listener IP address** for local access. By default, it is 127.0.0.1.
4. Specify **SSL listener IP address** for remote access. It is 0.0.0.0 or a specific valid address for your remote LDAP directory.

3.4.10.5 Monitoring Local LDAP

Local LDAP Monitor tool allows you to examine, in real time, how many operations per second LDAP operations are currently running, which is very useful to enhance the performance. You can use this tool to monitor the following tasks:

- Check LDAP Connectivity (LDAP Bind and LDAP Search)
- Modify or optimize LDAP cache/threading/memory settings to improve performance and remove bottlenecks
- Measure "number of changes" and "last modified date and time" on the LDAP server, which can be useful, for example, for verifying export/import operations

```
Local LDAP Statistics 15:22:07
Modify      : 0
Add         : 0
Delete      : 0
Bind        : 7
Unbind      : 0
Search       : 0
Compare     : 0
```

Figure 3-26: Local LDAP Statistics

3.4.10.6 Optimizing Local LDAP Settings

When the Local LDAP receives excessive requests, the requests are cached. However, if the cache is overloaded, it causes the LDAP to become unresponsive. From v9.1.0.3, a standard set of values for the cache that is required for optimal handling of the LDAP requests is set in the system. After you upgrade to v9.1.0.3 or higher, you can tune the cache parameters for the Local LDAP configuration. The default values for the cache parameters is shown in the following list.

- The *slapd.conf* file in the */etc/ldap* directory contains the following cache values:
 - *cachesize 10000* (10,000 entries)
 - *idlecachesize 30000* (30,000 entries)

- `dbconfig set_cachesize 0 209715200 0` (200 MB)
- The `DB_CONFIG` file in the `/opt/ldap/db` directory contains the following the cache values:
 - `set_cachesize 0 209715200 0` (200 MB)

Based on the setup and the environment in the organization, you can choose to increase the parameters.

Note:

Ensure that you back up the files before editing the parameters.

1. On the CLI Manager, navigate to **Administration > OS Console**.
2. Edit the values for the required parameters.
3. Restart the `slapd` service using the `/etc/init.d/slapd restart` command.

3.4.11 Rebooting and Shutting down

You can reboot or shut down your appliance if necessary using **Administration > Reboot and Shutdown**. Make sure the Data Security Platform users are aware that the system is being rebooted or turned off and no important tasks are being performed at this time.

Note:

In case of cloud platforms, such as, Azure, AWS or GCP, the instances run the appliance. Powering off the instance from the cloud console might not shut down the appliance gracefully. Hence, it is recommended to power off from the CLI Manager or Appliance Web UI.

3.4.12 Accessing the OS Console

You can access OS console using **Administration > OS Control**. You require `root` user credentials to access the OS console.

If you have System Monitor settings enabled in the Preferences menu, then the OS console will display the system monitor screen upon entering the OS console.

► To enable the System Monitor setting:

1. Select **Preferences** from the main menu in ESA CLI.
2. Change `Show System-Monitor` on OS-Console to Yes.
3. Select **Done**.
4. Press **ENTER**.

3.5 Working with Networking

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, and network firewall.

From the CLI Manager, navigate to **Networking** to manage your network settings.

The following figure shows the Networking Management screen.

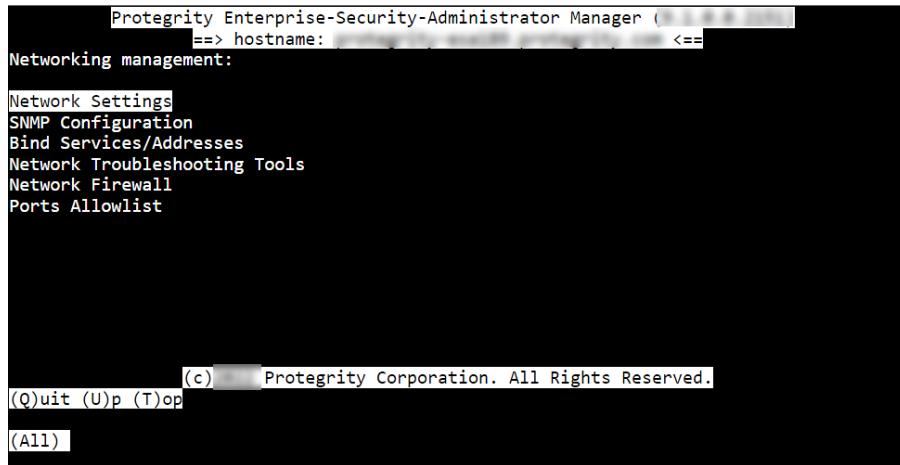


Figure 3-27: Networking Options Screen

Table 3-11: Network Screen Fields

Option	Description
Network Settings	Customize the network configuration settings for your appliance.
SNMP Configuration	Allow a remote machine to query different performance status of the Appliance, such as start the service, set listening address, show or set community string, or refresh the service.
Bind Services/ Addresses	Specify the network address or addresses for management and Web Services.
Network Troubleshooting Tools	Troubleshoot network and connectivity problems using the following Linux commands – Ping, TCPing, TraceRoute, MTR, TCPDump, SysLog, and Show MAC.
Network Firewall	Customize firewall rules for the network traffic.

3.5.1 Configuring Network Settings

When this option is selected, network configuration details added during installation are displayed. The network connection for the appliance are displayed. You can modify the network configuration as per the requirements.

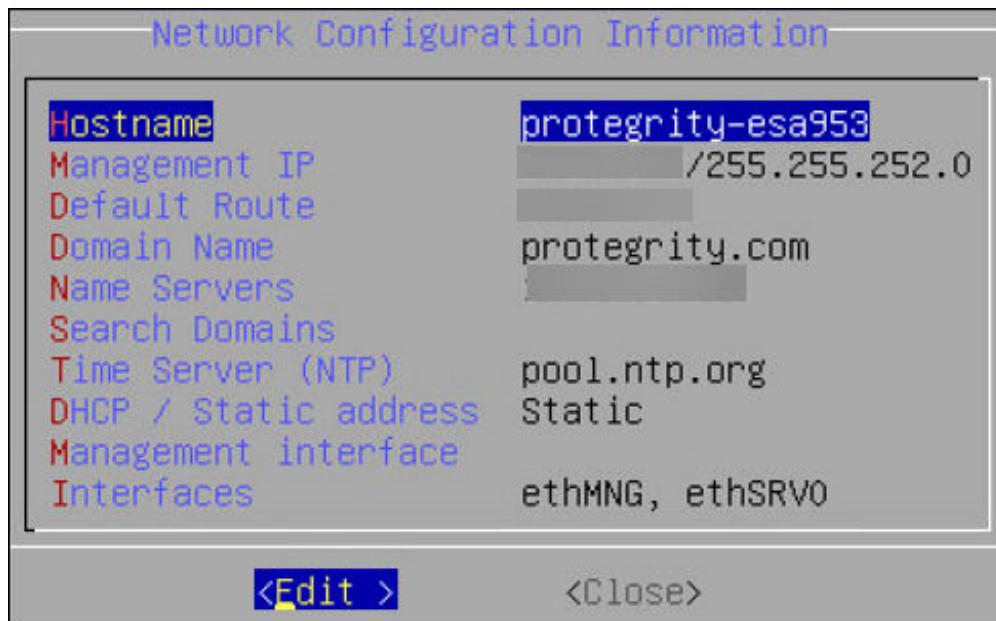


Figure 3-28: Networking Configuration Edit Screen

3.5.1.1 Changing Hostname

You can change the host name of the appliance.

► To change the hostname:

1. Navigate to **Networking > Network Settings**.
2. Choose **Hostname** and select **Edit**.
3. At the prompt, type the new hostname.
4. Select **OK** and press **ENTER**.
The hostname is changed.

3.5.1.2 Configuring Management IP Address

You can configure the management IP address for your appliance from the networking screen.

► To configure the management IP address:

1. Navigate to **Networking > Network Settings**.
2. Choose **Management IP** and select **Edit**.
3. Enter the IP address of the management NIC in the **Enter IP** text box.
4. Enter the subnet for the management NIC in the **Enter Netmask** text box.
5. Select **OK** and press **ENTER**.
The management IP is configured.

3.5.1.3 Configuring Default Route

The default route is a setting that defines the packet forwarding rule for a specific route. This parameter is required only if the appliance is on a different subnet than the Web UI or for the NTP service connection. If necessary, then request the default gateway address from your network administrator and set this parameter accordingly.

Note: The default route is the first IP address of subnet for the management interface.

► To configure the default route:

1. Navigate to **Networking > Network Settings**.
2. Choose **Default Route** and press **Edit**.
3. Enter the default route and select **Apply**.

3.5.1.4 Configuring Domain Name

You can configure the domain name for your appliance from the networking screen.

► To configure the domain name:

1. Navigate to **Networking > Network Settings**.
2. Choose **Domain Name** and select **Edit**.
3. Enter the domain name in the **Set Domain Name** text box.
4. Select **Apply** and press **ENTER**.
The domain name is configured.

3.5.1.5 Configuring Search Domain

You can configure a domain name that is used as in the domain search list.

► To configure the search domain:

1. Navigate to **Networking > Network Settings**.
2. Choose **Search Domain** and select **Edit**.
3. Enter the domain name and select **Ok**.

Note: Select **Add** to add another search domain.

Note: Select **Remove** to remove a search domain

3.5.1.6 Configuring Name Server

On the network settings screen you can configure the IP addresses for your domain name.

► To configure the domain IP address:

1. Navigate to **Networking > Network Settings**.
2. Choose **Name Servers** and select **Edit**.
3. In the **Domain Name Servers** screen, choose **Edit** to modify the server IP address.

Note: Select **Remove** to delete the domain IP address.

Note: Select **Add** to add another domain IP address

4. Enter the domain IP address and select **Ok**.
The IP address for the domain is configured.

3.5.1.7 Assigning a Default Gateway to the NIC

► To assign a default gateway to the NIC:

1. In the CLI Manager, navigate to **Network > Network Settings > Interfaces**.
The **Network Interface** screen appears.
2. Select the interface for which you want to add a default gateway.
3. Select **Edit**.
4. Select **Gateway**.
The **Gateway Settings** screen appears.
5. Enter the Gateway IP address and select **OK**.

3.5.1.8 Selecting Management NIC

When you have multiple NICs, you can specify the NIC that functions as a management interface.

► To select the management NIC:

1. Navigate to **Networking > Network Settings**.
2. Choose **Management interface** and select **Edit**.
3. Select the required NIC.
4. Choose **Select** and press **ENTER**.
The management NIC is changed.

3.5.1.9 Changing the management IP on ethMNG

► Change the management IP on ethMNG:

1. Navigate to **Networking Settings > Interfaces**.
2. Select **ethMNG** and click **Edit**.
3. Choose the network type and select **Update**.
4. In the Interface Settings screen, select **Edit**.
5. Enter the IP address and net mask.
6. Press **ENTER**.
7. At the prompt, press **ENTER** to confirm.

The IP address is updated, and the Address Management screen appears.

Caution:

Changes to IP addresses are immediate. Any changes to the management IP (on ethMNG) while you are connected to CLI Manager or Web UI will cause the session to disconnect.

3.5.1.10 Identifying an Interface

- To identify an interface:

1. Navigate to **Networking > Network Settings**.
2. Select **Interfaces** and select **Edit**.
3. Choose the network interface and select **Blink**.

This causes an LED on the NIC to blink and the **Network Interfaces** screen appears.

3.5.1.11 Adding a service interface address

Note:

From ESA v9.0.0.0, the default IP addresses assigned to the docker interfaces are between *172.17.0.0/16* and *172.18.0.0/16*. Ensure that the IP addresses assigned to the docker interface must not conflict with your organization's private/internal IP addresses.

For more information about reconfiguring the docker interface addresses, refer to section *Appendix: Configuring the IP address for the Docker Interface* in the *Protegy Installation Guide 9.1.0.5*.

- To add a service interface address:

1. From Web UI, proceed to **Network Settings > Interfaces**.
2. Navigate to the service interface to which you want to add an address and select **Update**.
3. Select **Add**.
4. At the prompt, type the IP address and the netmask.
5. Press **ENTER**.

The address is added, and the Address Management screen appears.

Caution:

Changes to IP addresses are immediate.

3.5.2 Configuring SNMP

The Simple Network Management Protocol (SNMP) is used for monitoring appliances in a network. It consists of two entities, namely, an agent and a manager that work in a client-server mode. The manager performs the role of the server and agent acts as the client. Managers collect and process information about the network provided by the client.

For more information about SNMP, refer to the following link.

<http://www.net-snmp.org/>

In Protegity appliances, you can use this protocol to query the performance figures of an appliance. Typically, the ESA acts as a manager that monitors other appliances or Linux systems on the network. In ESA, the SNMP can be used in the following two methods:

snmpd

The *snmpd* is an agent that waits for and responds to requests sent by the SNMP manager. The requests are processed, the necessary information is collected, the requested operation is performed, and the results are sent to the manager. You can run basic SNMP commands, such as, *snmpstart*, *snmpget*, *snmpwalk*, *snmpsync*, and so on. In a typical scenario, an ESA monitors and requests a status report from another appliance on the network, such as, DSG or ESA. By default, the *snmpd* requests are communicated over the UDP port *161*.

In the CLI Manager, navigate to **Networking > SNMP Configuration > Protegity SNMPD Settings** to configure the *snmpd* settings. The *snmpd.conf* file in the */etc/snmp* directory contains the configuration settings of the SNMP service.

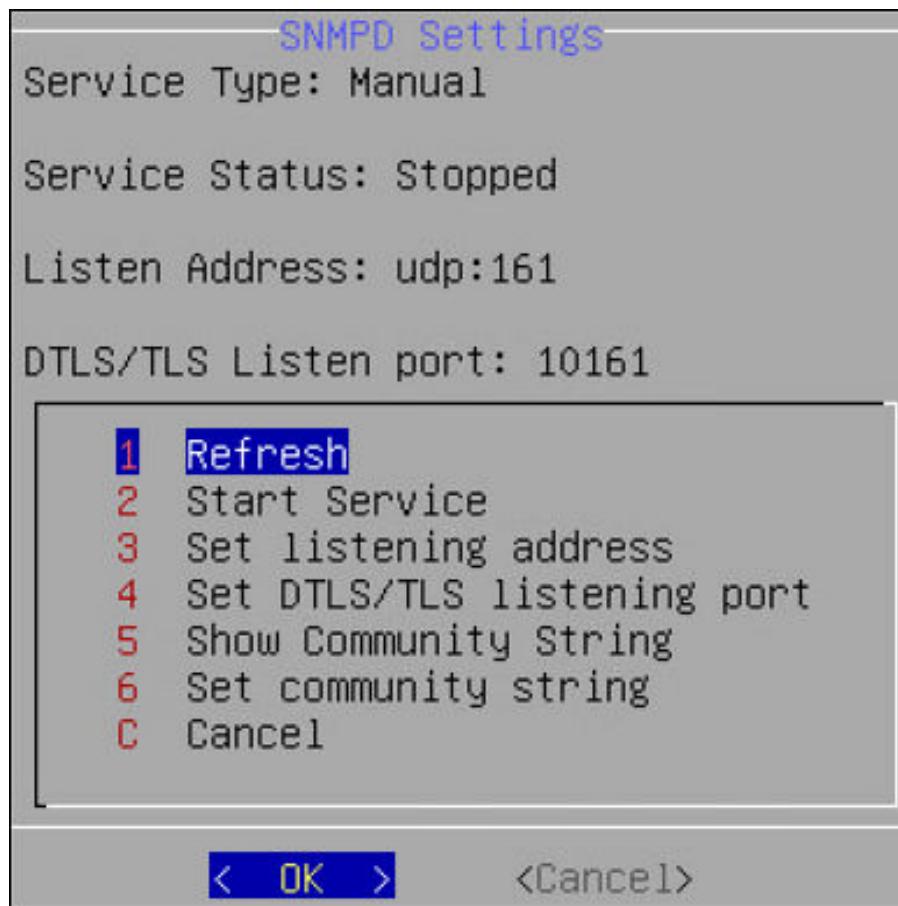


Figure 3-29: SNMPD Settings

snmptrapd

The *snmptrapd* is a service that sends messages to the manager in the form of traps. The SNMP traps are alert messages that are configured in the manager in a way that an event occurring at the client immediately triggers a report to the manager. In a typical scenario, you can create a trap in ESA to cold-start a system on the network in case of a power issue. By default, the *snmptrapd* requests are sent over the UDP port 162. Unlike *snmpd*, in the *snmptrapd* service, the agent proactively sends reports to the manager based on the traps that are configured.

In the CLI Manager, navigate to **Networking > SNMP Configuration > Protegility SNMPTRAPD Settings** to configure the *snmptrapd* settings. The *snmptrapd.conf* file in the */etc/snmp* directory can be edited to configure SNMP traps on ESA.

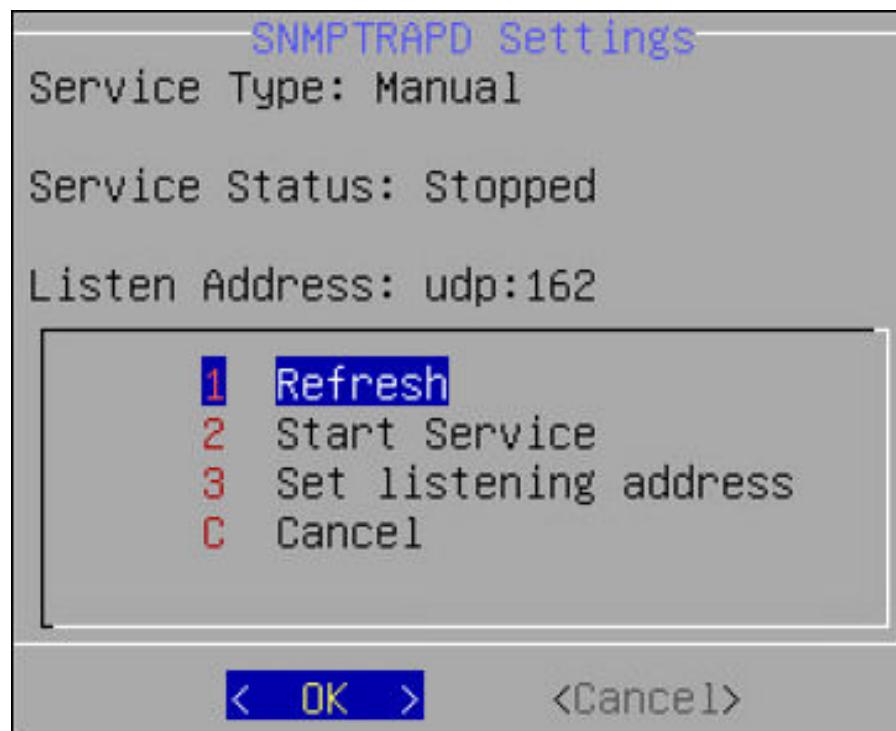


Figure 3-30: SNMPTRAPD Settings

The following table describes the different settings that you configure for *snmpd* and *snmptrapd* services.

Table 3-12:

Setting	Description	Applicable to SNMPD	Applicable to SNMPTRAPD	Notes
Managing service	Start, stop, or restart the service	✓	✓	Ensure that the SNMP service is running. On the Web UI, navigate to System > Services tab to check the status of the service.
Set listening address	Set the port to accept SNMP requests	✓	✓	<ul style="list-style-type: none"> The default port for SNMPD is <i>UDP 161</i> The default port for SNMPTRAPD is <i>UDP 162</i> <p>Note:</p>

Setting	Description	Applicable to SNMPD	Applicable to SNMPTRAPD	Notes
				You can change the listening address only once.
Set DTLS/TLS listening port	Configure SNMP on DTLS over UDP or SNMP on TLS over TCP	✓		The default listening port for SNMPD is set to <i>TCP 10161</i> .
Set community string	String comprising of user id and password to access the statistics of another device	✓		

The SNMPv1 is used as default a protocol, but you can also configure SNMPv2 and SNMPv3 to monitor the status and collect information from network devices. The SNMPv3 protocol supports the following two security models:

- User Security Model (USM)
- Transport Security Model (TSM)

3.5.2.1 Configuring SNMPv3 as a USM Model

► Configuring SNMPv3 as a USM Model:

1. From the CLI manager navigate to **Administration > OS Console**.
The command prompt appears.

2. Perform the following steps to comment the **rocommunity** string.

- a. Edit the *snmpd.conf* using the following command.

```
vi /etc/snmp/snmpd.conf
```

- b. Prepend a # to comment the **rocommunity** string.

- c. Save the changes.

3. Run the following command to set the path for the *snmpd.conf* file.

```
export datarootdir=/usr/share
```

4. Stop the SNMP daemon using the following command:

```
/etc/init.d/snmpd stop
```

5. Add a user with read-only permissions using the following command:

```
net-snmp-create-v3-user -ro -A <authorization password> -a MD5 -X <authorization password> -x DES snmpuser
```

For example,

```
net-snmp-create-v3-user -ro -A snmpuser123 -a MD5 -X snmpuser123 -x DES snmpuser
```

6. Start the SNMP daemon using the following command:

```
/etc/init.d/snmpd start
```

7. Verify if SNMPv1 is disabled using the following command:

```
snmpwalk -v 1 -c public <hostname or IP address>
```

8. Verify if SNMPv3 is enabled using the following command:

```
snmpwalk -u <username> [-A (authphrase)] [-a (MD5/SHA)] [-x DES] [-X (privaphrase)] (<ipaddress>)[:](<dest_port>) [<oid>]
```

For example,



```
snmpwalk -u snmpuser -A snmpuser123 -a MD5 -X snmpuser123 -x DES -l authPriv
127.0.0.1 -v3
```

9. Unset the variable assigned to the *snmpd.conf* file using the following command.

```
unset datarootdir
```

3.5.2.2 Configuring SNMPv3 as a TSM Model

► Configuring SNMPv3 as a TSM Model:

1. From the CLI manager navigate to **Administration > OS Console**.
The command prompt appears.
2. Set up the CA certificates, Server certificates, Client certificates, and Server key on the server using the following commands:

```
ln -s /etc/ksa/certificates/CA.pem /etc/snmp/tls/ca-certs/CA.crt
```

```
ln -s /etc/ksa/certificates/server.pem /etc/snmp/tls/certs/server.crt
```

```
ln -s /etc/ksa/certificates/client.pem /etc/snmp/tls/certs/client.crt
```

```
cp /etc/ksa/certificates/server.key /etc/snmp/tls/private/server.key
```

3. Change the mode of the *server.key* file under */etc/snmp/tls/private/* directory to read only using the following command:
`chmod 600 /etc/snmp/tls/private/server.key`
4. Edit the *snmpd.conf* file under */etc/snmp* directory.
5. Append the following configuration in the *snmpd.conf* file.

```
[snmp] localCert server
[snmp] trustCert CA
certSecName 10 client --sn <username>
Trouser -s tsm "< username>" AuthPriv
```

Alternatively, you can also use a field from the certificate using the *--cn* flag as a username as follows:

```
certSecName 10 client -cn
Trouser -s tsm "Protegrity Client" AuthPriv
```

Note: To use fingerprint as a certificate identifier, execute the following command:

```
net-snmp-cert showcerts --fingerprint
```

6. Restart the SNMP daemon using the following command:

```
/etc/init.d/snmpd restart
```

Note: You can also restart the SNMP service using the ESA Web UI.

7. Deploy the certificates on the client side.

3.5.3 Working with Bind Services and Addresses

The **Bind Services/Addresses** tool allows you to separate the management (Web UI/SSH) and the Web services. You can specify the network cards that will be used for Web management and Web services. For example, the DSG appliance uses the ethMNG

interface for Web UI and the ethSRV interface for enabling communication with different applications in an enterprise. The following steps describe how to select a management and service interfaces.

Note:

Ensure that all the NICs added to the appliance are configured in the *Network Settings* screen.

3.5.3.1 Binding Interface for Management

If you have multiple NICs, you can specify the NIC that functions as a management interface.

► To bind the management NIC:

1. On the CLI Manager, navigate to **Networking > Network Settings > Bind Services/Address**.

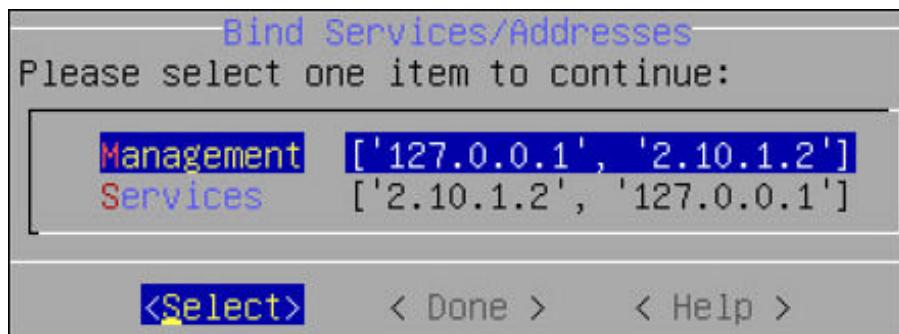


Figure 3-31: Bind Service/Addresses

2. Select **Management** and choose **Select**.
3. In the interface for ethMNG and select **OK**.
4. Choose **Select** and press **ENTER**.
The NIC for Management is assigned.
5. Select **Done**.
A message *Successfully done* appears and the NIC for service requests are assigned.
6. Navigate to **Administration > OS Console** and run the **netstat -tunlp** command to verify the status of the NICs.

```
root@protegility-esa895:/var/www# netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp        0      0  2.10.1.8:22             0.0.0.0:*              LISTEN     9174/sshd
```

Figure 3-32: Status of the Management NIC

3.5.3.2 Binding Interface for Services

If you have multiple service NICs, you can specify the NICs that will function to accept the Web service requests on port 8443.

► To bind the service NIC:

1. On the CLI Manager, navigate to **Networking > Network Settings > Bind Services/Address**.
2. Select **Service** and choose **Select**.
A list of service interfaces with their IP addresses is displayed.
3. Select the required interface(s) for and select **OK**.
The following message appears.

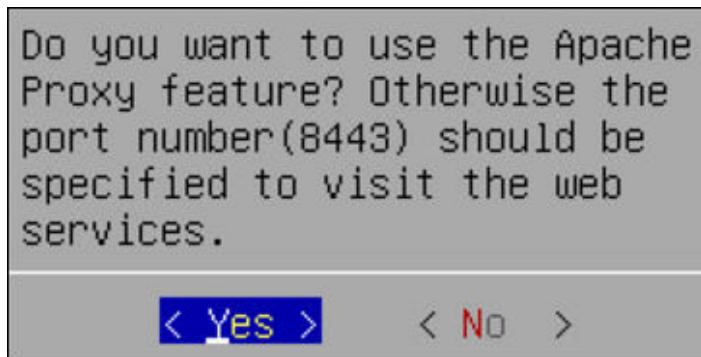


Figure 3-33: Apache Proxy Feature Message

4. Choose **Yes** and press **ENTER**.
5. Select **Done**.
A message *Successfully done* appears and the NIC for service requests are assigned.
6. Navigate to **Administration > OS Console** and run the `netstat -tunlp` command to verify the status of the NICs.

```
root@protegrity-esa895:/var/www# netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp        0      0 2.10.1.11:8443           0.0.0.0:*              LISTEN     8442/apache2
tcp        0      0 2.10.1.9:8443           0.0.0.0:*              LISTEN     8442/apache2
tcp        0      0 2.10.1.8:443            0.0.0.0:*              LISTEN     8442/apache2
```

Figure 3-34: Status of the Service NICs

3.5.4 Using Network Troubleshooting Tools

Using the **Network Troubleshooting Tools**, you can check the health of your network and troubleshoot problems. This tool is composed of several utilities that allow you to test the integrity of your network. The following table describes the utilities that make up the Network Utilities tool.

Table 3-13: Network Utilities

Name	Using this tool you can...	How...
Ping	Tests whether a specific Host is accessible across the network.	In the Address field, type the IP address that you want to test. Press ENTER.
TCPing	Tests whether a specific TCP port on a Host is accessible across the network.	In the Address field, type the IP address. In the Port field, type the port number. Select OK.
TraceRoute	Tests the path of a packet from one machine to another. Returns timing information and the path of the packet.	At the prompt, type the IP address or Host name of the destination machine. Select OK.
MTR	Tests the path of a packet and returns the list of routers traversed and some statistics about each.	At the prompt, type the IP address or Host name. Select OK.
TCPDump	Tests network traffic, and examines all packets going through the machine	To filter information (by network interface, protocol, Host, or port), type the criteria in the corresponding text boxes. Select OK.
SysLog	Sends syslog messages. Can be used to test syslog connectivity.	In the Address field, enter the IP address of the remote machine the syslogs will be sent to. In the Port field, enter a port number the remote machine is listening to. In the Message field, enter a test message. Select OK. On the remote machine, check if the syslog was successfully sent. Note that the appliance uses UDP syslog, so there is no way to validate whether the syslog server is accessible.
Show MAC	Finds out the MAC address for a given IP address. Detects IP collision.	At the prompt, type the IP address or Host name. Select OK.

3.5.5 Managing Firewall Settings

Protegility internal Firewall provides a way to allow or restrict inbound access from the outside to Protegility Appliances. Using the Network Firewall tool you can manage your Firewall settings. For example, you can allow access to the management-network interface only from a specific machine while denying access to all other machines.

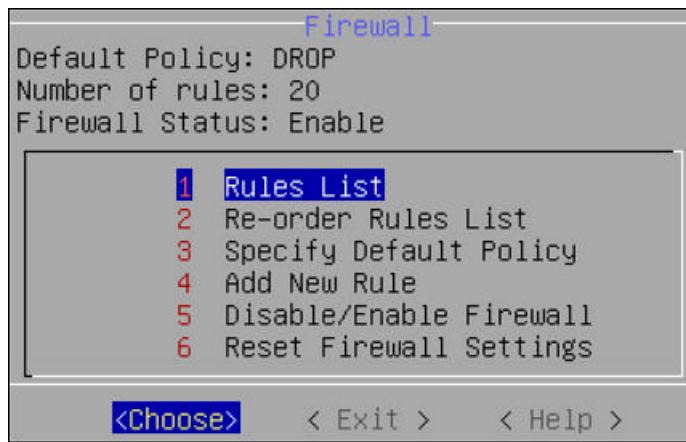


Figure 3-35: Manage Firewall Rules Main Screen

List the Rules

Using the Rules List option, you can view the available firewall rules. Alternatively, on the Web UI, navigate to **System > Information** to view the rules.

You can view the details of a selected rule, in CLI, by clicking **More** (policy, protocol, source IP address, interface, port and description information display). You can also delete a selected rule by clicking **Delete**. Once confirmed, the rule is deleted.

Reorder the Rules List

Using the Reorder Rules List option, you can reorder the list of rules. With buttons **Move up** and **Move down** you can move the selected rule. When done, click **Apply** for the changes to take effect.

The order of the specified rules are important. When reordering the firewall rules, take into account that rules which are in the beginning of the list are of the first priority. Thus, if there are conflicting rules in the list, the one which is the first in the list is applied.

Specify the Default Policy

The default policy determines what to do on packets that do not match any existing rule. Using the Specify Default Policy option, you can set the default policy for the input chains. You can specify one of the following options:

- Accept (Let the traffic pass through)
- Drop (Remove the packet from the wire and generate no error packet)

If not specified by any rule, then the incoming packet will be allowed or dropped depending on the default policy. If specified by a rule, then the incoming packet will be allowed/denied or dropped depending on the policy of the rule.

Add New Rule

Every new rule specifies the criteria for matching packets and the action required. You can add a new rule using the Add New Rule option. This paragraph explains how to add a firewall rule.

Adding a new rule is a multi-stage process that includes:

1. Specifying an action to be taken for matching incoming traffic:
 - a. Accept (allow the packets)
 - b. Drop (Remove the packet from the wire and generate no error packet)
 - c. Reject (Remove the packet from the wire and return an error packet).

2. Specifying the local service for this rule
3. Specifying the local network interface (it can be any or selected interface)
4. Specifying the remote machine criteria
5. Providing a description for the rule (optional)

When a Firewall rule is added, it is added to the end of the Firewall list. If there is a conflicting rule in the beginning of the list, then the new rule may be ignored by the Firewall. Thus, it is recommended to move the new rule somewhere to the beginning of the Firewall rules list.

Disable/Enable Firewall Rules

Using the Disable/Enable Firewall option, you can start your Firewall. All rules that are available in the firewall rules list will be affected by the Firewall when it is enabled. All new rules added to the list will be affected by the Firewall.

Note: You can also restart/start/stop the Firewall using Appliance Web UI.

Reset Firewall Settings

Using the Reset Firewall Settings option, you can delete all Firewall rules. If you use this option, then the Firewall default policy becomes accept and the Firewall is enabled.

If you require additional security, then change the default policy and add the necessary rules immediately after you reset the Firewall.

3.5.5.1 Adding a New Rule with Predefined List of Functionality

► To add a new rule with predefined list of functionality:

1. Select a policy for the rule (accept/drop/reject) which will define how a package from the specific machine will be treated by the appliance Firewall.
2. Click **Next**.
3. Specify what will be affected by the rule. Two options are available: to specify the affected functionality list (in this case, you do not need to specify the ports since they are already predefined), or to specify the protocol and the port.
 - a. Select the local service affected by the rule. You can select one or more items to be affected by the firewall rule.
 - b. Click **Next**.
 - c. If you want to have a number of similar rules, then you can specify multiple items from the functionality list. Thus, for example, if you want to allow access from a certain machine to the appliance LDAP, SNMP, High Availability, SSH Management, or Web Services Management, you can specify these items in the list.
 - d. Click **Manually**.
 - e. In the following dialog box, select a protocol for the rule. You can select between TCP/UDP/ICMP/any.
 - f. In the following screen, specify the **port number** and click **Next**.
4. In the following screen you are prompted to specify an interface. Select between ethMNG (Ethernet management interface), ethSRV0 (Ethernet security service interface), ethSRV1, or select Any.
5. In the following screen you are prompted to specify the remote machine. You can specify between *single/IP with subnet or domain name*.
 - a. When you select **Single**, you will be asked to specify the IP in the following screen.
 - b. When you select **IP with Subnet**, you will be asked to specify the IP first, and then to specify the subnet.

- c. When you select **Domain Name**, you will be asked to specify the domain name.
- 6. When you have specified the remote machine, the **Summary** screen appears. You can enter the description of your rule if necessary.
- 7. Click **Confirm** to save changes.
- 8. Click **OK** in the confirmation message listing the rules that will be added to the Rules list.

3.5.6 Using the Management Interface Settings

Using the Management Interface Settings option, you can specify the network interface that will be used for management (ethMNG). By default, the *first network* interface is used for management (ethMNG). The first management Ethernet is the one that is on-board.

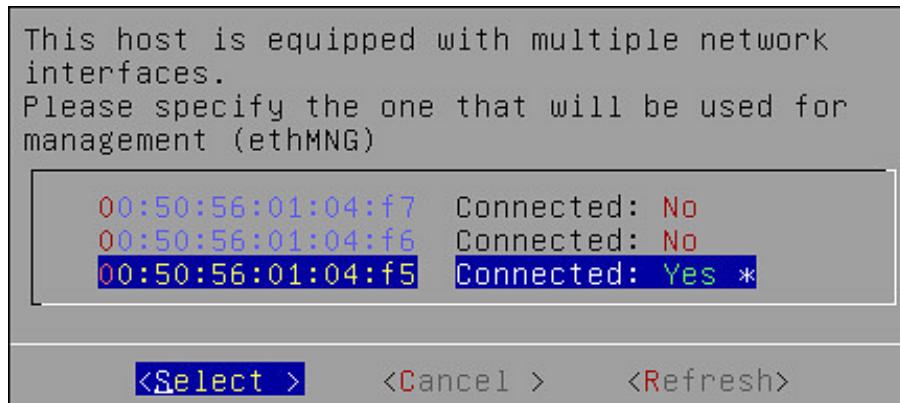


Figure 3-36: Management Interface Settings screen

If you change the network interface, then you are asked to reboot the appliance for the changes to take effect.

Note:

The MAC address is stored in the appliance configuration. If the machine boots/reboots and this MAC address cannot be found, then the default (the first network card) will be applied.

3.5.7 Ports Allowlist

On the **Proxy Authentication** screen of the Web UI, you can add multiple AD servers for retrieving users. The AD servers are added as URLs that contain the IP address/domain name and the listening port number. You can restrict the ports on which the LDAP listens to by maintaining a port allowlist. This ensures that only those ports that are trusted in the organization are mentioned in the URLs.

On the CLI Manager, navigate to **Networking > Ports Allowlist** to set a list of trusted ports. By default, port 389 is added to the allowlist.

The following figure illustrates the **Ports Allowlist** screen.

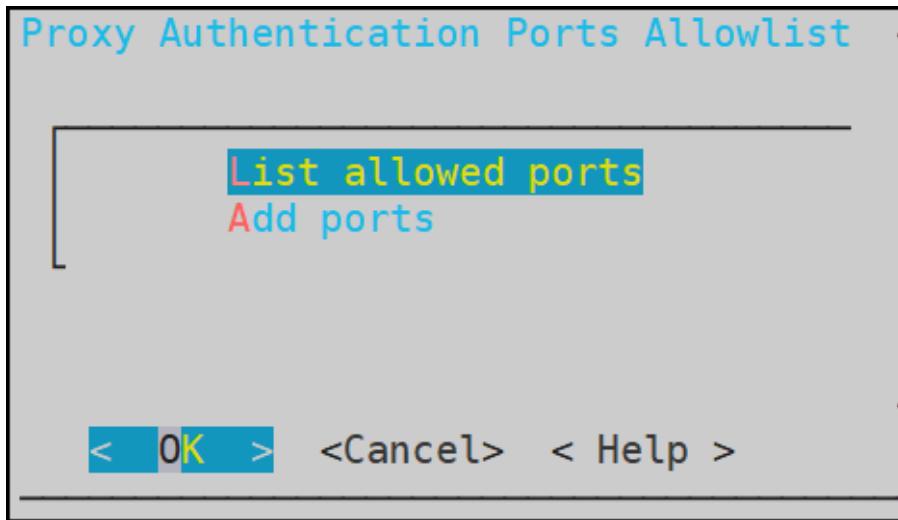


Figure 3-37: Allowlist

Note:

This setting is applicable only to the ports entered in the **Proxy Authentication** screen of the Web UI.

Viewing list of allowed ports

You can view the list of ports that are specified in the allowlist

1. On the CLI Manager, navigate to **Networking > Ports Allowlist**.
2. Enter the root credentials.
3. Select **List allowed ports**.

The list of allowed ports appears.

Adding ports to the allowlist

Ensure that multiple port numbers are comma-delimited and do not contain space between them.

1. On the CLI Manager, navigate to **Networking > Ports Allowlist**.
2. Enter the root credentials.
3. Select **Add Ports**.
4. Enter the required ports and select **OK**.

A confirmation message appears.

3.6 Working with Tools

Protegility appliances are equipped with a Tools menu. The following sections list and explain the available tools and their functionalities.

The screenshot shows a terminal window with the title "Protegility Enterprise-Security-Administrator Manager". The command "hostname" is entered and displayed. Below it, the "Tools:" section is listed:

- SSH Configuration
- Clustering --
 - Trusted Appliances Cluster
- Xen ParaVirtualization
- File Integrity Monitor
- Disk Management
- Rotate Appliance OS Keys
- Removable Media Management --
 - Disable CD/DVD Drives
 - Disable USB Flash Drives
- Web-Services Tuning
- Service Dispatcher Tuning
- AntiVirus
- PLUG - Forward logs to Audit Store
- Analytics Tools --
 - Migrate Analytics Configuration
 - Migrate Analytics Audits
 - Clear Analytics Migration Configuration
- Cloud Utility AWS Tools --
 - CloudWatch Integration
- Audit Store Tools --
 - Rotate Audit Store Certificates
 - Apply Audit Store Security Configs
 - Set Audit Store Repository Total Memory

(c) Protegility Corporation. All Rights Reserved.

(Q)uit (U)p (T)op

(All)

Figure 3-38: Tools Menu

3.6.1 Configuring the SSH

The SSH Configuration tool provides a convenient way to examine and manage the SSH configuration that would fit your needs. Changing the SSH configuration may be necessary for special needs, troubleshooting, or advanced non-standard scenarios. By default, the SSH is configured to deny any SSH communication with unknown remote servers. You can allow the authorized users with keys to communicate without passwords. Every time you add a remote host, the system obtains the SSH key for this host, and adds it to the known hosts.

Using **Tools > SSH Configuration** tool, you can specify the

- Specify SSH Mode
- Specify SSH configuration
- Manage the hosts that the Appliance can connect to
- Set the authorized keys
- Manage the keys that belong to local accounts
- Generate new SSH server keys.

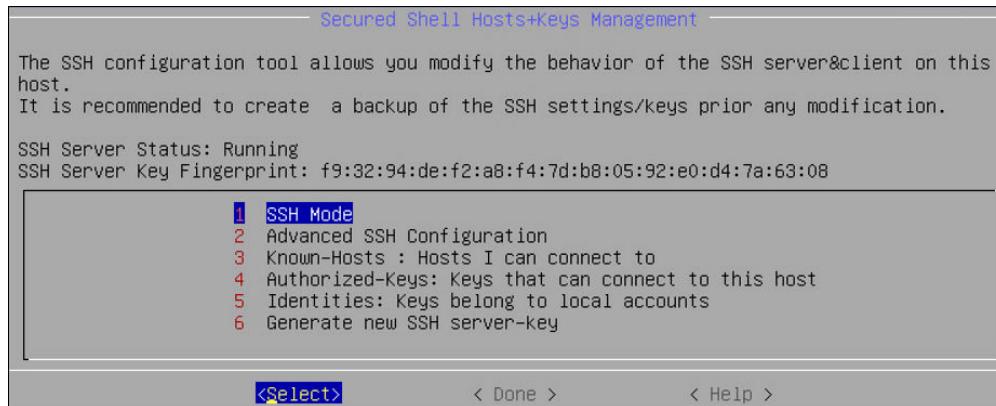


Figure 3-39: Secured Shell Hosts and Keys Management

Note: It is recommended to create a backup of the SSH settings/keys before you make any modifications.

For more information for Backup from CLI, refer to [Backup and Restore](#).

For more information for Backup from Web UI, refer to [System Backup and Restore](#).

3.6.1.1 Specifying SSH Mode

Using SSH Mode tool, you can set restrictions for SSH connections. The restrictions can be hardened or made slack according to your needs. Four modes are available, as described in the following table:

Table 3-14: SSH Mode

Mode	SSH Server	SSH Client
Paranoid	Disable root access	Disable password authentication (allow to connect only using public keys). Block connections to unknown hosts.
Standard	Disable root access	Allow password authentication. Allow connections to new (unknown) hosts, enforce SSH fingerprint of known hosts.
Open	Allow root access Accept connections using passwords and public keys.	Allow password authentication. Allow connection to all hosts – do not check hosts fingerprints.

3.6.1.2 Setting Up Advanced SSH Configuration

The following screen shows the Advanced SSH configuration.



Figure 3-40: Advanced SSH Configuration

- In the Idle Timeout field, Enter Idle timeout period in seconds. It will allow user to set idle timeout period for SSH server before logout.

- In the Client Authentications field, specify the order for trying the SSH authentication method. This allows you to prefer one method over another. The default for this option is *publickey, password*.

3.6.1.3 Managing SSH Known Hosts

Using **Known Hosts: Hosts I can connect to**, you can manage the hosts that you can connect to using SSH. The following table explains the options in the Hosts that I connect to dialog box:

Table 3-15: Hosts I Connect To dialog box

Using...	You can...
Display List	View the list of SSH allowed hosts you can connect to.
Reset List	Clear the SSH allowed hosts list. Only the local host, which is the default, appears.
Add Host	Add a new SSH allowed host.
Delete Host	Delete a host from the list of SSH allowed hosts.
Refresh (Sync) Host	Make sure that the available key is a correct key from each IP (go to each IP/host and re-obtain its key).

3.6.1.4 Managing Authorized Keys

SSH Authorized keys are used to specify SSH keys that are allowed to connect to this machine without entering the password. The system administrator can create such SSH keys and import the keys to this appliance. This is a standard SSH mechanism to allow secured access to machines without a need to enter a password.

Using the Authorized Keys tool, you can display the keys and delete the list of authorized keys (the Reset List option). This would reject all incoming connections that used the authorized keys reset with this tool.

Examine and manage the users that are authorized to access this host.

3.6.1.5 Managing Identities

Using the Identities menu, you can manage and examine which users can start SSH communication from this host using SSH keys. You can:

- Display the list of such keys that already exist
- Reset the SSH keys. This means that all SSH keys used for outgoing connections are deleted.
- Add an identity from the list already available by default or create one as required, using the Directory or Filter options.
- Delete an identity. This should be done with extreme care.

3.6.1.6 Generating SSH Keys

Using the Generate SSH Keys, you can create new SSH keys. If you recreate the SSH Keys, then the remote machines that store the current SSH key, will not be able to contact the appliance until you manually update the SSH keys on those machines.

3.6.1.7 Configuring the SSH

The SSH is a network protocol that ensures a secure communication over an unsecured network. It comprises of a utility suite which provides high-level authentication encryption over unsecured communication channels. The SSH utility suites provide a set of default rules that ensure the security of the appliances. These rules consist of various configurations such as password authentication, log level info, port numbers info, login grace time, strict modes, and so on. These configurations are enabled by default when the SSH service starts. These rules are provided in the *sshd_config.orig* file under the */etc/ssh* directory.

You can customize the SSH rules for your appliances as per your requirements. You can configure the rules in the *sshd_config.append* file under the */etc/ksa* directory.

Warning:

To add customised rules or configurations to the SSH configuration file, modify the *sshd_config.append* file only. It is recommended to use the console for modifying these settings.

For example, if you want to add a match rule for a test user, *test_user* with the following configurations:

- User can only login with a valid password.
- Only three incorrect password attempts are permitted.
- Requires host-based authentication.

You must add the following configuration for the match rule in the *sshd_config.append* file.

```
Match user test_user
    PasswordAuthentication yes
    MaxAuthTries      3
    HostbasedAuthentication yes
```

Ensure that you must enter the valid configurations in the *sshd_config.append* file.

Note:

Restart the SSH service to apply the updated configurations.

If the rule added to the file is incorrect, then the SSH service reverts to the default configurations provided in the *sshd_config.orig* file.

Consider an example where the SSH rule is incorrectly configured by replacing *PasswordAuthentication* with *Password---Authentication*. The following code snippet describes the incorrect configuration.

```
Match user test_user
    Password---Authentication yes
    MaxAuthTries      3
    HostbasedAuthentication yes
```

Then, the following message appears on the OS Console when the SSH services restart.

```
root@protegrity-esa858:/var/www# /etc/init.d/ssh restart
[ ok ] Stopping OpenBSD Secure Shell server: sshd.
The configuration(s) added is incorrect. Reverting to the default configuration.
/etc/ssh/sshd_config: line 274: Bad configuration option: Password---Authentication
/etc/ssh/sshd_config line 274: Directive 'Password---Authentication' is not allowed within a
Match block
[ ok ] Starting OpenBSD Secure Shell server: sshd.
```

If you want to configure the SSH settings for an HA environment, then you must add the rules to both the nodes individually before creating the HA.

For more information about configuring rules to SSH, refer to [Customizing the SSH Configurations](#).

3.6.1.8 Customizing the SSH Configurations

► To configure SSH rules:

1. Login to the CLI Manager with the *root* credentials.
2. Navigate to **Administrator > OS Console**.
3. Enter the following command to configure a new rule.

```
vi /etc/ksa/sshd_config.append
```

4. Configure the required SSH rule and save the file.
5. Restart the SSH service through the CLI or Web UI.

Note:

To restart from the Web UI, you can navigate to **System > Services > Secured Shell (SSH)**.

Alternatively, to restart the SSH service from CLI Manager, navigate to **Administration > Services > Secured Shell (SSH)**.

The SSH services starts with the customized rules or configurations.

3.6.1.9 Exporting/Importing the SSH Settings

You can backup or restore the SSH settings. To export these configurations, select the **Appliance OS configuration** option while exporting the custom files.

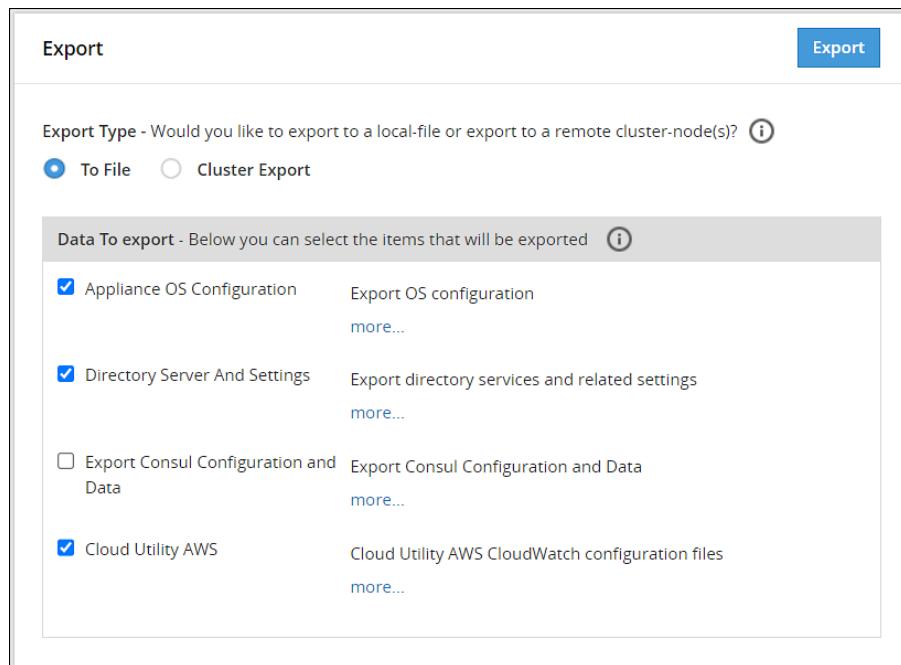


Figure 3-41: Exporting the SSH settings

To import the SSH configurations, select the **SSH Settings** option.

Import

Title	backup2
Description	
Component:	OS
<input type="checkbox"/> Appliance Configuration (ALL) OS configuration more...	
<input type="checkbox"/> Web Settings Web settings more...	
<input checked="" type="checkbox"/> SSH Settings SSH settings more...	
<input checked="" type="checkbox"/> Server Identity SSH server configuration and Keys more...	
<input type="checkbox"/> Certificates Certificates more...	
<input type="checkbox"/> Management and WebService Certificates Management and WebService Certificates more...	
<input type="checkbox"/> Firewall Settings Firewall settings more...	
<input type="checkbox"/> Authentication Settings Appliance Authentication Settings more...	
<input type="checkbox"/> JWT Configuration Appliance JWT Configuration more...	
<input type="checkbox"/> Kerberos SSO Configuration Appliance Kerberos SSO Configuration more...	
<input type="checkbox"/> SAML SSO Configuration Appliance SAML SSO Configuration more...	
<input type="checkbox"/> Timezone And NTP Time-zone and NTP settings more...	
<input type="checkbox"/> Services Status OS Services Status more...	
<input type="checkbox"/> FIM Policies and Settings Appliance FIM Policies and Settings more...	
<input type="checkbox"/> Custom Files and folders User custom list of files more...	

Password

Figure 3-42: Importing the SSH settings

Warning:

You can configure SSH settings and SSH identities that are server-specific. It is recommended to not export or import these SSH settings as it may break the SSH services on the appliance.

For more information on Exporting Custom Files, refer to [Exporting Custom Files](#).

3.6.1.10 Securing SSH Communication

When the client communicates with the server using SSH protocol, a key exchange process occurs for encrypting and decrypting the communication. During the key exchange process, client and server decide on the cipher suites that must be used for communication. The cipher suites contain different algorithms for securing the communication. One of the algorithms that Protegility appliances uses is SHA1, which is vulnerable to collision attacks. Thus, to secure the SSH communication, it is recommended to deprecate the SHA1 algorithm. The following steps describe how to remove the SHA1 algorithm from the SSH configuration.

- To secure SSH communication:

1. On the CLI Manager, navigate to **Administration > OS Console**.
2. Navigate to the `/etc/ssh` directory.
3. Edit the `sshd_config.orig` file.
4. Remove the following entry:

```
MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512
```

5. Remove the following entry:

```
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
```

6. Save the changes and exit the editor.
7. Navigate to the `/etc/ksa` directory.
8. Edit the `sshd_config.append` file.
9. Append the following entries to the file.

```
MACs hmac-sha2-256,hmac-sha2-512
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
```

10. Save the changes and exit the editor.
11. Restart the SSH service using the following command.

```
/etc/init.d/ssh restart
```

The SHA1 algorithm is removed for the SSH communication.

3.6.2 Clustering Tool

Using **Tools > Clustering > Trusted Appliances Cluster**, you can create the Trusted cluster. The trusted cluster can be used to synchronize data from one server to another other one.

3.6.2.1 Creating a TAC using the CLI Manager

This section describes the steps to create a TAC using the CLI Manager.

Before you begin

Important:

Before creating a TAC, ensure that the **SSH** Authentication type is set to **Public key** or **Password + PublicKey**.

► To create a cluster using the CLI Manager:

1. In the ESA CLI Manager, navigate to **Tools > Clustering > Trusted Appliances Cluster**.
The following screen appears.



Figure 3-43: Cluster Services Creation Screen

2. Select **Create: Create new cluster**.

The screen to select the communication method appears.

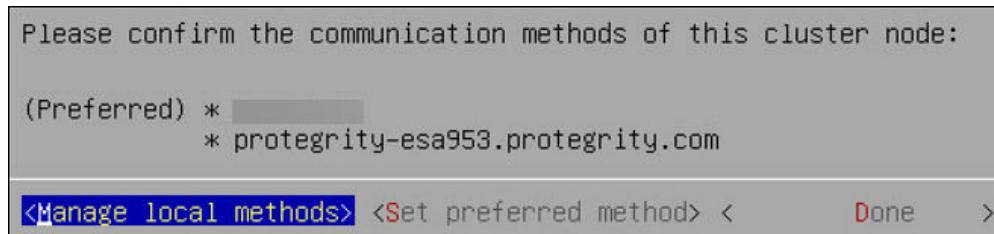


Figure 3-44: Set Communication Method Screen

3. Select **Set preferred method** to set the preferred communication method.

Note: Select **Manage local methods** to add, edit, or delete a communication method.

For more information about managing communication methods, refer to section [Managing Communication Methods for Local Node](#).

4. Select **Done**.
The **Cluster Services** screen appears and the cluster is created.

3.6.2.2 Joining an Existing Cluster using the CLI Manager

This section describes the steps to join a TAC using the CLI Manager.

- To join a cluster using the CLI Manager:

1. In the ESA CLI Manager, navigate to **Tools > Clustering > Trusted Appliances Cluster**.
2. In the **Cluster Services** screen, select **Join: Join an existing cluster**.

The following screen appears.

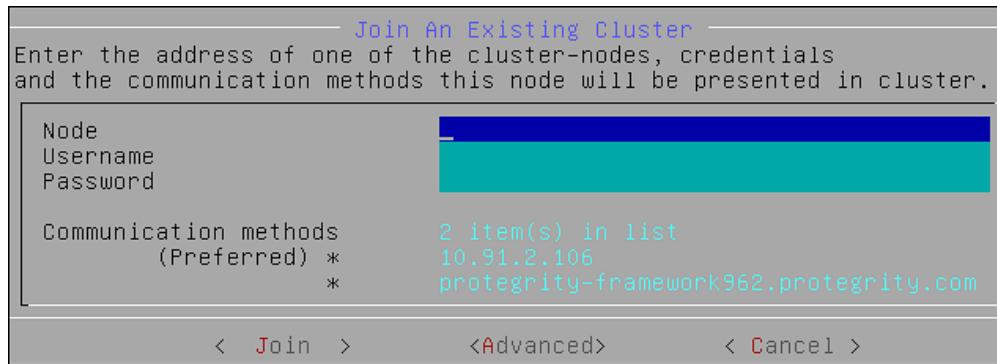


Figure 3-45: Join an Existing Cluster

3. Enter the IP address of the target node in the **Node** text box.
4. Enter the credentials of the user of the target node in the **Username** and **Password** text boxes.

Note: Ensure that the user has administrative privileges.

Note: Select **Advanced** to manage communication or set the preferred communication method.

For more information about managing communication methods, refer to section [Managing Communication Methods for Local Node](#).

5. Select **Join**.
The node is joined to an existing cluster.

3.6.2.3 Cluster Operations

Using **Cluster Operations**, you can execute the standard set of commands or copy files from the local node to other nodes in the cluster.

Note: You can only execute the commands or copy files to the nodes that are directly connected to the local node.

For more information about connection settings of nodes, refer to the section [Connection Settings](#).

The following figure displays the **Cluster Operations** screen.

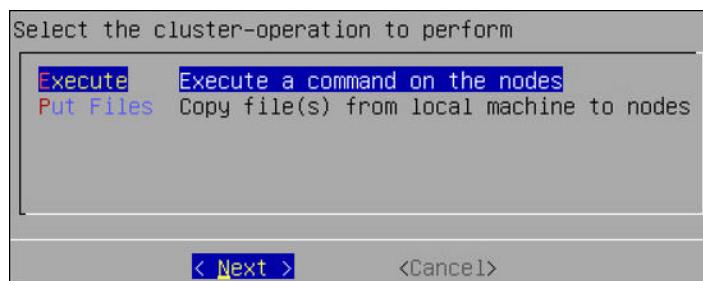


Figure 3-46: Cluster Operations

3.6.2.3.1 Executing Commands using the CLI Manager

This section describes the steps to execute commands using the CLI Manager.

► To execute commands using the CLI Manager:

1. In the CLI Manager, navigate to **Tools > Trusted Appliances Cluster > Cluster Operations: Execute Commands/Deploy Files**.
2. Select **Execute**.
The Select command screen appears with the following list of commands:
 - Display top 10 CPU Consumers
 - Display top 10 memory Consumers
 - Report free disk space
 - Report free memory space
 - Display TCP/UDP network information
 - Display performance and system counters
 - Display cluster tasks
 - Manually enter a command
3. Select the required command and select **Next**.

The following screen appears.

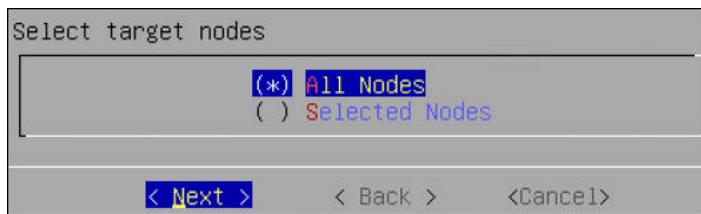


Figure 3-47: Select Target Nodes

4. Select the target node and select **Next**.
The **Summary** screen displaying the output of the selected command appears.

3.6.2.3.2 Copying Files from Local Node to Remote Node

This section describes the steps to copy files from local node to remote node.

► To copy files from local node to remote nodes:

1. In the CLI Manager, navigate to **Tools > Trusted Appliances Cluster > Cluster Operations: Execute Commands/Deploy Files**.
The screen with the appliances connected to the cluster appears.
 2. Select **Put Files**.
The list of files in the current directory appears.
- Note:** Select **Directory** to change the current directory
3. Select the required file and select **Next**.
The **Target Path** screen appears.

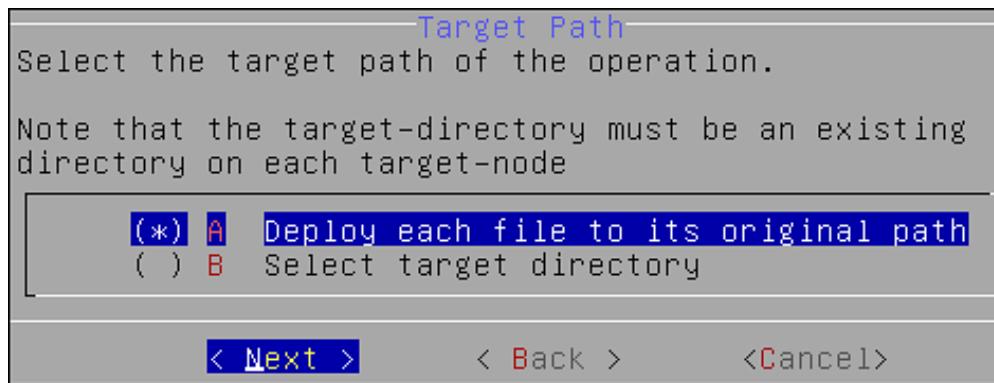
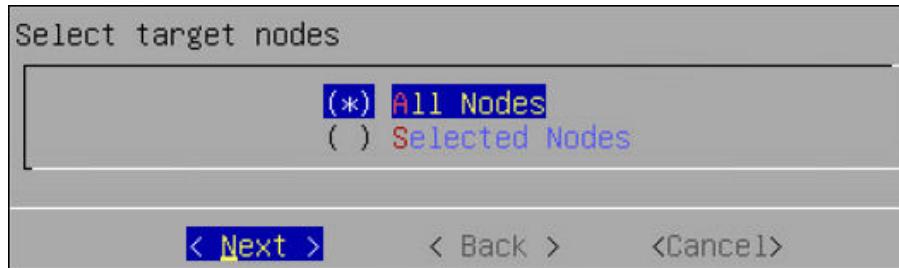


Figure 3-48: Target Path Screen

4. Select the required option and select **Next**.

The following screen appears.



5. Select the target node and select **Next**.

The **Summary** screen confirming the file to be deployed appears.

6. Select **Next**.

The files are deployed to the target nodes.

3.6.2.4 Managing a Site

This section describes how to manage a site.

Using **Site Management**, you can perform the following operations:

- Obtain Site Information
- Add a site
- Remove sites added to the cluster, if more than one site exists in the cluster
- Rename a site
- Set the master site

The following screen shows the **Site Management** screen.

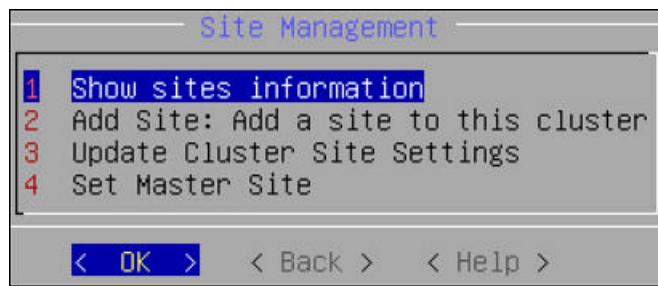


Figure 3-49: Site Management Screen

3.6.2.4.1 View a Site

You can view the information of all the sites in the cluster by selecting **Show sites information**. When a cluster is created, a master site with **site1** is created by default. The following screen displays the **Site Information** screen.

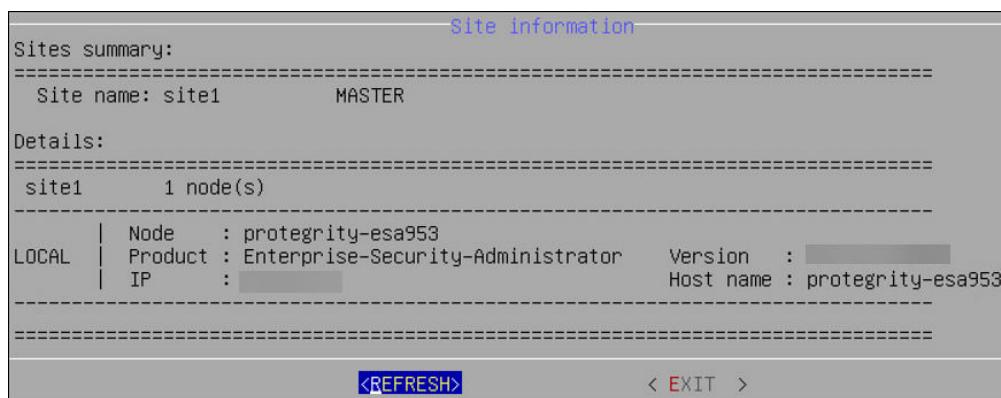


Figure 3-50: Site Information Screen

3.6.2.4.2 Adding Sites to a Cluster

This section describes the steps to add multiple sites to a cluster from the CLI Manager.

► To add a site to a cluster:

1. On the CLI Manager, navigate to **Tools > Trusted Appliances Cluster > Site Management > Add Site**. The following screen appears.

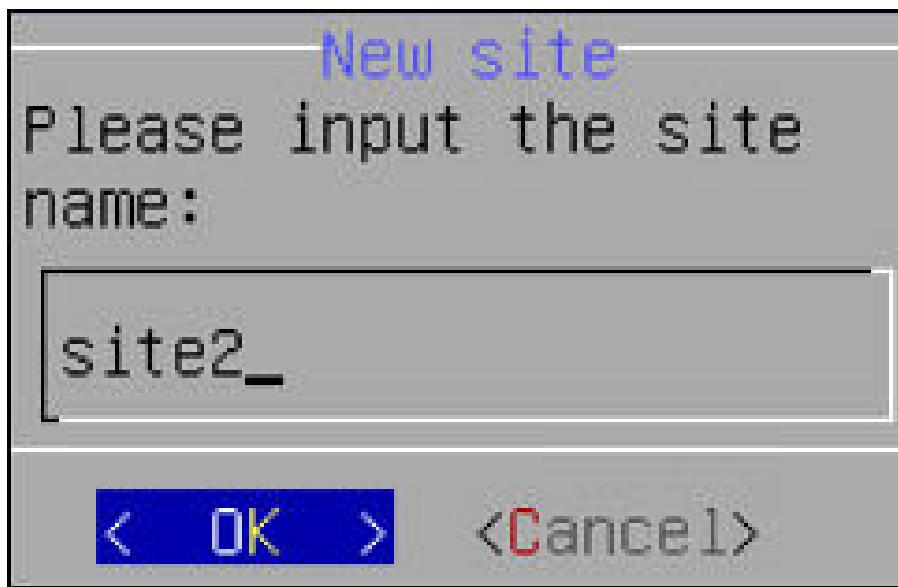


Figure 3-51: Add New Site Name Screen

2. Select **OK**.
The new site is added.

3.6.2.4.3 Renaming a Site

This section describes the steps to rename a site from the CLI Manager.

► To rename a site:

1. On the CLI Manager, navigate to **Tools > Trusted Appliances Cluster > Site Management > Update Cluster Site Settings**.
The **Rename Site** screen appears.
2. Select the required site and select **Rename**.
The **Rename Site** screen appears.
3. Type the required site name and select **OK**.
The site is renamed.

3.6.2.4.4 Setting a Master Site from the CLI Manager

This section describes the steps to set a master site from the CLI Manager.

► To set a master site from the CLI Manager:

1. On the CLI Manager, navigate to **Tools > Trusted Appliances Cluster > Site Management > Set Master Site**.
The **Set Master Site** screen appears.
2. Select the required site and select **Set Master**.
A message *Operation has been completed successfully* appears and the new master site is set.

Note: An empty cluster site does not contain any node. You cannot set an empty cluster site as a master site.

3.6.2.4.5 Deleting a Cluster Site

This section describes the steps to delete a cluster site CLI Manager.

► To delete a cluster site:

1. In the CLI Manager of the node hosting the appliance cluster, navigate to **Tools > Trusted Appliances Cluster > Site Management > Remove: Remove Cluster sites(s)**.
The **Remove Site** screen appears.
2. Select the required site and select **Remove**.
3. Select **OK**.
The site is deleted.

Note: You can only delete an empty cluster site.

3.6.2.5 Node Management

This section describes about Node Management.

Using **Node Management** (option 4), you can:

- List the nodes (the same option as List Nodes menu, refer to the section *Show Cluster Nodes and Status*).
- Add a node to the cluster (if your appliance is a part of the cluster, and you want to add a remote node to this cluster)
- Update cluster information (for updating the identification entries).

- Manage communication method of the nodes.
- Remove a remote node from the cluster

3.6.2.5.1 Show Cluster Nodes and Status

You can view the status of all the nodes in the cluster.

The following table describes the fields that appear on the status screen.

Table 3-16: Cluster Fields

Field	Description
Hostname	Hostname of the node
Address	IP address of the node
Label	Label assigned to the node
Type	Build version of the node
Status	Online/Blocked/Offline
Node Messages	Messages that appear for the node
Connection	Connection setting of the node (On/Off)

3.6.2.5.2 Viewing the Cluster Status using the CLI Manager

This section describes the steps to view the status of all the nodes in a cluster using the CLI Manager.

► To view the status of the nodes in a cluster using the CLI Manager:

1. In the CLI Manager, navigate to **Tools > Trusted Appliances Cluster > Node Management > List Nodes**.
The screen displaying the status of the nodes appears.

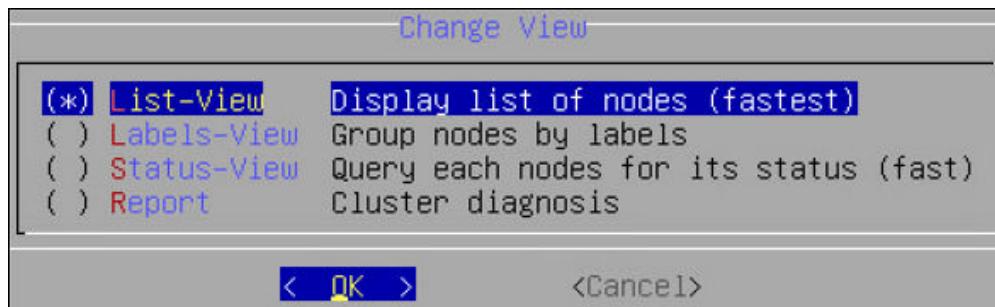


Figure 3-52: View Options for Nodes

2. Select **Change View** to change the view.

The list of different reports is as follows:

- List View: Displays the list of all the nodes
- Labels View: Displays a grouped view of the nodes
- Status View:
- Report view: Displays the cluster diagnostics, network or connectivity issues, and generate error or warning messages if required

3.6.2.5.3 Adding a Remote Node to a Cluster

This section describes the steps to add a remote node to a cluster.

► To add a remote node to the cluster:

- In the CLI Manager of the node hosting the cluster, navigate to **Tools > Trusted Appliances Cluster > Node Management > Add Node: Add a remote node to this cluster**.
The Add Node screen appears.

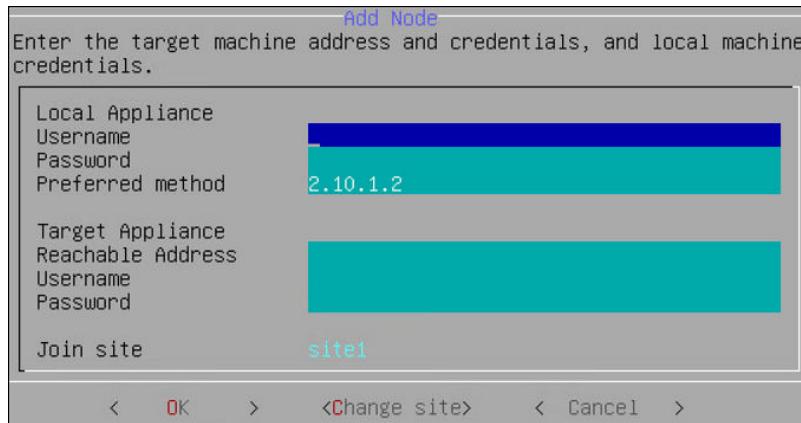


Figure 3-53: Add a remote Node

- Type the credentials of the local node user in the **Username** and **Password** text boxes.

Note:

Ensure that user has administrative privileges.

- Type the preferred communication method on the **Preferred Method** text box.
- Type the accessible communication method of the target node in the **Reachable Address** text box.
- Type the credentials of the target node user in the **Username** and **Password** text boxes.

Note:

Select **Change Site** to choose a different site.

- Select **OK**.

The node is invited to the cluster.

3.6.2.5.4 Updating Cluster Information using the CLI Manager

This section describes the steps to use the **Update Cluster Information** screen.

► To update cluster information:

- In the CLI Manager of the node hosting the cluster, navigate to **Tools > Trusted Appliances Cluster > Node Management > Update Cluster Information**.
The **Update Cluster Information** screen appears.

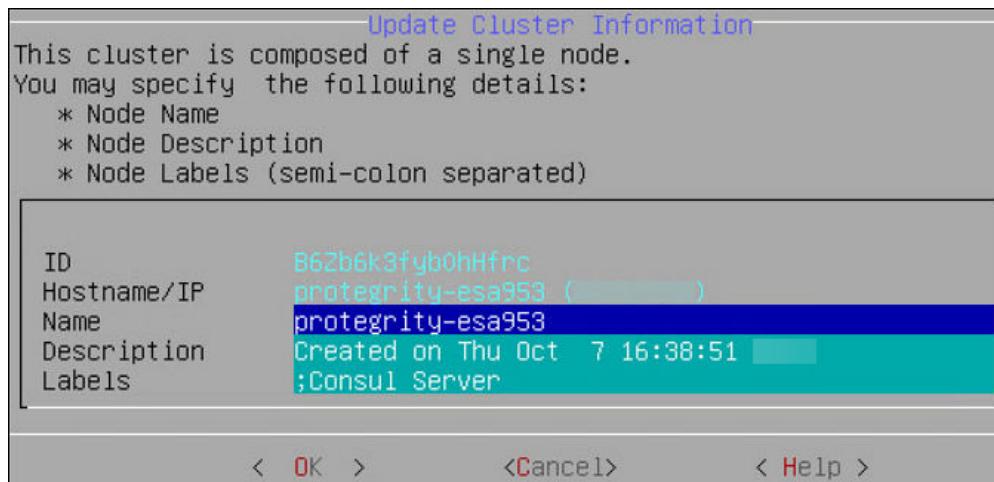


Figure 3-54: Update Cluster Information screen

2. Type the name of the node in the **Name** text box.

Note:

It is recommended not to change the name of the node after you create the cluster task.

3. Type the information describing the node in the **Description** text box.
4. Type the required label for the node in the **Labels** text box.
5. Select **OK**.

The details of the node are updated.

3.6.2.5.5 Managing Communication Methods for Local Node

Every node in a network is identified using a unique identifier. A communication method is a qualifier for the remote nodes in the network to communicate with the local node.

There are two standard methods by which a node is identified:

- Local IP Address of the system (ethMNG)
- Host name

The nodes joining a cluster use the communication method to communicate with each other. The communication between nodes in a cluster occur over one of the accessible communication methods.

3.6.2.5.5.1 Adding a Communication Method from the CLI Manager

This section describes the steps to add a communication method from the CLI Manager.

► To add a communication method from the CLI Manager:

1. In the ESA CLI Manager, navigate to **Tools > Clustering > Trusted Appliances Cluster**.
2. In the **Cluster Services** screen, select **Node Management: Add/Remove Cluster Nodes/ Information**.
3. In the **Node Management** screen, select **Manage node's local communication methods**.
4. In the **Select Communication Method** screen, select **Add**.

5. Type the required communication method and select **OK**.

The new communication method is added.

Note:

Ensure that the length of the text is less than or equal to 64 characters.

3.6.2.5.5.2 Editing a Communication Method from the CLI Manager

This section describes the steps to edit a communication method from the CLI Manager.

► To add a communication method from the CLI Manager:

1. In the ESA CLI Manager, navigate to **Tools > Clustering > Trusted Appliances Cluster**.
2. In the **Cluster Services** screen, select **Node Management: Add/Remove Cluster Nodes/ Information**.
3. In the **Node Management** screen, select **Manage node's local communication methods**.
4. In the **Select Communication Method** screen, select the communication method to edit and select **Edit**.
5. In the Edit method screen, enter the required changes and select **OK**.

The changes to the communication method are complete.

3.6.2.5.5.3 Deleting a Communication Method from the CLI Manager

This section describes the steps to delete a communication method from the CLI Manager.

► To delete a communication method from the CLI Manager:

1. In the ESA CLI Manager, navigate to **Tools > Clustering > Trusted Appliances Cluster**.
2. In the **Cluster Services** screen, select **Node Management: Add/Remove Cluster Nodes/ Information**.
3. In the **Node Management** screen, select **Manage node's local communication methods**.
4. In the **Select Communication Method** screen, select the required communication method and select **Delete**.

The communication method of the node is deleted.

3.6.2.5.6 Managing Local to Remote Node Communication

You can select the method using which a node communicates with another node in a network. The communication methods of all the nodes are visible across the cluster. You can select the specific communication mode to connect with a specific node in the cluster. In the Node Management screen, you can set the communication between a local node and remote node in a cluster.

You can also set the preferred method using which a node communicates with other nodes in a network. If the selected communication method is not accessible, then the other available communication methods of the target node are used for communication.

3.6.2.5.6.1 Selecting a Local to Remote Node Communication Method

This section describes the steps to select a local to remote node communication method.

► To select a local to remote node communication method:

1. In the ESA CLI Manager, navigate to **Tools > Clustering > Trusted Appliances Cluster**.
2. In the **Cluster Services** screen, select **Node Management: Add/Remove Cluster Nodes/ Information**.
3. In the **Node Management** screen, select **Manage local to other nodes communication methods**.
4. In the **Manage local to other nodes communication method**, select the required node for which you want to change the communication method.
5. Select **Change**.
6. Select the required communication method and select **Choose**.
7. Select **Ok**.

Note:

Select **Add New** to add a new communication method.

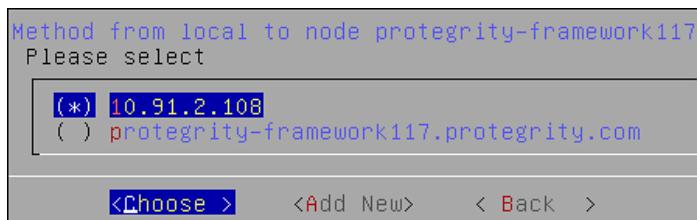
The communication method is selected to communicate with the remote node in the cluster.

3.6.2.5.6.2 Changing a Local to Remote Node Communication Method

This section describes the steps to change a local to remote node communication method.

► To change a local to remote node communication method:

1. In the ESA CLI Manager, navigate to **Tools > Clustering > Trusted Appliances Cluster**.
2. In the **Cluster Services** screen, select **Node Management: Add/Remove Cluster Nodes/ Information**.
3. In the **Node Management** screen, select **Manage local to other nodes communication methods**.
4. In the **Manage local to other nodes communication method**, select a remote node and select **Change**.
The following screen appears.



5. Select the required communication method.
6. Select **Choose**.

The new local to other nodes communication methods is set.

3.6.2.5.7 Removing a Node from a Cluster using CLI Manager

This section describes the steps to remove a remote node from a cluster using the CLI Manager.

Before you begin

Note:

If a node is associated with a cluster task that is based on the hostname or IP address, then the *Remove a (remote) cluster node* operation will not remove node from the cluster. Ensure that you delete all such tasks before removing any node from the cluster.

► To remove a node from a cluster using the CLI Manager:

1. In the ESA CLI Manager, navigate to **Tools > Trusted Appliances Cluster**.
2. In the **Cluster Services** screen, select **Node Management: Add/Remove Cluster Nodes/Information**.
The following screen appears.

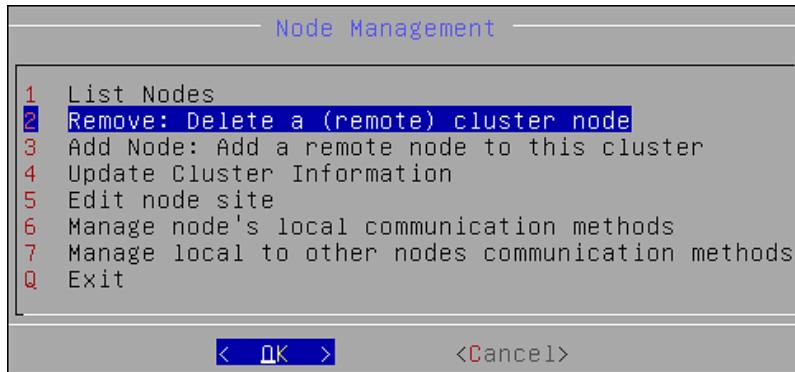


Figure 3-55: Remove an Existing Cluster Node

3. Select **Remove: Delete a (remote) cluster node** and select **OK**.
The screen displaying the nodes in the cluster appears.
4. Select the required node and select **OK**.
The following screen appears.

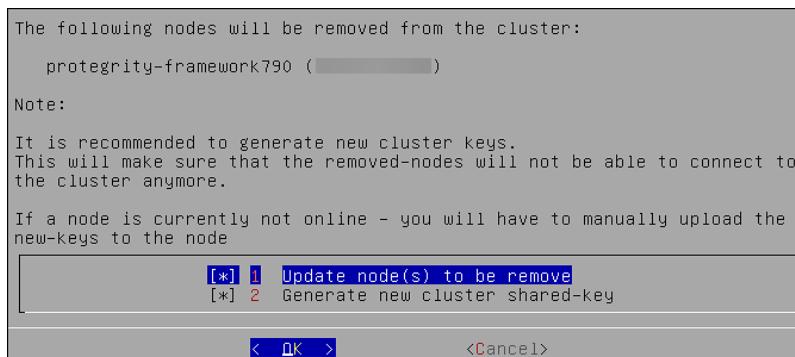


Figure 3-56: Confirmation and Removal of Node from Cluster

5. Select **OK**.
6. Select **REFRESH** to view the updated status.

3.6.2.5.8 Uninstalling Cluster Services

This section describes the steps to uninstall the cluster services on a node using the CLI Manager.

Before you begin

Note:

If a node is associated with a cluster task that is based on the hostname or IP address, then the *Uninstall Cluster Services* operation will not uninstall the cluster services on the node. Ensure that you delete all such tasks before uninstalling the cluster services.

► To remove a node from a cluster using the CLI Manager:

1. In the ESA CLI Manager, navigate to **Tools > Trusted Appliances Cluster**.
2. In the **Cluster Services** screen, select **7 Uninstall : Uninstall Cluster Services**.
3. A confirmation message appears.
4. Select **Yes**.
The cluster services are uninstalled.

3.6.2.6 Trusted Appliances Cluster

A Trusted Appliances cluster can be used to transfer data from one node to other nodes regardless of their location, as long as standard SSH access is supported. This mechanism allows you to run remote commands on remote cluster nodes, transfer files to remote nodes and export configurations to remote nodes. A typical scenario in which a Trusted Appliances cluster is used is for disaster recovery. The trusted appliance cluster can be configured and controlled using the Appliance Web UI as well as the Appliance CLI.

Clustering details are fully explained in section [Trusted Appliances Cluster \(TAC\)](#). In that section you will find information how to:

- Setup a trusted appliances cluster
- Add the appliance to an existing trusted appliances cluster
- Remove an appliance from the trusted appliances cluster
- Manage cluster nodes
- Run commands on cluster nodes

3.6.2.6.1 Cluster Maintenance

This section describes about Cluster Maintenance.

Using the cluster maintenance, you can perform the following functions:

- List cluster nodes
- Update cluster keys
- Redeploy local cluster configuration to all nodes
- Review cluster service interval
- Execute commands as OS root user

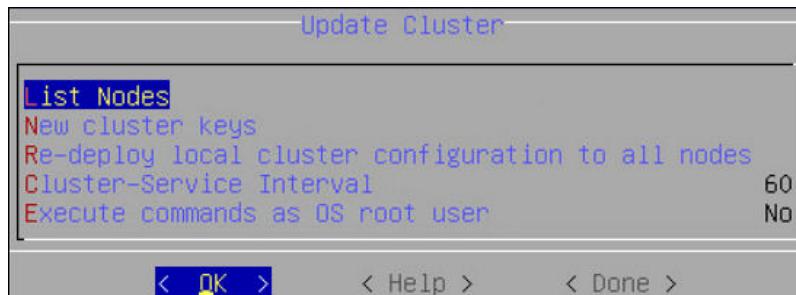
3.6.2.6.1.1 Updating Cluster Key

You can generate a new set of the cluster SSH keys to the nodes that are directly connected to the local node. This ensures that the trusted appliance cluster is secure.

► To re-generate cluster keys:

- In the ESA CLI Manager, navigate to **Tools > Clustering > Trusted Appliances Cluster > Maintenance: Update Cluster Settings**.

The following screen appears.



- Select **New Cluster Keys**.

A message to re-generate the cluster keys appears.

- Select **Yes**.

The new keys are deployed to the nodes that are directly connected.

Caution:

Ensure that all the nodes in the cluster are active, before changing the cluster key.

If a new key is deployed to a node that is unreachable, then connect the node to the cluster. In this scenario, remove the node from the cluster and re-join the cluster.

3.6.2.6.1.2 Redeploy Local Cluster Configuration to All Nodes

You can redeploy the local cluster configuration to force the local cluster configuration to be applied on all connected nodes. Usually there is no need for such operation since the configurations are synchronized automatically. However, if the cluster status service is stopped or you want to force a specific configuration, then you can use this option to force the configuration.

Note: When you select to redeploy the cluster configuration (Redeploy local cluster configuration to all nodes) in the Update Cluster dialog box, the operation is performed at once with no confirmation.

3.6.2.6.1.3 Cluster Service Interval

The cluster provides an auto-update mechanism that runs in the background as a background service which is responsible for updating local and remote cluster configurations and cluster health checks.

You can specify the cluster service interval in the Cluster Service Interval dialog box.

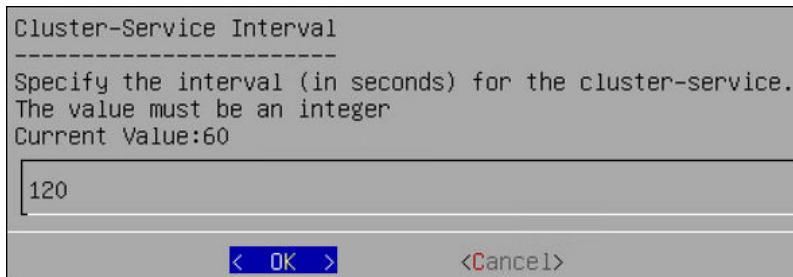


Figure 3-57: Cluster Service Interval dialog box

The interval (in seconds) specifies the sleep time between cluster background updates/operations. For example, if the specified value is 120 seconds, then every two minutes the cluster service will update its status and synchronize its cluster configuration with the other nodes (if changes identified).

3.6.2.6.1.4 Execute Commands as OS Root User

By default, the cluster user is a *restricted user* which means that the cluster commands will be restricted by the OS. There are scenarios where you would like to disable these restrictions and allow the cluster user to run as the OS root user.

Using this menu, you can specify whether to execute the commands as root or as a restricted user.

You can specify...	To...
Yes	Always execute commands as the OS root user. It is less secure, risky if executing the wrong command.
No	Always execute commands as non-root restricted user. It is more secure, but not common for many scenarios.
Ask	Always be asked before a command is executed.

3.6.3 Working with Xen Paravirtualization Tool

Using **Tools > Clustering Tool**, you can setup appliance virtual environment. The default installation of Protegity appliance uses hardware virtualization mode (HVM). The appliance can be reconfigured to use parallel virtualization mode (PVM) to optimize the performance of virtual guest machines.

Protegity supports these virtual servers:

- Xen®
- Microsoft Hyper-V™
- KVM Hypervisor

XEN paravirtualization details are fully covered in section [Xen Paravirtualization Setup](#). In that section you will find information how to:

- Set up Xen paravirtualization
- Follow the paravirtualization process

3.6.4 Working with the File Integrity Monitor Tool

Using **Tools > File Integrity Monitor**, you can make a weekly check and content modifications can be viewed by the Security Officer since the PCI (Section 11.5) specifications require that sensitive files and folders in the Appliance, such as password, certificate, and configuration files, be monitored and all changes made to these files be reviewed by authorized users.

3.6.5 Rotating Appliance OS Keys

When you install the appliance, it generates multiple security identifiers such as, keys, certificates, secrets, passwords, and so on. These identifiers ensure that sensitive data is unique between two appliances in a network. When you receive a Protegity

appliance image or replicate an appliance image on-premise, the identifiers are generated with certain values. If you use the security identifiers without changing their values, then security is compromised and the system might be vulnerable to attacks. Using the **Rotate Appliance OS Keys**, you can randomize the values of these security identifiers on an appliance. This tool must be run only when you finalize the ESA from a cloud instance.

Note:

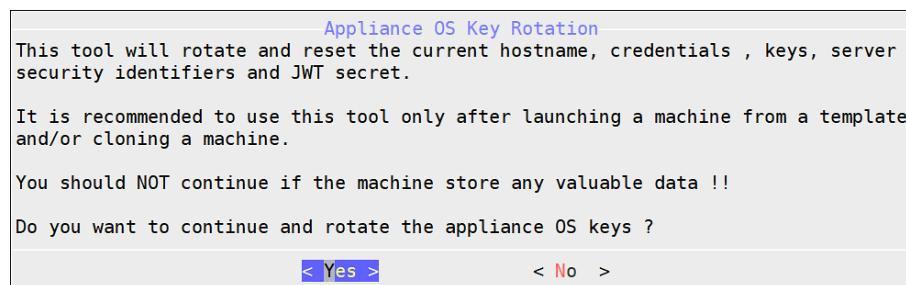
When an appliance, such as, DSG communicates with ESA, the Set ESA communication process must be performed. In such cases, ensure that appliance OS keys are rotated before running the Set ESA communication process.

For example, if the OS keys are not rotated, then you might not be able to add the appliances to a Trusted Appliances Cluster (TAC).

► To rotate appliance OS keys:

1. From the CLI Manager, navigate to to **Tools > Rotate Appliance OS Keys**.
2. Enter the *root* credentials.

The following screen appears.

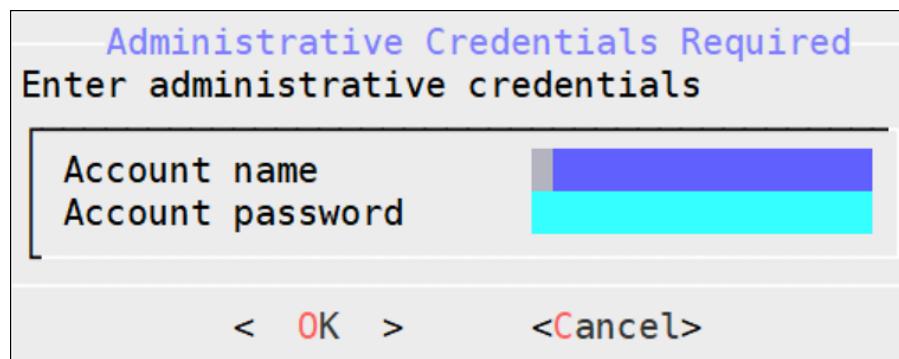


Note:

If you select **No**, then the **Rotate Appliance OS Keys** operation is discarded.

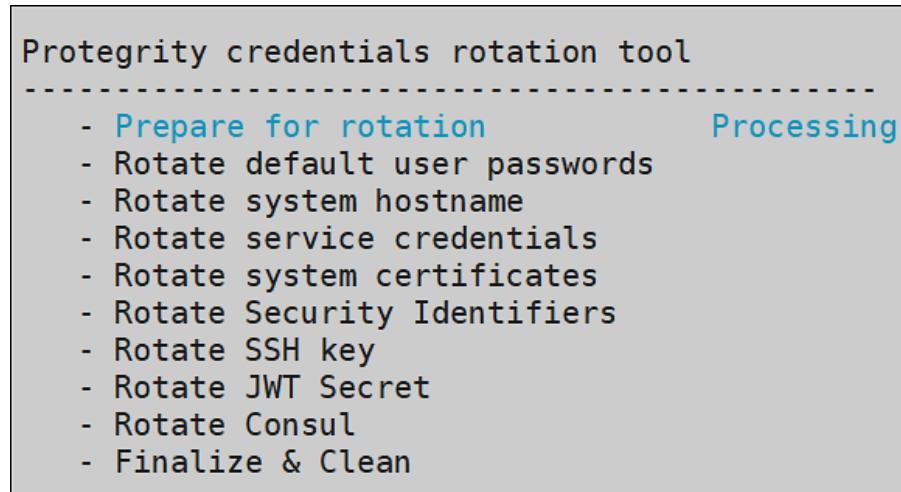
3. Select **Yes**.

The following screen appears.



4. Enter the administrative credentials and select **OK**.

The following screen appears.



The following screen appears.

The screenshot shows a configuration interface titled "User's Passwords". The title is displayed at the top center. Below the title, the text "Please provide user's passwords" is displayed. A list of users and their corresponding password fields is shown. Each user entry consists of two lines: the user name followed by "password verification". The password fields are represented by colored bars: a blue bar for the root password and verification, and cyan bars for all other users (admin, viewer, local_admin). At the bottom of the interface, there are two buttons: "<Apply>" and "<Help >".

5. To update the user passwords, provide the credentials for the following users.

- root
- admin
- viewer
- local_admin

Note:

If you delete any of the default users, such as, *admin* or *viewer*, then that user is not listed on the **User's Passwords** screen.

6. Select **Apply**.

The user passwords are updated and the appliance OS keys are rotated.

Note:

After rotating appliance keys, rotate the Audit Store certificates using the steps from *Rotating Audit Store Certificates* in the [Audit Store Guide 9.1.0.5](#).

3.6.6 Managing Removable Drives

As a security feature, you can restrict access to the removable drives attached to your appliances. You can enable or disable the access to the removable disks, such as, CD/DVD drive or USB Flash drives.

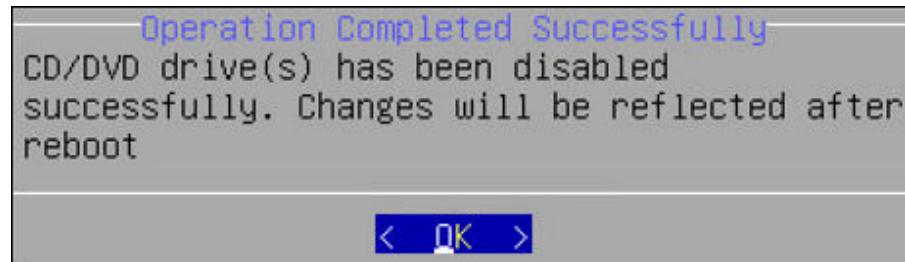
Note: The access to the removable disks is enabled by default.

3.6.6.1 Disabling CD or DVD drive

► To disable CD or DVD drive:

1. On the CLI Manager, navigate to **Tools > Removable Media Management > Disable CD/DVD Drives**.
2. Press **ENTER**.

The following message appears.

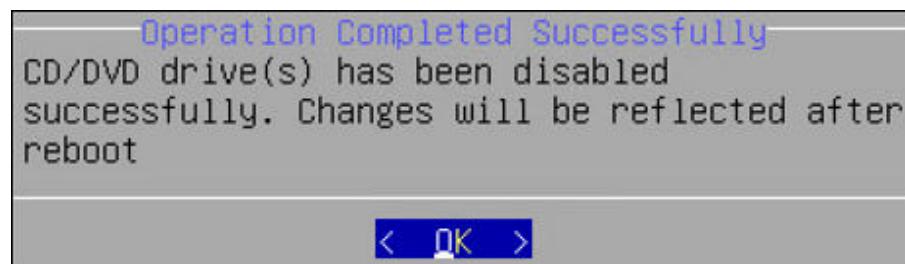


3.6.6.2 Disabling USB Flash Drive

► To disable USB flash drive:

1. On the CLI Manager, navigate to **Tools > Removable Media Management > Disable USB Flash Drives..**
2. Press **ENTER**.

The following message appears.



3.6.6.3 Enabling CD or DVD Drive

► To enable CD/DVD drive:

1. On the CLI Manager, navigate to **Tools > Removable Media Management > Enable CD/DVD Drives**.
2. Press **ENTER**.

3.6.6.4 Enabling USB Flash Drive

► To enable USB flash drive:

1. On the CLI Manager, navigate to **Tools > Removable Media Management > Enable Flash Drives**.
2. Press **ENTER**.

3.6.7 Tuning the Web Services

Using **Tools > Web Services Tuning**, you can monitor and configure the Application Protector Web Service Sessions. You can view such information as Session Shared Memory ID, maximum open sessions, open sessions, free sessions, and session timeout.

Caution: It is recommended to contact Protegity Support before applying any changes for Web Services.

Start Servers

In the StartServers field, you configure the number of child servers processes created on startup. Since the number of processes is dynamically controlled depending on the load, there is usually no reason to adjust the default parameter.

Minimum Spare Servers

In the MinSpareServers field, you set the minimum number of child server processes not handling a request. If the number of such processes is less than configured in the MinSpareServers field, then the parent process creates new children at a maximum rate of 1 per second. It is recommended to change the default value only when dealing with very busy sites.

Maximum Spare Servers

In the MaxSpareServers field, you set the maximum number of child server processes not handling a request. When the number of such processes exceeds the number configured in MaxSpareServers, the parent process kills the excessive processes.

It is recommended to change the default value only when dealing with very busy sites. If you try to set the value lower than MinSpareServers, then it will automatically be adjusted to MinSpareServers value +1.

Maximum Clients

In the MaxClients field, you set the maximum number of connections to be processed simultaneously.

Maximum Requests per Child

In the MaxRequestsPerChild field, you set the limit on the number of requests that an individual child server will handle during its life.

When the number of requests exceeds the value configured in MaxRequestsPerChild field, the child process dies. If you set MaxRequestsPerChild value to 0, then the process will never expire.

Maximum Keep Alive Requests

In the MaxKeepAliveRequest field, you can set the maximum number of requests that can be allowed during a persistent connection. If you set 0, then the number of allowed request will be unlimited. For maximum performance, leave this number high.

Keep Alive Timeout

In the KeepAliveTimeout field, you can set the number of seconds to wait for the next request from same client on the same connection.

3.6.8 Tuning the Service Dispatcher

Using **Tools > Service Dispatcher Tuning**, you can configure the parameters to improve service dispatcher performance.

Note: The Service Dispatcher parameters are the Apache Multi-Processing Module (MPM) worker parameters. The Apache MPM Worker module implements a multi-threaded multi-process web server that allows it to serve higher number of requests with limited system resources. For more information about the Apache MPM Worker parameters, refer to <https://httpd.apache.org/docs/2.2/mod/worker.html>.

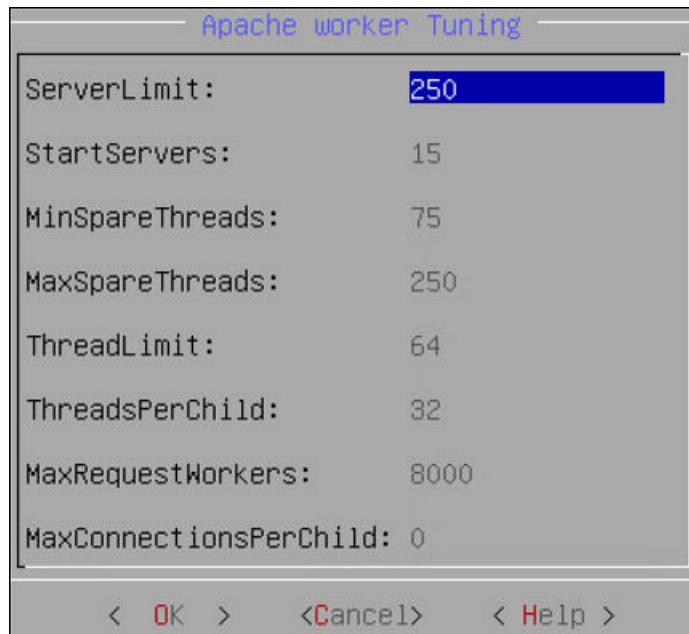


Figure 3-58: Service Dispatcher Tuning

The following table provides information about the configurable parameters and recommendations for Service Dispatcher performance.

Table 3-17:

Parameter	Default Value	Description
StartServers	15	The number of apache server instances that start at the beginning when you start Apache. It is recommended not to enter the StartServers value more than the value for MaxSpareThreads, as this results in processes being terminated immediately after initializing.
ServerLimit	250	The maximum number of child processes. It is recommended to change the ServerLimit value only if the values in MaxClients and ThreadsPerChild need to be changed.
MinSpareThreads	75	The minimum number of idle threads that are available to handle requests. It is recommended to keep the MinSpareThreads value higher than the estimated requests that will come in one second.

Parameter	Default Value	Description
MaxSpareThreads	250	The maximum number of idle threads. It is recommended to reserve adequate resources to handle MaxClients. If MaxSpareThreads are insufficient the webserver will terminate and frequently created child processes reducing performance.
ThreadLimit	64	The upper limit of the configurable threads per child process. To avoid unused shared memory allocation, it is recommended not to set the ThreadLimit value much higher than the ThreadsPerChild value.
ThreadsPerChild	32	The number of threads created by each child process. It is recommended to keep the ThreadsPerChild value such that it can handle common load on the server.
MaxClients	8000	The maximum number of requests that can be processed simultaneously. It is recommended to set the MaxClients values taking into consideration the expected load. Any connection that comes over the load, will drop, and the details can be seen in the error log. Error log file path - /var/log/apache2-service_dispatcher/errors.log
MaxRequestsPerChild	0	The maximum number of requests that a child server process can handle in its life. If the MaxRequestPerChild value is reached, this process expires. It is recommended to set the MaxRequestsPerChild value to 0 so that this process never expires.

3.6.9 Working with Antivirus

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, as required.

The Antivirus option allows you to perform the following actions.

Table 3-18: List of all options

Option	Description
Scan Result	Displays the list of the infected files in the system.
Scan now	Allows to start the scan.
Options	Allows to customize the Antivirus scan options.
View log	Displays the list of scan logs.

3.6.9.1 Customizing Antivirus Scan Options from the CLI

► To customize Antivirus scan options from the CLI:

1. Go to **Tools > AntiVirus**.
2. Select **Options**.
3. Press **ENTER**.



The following table provides a list of the choices available to you to customize scan options.

Table 3-19: List of all scan options

Option	Selection	Description
Action	Ignore	Ignore the infected file and proceed with the scan.
	Move to directory	Move the infected files to specific directory. In the text box, enter the path where the infected file should be moved.
	Delete infected file	Remove the infected file from the directory.
Recursive	True	Scan sub-directories.
	False	Do not scan sub-directories.
Scan directory		Path of the directory to be scanned.

3.7 Working with Preferences

You can set up your console preferences using the **Preferences** menu.

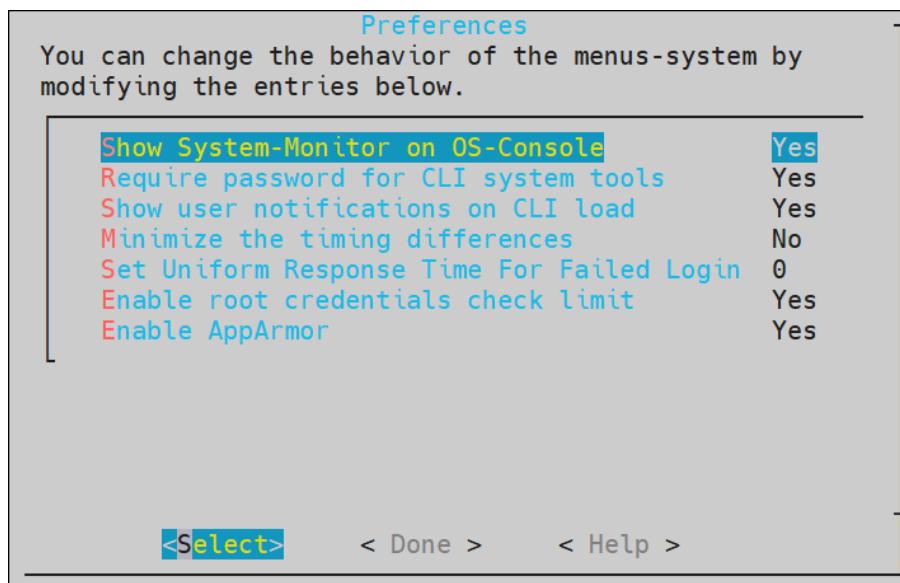


Figure 3-59: Preferences menu

You can choose to configure the following preferences:

- Show system monitor on OS Console
- Require password for CLI system tools
- Show user Notifications on CLI load
- Minimize the timing differences
- Set uniform response time for failed login
- Enable *root* credentials check kimit
- Enable AppArmor
- Local Console Keyboard/Font

3.7.1 Viewing System Monitor on OS Console

You can choose to show a performance monitor before switching to OS Console. If you choose to show the monitor, then the dialog delays for one second before the initialization of the OS Console. The value must be set to Yes or No.

3.7.2 Setting Password Requirements for CLI System Tools

Many CLI tools and utilities require different credentials, such as root and admin user credentials. You can choose to require/not to require a password for CLI system tools. The value must be set to Yes or No.

Specifying **No** here will allow you to execute these tools without having to enter the system passwords. This can be useful when the system administrator is the security manager as well. This setting is not recommended since it makes the Appliance less secure.

3.7.3 Viewing user notifications on CLI load

You can choose to display notifications in the CLI home screen every time a user logs in to the Appliance. These notifications are specific to the user. The value must be set to Yes or No.

3.7.4 Minimizing the Timing Differences

You sign in to the appliance to access different features provided. When you sign in with incorrect credentials, the request is denied and the server sends an appropriate response indicating the reason for failure to log in. The time taken to send the response varies based on the different authentication failures, such as invalid password, invalid username, expired username, and so on. This time interval is vulnerable to security attacks for obtaining valid users from the system. Thus, to mitigate such attacks, you can minimize the time interval to reduce the response time between an incorrect sign-in and server response. To enable this setting, toggle the value of the **Minimize the timing differences** option from the CLI Manager to **Yes**.

Note: The default value of the **Minimize the timing differences** option is **No**.

When you login with a locked user account, a notification indicating that the user account is locked appears. This notification will not appear when the value of **Minimize the timing differences** option is **Yes**. Instead you will get a notification indicating that the username or password is incorrect.

3.7.5 Setting a Uniform Response Time

If you login to the ESA Web UI with invalid credentials, then the time taken to respond to various authentication scenario failures, such as, invalid username, invalid password, expired username, and so on, varies. This variable time interval may introduce a timing attack on the system.

To reduce the risk of a timing attack, you need to reduce the variable time interval and specify a response time to handle invalid credentials. Thus, the response time for the authentication scenarios remains the same.

For example, if the response time for a valid login scenario is 5 seconds, then you can set the uniform response time as 5.

Note: The response time for the authentication scenarios are based on different factors such as, hardware configurations, network configurations, and system performance. Thus, the standard response time would differ between organizations. It is therefore recommended to set the response time based on the settings in your organization.

Enter the time interval (in seconds) and select **OK** to enable the feature. Alternatively, enter **0** in the text box to disable the feature.

3.7.6 Limiting Incorrect *root* Login

If you log in to a system with an incorrect password, the permission to access the system is denied. Multiple attempts to log in with an incorrect password open a route to brute force attacks on the system. Brute force is an exhaustive hacking method, where a hacker guesses a user password over successive incorrect attempts. Using this method, a hacker gains access to a system for malicious purposes.

In our appliances, the root user has access to various operations in the system such as accessing OS console, uploading files, patch installation, changing network settings, and so on. A brute force attack on this user might render the system vulnerable to other security attacks. Therefore, to secure the root login, you can limit the number of incorrect password attempts to the appliance. On the **Preferences** screen, enable the **Enable root credentials limit check** option to limit an LDAP user from entering incorrect passwords for the *root* login.

If you enable the **Enable root credentials limit check**, the LDAP user can login as root only with a fixed number of successive incorrect attempts. After the limit on the number of incorrect attempts is reached, the LDAP user is blocked from logging in as root, thus preventing a brute force attack. After the locking period is completed, the LDAP user can login as root with the correct password.

When you enter an incorrect password for the root login, the events are recorded in the logs.

By default, the root login is blocked for a period of five minutes after three incorrect attempts. You can configure the number of incorrect attempts and the lock period for the root login.

For more information about configuring the lock period and successive incorrect attempts, contact [Protegity Support](#).

Note:

The default value of the **Enable root credentials limit check** option is *Yes*.

3.7.7 Enabling Mandatory Access Control

For implementing Mandatory Access Control, the [AppArmor](#) module is introduced on Protegity appliances. You can define profiles for protecting files that are present in the appliance.

Chapter 4

Web User Interface (Web UI) Management

- [4.1 Working with the Web UI](#)
- [4.2 Logging Out of Appliance Web UI](#)
- [4.3 Shutting down the Appliance](#)
- [4.4 Description of Appliance Web UI](#)
- [4.5 Viewing User Notifications](#)
- [4.6 Web Interface Auto-Refresh Mode](#)
- [4.7 Working with System](#)
- [4.8 Working with Logs](#)
- [4.9 Working with Settings](#)
- [4.10 Managing Appliance Users](#)
- [4.11 Password Policy for the LDAP Users](#)

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.

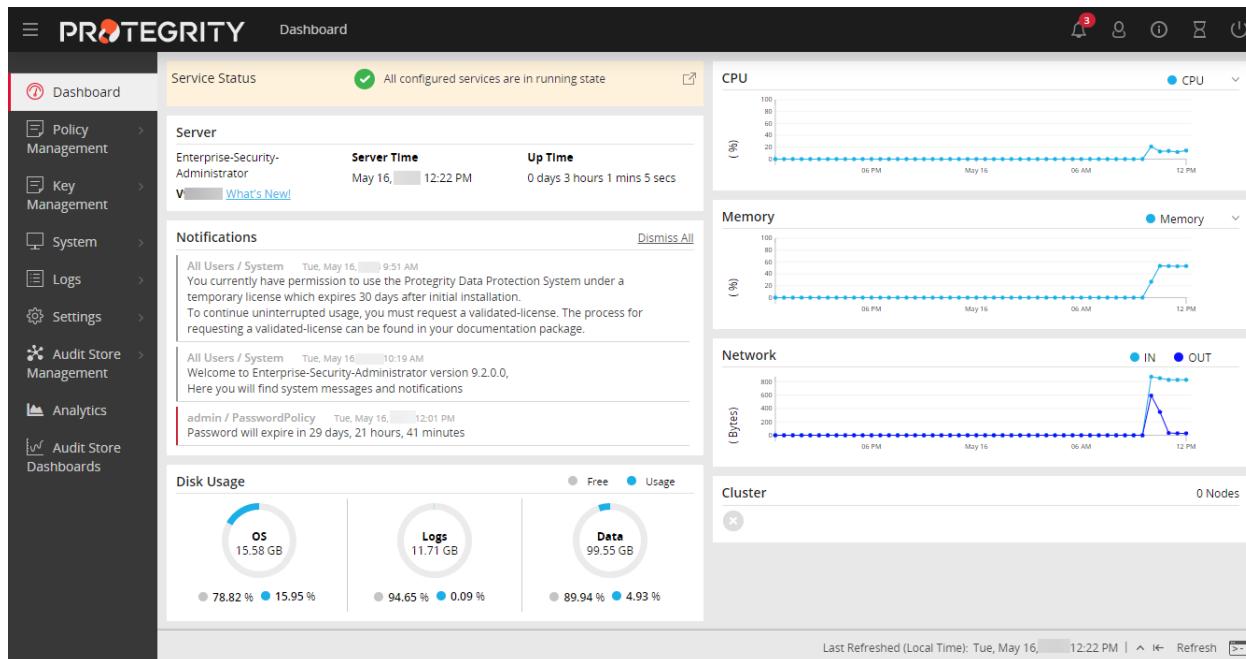


Figure 4-1: ESA Dashboard



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

Table 4-1: 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 <i>Protegrity Key Management Guide 9.1.0.5</i> .
Policy Management	Manage creating and deploying policies. For more information about keys, refer to the <i>Protegrity Policy Management Guide 9.1.0.5</i> .
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 <i>Audit Store Guide 9.1.0.5</i>
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 <i>Protegrity Analytics Guide 9.1.0.5</i> .

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

Table 4-2: 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

4.1 Working with the Web UI

You log into the Appliance Web User Interface (Web UI) to manage the Appliance settings and monitor your Appliance.

The following screen displays the login screen of the Web UI.

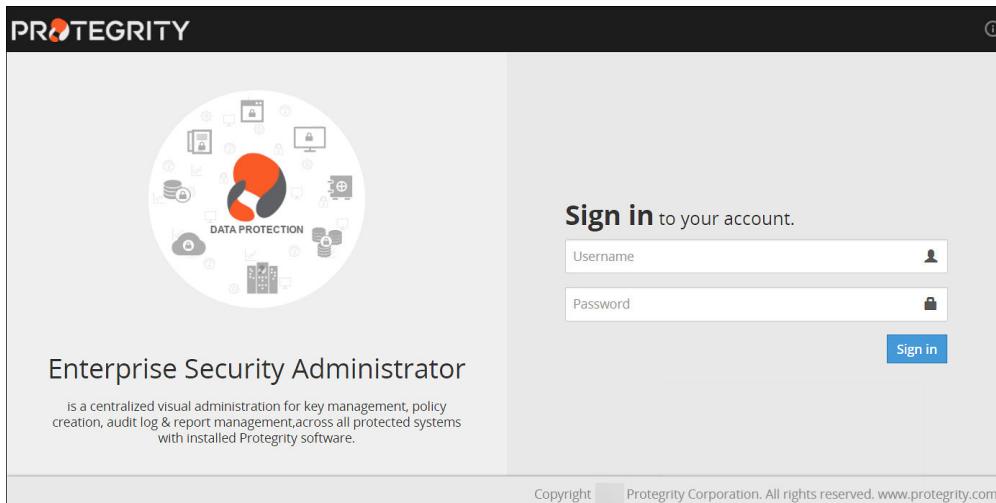


Figure 4-2: Web UI Login page

► To log into the Appliance Web UI:

1. From your web browser, type the Management IP address for your appliance using HTTPS protocol, for example, <https://192.168.1.x/>. The Web Interface splash screen appears.
2. Enter your user credentials.
If the credentials are approved, then the Appliance Dashboard appears.

Note:

When you login through the CLI or the Web UI for the first time, with the password policy enabled, the Update Password screen appears. It is recommended that you change the password since the administrator sets the initial password.

Note:

If you login to the Web UI for the first time with Shell Accounts role and with access to Shell(non-CLI) Access permissions, you cannot access the Web UI but you can update the password through the Update Password screen.

For more information about configuring the password policy, refer to section [Password Policy Configuration](#).

Note:

It is recommended to configure your browser settings such that passwords are not saved. If you save the password, then on your next login you would start the session as a previously logged-in user.

4.2 Logging Out of Appliance Web UI

There are two ways to log off the Appliance Web UI.

1. Log off as a user, while the Appliance continues to run.

2. Reboot or shut down the Appliance.

Note:

In case of cloud platforms, such as, Azure, AWS or GCP, the instances run the appliance. Powering off the instance running the appliance might not shut down the appliance. You must power off the appliance only from the CLI Manager or Appliance Web UI.

- To log out as a user:

1. Click the second icon that appears on the right of the Appliance Toolbar.

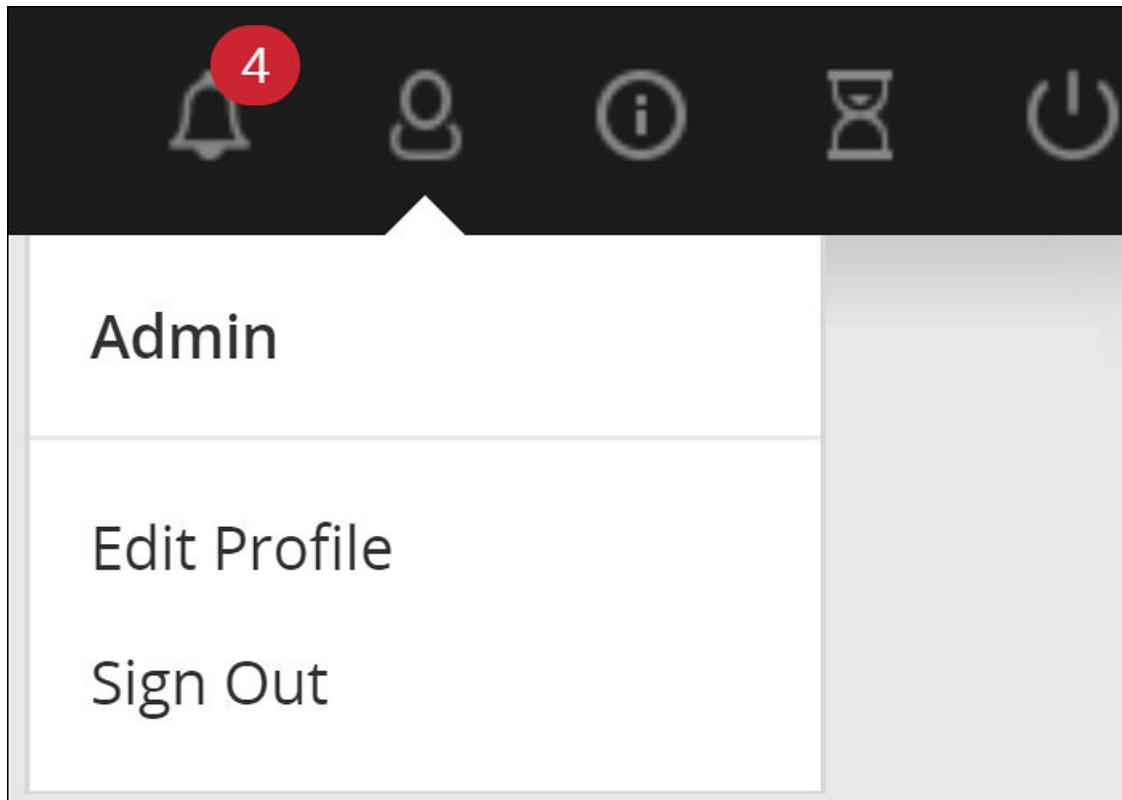


Figure 4-3: Log out option from the Appliance

2. Click **Sign Out**.
The login screen appears.

4.3 Shutting down the Appliance

- To shut down the appliance:

1. Click the last icon from Appliance Toolbar.

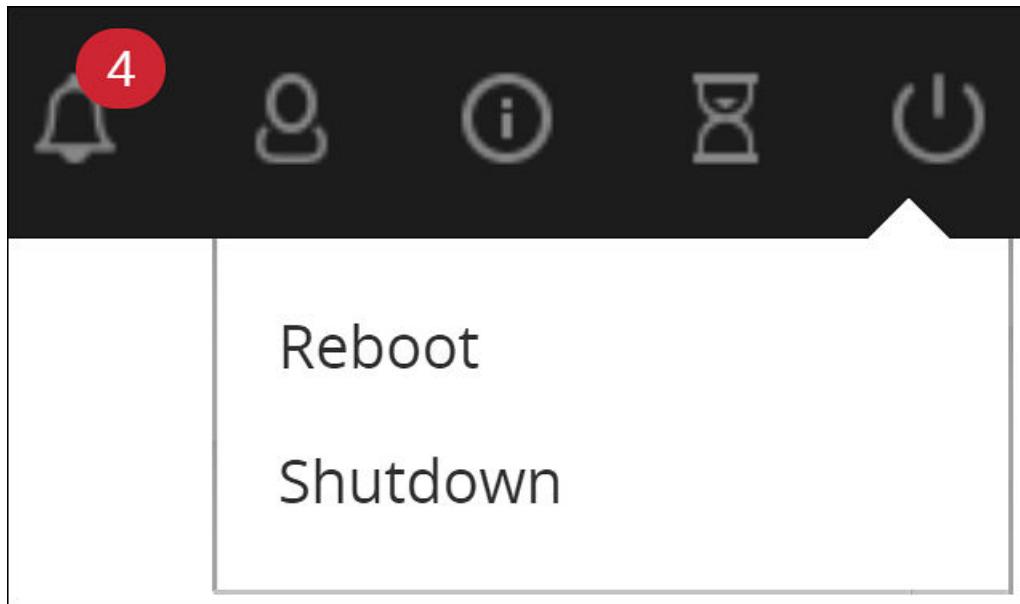


Figure 4-4: Log out option from the Appliance

2. Click **Shutdown**.
3. Enter your password to confirm.
4. Provide the reason for the shut down and click OK.

The Appliance server shuts down. The Web UI screen may continue to display on the window; however, the Web UI does not work.

Note: The Reboot option shuts down the Appliance and restarts it again. So you need to login again when the authentication screen appears.

Important:

In case of cloud platforms, such as, Azure, AWS or GCP, the instances run the appliance. Powering off the instance from the cloud console might not shut down the appliance gracefully. Hence, it is recommended to power off from the CLI Manager or Appliance Web UI.

4.4 Description of Appliance Web UI

The Appliance Web UI appears upon successful login. This page shows the Host to which you are attached, IP address, and the current user logged on.

The different menu options are given in the following table.

Table 4-3: Web Interface Navigation Menus

Option	Using this navigation menu you can...	Applicable to
Dashboard	It is a view-only window, which provides status at a glance – service, server, notifications, disk usage, and graphical representation of CPU, memory, and network usage.	ESA/DSG All

Option	Using this navigation menu you can...	Applicable to
		ESA/DSG
Policy	Create data stores, data elements, masks, roles, keys, and deploy a policy.	ESA
Keys Management	View information, rotate, or change the key states of the Master Key, Repository Key, and Data Store Keys. View information for the active Key store or switch the Key Store.	ESA
System	<ul style="list-style-type: none"> Has a mix of view-only windows and screens to add and update values. Start/stop services and access CLI Manager. Provide status for hardware, system, firewall, and open ports, either graphically or in values. Add high availability systems and trusted application clusters, view the performance and take backups and restore the system. 	All
Logs	View logs for separate tasks such as web services engine, policy management, DFSFP, and Appliance.	ESA
Settings	<ul style="list-style-type: none"> Update default security settings, if required, for the inbuilt anti-virus, two-factor authentication and file integrity. Upload/download configuration files, network settings, and SSH and SMTP settings. Add/delete LDAP users and passwords and activate licenses. 	All
PEP Server	Access license, files, logs, and configurations for the appliance.	DSG
Cloud Gateway	Create certificate, tunnel, service, Rules for traffic flow management, add DSG nodes to cluster, monitor cluster health, view logs.	DSG

The following graphic illustrates the different panes in the ESA Web UI.

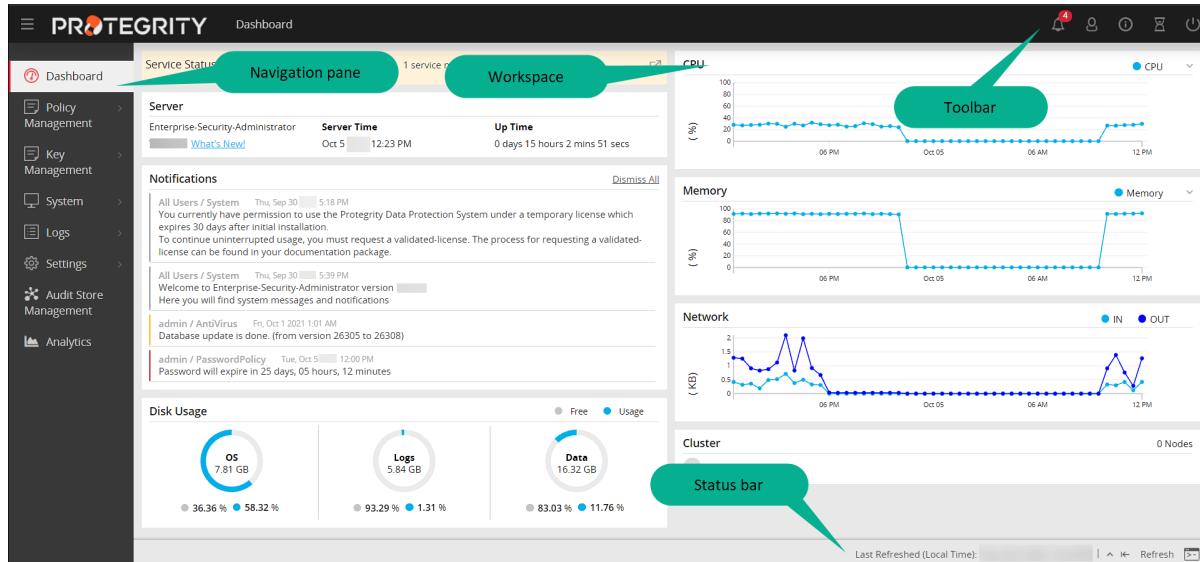


Figure 4-5: Appliance Dashboard Window

Component	Description
Navigation Pane	The number of options in the navigation menu depends on the installed Appliance. The functionality is also restricted based on the user permissions. You could have read-write or read-only permissions for certain options. Using the different options, you can create a policy, add a user, run a few security checks such as file integrity or scan for virus, review or change the network settings, among others.
Workspace	This window on the right includes either displayed information or fields where information needs to be added. When an option is selected, the resulting window appears.
Status Bar	The bar at the bottom displays the last refresh activity time. Also, if you click the rectangle a separate Appliance CLI screen opens. All these options are available in the CLI screen as well.
Toolbar	This bar at the top displays the name of the currently open window on the left and icons on the right.

The details of the icons in the toolbar is as follows:

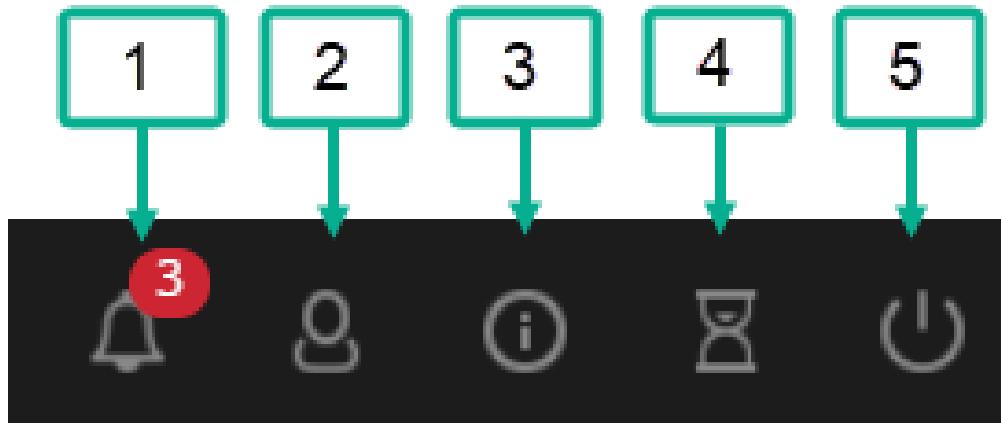


Figure 4-6: Notification Toolbar

Component	Icon Name	Description
1	Notification	The number is the total number of unopened messages for you
2	User	Change your password or log out as a user. ESA continues to run
3	Help	Download the file/s that are required by Protegity Support for troubleshooting
4	Session	Extend the session without timing out. You have to enter your credentials again to login
5	Power Option	Reboot or shut down the Appliance, after ensuring that the Appliance is not being used

4.4.1 Support

The **Help** option on the toolbar, allows you to download information about the status of the appliance and other services that is sometimes required by Protegity Services to troubleshoot.

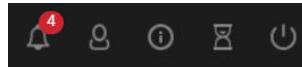
The screenshot shows the PROTEGERY Support tab interface. On the left is a navigation sidebar with links: Dashboard, Policy Management, Key Management, System, Logs, Settings, Audit Store Management, and Analytics. The main area has two sections: 'Download Information' and 'Custom Download Settings'. In 'Download Information', there are fields for 'Server Time' (Wed Oct [redacted]), 'Appliance' (Enterprise-Security-Administrator v [redacted]), 'File Name Prefix' (empty input field), 'Customer Description' (empty text area), and a checkbox for 'Create Password Protected'. Below these is a blue 'Download' button. In 'Custom Download Settings', there is a list of checked items: OS, LDAP, Service Dispatcher, Consul, Cluster-Consul-Integration, td-agent, Policy Management, Audit Store, Analytics, IMPS, and Cloud Utility AWS.

Figure 4-7: Support tab: Download settings

Check the boxes that you require and optionally provide a prefix to the automatically generated file name. You may optionally add a description and protect the resulting zip file and all the xml files inside with a password.

4.4.2 Extending Timeout from Appliance

The following icons are available for all Appliances on the top right corner of the Appliance Web UI page.



The hourglass icon enables you to extend the working time for the Appliance.

To extend the timeout for the Appliance Web UI, click on the hourglass icon.

A message appears mentioning *Session timeout extended successfully*.

4.5 Viewing User Notifications

The screenshot shows a 'Notifications' section with a 'Dismiss All' link. It lists three notifications:

- All Users / System Thu, Sep 30 Welcome to Enterprise-Security-Administrator version Here you will find system messages and notifications
- admin / AntiVirus Fri, Oct 1 Database update is done. (from version 26305 to 26308)
- admin / PasswordPolicy Fri, Oct 1

Figure 4-8: User Notifications Area

There is a message at the top of the screen with the number of notifications that appear on this page and other web pages. If you click on it, then you are directed to the **Services and Status** screen.

Note: You can list a view of scheduled tasks that generate these messages by navigating to **System > Task Scheduler**.

You can delete the messages after reading them. Now, you can store it in Log Store and use Insight Analytics to view the detailed logs. Messages that are older than a year are automatically deleted from the User Notification list, but retained in the logs.

On the **User Notifications** area of the ESA, the notifications and events occurring on the appliances communicating with it are also visible.

Note:

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 *Protegility Certificate Management Guide 9.1.0.5*.

4.6 Web Interface Auto-Refresh Mode

You can set the auto-refresh mode to refresh the necessary information according to a set time interval. The Auto-Refresh is available in the workspaces that show the dynamically changing status information, such as status and logs. Thus, for example, Auto Refresh pane is available in **System > Services**, at the bottom of the page.

The Auto-Refresh pane is not shown by default. You should click the Auto-Refresh button to view the pane.

To modify the auto-refresh mode, from the Appliance Web Interface, select the necessary value in the Auto-Refresh drop-down list. The refresh is applied in accordance with the set time.

4.7 Working with System

The System Information navigation folder includes all information about the appliance: services and their statuses, the hardware and software information, performance statistics, graphs, and real-time graphs, appliance logs, and High Availability status information if the appliance is a part of a cluster.

System option available on the left pane provides the following options:

- Services: View and manage OS, logging and reporting, policy management and other miscellaneous services.
- Information: View the health of the system.
- Trusted Appliances Cluster: View the status of trusted appliances clusters and saved files.
- System Statistics: View the performance of the hardware and networks.
- Backup and Restore: Take backups of files and restore these, as well as take backups of full OS and log files.
- Task Scheduler: Schedule tasks to run in the background such as anti-virus scans and password policy checks, among others.
- Graphs: View how the system is running in a graphical form.

4.7.1 Working with Services

You can manually start and stop services in the appliance. You can act upon all services at once, or select specific ones. For each security service, you can also set whether it restarts automatically (upon reboot) or manually (requires manual start).

In the **System > Services** page, the tabs list the available services and their statuses, and the Information tab appears with the system information (hardware information, system properties, system status, and open ports).

Note: If you stop the **Service Dispatcher** service from the Web UI, you might not be able to access ESA from the Web browser. Hence, it recommended to stop the **Service Dispatcher** service from the CLI Manager only.

Important:

Although the services can be started or stopped from the Web UI, the start/stop/restart action is restricted for some services. These services can be operated from the OS Console. Run the following command to start/stop/restart a service.

```
/etc/init.d/<service_name> stop/start/restart
```

For example, to start the docker service, run the following command.

```
/etc/init.d/docker start
```

4.7.1.1 Logfacade Services

The *Logfacade* services receive audits from the protectors and send it to the Audit Store, which is then used by the Insight Analytics. The following services are available on the ESA Web UI:

- *Logfacade*: If the ESA is configured with a 7.x protector or 8.x protector, then the *Logfacade* service is used.

For more information about the Audit Store, refer to the [Audit Store Guide 9.1.0.5](#).

4.7.1.2 Meteringfacade Service

The *Meteringfacade* service collects the total count of successful protect, unprotect, and reprotect operations from the connected protectors. The total count is then sent at periodic intervals, which is 20 minutes as configured in the *pepservice.cfg* configuration file, to the Audit Store for further analysis.

For more information about Metering, refer to the [Protegity Analytics Guide 9.1.0.5](#).

For more information about the Audit Store, refer to the [Audit Store Guide 9.1.0.5](#).

4.7.2 Viewing System Information

All hardware information, system properties, system statuses, open ports and Firewall rules are listed in the Information tab.

Hardware section includes information on system, chipset, processors, and number of total RAM. **System Properties** section appears with information on current Appliance, logging server, and directory server. **System Status** section lists such properties as data and time, boot time, up time, number of logged in users, and average load:

Information - Information about the system configuration and install patches		
Hardware		
System	VMware, Inc., VMware Virtual Platform, ([0.371422] Booting paravirtualized kernel on VMware hypervisor)	
Chipset	Intel Corporation , -440BX Desktop Reference Platform,	
Processors	8 x Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz	
Total RAM	32768 MB	
System Properties		
Appliance	Appliance-Framework-x64	
Directory Server	ldap://127.0.0.1:389/	
System Status		
Date/Time	Thursday, 03. March 03:24:27 PM	
Boot-Time	Thursday, 03. March 01:56:50 AM	
Up-Time	0 days 13 hours 27 mins 37 secs	
Logged-In Users	1	
Load-Average	0.45 0.43 0.23 1/385 19271	
Appliance Capabilities		
① Name	default	
② description	Install standard appliance	
③ install - kernel	generic	
④ install - filesystem	ext4	
⑤ install - scripts - before reboot		
⑥ install - scripts - after reboot		
⑦ system - backup partitions	True	
⑧ user interface - poweroff	True	
⑨ user interface - reboot	True	
Open Ports		
Type	Address	Service
TCP	2.10.1.8:22	Management - SSH
TCP	2.10.1.8:8443	Web Services
TCP	2.10.1.8:443	Management - Web Interface (HTTPS)
TCP	2.10.1.8:5671	Messaging System
TCP	2.10.1.8:2377	Docker Daemon
TCP	2.10.1.8:7946	Docker Daemon
UDP	0.0.0.0:40420	Appliance Heartbeat Server
UDP	2.10.1.8:7946	Docker Daemon
UDP	0.0.0.0:10100	Appliance Heartbeat Client
UDP	0.0.0.0:33771	Messaging System
Installed Patches		
Name	Title	Version
① Appliance OS Framework	Appliance OS	
② Consul	Consul component	2.1
③ Cluster-Consul-Integration	Cluster-Consul-Integration component	0.3

Figure 4-9: Information tab: Hardware, System Properties, System Status

Open Ports section lists types, addresses and names of services that are running:

Open Ports		
Type	Address	Service
TCP	2.10.1.8:22	Management - SSH
TCP	2.10.1.8:8443	Web Services
TCP	2.10.1.8:443	Management - Web Interface (HTTPS)
TCP	2.10.1.8:5671	Messaging System
TCP	2.10.1.8:2377	Docker Daemon
TCP	2.10.1.8:7946	Docker Daemon
UDP	0.0.0.0:40420	Appliance Heartbeat Server
UDP	2.10.1.8:7946	Docker Daemon
UDP	0.0.0.0:10100	Appliance Heartbeat Client
UDP	0.0.0.0:33771	Messaging System

Figure 4-10: Information tab: Open Ports

Firewall section in **System > Information** lists all Firewall rules, Firewall status (enabled/disabled), and the default policy (drop/accept) which determines what to do on packets that do not match any existing rule.



Firewall					
Status : Enabled Default Policy : X (DROP)					
Policy	Source	Protocol	Interface	Port(s)	Description
✓	ALL	tcp	ethMNG	443	Allow Web-Interface to ethMNG access from all
✓	ALL	tcp	ethMNG	22	Allow SSH access from all (via ethMNG)
✓	ALL	tcp	ALL	8443	Allow Web-Services from all
✓	ALL	udp	ALL	694	Allow High-Availability UDP port 694
✓	ALL	tcp	ALL	7788	Allow High-Availability TCP port 7788
✓	ALL	icmp	ALL	ALL	Allow the ICMP protocol
✓	ALL	udp	ALL	123	Allow NTP Time Synchronization
✓	ALL	udp	ALL	10100	Allow Appliance Heartbeat UDP port 10100
✓	ALL	tcp	ALL	5671	Allow Messaging-System SSL connection to port 5671
✓	ALL	udp	ALL	67	Allow DHCP Server requests
✓	ALL	udp	ALL	68	Allow DHCP Client requests
✓	ALL	udp	ALL	161	Allow SNMP requests
✓	ALL	udp	ALL	10161	Allow SNMP over DTLS requests
✓	ALL	tcp	ALL	10161	Allow SNMP over TLS requests
✓	ALL	tcp	ALL	389,636	Allow LDAP traffic
✓	ALL	tcp	ALL	8300,8301,8302,9000,8600	Allow Consul TCP traffic from all networks
✓	ALL	udp	ALL	8301,8302,8600	Allow Consul UDP traffic from all networks
✓	ALL	tcp	ethMNG	15500	Allow legacy policy deployment - Allow pepservers to download token elements and roles
✓	ALL	tcp	ethMNG	24224	Allow plug messages - Allow receiving audit, metering and log messages from pepservers
✓	ALL	tcp	ethMNG	9200	Elasticsearch REST
✓	ALL	tcp	ethMNG	9300	Elasticsearch inter-node communication
✓	ALL	tcp	loopback	8588	Elasticsearch Clustering web

Figure 4-11: Information tab: Firewall Rules section

4.7.3 Viewing System Statistics

Using **System > System Statistics**, you can view performance statistics to assess system usage and efficiency. The Performance page refreshes itself every few seconds and shows the statistics in the real time.

The Performance page shows system information:

- Hardware (system, chipset, processors, total RAM)
- System Status (date/time, boot time, up-time, users connected, load average)
- Networking (Interface, address, bytes sent/received, packets sent/received)
- Partitions (partition name and size, used and avail)
- Kernel (idle time, kernel time, I/O time, user time)
- Memory (memory total, swap cached, and inactive, among others)

You can customize the page refresh rate, so that you are viewing the latest information at any time.

4.7.4 Viewing Performance Graphs

Using **System > Graphs**, you can 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:

- CPU application use, % (CPU I/O wait, CPU system use)
- Total RAM (free RAM, used RAM)
- Total Swap (free Swap, used Swap)
- Free RAM



- Used RAM
- System CPU usage
- Application CPU use, %
- Log space used (log space available, log space total)
- Application data used (application data available space, application data total size)
- Total page faults
- File descriptor usage
- ethMNG incoming/ethMNG outgoing
- ethSRV0 incoming/ethSRV0 outgoing
- ethSRV1 incoming/ethSRV1 outgoing

In the Realtime Graphs tab you can monitor current state of performance statistics for these items:

- CPU usage
- Memory Status (free and used RAM)

The following figure illustrates the Realtime Graphs tab.

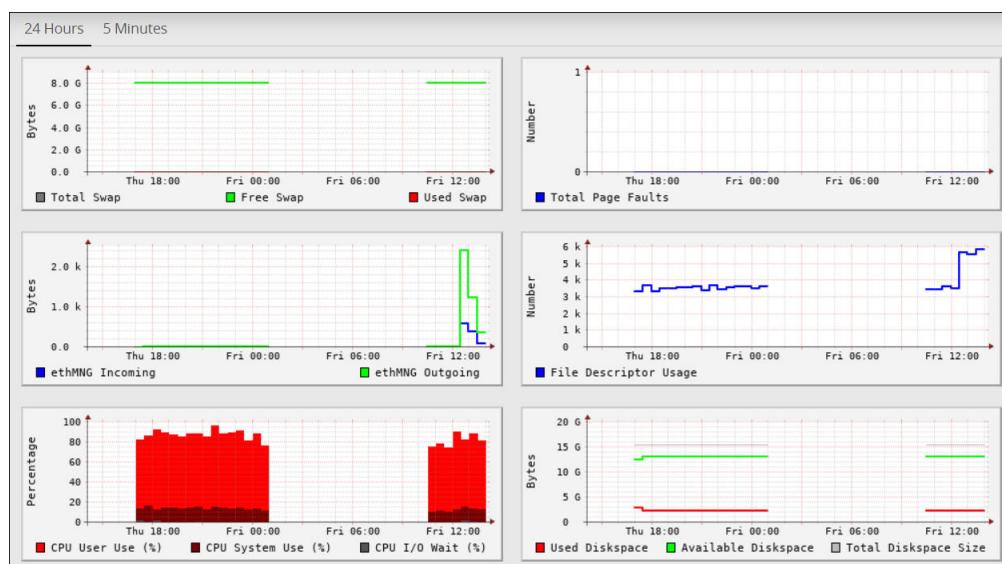


Figure 4-12: Real-time Graphs tab

4.7.5 Working with Trusted Appliances Cluster

Clustering menu becomes available in the appliance Web Interface, **System > Appliance**. The status of the cluster is by default updated every minute, and it can be configured using Cluster Service Interval, available in the CLI Manager.

Status tab appears with the information on nodes which are in the cluster. In the Filter drop-down combo box, you can filter the nodes by the name, address and label.

In the Display drop-down combo box, you can select to display node summary, top 10 CPU consumers, top 10 Memory consumers, free disk report, TCP/UDP network information, system information, and display ALL.

Saved Files tab appears with the files that were saved in the CLI Manager. These files show the status of the appliance cluster node or the result of the command run on the cluster.

4.7.6 Working with System Backup and Restore

The backup process copies or archives data. The restore process ensures that the original data is restored if data corruption occurs.

You can back up and restore configurations and the operating system from the Backup/Restore page. It is recommended to have a backup of all system configurations.

The Backup/Restore page includes **Export**, **Import**, **OS Full**, and **Log Files** tabs, which you can use to create configuration backups and restore them later.

Using **Export**, you can also export a configuration to a trusted appliances cluster, and schedule periodic replication of the configuration on all nodes that are in the trusted appliances cluster. Using such export, you can periodically update the configuration on all, or just necessary nodes of the cluster.

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.

4.7.6.1 Backing Up Data

Using the Export tab, you can create backups of the product configurations and/or appliance OS core configuration.

Export

Export Type - Would you like to export to a local-file or export to a remote cluster-node(s)? [i](#)

To File Cluster Export

Data To export - Below you can select the items that will be exported [i](#)

<input checked="" type="checkbox"/> Appliance OS Configuration	Export OS configuration more...
<input checked="" type="checkbox"/> Directory Server And Settings	Export directory services and related settings more...
<input type="checkbox"/> Export Consul Configuration and Data	Export Consul Configuration and Data more...
<input checked="" type="checkbox"/> Cloud Utility AWS	Cloud Utility AWS CloudWatch configuration files more...

Export

Figure 4-13: Export Tab

4.7.6.1.1 Backing up Configuration to Local File

► To back up a configuration to a local file:

1. Navigate to **System > Backup & Restore > Export**.
2. In the Export Type area, select *To File* radio button.
3. In the *Data To export* area, select the items to be exported.
Click *more..* for the description of every item.

Note:

Starting from the Big Data Protector 7.2.0 release, the HDFS File Protector (HDFSF) is deprecated. The HDFSF-related sections are retained to ensure coverage for using an older version of Big Data Protector with the ESA 7.2.0.

Note:

If you plan to use ESAs in a Trusted Appliances Cluster, and you are using HDFSF with the DFSFP patch installed on the ESA, then ensure that you clear the *DFSFP_Export* check box when exporting the configurations from the ESA, which will be designated as the Master ESA.

In addition, for the Slave ESAs, ensure that the HDFSF datastore is not defined and the HDFSF service is not added.

The HDFSF data from the Master ESA should be backed up to a file and moved to a backup repository outside the ESA, which will help in retaining the data related to HDFSF, in cases of any failures.

4. Click **Export**.

The **Output File** screen appears.

5. Enter information in the following fields:

- **Output File:** Name of the file

Note: If you want to replace an existing file on the system with this file, click the **Overwrite existing file** check box.

- **Password:** Password for the file
- **Export Description:** Information about the file

6. Click **Confirm**.

A message *Export operation has been completed successfully* appears. The created configuration is saved to your system.

4.7.6.2 Exporting Configuration to Cluster

You can export your appliance configuration to the trusted appliances cluster, which your appliance belongs to. The procedure of creating the backup is almost the same as exporting to a file.

You need to define what configurations to export, and which nodes in the cluster receive the configuration. You need not to import the files as you were required to do when you back up the selected configuration. The configuration will be automatically replicated on the selected nodes when you export the configuration to the cluster.

► To export a configuration to a trusted appliances cluster:

1. Navigate to **System > Backup & Restore > Export**.
2. In the Export Type area, select *To Cluster* radio button.
3. In the Data to import area, customize the items that you want to export from your machine and import to the cluster nodes.

Note:

Starting from the Big Data Protector 7.2.0 release, the HDFS File Protector (HDFSF) is deprecated. The HDFSF-related sections are retained to ensure coverage for using an older version of Big Data Protector with the ESA 7.2.0.

Note:

If you plan to use ESAs in a Trusted Appliances Cluster, and you are using HDFSF with the DFSFP patch installed on the ESA, then ensure that you clear the *DFSFP_Export* check box when exporting the configurations from the ESA, which will be designated as the Master ESA.

In addition, for the Slave ESAs, ensure that the HDFSF datastore is not defined and the HDFSF service is not added.

The HDFSF data from the Master ESA should be backed up to a file and moved to a backup repository outside the ESA, which will help in retaining the data related to HDFSF, in cases of any failures.

4. In the Target Cluster Nodes area, select which nodes you want to export the configuration to. You can specify them by label or select individual nodes. You can select to show command line, if necessary.
5. Click **Export**.

Note: When you are exporting data from one ESA to other, ensure that you run separate tasks to export the LDAP settings first and then the OS settings.

4.7.6.3 Scheduling Configuration Export to Cluster Tasks

You can schedule configuration export tasks to periodically replicate a specified configuration on the necessary cluster nodes.

The procedure of creating a configuration export task is almost the same as exporting a configuration to the cluster. The difference between these processes is that exporting a configuration to the cluster is a one-time procedure which you need to manually run, whereas a scheduled task makes periodic updates and can be run a number of times in accordance with the schedule that you specify.

► To schedule a configuration export to a trusted appliances cluster:

1. Navigate to **System > Backup & Restore > Export**.
2. In the Export Type area, select **Schedule Cluster Report** radio button.
3. In the Data to import area, customize the items that you need to export from your machine and import to the cluster nodes.

Note:

If you plan to use ESAs in a Trusted Appliances Cluster, and you are using HDFSFP with the DFSFP patch installed on the ESA, then ensure that you clear the *DFSFP_Export* check box when exporting the configurations from the ESA, which will be designated as the Master ESA.

In addition, for the Slave ESAs, ensure that the HDFSFP datastore is not defined and the HDFSFP service is not added.

The HDFSFP data from the Master ESA should be backed up to a file and moved to a backup repository outside the ESA, which will help in retaining the data related to HDFSFP, in cases of any failures.

4. In the Target Cluster Nodes area, select which nodes you want to export the configuration to. You can specify them by label or select individual nodes. You can select to show command line, if necessary.
5. In the Scheduled Task Properties area, specify the Task Name, the Description, and the Frequency fields. You can specify advanced frequency settings by selecting the **Advanced** check box.
6. Click **Add Schedule Task** when all fields are specified. The task is added and available in the **System > Task Scheduler**, where you can modify and customize the task.
7. In the Scheduler area, select the task that you have created and click **Run Now** button. You can check appliance logs for details.

4.7.6.4 Exporting Custom Files

In the ESA, 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, which contains the list of files that you want to include for export and import.

The following figure displays a sample snippet of the *customer.custom* file.

The screenshot shows a web-based interface for managing customer custom files. At the top, there's a header with a back button and the title "customer.custom : Export Import customer custom files and directorie...". Below the header are three buttons: "Edit", "Download", and a trash can icon. The main area contains the content of the "customer.custom" file, which is a text-based configuration file with various comments and instructions. The file includes sections for files and directories, with specific syntax for paths and file names.

```

1 # This file contain list of all the extra files customer would like to
2 # export and import.
3 # ..... #
4 # ..... USE WITH CAUTION ..... #
5 # ..... #
6 # watch out from overwriting system files
7 # Avoid replacing server sensitive files to other appliances
8 # ..... #
9 # How to use:
10 ## used for comments
11 # Ensure none of the available export-import functionalities are included in this file. Please use cluster export wizard or file export-import to do so.
12 # Files:
13 # /opt/example-full-path - Full path to files. if file doesn't exist export will fail.
14 # optional:/opt/example1 - Start with "optional" prefix for files that are not mandatory.
15 # /opt/example* - use * for multiple files, directories are not supported only files.
16 # Directories:
17 # /opt/example_dir/* - All files under dir. only 1st level of files in the directory are imported, subdirectories will be ignored.
18 # recursive:/opt/example_dir - same as /opt/example_dir but sub directories are also copied. If subdirectory exists it will be ignored.

```

Figure 4-14: Customer.custom file

If you include a file, then you must specify the full path of the file. The following snippet explains the format for exporting a file.

```
/<directory path>/<filename>.<extension>
```

For example, to export the *abc.txt* file that is present in the *test* directory, you must add the following line in the *customer.custom* file.

```
/test/abc.txt
```

If the file does not exist, then an error message appears and the import export process terminates. In this case, you can add the prefix *optional* to the file path in the *customer.custom* file. This ensures that if the file does not exist, then the import export process continues without terminating abruptly.

Note: If the file exists and the prefix optional is added, then the file is exported to the other node.

For example, if the file *123.txt* is present in the *test* directory, then it is exported to the other node. If the file does not exist, then the export of this file is skipped and the other files are exported.

```
optional:/abc/test/123.txt
```

For more information about exporting files, refer to the section [Editing the customer.custom File to Export Files](#).

If you include a directory, then you must specify the full path for the directory. All the files present within the directory are exported. The following snippet explains the format for exporting all the files in a directory.

```
/<directory path>/*
```

For example, to export a directory *test_dir* that is present in the */opt* directory, add the following line in the *customer.custom* file.

```
/opt/test_dir/*
```

You can also include all the files present under the subdirectories for export. If you prefix the directory path with the value *recursive*, then all the files within the subdirectories are also exported.

For example, to export all the subdirectories present in the *test_dir* directory, add the following line in the *customer.custom* file.

```
recursive:/opt/test_dir/
```

For more information about exporting directories, refer to the section [Editing the customer.custom File to Include Directories](#).

You must export the custom files before importing them to a file or on the other nodes on a cluster.

4.7.6.4.1 Exporting the customer.custom file to a Local File from the Web UI

This section describes the steps to export the *customer.custom* file to a local file using the Web UI.

► To perform a cluster export of the custom file from the Web UI:

1. Navigate to **System > Backup & Restore > Export**.
2. In the Export Type area, select **To File**.
3. In the Data To Export area, select **Appliance OS Configuration**.
4. Click **Export**.
The **Output file** screen appears.
5. Enter the name of the file in the **Export Name** text box.
6. Enter the required password in the **Password** text box.
7. Click **Confirm**.
The message *Export operation has been completed successfully* appears.
8. Click **Done** button.
The file is exported and is stored in the */products/exports* directory.

4.7.6.4.2 Exporting the customer.custom file to a Local File from the CLI Manager

► To perform a cluster export of the custom file from the CLI Manager:

1. On the CLI Manager, navigate to **Administration > Backup/Restore Center > Export data/configurations to a local file**.
2. Select **Appliance OS Configuration** and select **OK**.
A screen to enter the export information appears.
3. Enter the required name of the file in the **Export Name** text box.
4. Enter the required password in the **Password** and **Confirm** text boxes.
5. Select **OK**.
6. Select **Done** after the export operation completes.

4.7.6.4.3 Exporting the customer.custom file on a Cluster from the Web UI

This section describes the steps to export the *customer.custom* file to a cluster using the Web UI.

► To export the custom file in a cluster from the Web UI:

1. On the Web UI, navigate to **System > Backup & Restore > Export**.
2. In the **Export Type** area, select **Cluster Export** option.
3. Click **Start Wizard**.
4. Select **User custom list of files** in the **Data To Import** tab.
5. Click **Next**.
6. Select the required options in the **Source Cluster Nodes** tab and click **Next**.
7. Select the required options in the **Target Cluster Nodes** tab and click **Review**.
8. Enter the required data in the *Basic Properties*, *Frequency*, *Logging*, and *Restriction* areas.
For more information about *Basic Properties*, *Frequency*, *Logging*, and *Restriction* areas, refer to section [*Schedule Appliance Tasks*](#).
The message *Export operation has been completed successfully* appears.
9. Click **Save**.

4.7.6.4.4 Exporting a Cluster Export of the Custom File from the CLI Manager

This section describes the steps to export the *customer.custom* file to a cluster using the CLI Manager.

- To perform a cluster export of the custom file from the CLI Manager:

1. On the CLI Manager, navigate to **Administration > Backup/Restore Center > Export data/configurations to remote appliance(s)**.
2. Select the required file or configuration to export and select **OK**.
3. Enter the required password for the file or configuration.
4. Select **Custom Files and folders** and select **OK**.
5. Enter the required credentials for the target appliance on the **Target Appliance(s)** screen.
6. Select **OK**.
The custom files and configurations are exported to the target node.
7. Click **Save**.

4.7.6.4.5 Importing the *customer.custom* File from the Web UI

This section describes the steps to import the *customer.custom* file from the Web UI.

- To perform a cluster import of the custom file from the Web UI:

1. On the Web UI, navigate to **System > Backup & Restore > Import**.
2. Select the exported file.
3. Click **Import**.
4. On the following screen, select **Custom Files and folders**.

The screenshot shows the 'Import' configuration dialog box. At the top, there are fields for 'Title' (set to 'backup2') and 'Description'. Below these, a section labeled 'Component:' has a dropdown menu set to 'OS'. A list of configuration items follows, each with a checkbox and a 'more...' link:

- Appliance Configuration (ALL) OS configuration [more...](#)
- Web Settings Web settings [more...](#)
- SSH Settings SSH settings [more...](#)
- Server Identity SSH server configuration and Keys [more...](#)
- Certificates Certificates [more...](#)
- Management and WebService Certificates Management and WebService Certificates [more...](#)
- Firewall Settings Firewall settings [more...](#)
- Authentication Settings Appliance Authentication Settings [more...](#)
- JWT Configuration Appliance JWT Configuration [more...](#)
- Kerberos SSO Configuration Appliance Kerberos SSO Configuration [more...](#)
- SAML SSO Configuration Appliance SAML SSO Configuration [more...](#)
- Timezone And NTP Time-zone and NTP settings [more...](#)
- Services Status OS Services Status [more...](#)
- FIM Policies and Settings Appliance FIM Policies and Settings [more...](#)

At the bottom, a note says 'Use with Caution! When attempting to import custom files and directories, avoid overwriting server configurations and server-specific settings. If available prefer using existing Import and export services over the custom list. The custom list of files and directories can be found under the settings->system->files page.' There is a 'less...' link.

Below the list are three buttons: 'Password' (with a redacted password), 'Import' (highlighted in blue), and 'Cancel'.

Figure 4-15: Import Options

- Enter the password for the file in the **Password** text box and click **Import**.

The message *File <filename> has been imported successfully* appears.

- Click **Done**.

4.7.6.4.6 Importing the customer.custom File from the CLI Manager

► To perform a cluster import of the *customer.custom* file from the CLI Manager:

- On the CLI Manager, navigate to **Administration > Backup/Restore Center > Import configurations from a local file**. The *Select an item* to import screen appears.
- Select the required file or configuration to export and select **OK**. The contents of the file appear.
- Select **OK**.
- Enter the required password on the following screen and select **OK**.
- Select the required components.

Warning:

Ensure to select each component individually.

- Select **OK**.

The file import process starts.

7. Select **Done** after the import process completes.

4.7.6.4.7 Editing the *customer.custom* File to Export Files

This section describes the various options that are applicable when you export a file.

Consider the following scenarios for exporting a file:

- Include a file *abc.txt* present in the */opt/test* directory
- Include all the file extensions that start with *abc* in the */opt/test/check* directory
- Include multiple files using regular expressions

► To edit the *customer.custom* file from the Web UI:

1. On the Web UI, navigate to **Settings > System > Files**.
2. Click **Edit** beside the *customer.custom* file.
3. Configure the following settings to export the file.

```
#To include the abc.txt file
/opt/test/abc.txt
#if the file does not exist, skip the export of the file
optional:/opt/test/pqr.txt
#To include all text files
/opt/test/*.txt
#To include all the files extensions for file abc present in the /opt/test/check directory
/opt/test/check/abc.*
#To include files file1.txt, file2.txt, file3.txt, file4.txt, and file5.txt
/opt/test/file[1-5].txt
```

4. Click **Save**.

Note: Administration privileges are required for editing the *customer.custom* file.

Note:

It is recommended to use the Cluster export task to export *Appliance Configuration settings, SSH settings, Certificates, Firewall settings, LDAP settings, and HA settings*.

Note:

If the files exist at the target location, then they are overwritten.

4.7.6.4.8 Editing the *customer.custom* File to Include Directories

This section describes the various options that are applicable when you export a file.

Consider the following scenarios for exporting files in a directory:

- Export files is the directory *abc_dir* present in the */opt/test* directory
- Export all the files present in subdirectories under the *abc_dir* directory

► To edit the *customer.custom* file from the Web UI:

1. On the Web UI, navigate to **Settings > System > Files**.
2. Click **Edit** beside to the *customer.custom* file.

The following is a snippet listing the sample settings for exporting a directory.

```
#To include all the files present in the abc directory  
/opt/test/abc_dir/*  
#To include all the files in the subdirectories present in the abc_dir directory  
recursive:/opt/test/abc_dir
```

If you have a Key Store configured with ESA, then you can export the Key Store libraries and files using the *customer.custom* file. The following is a sample snippet listing the settings for exporting a Key Store directory.

```
#To include all the files present in the Safeguard directory  
/opt/safeguard/*  
#To include all the files present in the Safenet directory  
/usr/safenet/*
```

The following is a sample snippet listing the settings for exporting the self-signed certificates.

```
#To include all the files present in the Certificates directory  
/etc/ksa/certificates
```

Note:

Ensure that the files mentioned in the *customer.custom* file are not specified in the *exclude* file.

For more information about the *exclude* file, refer to the section [Editing the Exclude File](#)

3. Click **Save**.

4.7.6.4.9 Editing the customer.custom File to Include Files

The library files and other settings that are not exported using the cluster export task can be addressed using the *customer.custom* file.

► To edit the *customer.custom* file from the Web UI:

1. On the Web UI, navigate to **Settings > System > Files**.
2. Click **Edit** beside to the *customer.custom* file.

If you have a Key Store configured with ESA, then you can export the Key Store libraries and files using the *customer.custom* file. The following is a sample snippet listing the settings for exporting a Key Store directory.

```
#To include all the files present in the Safeguard directory  
/opt/safeguard/*  
#To include all the files present in the Safenet directory  
/usr/safenet/*
```

The following is a sample snippet listing the settings for exporting the self-signed certificates.

```
#To include all the files present in the Certificates directory  
/etc/ksa/certificates
```

Note:

Ensure that the files mentioned in the *customer.custom* file are not specified in the *exclude* file.

For more information about the *exclude* file, refer to the section [Editing the Exclude File](#)

3. Click **Save**.

4.7.6.4.10 Editing the exclude File

The *exclude* file contains the list of system files and directories that you don't want to export. You can access the exclude file from the CLI Manager only. The exclude file is present in the `/opt/ExportImport/filelist` directory.

Note:

A user which has *root* privileges is required to edit the *exclude* file, as it lists the system directories that you cannot import.

Note:

If a file or directory is present in both the *exclude* file and the *customer.custom* file, then the file or directory is not exported.

The following directories are in the exclude file:

- `/etc`
- `/usr`
- `/sys`
- `/proc`
- `/dev`
- `/run`
- `/srv`
- `/boot`
- `/mnt`
- `/OS_bak`
- `/opt_bak`

Note: The list of files mentioned in the *exclude* file affect only the *customer.custom* file and not the standard cluster export tasks.

If you want to export or import files, then ensure that these files are not listed in the *exclude* file.

► To edit the exclude file:

1. On the CLI Manager, navigate to **Administration > OS Console**.
2. Navigate to the `/opt/ExportImport/filelist/` directory.
3. Edit the *exclude* file using an editor.
4. Perform the required changes.
5. Save the changes.

4.7.6.5 Restoring Configurations

Using **Import** tab, you can restore the created backups of the product configurations and/or appliance OS core configuration.

Using the **Import** tab, you also can upload a configuration file saved on your local machine to the appliance. You can also download a configuration file from the appliance and save it to your local machine.

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 **Consul Configuration and Data**, ensure that the Consul product is installed in the appliance

► To restore a configuration from backup:

1. Navigate to the **System > Backup & Restore**.
2. Navigate to the Import tab, select a saved configuration from the list and click **Import**.
3. Choose specific components from the exported configuration and select the configurations that want to restore.

Note: If you want to restore all the components, you must select each component individually.

Before importing certificates using the **Certificates** option, navigate to **System > Services > Misc** and stop the services in the following order:

- a. **td-agent**
- b. **Analytics**
- c. **Audit Store Management**
- d. **Audit Store Repository**

After the import is complete, navigate to **System > Services > Misc**, and start the services in the following order:

- a. **Audit Store Repository**
- b. **Audit Store Management**
- c. **Analytics**
- d. **td-agent**

4. In the Password field, enter the configuration password and click **Import**.

Using the Import tab, you also can:

- Upload a configuration file saved on your local machine to the appliance
- Download a configuration file from the appliance and save it to your local machine

4.7.6.6 Working with OS Full Backup and Restore

It is recommended to perform the full OS back up before any important system changes, such as appliance upgrade or creating a cluster, among others.

4.7.6.6.1 Backing up Appliance OS from Web UI

► To back up the appliance OS from Web UI:

1. Login to the Appliance Web UI.
2. Proceed to **System > Backup & Restore**.
3. Navigate to the **OS Full** tab and click **Backup**.
A confirmation message appears.

Note:

The backup process may take several minutes to complete.

4. Press **ENTER**.
The **Backup Center** screen appears and the OS backup process is initiated.
5. Navigate to Appliance **Dashboard**.
A notification *OS Backup has been initiated* appears. After the backup is complete, a notification *O.S Backup has been completed* appears.

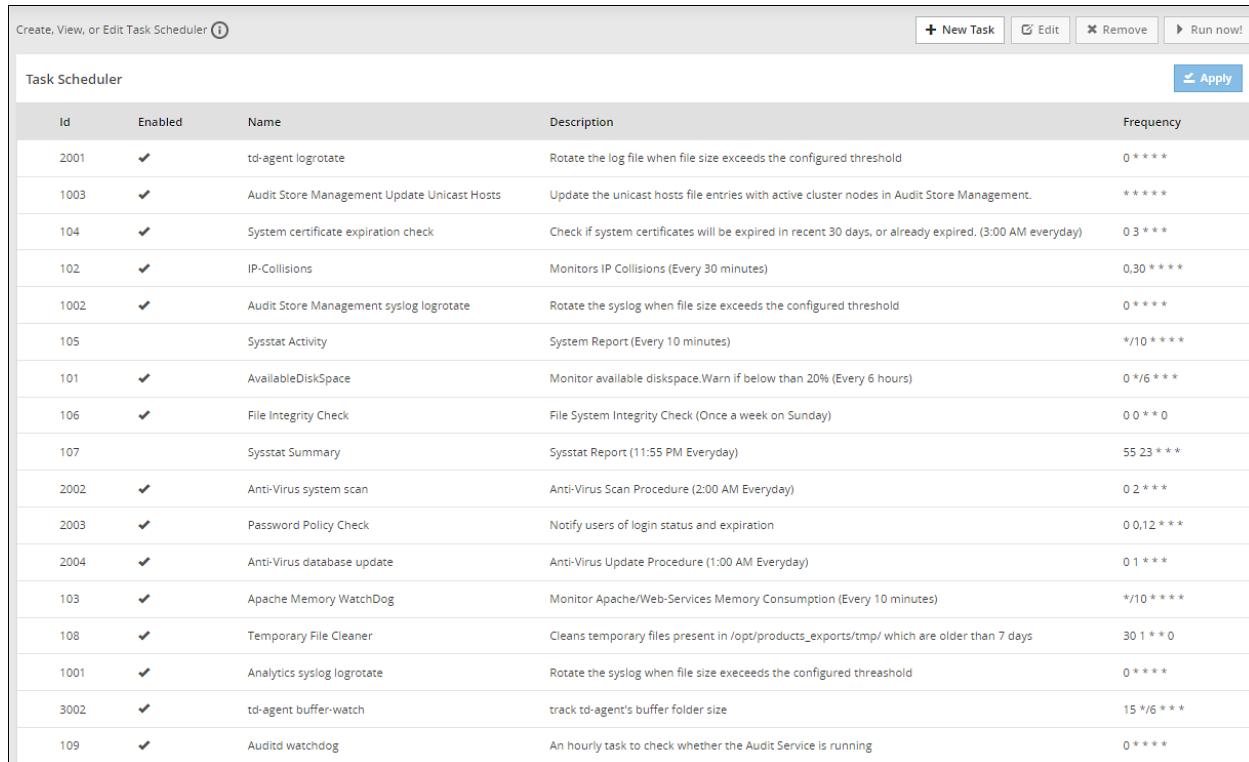
4.7.6.7 Viewing Export/Import Logs

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.

4.7.7 Scheduling Appliance Tasks

Using **System > Task Scheduler** you can schedule appliance tasks to run automatically. You can create or manage tasks from the ESA Web UI.

The following figure illustrates the default scheduled tasks that are available after you install the appliance.



The screenshot shows a table titled "Task Scheduler" with columns: Id, Enabled, Name, Description, and Frequency. The table lists 20 default scheduled tasks. The "Enabled" column contains checkboxes, all of which are checked. The "Apply" button is highlighted in blue at the top right of the table area.

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. (8:00 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 exceeds the configured threshold	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 4-16: Scheduler page



The Scheduler page displays the list of available tasks.

To edit a task, click **Edit**. Click **Save** and then click **Apply** after performing the required changes.

To delete a task, click **Remove**.

On the ESA Web UI, navigate to **Insight Analytics** screen to view the logs of a scheduled task.

4.7.7.1 Creating a Scheduled Task

This section describes the procedure to create a scheduled task.

► 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** section.
For more information about the basic properties, refer to section [*Basic Properties*](#).
4. Enter the required information in the **Frequencies** section.
For more information about the frequencies, refer to section [*Frequencies*](#).
5. Enter the required information in the **Command Line** section.
For more information about the command line, refer to section [*Execution*](#).
6. Enter the required information in the **Restrictions** section.
For more information about the command line, refer to section [*Restrictions*](#).
7. Enter the required information in the **Logging** section.
For more information about the logging, refer to section [*Logging*](#).
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 is now operational.

Note:

Click **Run Now** to run the scheduled task immediately.

Additionally, you can create a scheduled task, for exporting a configuration to a trusted appliances cluster using **System > Backup/Restore > Export**.

4.7.7.2 Basic Properties

In the Basic Properties section, you must specify the basic and mandatory attributes of the new task. The following table lists the basic attributes that you need to specify.

Table 4-4: Basic Identification Attributes

Attribute	Description
Name	A unique numeric identifier which is assigned automatically later by the scheduler.
Description	The task displayed name, which should also be unique.
Frequency	<p>You can specify the frequency of the task:</p> <ul style="list-style-type: none"> • Every 10 minutes • Every 30 minutes • Every hour • Every 4 hours • Every 12 hours • Daily (every midnight) • Weekly (every Sunday) • Monthly (first day of the month) • Custom (specify the custom frequency in the Frequency section)

4.7.7.3 Customizing Frequency

In the Frequency section of the new scheduled task, you can customize the frequency of the task execution. The following table lists the frequency parameters which you can additionally define.

Table 4-5: Frequency Attribute List

Attribute	Description	Notes
Minutes	<p>Defines the minutes when the task will be executed:</p> <ul style="list-style-type: none"> • Every minute • Every 10 minutes • Every 30 minutes • From 0 to 59 	<p>Every minute is the default. You can select several options, or clear the selection.</p> <p>For example, you can select to execute the task on the first, second, and 9th minute of the hour.</p>
Days	<p>Defines the day of the month when the task will be executed:</p> <ul style="list-style-type: none"> • Every day • Every two days • Every seven days • Every 14 days • From 1 to 31 	Every day is the default. You can select several options, or clear the selection.
Days of the week	<p>Defines the day of the week when the task will be executed:</p> <ul style="list-style-type: none"> • From Sun to Mon • Every DOW (day of the week) • Every 2nd Sun to every 2nd Mon. • Every 4 hours • Every 12 hours • Daily (every midnight) • Weekly (every Sunday) • Monthly (first day of the month) • Custom (specify the custom frequency in the Frequency section) 	Every DOW (day of week) is the default. You can select several options, or clear the selection.



Attribute	Description	Notes
Hours	Defines the hour when the task will be executed: <ul style="list-style-type: none">• Every hour• From 0 to 23• Every two hours• Every four hours• Every eight hours• */6 (every six hours).	Every hour is the default. You can select several options, or clear the selection. If you select *, then the task will be executed each hour. If you select */6, then the task will be executed every six hours (at 0, 6, 12, and 18).
Month	Defines the month when the task will be executed: <ul style="list-style-type: none">• Every month• From Jan to Dec• Every two months• Every three months• Every four months• Every six months	Every month is the default. You can select several options, or clear the selection. If you select *, then the task will be executed each month.

Description field of Frequency section will be automatically populated with the frequency details that you specified in the fields mentioned in the following table. **Task Next Run** will hint when the task next run will occur.

4.7.7.4 Execution

In the Command Line section, you need to specify the command which will be executed, and the user who will execute this command. You can optionally specify the command parameters separately.

Command Line

In the Command Line edit field, specify a command that will be executed. Each command can include the following items:

- The task script/executable command
- User name to execute the task (optional)
- Parameters to the script as part of the command (optional, can be specified separately in the Parameters section).

Parameters

Sometimes it is easier to specify the parameters to the command outside the command itself. Using the Parameters section, you can specify the command parameters separately.

You can add as many parameters as you need using **Add Param** button, and remove the unnecessary ones by clicking Remove button.

For each new parameter you need to enter *Name* (any), *Type* (option), and *Text* (any).

Each parameter can be of *text* (default) and *system* type. If you specify *system*, then the parameter will be actually a script that will be executed, and its output will be given as the parameter.

Username

In the Username edit field, specify the user who owns the task. If not specified, then tasks run as *root*.

Note: Only *root*, *local_admin*, and *ptycluster* users are applicable.

4.7.7.5 Restrictions

In a Trusted Appliance cluster, **Restrictions** allow you to choose the sites on which the scheduled tasks will be executed. The following table lists the restrictions that you can select.

Attribute	Description
On master site	The scheduled tasks are executed on the Master site
On non-master site	The scheduled tasks are executed on the non-Master site

If you select both the options, **On master site** and **On non-master site**, then the scheduled task is executed on both the sites.

4.7.7.6 Logging

In the Logging section, you should specify the logging details explained in the table below:

Table 4-6: Logging

Logging Detail	Description	Notes
Show command line in logs?	Select a check-box to show the command line in the logs	It is advisable not to select this option if the command includes sensitive data, such as passwords.
SysLog	Define the following details: <ul style="list-style-type: none"> • Success severity • Success title • Fail severity • Fail title 	You should configure these fields to be able to easily analyze the incoming logs. Specifies whether to send an event to the Log Server (ESA) and the severity: No event, Lowest, Low, Medium, High, Critical) for failed/success task execution.
Log Server	Specify the files names where the success and failed operations are logged.	Specifies whether to store the task execution details in local log files. You can specify to use the same file for successful and failed events. These files will be located in <code>/var/log</code> . You can also examine the success and failed logs in the Appliance Logs, in the appliance Web Interface.
Log File		

4.8 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 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 to view the previously generated logs.

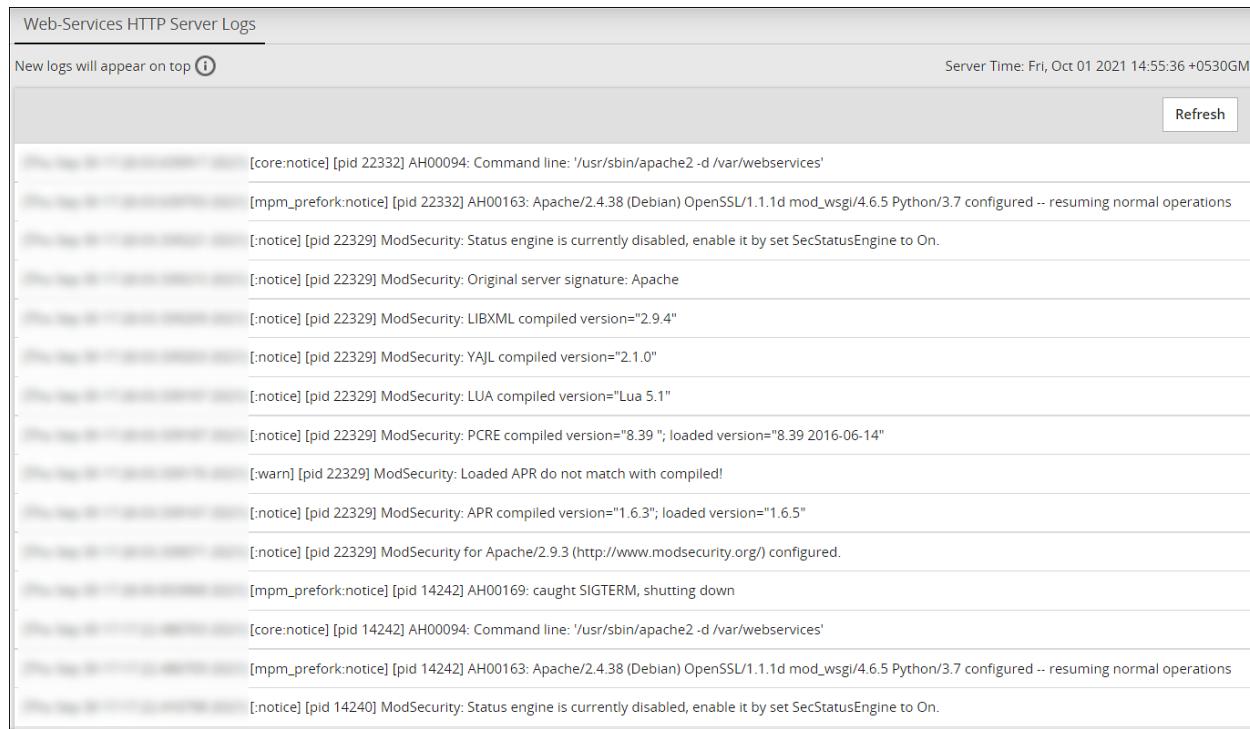
4.8.1 Viewing Web Services Engine Logs

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.



The screenshot shows a web-based log viewer titled "Web-Services HTTP Server Logs". At the top, it says "New logs will appear on top" with an info icon. On the right, it shows the "Server Time: Fri, Oct 01 2021 14:55:36 +0530GMT". A "Refresh" button is also present. The main area displays a list of log entries from two different Apache processes (pid 22332 and pid 14242). The logs include notices about command lines, OpenSSL, Python, and ModSecurity configurations, as well as warnings about APR version mismatch and SIGTERM handling.

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

Figure 4-17: HTTP Server Logs

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

4.8.2 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.

The screenshot shows a web-based log viewer for the Service Dispatcher. At the top, there are two tabs: "Service Dispatcher Server Logs" (which is active) and "Service Dispatcher access Logs". Below the tabs, a message says "New logs will appear on top" with an information icon. On the right, there is a "Server Time:" field and a "Refresh" button. The main area displays a list of log entries:

- [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/
- [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/
- [core:notice] [pid 17702:tid 139854581261440] AH00094: Command line: '/usr/sbin/apache2 -d /var/service_dispatcher'
- [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
- [notice] [pid 17702:tid 139854581261440] mod_python: using mutex_directory /tmp
- [notice] [pid 17702:tid 139854581261440] mod_python: Creating 8 session mutexes based on 16 max processes and 32 max threads.
- [mpm_worker:notice] [pid 17702:tid 139854581261440] AH00297: SIGUSR1 received. Doing graceful restart
- [core:notice] [pid 17702:tid 139854581261440] AH00094: Command line: '/usr/sbin/apache2 -d /var/service_dispatcher'
- [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
- [notice] [pid 17702:tid 139854581261440] mod_python: using mutex_directory /tmp

Figure 4-18: Service Dispatcher Logs

4.8.3 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 i

Enterprise-Security-Administrator - Event Logs : Current Ever ▼

Server Time

Print Download Refresh Save a copy Purge log

protegility-es953 /mod_wsgi: User admin has request to view file customer.custom.
 protegility-es953 /mod_wsgi: User admin logged into the web-interface from 10.10.3.16.
 protegility-es953 /mod_wsgi: User: admin was logged out from web-interface after his session has timed out. (web-user 'admin' , IP: '10.10.3.16')
 protegility-es953 /mod_wsgi: Reset web session timeout (web-user 'admin' , IP: '10.10.3.16')
 protegility-es953 /mod_wsgi: User admin logged into the web-interface from 10.10.3.16.
 protegility-es953 /mod_wsgi: User: admin was logged out from web-interface after his session has timed out. (web-user 'admin' , IP: '10.10.3.16')
 protegility-es953 /mod_wsgi: Reset web session timeout (web-user 'admin' , IP: '10.10.3.16')
 protegility-es953 /mod_wsgi: User admin logged into the web-interface from 10.10.3.16.
 protegility-es953 CLI: [INFO] User admin (web/local user) logged-in to the CLI-Manager
 protegility-es953 ksa.common[42961]: SSH/CLI: User admin has been authenticated
 protegility-es953 /usr/local/lib/python3.7/dist-packages/ksa/password_policy.py: New message has been delivered for viewer by subsystem: Password Policy, Message: Password will expire in 29 days, 05 hours, 12 minutes
 protegility-es953 /usr/local/lib/python3.7/dist-packages/ksa/password_policy.py: New message has been delivered for admin by subsystem: Password Policy, Message: Password will expire in 29 days, 05 hours, 12 minutes

Figure 4-19: Appliance Logs

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

Table 4-7: 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](#).

Note:

If the new logging/fluentd component is installed in the appliance, logs are sent to the Audit Store. If the new logging/fluentd component is not installed 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.

4.9 Working with Settings

The **Settings** menu on the appliance Web UI allows you to configure various features, such as, antivirus, two-factor authentication, networking, file management, user management, and licences. The following section provide a detailed description of all the features that can be accessed from the **Settings** menu.

4.9.1 Working with Antivirus

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, as required.

You can use AntiVirus to perform the following functions:

- Schedule the scans or run these on demand
- Update the virus data signature or database files, or run the update on demand
- View the logs generated for every virus found.

Simple user interfaces and standard configurations for both Web UI and CLI of the Appliance make viewing logs, running scans, or updating the virus signature file easy.

4.9.1.1 Customizing Antivirus Scan Options

On the Antivirus section, you can customize the scan by setting the following options:

- **Action:** Ignore the scan result, move the file to a separate directory, or delete the infected files
- **Recursive:** Implement and scan directories, sub-directories, and files
- **Scan Directory:** Specify the directory

► To customize Antivirus scan options:

1. Navigate to **Settings > Security > AntiVirus**.
2. Click **Options**.
3. Choose the required options and click **Apply**.

A message *Option changes are accepted!* appears.

4.9.1.2 Scheduling AntiVirus Scan

An AntiVirus scan can be scheduled only from the Web UI.

1. Go to **System > Task Scheduler**.
2. Search Anti-Virus system scan.
If it is present, then scanning is already scheduled.

Verify the Frequency and update if required.

3. If Anti-Virus system scan is not present, then follow these steps:
 - a. Click **+New Task**.

- b. Add the details, such as the Name, Description, and Frequency.
 - c. Add the command line steps, and Logging details.
4. Click **Save** at the top right of the window.

The AntiVirus scanning automatically begins at the scheduled time and logs are saved.

4.9.1.3 Updating the Antivirus Database

You must update the AntiVirus database or the signature files frequently. These ensures that the antivirus is updated to pick any new threats to the appliance. The antivirus database can either be updated from the official ClamAV website, local websites, mirrors, or using the signature files. The signature files are downloaded from the website and uploaded on the appliance Web UI. The following are the Antivirus signature database files that must be downloaded:

- *main.cvd*
- *daily.cvd*
- *bytecode.cvd*

The Antivirus signature database files can be updated in one of the following two ways:

- SSH/HTTP/HTTPS/FTP
- Official website/mirror/local sites

It is recommended that you update the signature database files directly from the official website.

4.9.1.3.1 Updating the AntiVirus Signature Files Manually

► To update the Antivirus signature files the Web UI:

1. On the appliance Web UI, navigate to **Settings > Security > AntiVirus**.
2. Click **Database Update > Settings**.
3. Select one of the following settings.
 - *Table 4-8: Antivirus Update*

Settings	Description
Local/remote mirror server	Server containing the database update. Enter the URL of the server in Input the target URL text box.
Official website through HTTP proxy server	Proxy server of ClamAV containing the database update. Enter the following information: <ul style="list-style-type: none"> • Username and Password: User credentials for logging in to the proxy server • Server: IP address or URL of the proxy server • Port Number: Port number of the proxy server. If no port number is specified, the default port is considered.
Local directory	Local directory where the updated database signature files, such as, <i>main.cvd</i> , <i>daily.cvd</i> and <i>bytecode.cvd</i> are stored. Enter the directory path in Input the target directory text box.
Remote host	Host containing the updated database signature files. Connect to this host using an SSH, HTTP, HTTPS, or FTP connection. Enter information in the required fields to establish a connection with the remote host.

4. Select **Confirm**.

The database update is initiated.

4.9.1.3.2 Updating the AntiVirus Signature Files Manually

In case network is not available or the Internet is disconnected, you can manually update the signature database files. The signature files are downloaded from the website and placed in a local directory. The following are the Antivirus signature database files that must be downloaded:

- *main.cvd*
- *daily.cvd*
- *bytecode.cvd*

It is recommended that you update the signature database files directly from the official website.

► To manually update the Antivirus database signature files:

1. Download the AntiVirus signature database files: *main.cvd*, *daily.cvd*, and *bytecode.cvd*.
2. On the CLI Manager, navigate to **Administration > OS Console**.
3. Create the following directory in the appliance.
/home/admin/clam_update/
4. Save the downloaded signature database files in the */home/admin/clam_update/* directory.

4.9.1.3.3 Scheduling Update of AntiVirus Signature Files

Scheduling an update is possible only from the Web UI.

► To schedule update of antivirus signature files:

1. Go to **System > Task Scheduler**.
2. Select the **Anti-Virus database update** row.
3. Click **Edit** from the Scheduler task bar.
For more information about scheduling tasks, refer to [Scheduling Appliance Tasks](#).
4. Click **Save** at the top right corner of the workspace window.

4.9.1.4 Viewing AntiVirus Logs

Log files are generated for all system and database activities. These logs are stored in the local log file, *runtime.log* which is saved in the */etc/opt/AntiVirus/* directory. You can view and delete the local log files.

4.9.1.4.1 Viewing Antivirus Logs

The logs for the Antivirus can be viewed from the appliance Web UI. The logs consist of antivirus database updates, scan results, infections found, and so on. These logs are also available on the **Insight Analytics** screen. You can view all logs, including those deleted in the local file.

► To view logs from the Web UI:

1. Go to **Settings > Security > AntiVirus**.
2. Click **Log**.

4.9.1.4.2 Deleting Logs from Local File Using the Web UI

► To delete logs from local file using the web ui:

1. Go to **Settings > Security > AntiVirus**.
2. Click **Log**.
3. Click **Purge**.

All existing logs in the local log file are deleted.

4.9.1.4.3 Viewing Logs from the Appliance CLI

► To view logs from appliance CLI:

1. Go to **Status and Logs > Appliance Logs**.
2. Select **System event logs**.
3. Press **View**.
4. From the list of available installed patches, select **patches**.
5. Press **Show**.

A detailed list of patch related logs are displayed on the ESA Server window.

4.9.1.4.4 Configuring Log Rotation and Log Retention

► To configure log rotation and log retention:

Perform the following steps to configure log rotation and log retention.

1. Append the following configuration to the `/etc/logrotate.conf` file:

```
/var/log/clamav/*.log
{ missingok monthly size 10M rotate 1 }
```

2. For periodic log rotation, run the following command:

```
cd /etc/opt/AntiVirus/
mv /etc/opt/AntiVirus/runtime.log /var/log/clamav
ln -s /var/log/clamav/runtime.log runtime.log
```

4.9.2 Configuring Appliance 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.

In order to provide this functionality, a *trust* is created between the appliance and the mobile device being used for authentication. The trust is simply a shared-secret or a graphic barcode that is generated by the system and is presented to the user upon first login.

The advantage of using the two-factor authentication feature is that if a hacker manages to guess your password, then entry to your system is not possible as a device is required to generate the verification code.

The verification code is a dynamic code that is generated by any smart device such as smartphone or tablet. The user enters the shared-secret or scans the barcode into the smart device, and from that moment onwards the smartphone generates a new verification-code every 30-60 seconds. The user is required to enter this verification code every time as part of the login process.

For Protegility appliances, a prerequisite, download and install the Google Authenticator app from the app store into your mobile device, or use any other TOTP-compatible device or application.

Note:

On a Protegility appliance, only the Google Authenticator app and Radius Authenticator is supported for the Two Factor Authentication.

The Security Officer configures the Appliance Two Factor Authentication by any one of the following three methods:

- **Automatic per-user shared-secret** is the default and recommended method. It allows having a separate shared-secret for each user, which is generated by the system for them. The shared-secret will be presented to the user upon the first login.
- **Radius Authentication** is the authentication using the RADIUS protocol.
- **Host-based shared-secret** allows a common shared-secret for all users, which can be specified and distributed to the users by the Security Officer. Host-based shared-secret method is useful to force the same secret code for multiple appliances in clustered environments.

4.9.2.1 Configuring Two Factor Authentication with Automatic Per User Shared Secret

► To configure Two Factor Authentication with Automatic per-user shared-secret:

1. From the Appliance Web UI, navigate to **Settings > Security > Two Factor Authentication**.
2. Check the **Enable Two-Factor-Authentication** checkbox.
3. Select the **Automatic per-user shared-secret** option.

The following pane appears with the options to enable this authentication mode.

Two Factor Authentication

Enable Two-Factor-Authentication
Two Factor Authentication provides an enhanced method of authentication. In addition to the traditional credentials (user name and password), the user will have to provide a shared code generated by a smartphone or hardware device.

Authentication Mode

- Automatic per-user shared-secret**
Each user will have their own shared secret. Once a new user attempts to log in, the system will automatically create a shared code and present it to the user.
- Host-based shared-secret**
All users have the same shared secret. This method is recommended for clustered environments, allowing users to use the same code for multiple machines.

[Modify](#)

- Remote Authentication**
Use another Protegity-Appliance server (e.g. remote ESA) for authentication.

[Validate](#)

- * Radius Server**
Use any External Server which supports Radius Protocol using PAP (Password Authentication Protocol).

*** Radius secret** - Secret needed to communicate with a RADIUS server

Radius pap (password authentication protocol) port - If not provided default port (1812) will be used.

Radius Validation - * It is recommended to validate the Radius mode configuration, before enabling it.

Validation User Name

Validation OTP - One Time Password

[Validate](#)

Figure 4-20: Two Factor Authentication with Automatic per-user shared-secret pane

4. If required, then you can customize the message that will be presented to users upon their first login. Check the **Advanced Settings** checkbox to display the **Console Message** and **Browser Message** buttons. By clicking **Console Message** or **Browser Message**, a new window appears where you can review and modify the message that will be presented to the user.

Note:

In the browser-message window you can specify HTML tags and even include your company's logo.

Welcome to Appliance Authentication System
Username: \${USERNAME}

As a security-measure please enter the provided security-code into your authentication-application on your smart-phone/tablet or security-device :

\${SHARED_SECRET}

When done, your authentication-application will provide you the verification-code for login .

Enter the verification code:

Variables:	
\${SHARED_SECRET}	Shared-Secret
\${USERNAME}	Username

[Preview](#) [Save](#) [Close](#)

Figure 4-21: Reviewing the user-message for CLI users

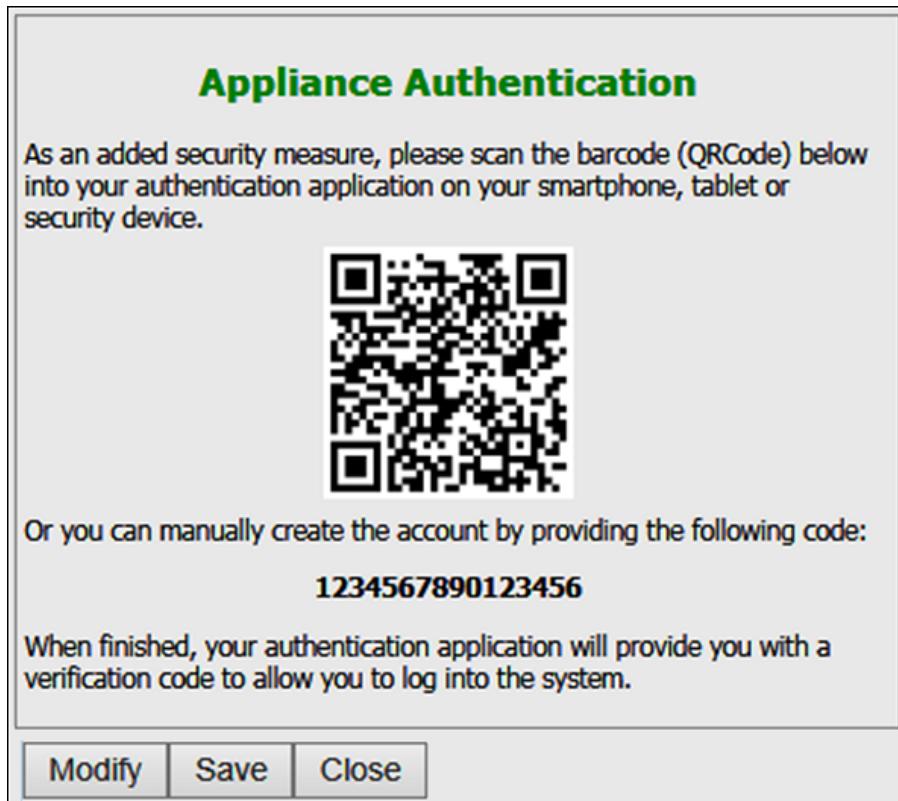


Figure 4-22: Reviewing the user-message for browser users

5. You can apply the following logging-settings in order to specify what to log:
 - Log failed log-in attempts
 - Log any successful log-ins
 - Log only first-successful log-in
6. Click **Apply** to save the changes.

4.9.2.2 Configuring Two Factor Authentication with Host-Based Shared-Secret

► To configure Two Factor Authentication with Host-based shared-secret:

1. On the ESA Web UI, navigate to **Settings > Security > Two Factor Authentication**.
2. Check the **Enable Two-Factor-Authentication** checkbox.
3. Select **Host-based shared-secret** from Authentication Mode.
4. Click **Modify**.
The key **Host-shared secret key** appears.

Note:

If required, click **Generate** to modify the **Host-shared secret key**. Ensure that you note the **Host-shared secret key** to generate TOTP.

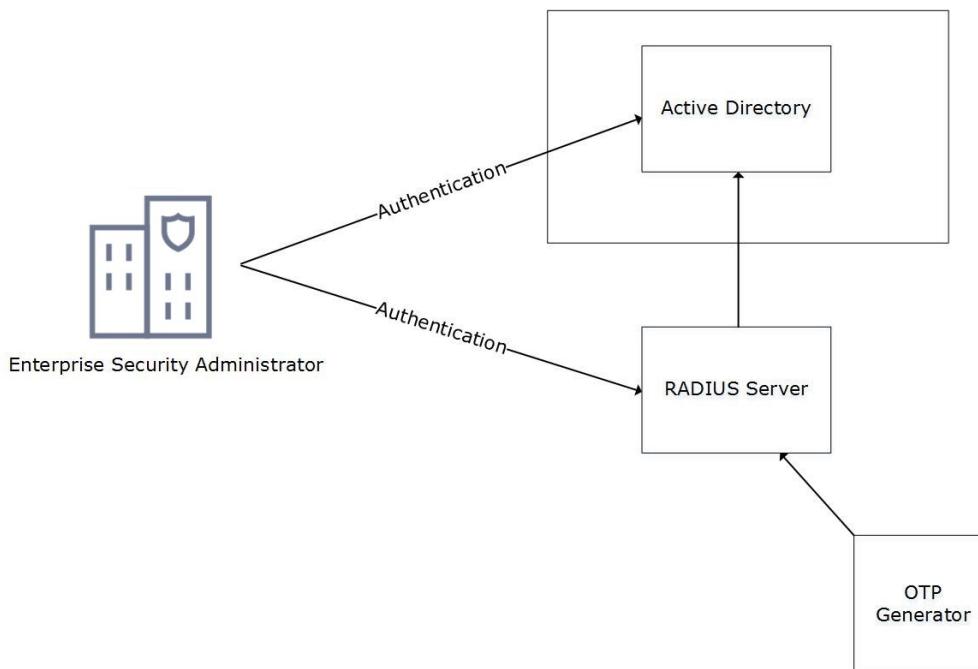
5. You can apply the following logging-settings in order to specify what to log:
 - Log failed log-in attempts
 - Log any successful log-ins

6. Click **Apply** to save the changes.
A confirmation message appears.

4.9.2.3 Working with Remote Authentication Dial-up Service (RADIUS) Authentication

The Remote Authentication Dial-up Service (RADIUS) is a networking protocol for managing authentication, authorization, and accounting in a network. It defines a workflow for communication of information between the resources and services in a network. The RADIUS protocol uses the UDP transport layer for communication. The RADIUS protocol consists of two components, the RADIUS server and the RADIUS client. The server receives authentication and authorization requests of users from the RADIUS clients. The communication between the RADIUS client and RADIUS server is authenticated using a shared secret key.

You can integrate the RADIUS protocol with an ESA for two-factor authentication. The following figure describes the implementation between ESA and the RADIUS server.



- The ESA is connected to the AD that contains user information.
- The ESA is a client to the RADIUS sever that contains the network and connection policies for the AD users. It also contains a RADIUS secret key to connect to the RADIUS server. The communication between the ESA and the RADIUS sever is through the Password Authentication Protocol (PAP).
- An OTP generator is configured with the RADIUS server. An OTP is generated for each user. Based on the secret key for each user, an OTP for the user is generated.

In ESA, the following two files are created as part of the RADIUS configuration:

- The *dictionary* file that contains the default list of attributes for the RADIUS server.
- The *custom_attributes.json* file that contains the customized list of attributes that you can provide to the RADIUS server.

Figure 4-23: RADIUS Implementation

4.9.2.3.1 Configuring Radius Two-Factor Authentication

- To configure Radius two-factor authentication:

1. On the Appliance Web UI, navigate to **Settings > Security > Two Factor Authentication**.
2. Check the **Enable Two-Factor-Authentication** checkbox.
3. Select the **Radius Server** option as shown in the following figure.

The screenshot shows a configuration form for a Radius server. At the top, there is a note: "Use any External Server which supports Radius Protocol using PAP (Password Authentication Protocol)." Below this is a text input field containing "2.10.1.17". The next section is labeled "* Radius secret - Secret needed to communicate with a RADIUS server" with a text input field containing ".....". A note below it says "Radius pap (password authentication protocol) port - If not provided default port (1812) will be used." with a text input field containing "1812". The following sections are "Radius Validation" (with a note about validating before enabling) and "Validation User Name" (with an empty text input field). Below that is "Validation OTP - One Time Password" (with an empty text input field). At the bottom is a blue "Validate" button.

4. Type the IP address or the hostname of the RADIUS server in the **Radius Server** text box.
5. Type the secret key in the **Radius Secret** text box.
6. Type the port of the RADIUS server in the **Radius port** text box.
Alternatively, the default port is *1812*.
7. Type the username that connects to the RADIUS server in the **Validation User Name** text box.
8. Type the OTP code for the user in the **Validation OTP** text box.
9. Click **Validate** to validate the configuration.
A message confirming the configuration appears.
10. Click **Apply** to apply the changes.

4.9.2.3.2 Logging to the Web UI

► To login to the Web UI:

1. Open the ESA login page.
2. Type the user credentials in the **Username** and **Password** text boxes.
3. Click **Sign-in**.

The following screen appears.

2 step authentication

Input the code generated by your Authenticator

Tip: Make sure the code is entered before the time limit.

Enter authentication code

Verify

Switch User

4. Type the OTP code and select **Verify**.
After the OTP is validated, the ESA home page appears.

4.9.2.3.3 Editing the Radius Configuration Files

► To edit the configuration files:

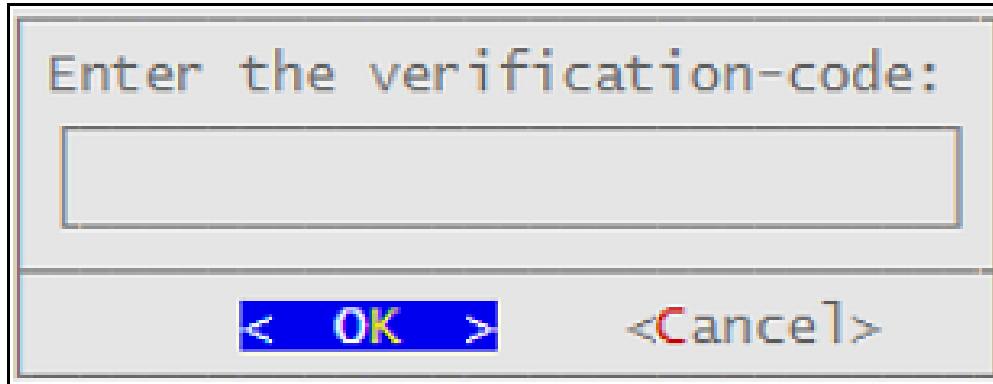
1. On the Appliance Web UI, navigate to **Settings > System**.
2. Under OS-Radius Server tab, click **Edit** corresponding to the *custom_attributes.json* or *directory* to edit the attributes.
3. If required, modify the attributes to the required values.
4. Click **Save**.
The changes are saved.

4.9.2.3.4 Logging to the CLI

► To login to CLI Manager:

1. Open the Appliance CLI Manager.
2. Type the user credentials.
3. Press **ENTER**.

The following screen appears.



4. Type the verification code and select **OK**.

After the code is validated, the main screen for the CLI Manager appears.

4.9.2.4 Working with Shared-Secret Lifecycle

All users of the Appliance Two Factor Authentication get a shared-secret for verification. This shared-secret for a user remains in the two factor authentication group list until it is manually deleted. Even if a user becomes ineligible to access the system, the username remains linked to the shared-secret.

This exception is valid for those users opting for *per-user* authentication.

If the same user or another user with the same name is again added to the system, then the user becomes eligible to use the already existing shared-secret.

To prevent this exception, ensure that an ineligible user is manually removed from the Two Factor Authentication group.

4.9.2.4.1 Revoking Shared-Secret for the User

► To revoke shared-secret for the user: edit the configuration files:

1. On the Appliance Web UI, navigate to **Settings > Security > Two Factor Authentication**.
2. Ensure that the **Enable Two-Factor-Authentication** and **Automatic per-user shared-secret** checkbox are checked.
3. Inspect *Users Shared Secrets* area to identify user account to revoke.
You can revoke users who have already logged in to the Appliance.
4. Click **Revoke**.

The screenshot shows a list of users under the heading 'Users Shared Secrets'. There are two entries: 'admin' and 'viewer'. To the left of each entry is a checkbox icon. The 'admin' entry has a checked checkbox, indicating the user has logged in. The 'viewer' entry has an unchecked checkbox, indicating the user has not logged in yet. To the right of the list is a legend box with the title 'Legend:' containing two items: 'User has logged-in' with a checked checkbox icon, and 'User has not logged-in yet' with an unchecked checkbox icon. At the bottom of the main area are two buttons: 'Revoke' and 'Refresh'.

5. Select the user to discard by clicking the checkbox next to the username.
6. Click **Apply** to save the changes.
A new shared-secret code will be created for the revoked user and is presented upon the next login.

Note: The option to revoke shared-secret is useful when user needs to switch to another mobile device or the previous shared-secret cannot be retrieved from the earlier device.

4.9.2.5 Logging in Using Appliance Two Factor Authentication

► To log in using Appliance Two Factor Authentication:

1. Go to ESA login page.
The ESA login page appears.
2. Enter your username.
3. Enter your password.
4. Click **Sign in**.
After verification, a separate login dialog appears.

The screenshot shows a login interface for two-factor authentication. At the top, it says 'Input the code generated by your Authenticator'. Below that is a tip: 'Tip: Make sure the code is entered before the time limit.' There is a text input field labeled 'Enter authentication code' with a placeholder 'Enter authentication code'. Below the input field is a dark button labeled 'Verify'. At the bottom, there is a note in a pink box: 'Enter the verification code provided you by your security-administrator'. At the very bottom, there is a link 'Switch User'.

Figure 4-24: Verification Code Screen

Note:

As a prerequisite, a new user must setup an account on Google Authenticator. Download the Google Authenticator app in your device and follow the instructions to create a new account.

5. Enter the shared-secret in your device.
If the system is configured for per-user shared-secret, then this secret code is made available. If this is a web-session, then you are presented with a barcode and the applications that support it.
6. After you accept the shared-secret, the device displays a verification code.
7. Enter this verification code in the screen displayed in step 4.
8. Click **Verify**.

4.9.2.6 Disabling Appliance Two Factor Authentication

► To disable Appliance Two Factor Authentication:

1. Using the Appliance Web UI, navigate to **Settings > Security > Two Factor Authentication**.
2. Clear the **Enable Two-Factor-Authentication** checkbox.
3. Click **Apply** to save the changes.

Note:

You can also disable two-factor authentication from the local console.

You need to switch to OS console and execute the following command.

```
# /etc/opt/2FA/2fa.sh --disable
```

4.9.3 Working with File Integrity

PCI (Section 11.5) specifications require that sensitive files and folders in the appliance, such as password, certificate, and configuration files, be monitored and all changes made to these files be reviewed by authorized users. The File Integrity Monitor makes a weekly check and content modifications can be viewed by the Security Officer.

Figure 4-25: File Integrity Monitor page

To check file modifications at any given time, click **Settings > Security > File Integrity > Check**. The Security Officer views and accepts the changes, writing comments as necessary, in the comment box. Accepting changes means that the changes are removed from the viewable list. Changes cannot be rejected.

Only the last modification made to a file appears.

Caution:

You cannot accept deletion of system files. These needs to be shown.

All the changes can also be viewed on the Insight Analytics screen. Another report shows all accepted changes.

Before applying a patch, it is recommended to check the files and accept the required changes under **Settings > File Integrity > Check**.

After installing the patches for appliances such as ESA or DSG, check the files and accept the required changes again under **Settings > Security > File Integrity > Check**.

4.9.4 Working with 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 **Settings > System > 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.

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

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



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 <div style="background-color: #e0f2e0; padding: 5px; margin-top: 10px;"> Note: When you upload a file, it replaces the existing file in the system. </div>
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.

4.9.4.1 Viewing a Configuration File

You can view the contents of the configuration file from the Web UI.

Note:

If the file size is greater than 5 MB, you must download the file to view the contents.

► To view a file:

1. Navigate to **Settings > System > Files**.

The screen with the files appears.

2. Click on the required file.

The contents of the file appear.

Note:

You can modify, download, or delete the file using the Edit, Download and Delete icon respectively.

4.9.4.2 Uploading a Configuration File

► To upload a file:

1. Navigate to **Settings > System > Files**.
The screen with the files appears.
2. Click on the upload icon.
the file browser icon appears.
3. Select the configuration file and click **Upload File**.
A confirmation message appears.
4. Click **Ok**.
A message confirming the upload appears.

4.9.4.3 Modifying a Configuration File

In addition to editing the file from the Files screen, you can also modify the content of the file from the view option.

Note:

If you want to modify the content of a file whose size is greater than 5 MB, you must download the file to the local machine, modify the content, and then upload the file through the Web UI.

► To modify a file:

1. Navigate to **Settings > System > Files**.
The screen with the files appears.
2. Click on the required file.
The contents of the file appear.
3. Click the **Edit** to modify the file.
4. Perform the required changes and click **Save**.
A message confirming the changes appears.

4.9.4.4 Deleting a Configuration File

In addition to deleting the file from the Files screen, you can also delete the file from the view option. After you delete the file, an exclamation icon appears indicating that the file does not exist on the server. Using the reset functionality, you can restore the deleted file.

► To delete a file:

1. Navigate to **Settings > System > Files**.
The screen with the files appears.

2. Click on the required file.
The contents of the file appear.
3. Click the **Delete** () icon to modify the file.
A message confirming the deletion appears.
4. Select **Yes**.

4.9.4.5 Resetting a File

The Reset functionality is used to restore the changes that are done to your file. For every configuration file, the Reset icon is disabled. This icon is enabled when you perform any of the following changes:

- Modify the configuration file
- Delete the configuration file

When you modify or delete a file, the original file is backed up in the `/etc/configuration-files-backup` directory. For every modification, the file in the directory is overwritten. When you click the Reset icon, the file is retrieved from the directory and restored on the Files screen.

Note:

Only the changes that are performed on the files through the Web UI are backed up. Changes performed on the files through the CLI Manager are not backed up and cannot be restored.

► To restore a file:

1. Navigate to **Settings > System > Files**.
The screen with the files appears.
2. Click the **Reset** () icon to restore a file.
The file that is edited or deleted is restored.

4.9.5 Managing Upload Files

You can upload patch files from the File Upload screen in the ESA Web UI. The files uploaded from the Web UI are available in the `/products/uploads` directory.

After you upload files the files, you can delete them or save them to a specific location.

► To upload a file:

1. Navigate to **Settings > System > File Uploads**.
The Uploads page appears.
2. In the File Selection section, click **Choose File**.
The file upload dialog appears.

3. Select the required file and click **Open**.

Note:

You can only upload files with *.pty*, and *.tgz* extensions.

If the file uploaded exceeds 25 MB, then a password prompt appears. Only a user with the administrative role can perform this action. Enter the password and click **Ok**.

4. Click **Upload**.

The file is uploaded to the */products/uploads* location.

Note:

You cannot upload a file containing special characters in its name. If a file contains spaces in its name, then it will be automatically replaced with underline character (*_*).

The files are scanned by the internal anti-virus before they are uploaded in the appliance.

5. After the file is uploaded successfully, then from the **Uploaded Files** area, choose the uploaded patch.

The information for the selected patch appears.

The screenshot shows the 'File Upload' interface. In the 'File Selection' section, there is a 'Select File' button, a 'Browse...' button, a message 'No file selected.', a note 'Maximum upload size: 25M', and a blue 'Upload' button. In the 'Uploaded Files' section, there is a 'Select File' dropdown menu with 'ESA_PAP-ALL-' selected, and 'Delete' and 'Download' buttons. In the 'Uploaded Files Information' section, there are details about the uploaded file: File name (ESA_PAP-ALL-), File size (51228273 bytes), MDS Checksum (redacted), SHA512 Checksum (redacted), Patch Title (Enterprise Security Administrator Web Guide), and Patch Description (Enterprise Security Administrator Web Guide). A note at the bottom states 'This patch is installed in the system.'

Note:

To verify the integrity of the uploaded file, validate the checksum values displayed on the screen with the checksum values of the downloaded patch file.

You can obtain the checksum values from the [My.Protegity](#) portal or contact Protegity Support.

4.9.6 Configuring Date and Time

You can use the Date/Time tab to change the date and time settings. To update the date and time, navigate to **Settings > System > Date/Time**.

The Date and Time screen with the **Update Time Periodically** option enabled is shown in the following figure.

Date/Time Configuration Settings

Name	Setting	Action
Update Time Periodically	<input checked="" type="checkbox"/> Disabled	Enable
Current Appliance Date/Time	Mon Oct 4 [REDACTED]	
Set Time Zone	Asia/Calcutta	Set Time Zone
Manually Set Date/Time(MM/DD/YYYY HH:MM)	MM/DD/YYYY HH:MM	Set Date/Time

Figure 4-26: Date/Time page

The date and time options are described in the following table.

Table 4-9: Change Date and Time options

Setting	Details	How to configure/change
Update Time Periodically	Synchronize the time with the specified NTP Server (upon boot and once an hour).	You can enable this option using Enable button and disable it using Disable .
Current Appliance Date/Time	Manually synchronize the time with the specified NTP Server. You can use NTP Server synchronization only if NTP service is running.	You can force and restart time synchronization using Reset NTP Sync . You can display NTP analysis using NTP Query button.
Set Time Zone	Specify the time zone for your appliance.	Select your local time zone from the Set Time Zone list and click Set Time Zone .
Set Manually Date/Time (mm/dd/yyyy hh:mm)	Set the time manually.	Type the date and time using the format mm/dd/yyyy hh:mm. Click Set Date/Time . Note: Note: The Set Manually Date/Time (mm/dd/yyyy hh:mm) text box appears only if the Update Time Periodically functionality is disabled.

Important:

You must enable/disable the NTP settings only from the CLI Manager or the Web UI.

4.9.7 Configuring Email

The SMTP setting allows the system to send emails to outside. This is already available in the CLI.

SMTP Setting

The following wizard will allow you to configure the e-mail settings on this machine.

Enable

* Server Address: * Port:

Use SSL/TLS Use Start TLS

Authentication

* Contact Address: * Host Identification:

Figure 4-27: Email Settings screen

You can test that the email works by clicking Test. Error logs can be viewed on the **Insight Analytics** screen.

Some scripts run after you click Save.

Email address

Send Now! Close Test

Show Test Communication

```
[->] EHLO protegriy-esas
[<-] 250 CHUNKING
[->] AUTH LOGIN
[<-] 334 VXNlcm5hbWU6
[>]
[<-] 334 UGFzc3dvcmQ6
[<-] 535 5.7.8 http://support.google.com/mail/bin/answer.py?answer=14257 u59sm22412480qga.8 - gsmtp
ssmtp: Authorization failed (535 5.7.8 http://support.google.com/mail/bin/answer.py?answer=14257 u59sm22412480qga.8 - gsmtp)
```

! Testing SMTP does not save the configuration. Please remember to save if SMTP is working.

Figure 4-28: Text Communication in Email Settings screen

If the email address cannot be authenticated, then the Show Test Communication area displays the communication between the appliance and the SMTP server for debugging.

4.9.8 Configuring Network Settings

On the **Network Settings** screen, you can configure the network details for the appliance. The following table explains the different settings that you can be configured.

Table 4-10: Network Configuration Settings

Setting	Details	How to configure/change
Hostname	The hostname is a unique name for a system or a node in a network.	Click Apply on the Web UI or change the hostname of the appliance from the Network Settings screen in the CLI Manager.
Management IP	The management IP (the IP address of the appliance) is defined through CLI Manager.	Select Blink to identify the interface. This will cause a LED on the NIC to blink and then click Change .
Default Route	The default route (IP address of your LAN router in the IP address format, for example, 172.16.8.12) is an optional destination for all network traffic that does not belong to the LAN segment. It is required only if the appliance is on a different subnet than the Appliance Web Interface.	Click Apply to set the default route.
Domain	The appliance domain name specified during appliance installation.	You can change it by specifying a new name and clicking Apply .
Search Domains	The appliance can belong to one domain and search an additional three domains.	You can add them using Add button.
Domain Name Servers	If your appliance uses domain names and IP addresses, then you must configure a domain name server (DNS) to help resolve Internet name addresses. The domain name should be for your local network (like <i>Protegrity.com</i> or <i>math.mit.edu</i>) and the name servers should be IP addresses. The appliance can use up to three DNS servers for name resolving. Once you have configured a DNS, the system can be managed using an SSH connection.	You can add them using Add button, and remove them using Remove . You can specify them using Apply button.

4.9.8.1 Managing Network Interfaces

Using **Settings > Network > Network Settings**, you can view appliance network interfaces names and addresses and add them from the Interfaces page.

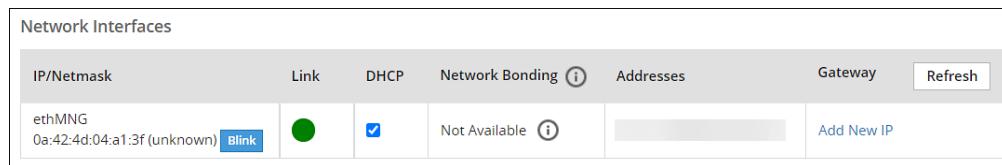


Figure 4-29: Network Interfaces page

Note:



Changes to IP addresses are immediate. Changes to the management IP (on ethMNG), while connected via SSH or the Appliance Web Interface, causes the session to disconnect.

4.9.8.1.1 Assigning an Address to an Interface

► To assign an address to an interface:

1. Navigate to **Settings > Network**.
2. Click **Network Settings**.
The Interfaces page appears.
3. Identify the interface on the appliance by clicking **Blink** for the interface you want to identify. Select a LED on the NIC blinks to indicate that interface.
4. In the interface row, type the address and Net mask of the interface, and then click **Add**.

4.9.8.1.2 Assigning an Address to an Interface Using Web UI

► To assign an address to an interface:

1. In the Web UI, navigate to **Settings > Network > Network Settings**.
The **Network Settings** page appears.
2. In the **Network Interfaces** area, select **Add New IP** in the **Gateway** column.

Note:

Ensure that the IP address for the NIC is added.

3. Enter the IP address of the default gateway and select **OK**.
The default gateway for the interface is added.

4.9.8.2 NIC Bonding

The NIC is a device through which appliances, such as ESA or DSG, on a network connect to each other. If the NIC stops functioning or is under maintenance, the connection is interrupted, and the appliance is unreachable. To mitigate the issues caused by the failure of a single network card, Protegrity leverages the NIC bonding feature for network redundancy and fault tolerance.

In NIC bonding, multiple NICs are configured on a single appliance. You then bind the NICs to increase network redundancy. NIC bonding ensures that if one NIC fails, the requests are routed to the other bonded NICs. Thus, failure of a NIC does not affect the operation of the appliance.

You can bond the configured NICs using different bonding modes.

4.9.8.2.1 Bonding Modes

The bonding modes determine how traffic is routed across the NICs. The MII monitoring (MIIMON) is a link monitoring feature that is used for inspecting the failure of NICs added to the appliance. The frequency of monitoring is 100 milliseconds. The following modes are available to bind NICs together:

- Mode 0/Balance Round Robin
- Mode 1/Active-backup
- Mode 2/Exclusive OR
- Mode 3/Broadcast
- Mode 4/Dynamic Link Aggregation
- Mode 5/Adaptive Transmit Load Balancing
- Mode 6/Adaptive Load Balancing

The following two bonding modes are supported for appliances:

- **Mode 1/Active-backup policy:** In this mode, multiple NICs, which are slaves, are configured on an appliance. However, only one slave is active at a time. The slave that accepts the requests is active and the other slaves are set as standby. When the active NIC stops functioning, the next available slave is set as active.
- **Mode 6/Adaptive load balancing:** In this mode, multiple NICs are configured on an appliance. All the NICs are active simultaneously. The traffic is distributed sequentially across all the NICs in a round-robin method. If a NIC is added or removed from the appliance, the traffic is redistributed accordingly among the available NICs. The incoming and outgoing traffic is load balanced and the MAC address of the actual NIC receives the request. The throughput achieved in this mode is high as compared to mode 1.

4.9.8.2.2 Prerequisites

Ensure that you complete the following pre-requisites when binding interfaces:

- The IP address is assigned only to the NIC on which the bond is initiated. You must not assign an IP address to the other NICs.
- The NIC is not configured on an HA setup.
- The NICs are on the same network.

4.9.8.2.3 Creating a Bond

The following procedure describes the steps to create a bond between NICs.

Note: Ensure that the IP address of the slave nodes are static.

► To create a bond:

1. On the Web UI, navigate to **Settings > Network > Network Settings**.
The *Network Settings* screen appears.
2. Under the Network Interfaces area, click **Create Bond** corresponding to the interface on which you want to initiate the bond.
The following screen appears.

Create Network Teaming : ethMNG (00:50:56:01:1f:39 (VMware, Inc.))

Network bonding policy mode :		Active-backup policy	
<input type="checkbox"/>	Name	MAC ID	
<input type="checkbox"/>	ethSRV8	00:50:56:01:26:84 (VMware, Inc.)	
<input type="checkbox"/>	ethSRV7	00:50:56:01:26:83 (VMware, Inc.)	
<input type="checkbox"/>	ethSRV6	00:50:56:01:26:1b (VMware, Inc.)	
<input type="checkbox"/>	ethSRV5	00:50:56:01:26:1a (VMware, Inc.)	
<input type="checkbox"/>	ethSRV4	00:50:56:01:23:1a (VMware, Inc.)	
<input type="checkbox"/>	ethSRV3	00:50:56:01:22:d3 (VMware, Inc.)	
<input type="checkbox"/>	ethSRV2	00:50:56:01:22:d2 (VMware, Inc.)	

Establish Network Bonding **Cancel**

Note: Ensure that the IP address is assigned to the interface on which you want to initiate the bond.

3. Select the following modes from the drop-down list:

- *Active-backup policy*
- *Adaptive Load Balancing*

For more information about the bonding nodes, refer to section [Bonding Modes](#).

4. Select the interfaces with which you want to create a bond.

5. Select **Establish Network Bonding**.

A confirmation message appears.

6. Click **OK**.

The bond is created, and the list appears on the Web UI.

4.9.8.2.4 Removing a Bond

The following procedure describes the steps to remove a bond between NICs.

► To remove a bond:

1. On the Web UI, navigate to **Settings > Network > Network Settings**.

The *Network Settings* screen appears with all the created bonds as shown in the following figure.

IP/Netmask	Link	DHCP	Network Teaming 	Addresses
ethMNG 00:50:56:01:1f:da (VMware, Inc.) 		<input type="checkbox"/>	Slaves : ethSRV0 Mode : 1 Remove Bond	2.10.1.2/255.255.252.0 Edit
ethSRV1 00:50:56:01:1f:de (VMware, Inc.) 		<input checked="" type="checkbox"/>	Not Available 	10.10.96.189/255.255.240.0
ethSRV2 00:50:56:01:1f:ea (VMware, Inc.) 		<input checked="" type="checkbox"/>	Slaves : ethSRV3 Mode : 6 Remove Bond	10.10.96.193/255.255.240.0

2. Under the *Network Interfaces* area, click **Remove Bond** corresponding to the interface on which the bonding is created. A confirmation screen appears.
 3. Select **OK**.
- The bond is removed and the interfaces are visible on the *IP/Network* list.

4.9.8.2.5 Viewing a Bond

Using the DSG CLI Manager, you can view the bonds that are created between all the interfaces.

► To view a bond:

1. On the DSG CLI Manager, navigate to **Networking > Network Settings**.
The *Network Configuration Information Settings* screen appears.
2. Navigate to **Interface Bonding** and select **Edit**.
The *Network Teaming* screen displaying all the bonded interfaces appears as shown in the following figure.

IP/Netmask	Link	DHCP	Network Teaming 	Addresses
ethMNG 00:50:56:01:1f:da (VMware, Inc.) 		<input type="checkbox"/>	Slaves : ethSRV0 Mode : 1 Remove Bond	2.10.1.2/255.255.252.0 Edit
ethSRV1 00:50:56:01:1f:de (VMware, Inc.) 		<input checked="" type="checkbox"/>	Not Available 	10.10.96.189/255.255.240.0
ethSRV2 00:50:56:01:1f:ea (VMware, Inc.) 		<input checked="" type="checkbox"/>	Slaves : ethSRV3 Mode : 6 Remove Bond	10.10.96.193/255.255.240.0

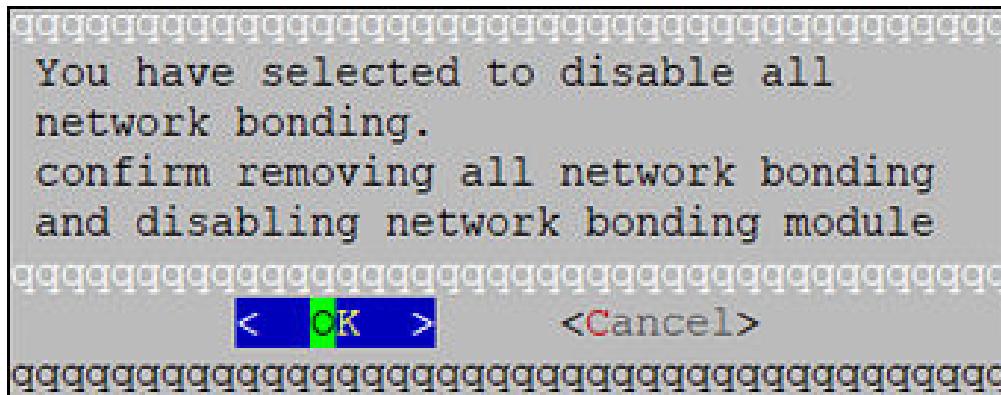
4.9.8.2.6 Resetting the Bond

You can reset all the bonds that are created for an appliance. When you reset the bonds, all the bonds created are disabled. The slave NICs are reset to their initial state, where you can configure the network settings for them separately.

► To reset all the bonds:



1. On the DSG CLI Manager, navigate to **Networking > Network Settings**.
The *Network Configuration Information Settings* screen appears.
2. Navigate to **Interface Bonding** and select **Edit**.
The *Network Teaming* screen displaying all the bonded interfaces appears.
3. Select **Reset**.
The following screen appears.



4. Select **OK**.
The bonding for all the interfaces is removed.

4.9.9 Configuring Web Settings

The Web Settings pane contains the following sections:

- General Settings
- Session Management
- Shell In A Box Settings
- SSL Cipher Settings

4.9.9.1 General Settings

The maximum size limit of a file that can be uploaded using the Web Interface is set as default to 25 MB. You can increase the limit up to 2048 MB.

► To Increase the Maximum File Upload Size using Appliance Web UI:

1. From the Appliance Web UI, proceed to **Settings > Network > Web Settings**.
The following screen appears.

The screenshot shows the 'Web Settings' page. The 'General Settings' section contains a slider for 'Max File Upload Size' set at 25 MB. The 'Session Management' section includes a checked checkbox for 'Allow user to extend timeout' and an unchecked checkbox for 'Is hard timeout'. A slider for 'Session Timeout' is set at 15 Minutes. A blue 'Update' button is visible.

Figure 4-30: Increasing Maximum File Upload Size

2. Move the *Max File Upload Size* slider to the right to increase the limit.
3. Click **Update**.

4.9.9.2 Session Management

Only the admin user can extend the time using this option. The extended time becomes applicable to all users of the Appliance.

► To Timeout using Appliance Web UI Option

1. From the Appliance Web UI, proceed to **Settings > Network**.
2. Click **Web Settings**.

The following screen appears.

The screenshot shows the 'Web Settings' page with a 'General Settings' section. It includes a 'Max File Upload Size 25 MB' slider, two checked checkboxes for 'Allow user to extend timeout' and 'Is hard timeout', a 'Session Timeout 15 Minutes' slider, and a blue 'Update' button.

Figure 4-31: Extending Session Timeout

3. Move the *Session Timeout* slider to the right to increase the time, in minutes
4. Click **Update**.

4.9.9.3 Fixing the Session Timeout

► To Fix Session Timeout:

There may be cases where the timeout session should be fixed, and the Appliance logs out even if the session is an active session.

1. From the Appliance Web UI, proceed to **Settings > Network**.
2. Click **Web Settings**.

The following screen appears.

The screenshot shows the 'Web Settings' page with a 'General Settings' section. It includes a 'Max File Upload Size 25 MB' slider, a 'Session Management' section with two checked checkboxes ('Allow user to extend timeout' and 'Is hard timeout'), a 'Session Timeout 15 Minutes' slider, and a blue 'Update' button.

Figure 4-32: Extending Session Timeout

3. Move the *Session Timeout* slider to the right or left to increase or decrease the time, in minutes.
4. Select the *Is hard timeout* check box.
5. Click **Update**.

4.9.9.4 Shell In A Box Settings

This setting allows a user with Appliance Web Manager permission to configure access to the ShellInABox feature which is available through the Web UI. This setting applies to all the users that have access to the Web UI.

When enabled the users are able to view the CLI icon on the bottom right corner of the web page.

The screenshot shows the 'Shell In A Box Settings' page with a single checkbox labeled 'Allow Shell In A Box' which is checked. Below it is a blue 'Update' button. At the bottom of the page, there is a status bar showing 'Last Refreshed (Local Time): Mon,' followed by a progress bar, and a set of navigation icons.

► To enable/disable Shell In A Box Settings:

1. From the Appliance Web UI, proceed to **Settings > Network**.
2. Click **Web Settings**.

The following screen appears.



Figure 4-33: Shell In A Box settings

3. To enable or disable the **Shell In a Box Settings**, select the **Allow Shell In a Box** check box.
4. Click **Update**.

4.9.9.5 SSL Cipher Settings

The appliance uses OpenSSL library to encrypt and secure connections. You can configure an encrypted connection using the following two strings:

- SSL Protocols
- SSL Cipher Suites

The protocols and the list of ciphers supported by the appliance are included in the **SSLProtocol** and **SSLCipherSuite** strings respectively. The **SSLProtocol** supports TLS v1.2 and TLS v1.3 protocols.

To disable any protocol from the **SSLProtocol** string, prepend a hyphen (-) to the protocol. To disable any cipher suite from the **SSLCipherSuite** string, prepend an exclamation (!) to the cipher suite.

For more information about the OpenSSL library, refer to <http://www.openssl.org/docs>.

4.9.9.6 Updating a Protocol from the ESA Web UI

► To update a protocol from the ESA Web UI:

1. In the ESA Web UI, navigate to **Settings > Network > Web Settings**.
The *Web Settings* page appears.
2. Under *SSL Cipher Settings* tab, the **SSLProtocol** text box contains the value *ALL-SSLv2-SSLv3*.
3. Add – to the required protocol.
For example, to disable TLS1.1, type -TLSv1.1 in the **SSLProtocol** text box.

The screenshot shows the 'SSL Cipher Settings' configuration page. It includes fields for 'SSLProtocol' (set to 'ALL -SSLv2 -SSLv3 -TLSv1 -TLSv1.1') and 'SSLCipherSuite' (set to 'TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_'). There is also a checked checkbox for 'SSLHonorCipherOrder'. A blue 'Update' button is located at the bottom.

Figure 4-34: SSL Cipher Settings

- Click **Update** to save the changes.

Note: To re-enable TLSv1.1 using the Web UI, remove –TLSv1.1 from the **SSLProtocol** text box.

- Click **Test Cipher with openssl** to view the appropriate cipher list.

4.9.10 Working with Secure Shell (SSH) Keys

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.

If you add a Private key without a passphrase, it is encrypted with a random passphrase. This passphrase is scrambled and stored.

If you choose a Private key with a passphrase, then the Private key is stored as it is. This passphrase is scrambled and stored.

For more information about generating the SSH key pairs, refer to [Adding a New Key](#).

The SSH protocol allows an authorized user to connect to the host machines from the remote machines. Both inbound communication and outbound communication are supported using the SSH protocol. An authorized user is a combination of an appliance user associated with a valid key pair. An authorized user must be listed as a valid recipient to connect using the SSH protocol.

The SSH protocol allows the authorized users to run tasks securely on the remote machine. When the users connect to the appliance using the SSH protocol, then the communication is known as inbound communication.

For more information about inbound SSH configuration, refer to [Configuring Inbound Communications](#).

When the users connect to a known host using their private keys, then the communication is known as outbound communication. The authorized users are allowed to initiate the SSH communication from the host.

For more information about outbound SSH configuration, refer to [Configuring Outbound Communications](#).

On the ESA Web UI, you can configure all the following standard aspects of SSH:

- Authorized Keys
- Identities

- Known Hosts

SSH Pane

With the SSH configuration Manager you can examine and manage the SSH configuration. The SSH keys can be configured in the **Authentication Configuration** pane on the ESA Web UI.

The following figure shows the **SSH Configuration Manager** pane.

The screenshot shows the 'Authentication Configuration' section of the SSH Configuration Manager. It includes fields for 'Authentication Type' (set to 'Password + Publickey') and 'SSH Mode' (set to 'Standard'). A large 'Apply' button is present. Below these are tabs for 'Authorized Keys (Inbound)', 'Identities Keys (Outbound)', and 'Known Hosts'. The 'Known Hosts' tab is selected. It contains a table with columns: User Name, Key Type, Key, and Comments. Buttons for 'Add New Key', 'Reset List', 'Download Public Key', and 'Delete Authorized Key' are located at the bottom. A note below the table says: 'Using "Authorized Keys" you can examine and manage the users that are authorized to access this host.'

Figure 4-35: SSH Configuration Manager

Authentication Type

The SSH Server is configured in the following three ways:

- Password
- Public Key
- Password + Key

Table 4-11: SSH Authentication Type

Authentication Type	Description
Password	In this authentication type, only the password is required for authentication to the SSH server. The public key is not required on the server for authentication.
Public Key	In this authentication type, the server requires only the public key for authentication. The password is not required for authentication.
Password + Public key	In this authentication type, the server can accept both, the keys and the password, for authentication.

SSH Mode

Using the SSH mode, restrictions for SSH connections can be set. The restrictions can be hardened or loosened based on the needs. There are four modes SSH mode types are shown below.

Table 4-12: SSH Mode

Mode	SSH Server	SSH Client
Paranoid	Disable root access	Disable password authentication (allow to connect only using public keys). Block connections to unknown hosts.
Standard	Disable root access	Allow password authentication. Allow connections to new (unknown) hosts, enforce SSH fingerprint of known hosts.
Open	Allow root access Accept connections using passwords and public keys.	Allow password authentication.

Mode	SSH Server	SSH Client
		Allow connection to all hosts – do not check hosts fingerprints.

4.9.10.1 Configuring the SSH Key

► To configure the SSH Key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the **SSH** tab.
The *SSH Configuration Manager* pane appears.
3. Select the authentication type from the **Authentication Type** drop down menu.

The screenshot shows the 'Authentication Configuration' screen. It has two dropdown menus: 'Authentication Type' (set to 'Password + Publickey') and 'SSH Mode' (set to 'Standard'). Below the dropdowns is a blue 'Apply' button.

Figure 4-36: Authentication Configuration

4. Select the SSH mode from the **SSH Mode** drop down menu.
 5. Click **Apply**.
- A message *Configuration saved successfully* appears.

4.9.10.1.1 Configuring Inbound Communications

The users who are allowed to connect to the appliance using the SSH are listed in the **Authorized Keys (Inbound)** tab.

The following screen shows the Authorized Keys.

User Name	Key Type	Key
es_cluster	ssh-rsa	47:c6:c8:a7:aa:46:13:d3:7a:9a:f7:83:7f:43:f3:ba

Figure 4-37: Authorized Keys (Inbound)

4.9.10.1.1.1 Adding a New Key

An authorized key has to be created for a user or a machine to connect to an appliance on the host machine.

► To add a new key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Authorized Keys (Inbound)* tab.
4. Click **Add New Key**.
The *Add New Authorized Key* dialog box appears.
5. Select a user.
6. Select **Generate new public key**.
7. **Root password is required to create Authorized Key** prompt appears. Enter the root password and click **Ok**.
8. If the private key is to be saved, then select **Click To Download Private Key**.
The private key is saved to the local machine.
9. If the public key is to be saved, then select **Click To Download Public Key**.
The public key is saved to the local machine.
10. Click **Finish**.
The new authorized key is added.

4.9.10.1.1.2 Uploading a Key

You can assign a public key to a user by uploading the key from the Web UI.

► To upload a key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.

3. Select the *Authorized Keys (Inbound)* tab.
4. Click **Add New Key**.
The *Add New Authorized Key* dialog box appears.
5. Select a user.
6. Select **Upload public key**.
The file browser dialog box appears.
7. Select a public key file.
8. Click **Open**.
9. **Root password is required to create Authorized Key** prompt appears. Enter the root password and click **Ok**.
The key is assigned to the user.

4.9.10.1.1.3 Downloading a Public Key

From the Web UI, you can download the public of a user to the local machine.

► To download a key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Authorized Keys (Inbound)* tab.
4. Select a user.
5. Select **Download Public Key**.
The public key is saved to the local directory.

4.9.10.1.1.4 Choosing from Existing Keys

The public key of one user can assigned as a public key of another user.

► To upload an existing key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Authorized Keys (Inbound)* tab.
4. Click **Add New Key**.
The *Add New Authorized Key* dialog box appears.
5. Select a user.
6. Select **Choose from existing keys**.
7. Select the public key.
8. **Root password is required to create Authorized Key** prompt appears. Enter the root password and click **Ok**.
The public key is assigned to the user.

4.9.10.1.1.5 Deleting an Authorized Key

You can remove a key from the authorized users list. Once the key is removed from the list, the remote machine shall no longer be able to connect to the host machine.

► To delete an authorized key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Authorized Keys (Inbound)* tab.
4. Select a user.
5. Select **Delete Authorized Key**.
A message confirming the deletion appears.
6. Click **Yes**.
7. **Root password is required to delete Authorized Key** prompt appears. Enter the root password and click **Ok**.
The key is deleted from the authorized keys list.

4.9.10.1.1.6 Clearing all Authorized Key

You can remove all the public keys from the authorized keys list.

► To clear all keys:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Authorized Keys (Inbound)* tab.
4. Click **Reset List**.
A message confirming the deletion of all authorized keys appears.
5. Click **Yes**.
6. **Root password is required to delete all Authorized Keys** prompt appears. Enter the root password and click **Ok**.
All the keys are deleted.

4.9.10.1.2 Configuring Outbound Communications

The users who can connect to the known hosts with their private keys are listed in the **Identities (Outbound)** tab.

The following screen shows the Identities.

User Name	Key Type	Key
es_cluster	ssh-rsa	47:c6:c8:a7:aa:46:13:d3:7a:9a:f7:83:7f:43:f3:ba
root	ssh-dss	76:72:62:8d:5f:56:f0:12:f6:40:5c:23:20:3e:79:df

Figure 4-38: Identities (Outbound)

4.9.10.1.2.1 Adding a New Key

A new public key can be generated for the host machine to connect with another machine.

► To add a new key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Identities Keys (Outbound)* tab.
4. Click **Add New Key**.
The *Add New Identity Key* dialog box appears.
5. Select a user.
6. Select **Generate new keys**.
7. **Root password is required to create Identity Key** prompt appears. Enter the root password and click **Ok**.
8. If the public key is to be saved, then select **Click to Download Public Key**.
The public key is saved to the local machine.
9. Click **Finish**.
The new authorized key is added.

4.9.10.1.2.2 Downloading a Public Key

You can download the host's public key from the Web UI.

► To download a key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.

2. Select the **SSH** tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Identities Keys (Outbound)* tab.
4. Select a user.
5. Select **Download Public Key**.
The public key is saved to the local machine.

4.9.10.1.2.3 Choosing from Existing Keys

The public and private key pair of one user can assigned as a public and private key pair of another user.

► To choose from an existing key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the **SSH** tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Identities Keys (Outbound)* tab.
4. Click **Add New Key**.
The *Add New Identity Key* dialog box appears.
5. Select a user.
6. Select **Choose from existing keys**.
7. Select the public key.
8. **Root password is required to create Identity Key** prompt appears. Enter the root password and click **Ok**.
The public key is assigned to the user.

4.9.10.1.2.4 Uploading Keys

► To upload an existing key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the **SSH** tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Identities Keys (Outbound)* tab.
4. Click **Add New Key**.
The *Add New Identity Key* dialog box appears.
5. Select a user.
6. Select **Upload Keys**.
The list of public keys with the users that they are assigned to appears.
7. Select **Upload Public Key**.
The file browser dialog box appears.
8. Select a public key file from your local machine.
9. Click **Open**.
The public key is assigned to the user.
10. Select **Upload Private Key**.

The file browser dialog box appears.

11. Select a private key file from your local machine.
12. Click **Open**.
13. If the private key is protected by a passphrase, then the text field *Private Key Passphrase* appears.
Enter the private key passphrase.

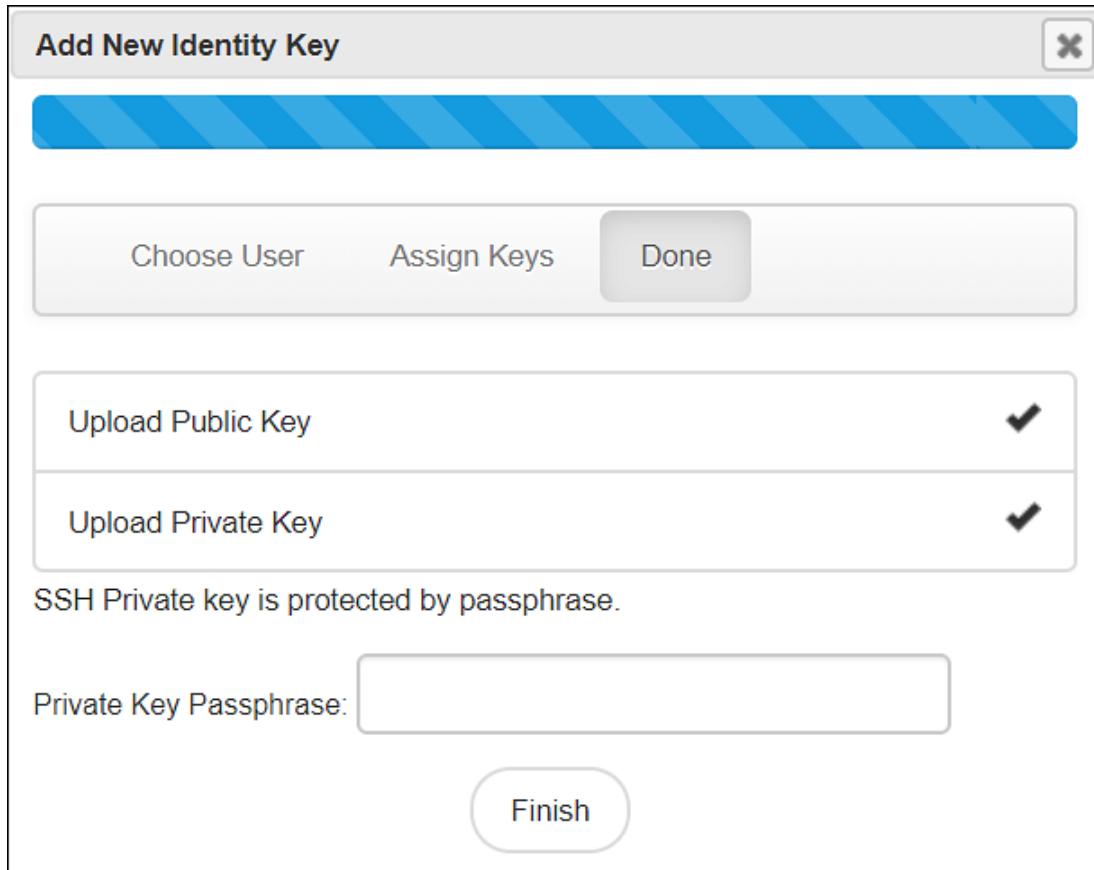


Figure 4-39: SSH Passphrase

14. Click **Finish**.
The new identity key is added.

4.9.10.1.2.5 Deleting an Identity

You can delete an identity for a user. Once the identity is removed, the user shall no longer be able to connect to another machine.

► To delete an identity:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Identities Keys (Outbound)* tab.
4. Select a user.
5. Click **Delete Identity**.
A message confirming the deletion appears.

6. Click **Yes**.
7. **Root password is required to delete the Identity Key** prompt appears. Enter the root password and click **Ok**.
The identity is deleted.

4.9.10.1.2.6 Clearing all Identities

You can remove all the public keys from the authorized keys list.

► To clear all identities:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Identities Keys (Outbound)* tab.
4. Click **Reset Identity List**.
A message confirming the deletion of all identities appears.
5. Click **Yes**.
6. **Root password is required to delete all Identity Keys** prompt appears. Enter the root password and click **Ok**.
All the identities are deleted.

4.9.10.1.3 Configuring Known Hosts

By default, the SSH is configured to deny all the communications to unknown remote servers. Known hosts list the machines or nodes to which the host machine can connect to. The SSH servers to which the host can communicate with are added under Known Hosts.

Note:

In an HA setup, you must add, upload, or copy new *Known Hosts* on the primary and secondary nodes.

4.9.10.1.3.1 Adding a New Host

You add a host to the list of known hosts with which a connection is to be established.

► To add a host:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Known Hosts* tab.
4. Click Add Host.
The **Enter the ip/hostname** dialog box appears.
5. Enter the IP address or hostname in the **Enter the ip/hostname** text box.
6. Click **Ok**.

All host is added to the known hosts list.

4.9.10.1.3.2 Updating the Host Keys

You can refresh the hostnames to check for updates to host's public keys.

► To updated a host key:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Known Hosts* tab.
4. Select a host name.
5. Click **Refresh Host Key**.
The key for the host name is updated.

4.9.10.1.3.3 Deleting a Host

If a connection to a host is no longer required, then you can delete the host from the known host list.

► To delete a known host:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Known Hosts* tab.
4. Select a host name.
5. Click **Delete Host**.
A message confirming the deletion appears.
6. Click **Yes**.
The host is deleted.

4.9.10.1.3.4 Resetting the Host Keys

You can set the keys of all the hosts to a default value.

► To reset all the host keys:

1. From the ESA Web UI, navigate to **Settings > Network**.
The *Network Settings* pane appears.
2. Select the *SSH* tab.
The *SSH Configuration Manager* pane appears.
3. Select the *Known Hosts* tab.
4. Select **Reset Host Keys**.

- A message confirming the reset appears.
5. Click **Yes**.
The host keys for all the hostnames is set to a default value.

4.10 Managing Appliance Users

Only authorized users can access the Appliances. These users are system users and LDAP administrative users. The roles of these users are explained in detail in the following sections.

Appliance Users

The root and local_admin users are appliance system users. These users are initialized during installation.

root and local_admin

As a root user, you can be asked to provide the root account password to log in to some CLI Manager tools, for example, Change Accounts and Passwords tool or Configure SSH tool.

The root account is used to exit the appliance command line interface and go directly into the host operating system command line, thus giving the system administrator full control over the machine.

The local_admin is necessary for LDAP maintenance when the LDAP is not working or is not accessible.

LDAP Users

The admin and viewer user accounts are LDAP users that are initialized during installation.

For more information about users, refer to section [Managing Users](#).

admin and viewer Accounts

The admin and viewer accounts are used to log onto CLI Manager or Appliance Web UI. These user accounts can be modified by using CLI Manager (for instructions, refer to section [Accounts and Passwords](#)), Web UI (where these accounts are the part of the LDAP) or Policy management.

When these passwords are changed in the CLI Manager or Appliance Web UI, the change applies to all other installed components, thus synchronizing the passwords automatically.

LDAP Target Users

When you have your appliance installed and configured, you can create LDAP users and assign necessary permissions to these users. You can also create groups of users. The system users are by default predefined in the internal LDAP directory.

For more information about creating users in LDAP and define their security permissions, refer to section [Managing Users](#).

System Roles

Protegility Data Security Platform role-based access defines a list of roles, including a list of operations that a role can perform. Each user is assigned to one or more roles. User-based access defines a user to whom the operations are granted. There are several predefined roles on ESA.

The following table describes these roles.

Role	Is used by...
root user	The OS system administrator who maintains the Appliance machine, which could be ESA or DSG.
admin user	The user who specifically manages the creation of roles and members in the LDAP directory. This user could also be the as DBA, System Administrator, Programmer, and others responsible for installing, integrating, or monitoring Protegility platform components into their corporate

Role	Is used by...
	infrastructure for the purpose of implementing the Protegility-based data protection solution.
viewer user	Personnel who can only view and not create or make changes.

4.11 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:

- Protegility123 (alphabetic and numeric)
- Protegility!@#\$ (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](#).

4.11.1 Managing Users

After you configure the LDAP server, you can either add users to internal LDAP or import users from the external LDAP. The users are then assigned to roles based on the permissions you want to grant them.

The default users packaged with ESA that are common across appliances are provided in the following table. You can edit each of these roles to provide additional privileges.



User Name	Description	Role
admin	Administrator account with full 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
ldap_bind_user	User who accesses the local LDAP in ESA or other appliances.	n/a
PolicyUser	Users who can perform security operations on the DSG Test Utility.	Policy User
ProxyUser	Users who can perform security operations on behalf of other policy users on the Protection Server. Note: The Protection Server is deprecated. This user is should not to be used.	ProxyUser

The following table describes the three types of proxy users in ESA:

Callout	Description
Local	Users that are authenticated using the local LDAP or created during installation.
Manual	Users that are manually created or imported manually from an external directory service.
Automatic	Users that are imported automatically from an external directory service and a part of different External Groups. For more information about External Groups, refer to section Working with External Groups .

User Management Web UI

The user management screen allows you to add, import, and modify permissions for the users. The following screen displays the ESA User Management Web UI.

The screenshot shows the User Management screen with the following numbered callouts:

- (1) Filter icon and search bar.
- (2) Password Policy column header.
- (3) User Password Status column header.
- (4) Lock Status column header.
- (5) Expiration Date column header.
- (6) User Type column header.
- (7) Last Unsuccessful Login (UTC) column header.
- (8) Roles column header.
- (9) Add User button.
- (10) Import Users button.
- (11) Action column header.
- (12) Page navigation buttons.
- (13) Show entries dropdown.
- (14) Local and Automatic user counts.

User Name	Password Policy	User Password Status	Lock Status	Expiration Date	User Type	Last Unsuccessful Login (UTC)	Roles	Action
admin	Off	Valid	Unlocked	Never expires	Local	Security Administrator		
viewer	On	Valid	Unlocked	Never expires	Local	May 04 2020 09:03:20	Security Administrator Viewer	
ldap_bind_user	Off	Valid	Unlocked	Never expires	Local			
samba_admin_user	Off	Valid	Unlocked	Never expires	Local			
PolicyUser	Off	Valid	Unlocked	Never expires	Local	Policy User		
ProxyUser	Off	Valid	Unlocked	Never expires	Local	Policy Proxy User		
egsyncd_service_admin	Off	Valid	Unlocked	Never expires	Local			
arad2	Off	Valid	Unlocked	Never expires	Automatic	Security Administrator Viewer Security Administrator, Directory Administrator		
azUayYqefXndTPvop	Off	Valid	Unlocked	Never expires	Automatic	Security Administrator Viewer Security Administrator, Directory Administrator		
app2	Off	Valid	Unlocked	Never expires	Automatic	Security Administrator Viewer Security Administrator, Directory Administrator		

Figure 4-40: User Management Screen

Callout	Column	Description
1	User Name	Name of the user. This user can either be added to the internal LDAP server or imported from an external LDAP server.
2	Password Policy	Enable password policy for selected user. This option is available only for local users. For more information about defining password policy for users, refer to Password Policy Configuration .
3	User Password Status	Indicates status of the user. The available states are as follows. Valid – user is active and ready to use ESA. Warning – user must change password to gain access to ESA. When the user tries to login after this status is flagged, it will be mandatory for the user to change the password to access the appliance. Note: As the administrator sets the initial password, it is recommended to change your password at the first login for security reasons.
4	Lock Status	User status based on the defined password policy. The available states are as follows: Locked – Users who are locked after series of incorrect attempts to log in to ESA. Unlocked – Users who can access ESA. <value> - Number of attempts remaining for a user after entering incorrect password.
5	Expiration Date	Indicates expiry status for a user. The available statuses are as follows: Time left for expiry – Displays
6	User Type	Indicates if user is a local, manual or automatically imported user.
7	Last Unsuccessful Login (UTC)	Indicates the time of the last unsuccessful login attempted by the user. The time displayed is in UTC. Note: If a user successfully logs in through the Web UI or the CLI manager, then the time stamp for any previous unsuccessful attempts is reset.
8	Roles	Linked roles to that user.
9	Add User	Add a new internal LDAP user.
10	Import User	Import users from the external LDAP server. Note: Note: This option is available only when Proxy Authentication is enabled.
11	Action	The following Actions are available.  - Click to reset password for a user. Note: When you reset password for a user, Enter your password prompt appears. Enter the password and click Ok .

Callout	Column	Description
		<p>If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.</p>
		 - Click to remove a user. Note: When you remove a user, Enter your password prompt appears. Enter the password and click Ok . If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.
		 - Click to convert the external LDAP user to a local LDAP user. Note: When you convert a user to a local LDAP user, ESA creates the user in its local LDAP server.
12	Page Navigation	Navigate through pages to view more users.
13	View Entries	Select number of users to be displayed in a single view. You can select to view up to 50 users.
14	Search User Name	Enter the name of the user you want to filter from the list of users.

4.11.1.1 Adding Users to Internal LDAP

You can create users with custom permissions and roles, and add them to the internal LDAP server. Consider an example user, John Doe, is added to the internal LDAP.

► To add users to internal LDAP:

1. In the Web UI, navigate to **Settings > Users > User Management**.
2. Click **Add User** to add new users.

Note: Click **Cancel** to exit the adding user screen.

Note:

The **&** character is not supported in the **Username** field.

3. Enter John as **First Name**, Doe as **Last Name**, and provide a **Description**. The **User Name** text box is auto-populated. You can edit it, if required.

Note: The maximum number of characters that you can enter in the **First Name**, **Last Name**, and **User Name** fields is 100. The maximum number of characters that you can enter in the **Description** field is 200.

4. Click **Continue** to configure password.
5. Enter the password and confirm it in the consecutive text box.
6. Verify that the **Enable Password Policy** toggle button is enabled to apply password policy for the user.
The **Enable Password Policy** toggle button is enabled as default. For more information about password policy, refer to [Password Policy Configuration](#).
7. Click **Continue** to assign role to the user.
8. Select the role you want to assign to the user. You can assign the user to multiple roles.
9. Click **Add User**.
10. **Enter your password** prompt appears. Enter the password and click **Ok**.

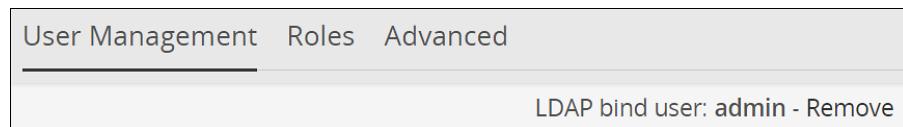
Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

Note: If you are trying to add users and are not authorized to add users, then you can temporarily add users by providing credentials of a user with LDAP Manager permissions. This session remains active and lets you add users for a timeout period of 5 mins. During the active session, if you need to revoke this user and return to your session, you can click **Remove**.

After 5 mins, the session ends, and you can no longer add users. The following figure shows this feature in the Web UI.



4.11.1.2 Importing Users to Internal LDAP

In the User Management screen, you can import users from an external LDAP to the internal LDAP. This option gives you the flexibility to add selected users from your LDAP to the ESA.

Note:

Ensure that Proxy Authentication is enabled before importing users from an external directory service.

For more information about Proxy Authentication, refer to [Working with Proxy Authentication](#).

Note:

The username in local LDAP is case-sensitive and the username in Active Directory is case-insensitive. It is recommended not to import users from external LDAP where the username in the local LDAP and the username in the external LDAP are same.

► To import users to internal LDAP:

1. In the Web UI, navigate to **Settings > Users > User Management**.

2. Click **Import Users** to add external LDAP user to the internal LDAP.
The **Import Users** screen appears.
3. Select **Search by Username** to search the users by username or select **Search by custom filter** to search the users using the LDAP filter.
4. Type the required number of results to display in the **Display Number of Results** text box.
5. If you want to overwrite existing user, click **Overwrite Existing Users**.
6. Click **Next**.
The users matching the search criteria appear on the screen.
7. Select the required users and click **Next**.
The screen to select the roles appears.
8. Select the required roles for the selected users and click **Next**.
9. **Enter your password** prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

The screen displaying the roles imported appears.

The users, along with the roles, are imported to the internal LDAP.

Note:

The users imported are not local users of the internal LDAP. You cannot apply password policy to these users. To convert the imported user to a local user, navigate to **Settings > Users > User Management**, select the user, and then click Convert to Local user (). When you convert a user to a local LDAP user, ESA creates the user in its local LDAP server.

4.11.1.3 Password Policy Configuration

The user with administrative privileges can define password policy rules. PolicyUser and ProxyUser have the *Password Policy* option as disabled, by default.

4.11.1.3.1 Defining a Password Policy

► To define a password policy:

1. On the ESA Web UI, navigate to **Settings > Users**.
2. On the **User Management** tab under the **Define Password Policy** area, click **Edit** ().

Define Password Policy

Edit The default password policy here

Min Period for Changeover Minimum days password must be in effect before the user can change it. ⓘ

Password Expiry Maximum days before password must be changed. ⓘ

Lock on Max Failures Maximum number of failures before user password is locked. ⓘ

Password History Number of unique new passwords before an old password can be reused. ⓘ

Reset Apply changes

- Select the password policy options for users which is described in the following table:

Table 4-13: Password Policy Configuration

Password Policy Option	Description	Default Value	Possible Values
Minimum period for changeover	Number of days since the last password change	1	0-29
Password expiry	Number of days a password remains valid	30	0-720
Lock on maximum failures	Number of attempts a user makes before the account is locked and requires Admin help for unlocking	5	0-10
Password history	Number of older passwords that are retained and checked against when a password is updated	1	0-64

- Click on **Apply Changes**.

- Enter your password prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

4.11.1.3.2 Resetting the password policy to default settings

- To reset the password policy to default settings:

- Click **Reset**.

A confirmation message appears.

- Click **Yes**.

- Enter your password prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

The password policy is set to default values as mentioned in the Password Policy Configuration table.

The users imported into LDAP have Password Policy disabled, by default. This option cannot be enabled for imported users.

4.11.1.3.3 Enabling password policy for Local LDAP users

► To enable password policy for Local LDAP users:

1. On the ESA Web UI, navigate to **Settings > Users**.
2. In the Manage Users area, click **Password Policy** toggle for the user.
A dialog box appears requesting LDAP credentials.
3. **Enter your password** prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

After successful validation, password policy is enabled for the user.

In case of a locked user (users who had maximum failures during login with this error message Login Failure: Account locked), the user with administrative privileges unlocks the locked user by resetting the password. For more information on password reset, refer to section [Password Policy for the LDAP Users](#). In case the Admin user is locked, then the local_admin user can be used to unlock the Admin user from the CLI. Note that local_admin is not a part of the LDAP so cannot be locked.

4.11.1.4 Editing Users

To make changes to a user, navigate to **Settings > Users > User Management**. Click on a User Name.

You can make the following changes to the user:

- Under the **General Info** section, edit the **Description**.
- Under the **Password Policy** section, toggle to enable or disable the Password Policy.
- Under the **Roles** section, select role(s) from the list for the user.
- Click **Reset Password** to reset password for the user.
- Click the  icon to delete the user.

Note:

For every change done for the user, **Enter your password** prompt appears. Enter the password and click **Ok**.

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

4.11.2 Managing Roles

Users in the appliance must be attached to a role. Roles are templates that include permissions and users can be assigned to one or more roles.

The default roles packaged with ESA are as follows:

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 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. The permissions that are available to map with a user and packaged with ESA as default permissions are as follows:

The following scenarios occur when synchronization is performed between the external groups and the directory services.

Permissions	Description
Appliance CLI Administrator	Allows users to perform all operations available as part of ESA CLI Manager.
Appliance web manager	Allows user to perform all operations available as part of the ESA Web UI.
Customer Business manager	Allows users to retrieve metering reports.
DPS Admin	Allows user to use the DPS admin tool on the protector node.
Export Certificates	Allows user to use download certificates from ESA.
Key Manager	Allows user to access the Key Management Web UI, rotate ERK or DSK, and modify ERK states.
Policy-User	Allows user to connect to Data Security Gateway (DSG) via REST and perform security operations using Application Protector (AP).
RLP Manager	Allows user to manage (access, view, create, etc.) rules stored on Row-Level Security Administrator (ROLESA).
Reports Viewer	Allows user to only view reports.



Permissions	Description
Security Viewer	Allows user to have read only access to policy management in the Appliance.
Appliance CLI Viewer	Allows user to login to the Appliance CLI as a viewer and view the appliance setup and configuration.
Appliance web viewer	Allows user to login to the Appliance web-interface as a viewer.
AWS Admin	Allows user to configure and access AWS tools if the AWS Cloud Utility product is installed.
Directory Manager	Allows user to manage the Appliance LDAP Directory Service.
Export Keys	Allows user to export keys from ESA.
Reports Manager	Allows user to manage (access, view, create, schedule, etc.) reports and do functions related to reports.
Security Officer	Allows user to manage (access, view, create, deploy, etc.) policy and keys and do functions related to policy and key management.
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.
Export IMP	Allows user to export policy from the ESA by using the IMP APIs.

The ESA Roles web UI is as seen in the following image.

Role Name	Description	Permissions	Action
Policy User	Grant Application-Protector access	Policy-User	
Shell Accounts	Accounts that have shell access	Shell (non-CLI) Access	
Directory Administrator	Local LDAP Administrator Role	Directory Manager	
Policy Proxy User	Grant Application-Protector B2B Proxy-login	Proxy-User	
Security Administrator Viewer	Security Administrator Viewer Role	Security Viewer,Appliance web viewer,Appliance CLI Viewer	
Security Administrator	Security Administrator Role	ES Admin,AWS Admin,Key Manager,Directory Manager,RLP Manager,Security Officer,Can Create JWT Token,Appliance web manager,Export Certificates,Insight Admin,DPS Admin,Export Keys,Appliance CLI Administrator	

Callout	Column	Description
1	Role Name	<p>Name of the role available on ESA.</p> <p>Note: If you want to edit an existing role, click the role name from the displayed list. After making required edits, click Save to save the changes.</p>

Callout	Column	Description
2	Description	Brief description about the role and its capabilities.
3	Permissions	Permission mapped to the role. The tasks that a user mapped to a role can perform is based on the permissions enabled.
4	Action	<p>The following Actions are available.</p> <ul style="list-style-type: none"> • - Click to duplicate the role with mapped permissions. • - Click to delete a role. <div style="background-color: #e0f2e0; padding: 5px; margin-top: 10px;"> Note: When you duplicate or delete a role, Enter your password prompt appears. Enter the password and click Ok. </div> <div style="background-color: #e0f2e0; padding: 5px; margin-top: 10px;"> If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked. </div>
5	Add Role	Add a custom role to ESA.

Note:

It is recommended to delete a role from the Web UI only. This ensures that the updates are reflected correctly across all the users that were associated with the role.

4.11.2.1 Adding a Role

You can create a custom business role with permissions and privileges that you want to map with that role. Custom templates provide the flexibility to create additional roles with ease.

Consider an example business role, Security Viewer, is to be created.

► To add a role:

1. In the Web UI, navigate to **Settings > Users > Roles**.

Note:

If you want to edit an existing role, click the role name from the displayed list. After making required edits, click **Save** to save the changes.

2. Click **Add Role** to add a business role.
3. Enter Security Viewer as the **Name**.
4. Enter a brief description in the **Description** text box.
5. Select **custom** as the template from the **Templates** drop-down.
6. Under **Role Permissions and Privileges** area, select the permissions you want to grant to the role.

Click **Uncheck All** to clear all the check boxes. Ensure that you do not select the **Shell (non-CLI) Access** permission for users who require Web UI and CLI access.

7. Click **Save** to save the role.
8. **Enter your password** prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

4.11.3 Configuring the Proxy Authentication Settings

You can configure proxy authentication from the Web UI.

For more information about configuring LDAP from the CLI manager, refer to Section [Working with Proxy Authentication](#).

► To configure external LDAP:

1. In the Web UI, navigate to **Settings > Users > Proxy Authentication**. The following figure shows example LDAP configuration.

Proxy Authentication Settings - (Disabled)	
LDAP Server(s):	ldap://10.10.199.82:389 + i
Base DN:	dc=sherwood,dc=com i
Bind DN:	Administrator@sherwood.com i
Bind Password: i
StartTLS Method:	<input type="checkbox"/> i
Verify Peer:	<input checked="" type="checkbox"/> i
LDAP Filter:	sAMAccountName i

Figure 4-41: External LDAP configuration

2. Enter the LDAP IP address for the external LDAP in **LDAP URI**.

The accepted format is *ldap://host:port*.

Note:

Click the + icon to add multiple LDAP servers. Click the - icon to remove the LDAP server from the list.

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

Fields	Description
Base DN	The LDAP Server Base distinguished name. For example: Base DN: dc=sherwood, dc=com.
Bind DN	Distinguished name of the LDAP Bind User. Note: It is recommended that this user is granted viewer permissions. For example: Bind DN: administrator@sherwood.com
Bind Password	The password of the specified LDAP Bind User.
StartTLS Method	Set this value based on configuration at the customer LDAP.
Verify Peer	Enable this setting to validate the certificate from an AD. If this setting is enabled, ensure that the following points are considered: <ul style="list-style-type: none"> • You must require a CA certificate to verify the server certificate from AD. For more information about certificates, refer to Protegility Certificate Management Guide 9.1.0.5. • The LDAP Uri matches the hostname in the server and CA certificates. • LDAP AD URI hostname is resolved in the hosts file.
LDAP Filter	Provide the attribute to be used for filtering users in the external LDAP. For example, you can use the default attribute, <i>sAMAccountName</i> , to authenticate users in a single AD. Note: In case of same usernames across multiple ADs, it is recommended to use LDAP filter such as <i>UserPrincipalName</i> to authenticate users.

4. Click **Test** to test the provided configuration.
A *LDAP test connectivity passed successfully* message appears.
5. Click **Apply** to apply and save the configuration settings.
6. **Enter your password** prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

- A *Proxy Authentication was ENABLED and configuration were saved successfully* message appears.
7. Navigate to **System > Services** and verify that the *Proxy Authentication Service* is running.

Services	Status	Mode	Actions
LDAP			
LDAP Server	Running	Automatic	 
Proxy Authentication Service	Running	Automatic	 
External Groups Sync Service	Running	Automatic	 
Name Service Cache Daemon	Running	Automatic	 

Figure 4-42: Proxy Authentication Service

If you make any changes to the existing configuration, click **Save** to save and apply the changes. Click **Disable** to disable the proxy authentication.

After enabling Proxy Authentication, you can proceed to adding users and mapping roles to the users. For more information about importing users, refer to [Managing Users](#).

Note:

After the Proxy Authentication is enabled, the user **egsyncd_service_admin** is enabled. It is recommended not to change the password for this user.

4.11.4 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.

Add, Edit or Delete External Group (i)							
						Add External Group	Refresh
Search	Title	Description	Roles	Group	Last Sync	Action	
<input type="checkbox"/>	TEST	TEST	Security Administrat...	test		  	

Figure 4-43: 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 4-14: 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.

4.11.4.1 Adding an External Group

You can add an external group to assign roles for a group of users. For example, consider a scenario to add an external group with data entered in the **Search Filter** textbox.

► To add an External Group:

1. In the ESA Web UI, navigate to **Settings > Users > External Groups**.
2. Click **Create**.
3. Enter the required information in the **Title** and **Description** fields.

External Group

Title * Title

Description Description

Group Query By User

Group Properties

Group DN * CN=group_name,OU=ou_name,DC=example,DC=com

Member Attribute Name * memberOf

Search Filter

Preview Users

Roles

Select Roles for Users Belonging to this group

Figure 4-44: Creating an External Group

4. If you select **Group Properties**, then enter the **Group DN** and **Member Attribute Name**.

For example,

Enter the following DN in the **Group DN** text box:

`cn=Joe,ou=groups,dc=sherwood,dc=com`

Enter the following attribute in the **Member Attribute Name** text box:

`memberOf`

Note:

This text box is not applicable for ODSEE.

5. If you select **Search Filter**, enter the search criteria in the **Search Filter** text box.

For example,

For AD, you can enter the search filter as follows:

`(&(memberOf=cn=John,dc=Bob,dc=com))`

For ODSEE, you can enter the search filter as follows:

`isMemberOf=cn=Alex,ou=groups,dc=sherwood,dc=com`

6. Click **Preview Users** to view the list of users for the selected search criteria.

7. Select the required roles from the **Roles** tab.

8. Click **Save**.

An external group is added.

The **Users** tab is visible, displaying the list of users added as a part of the external group.

Note:

If you are importing users from ODSEE, then the usernames containing special characters such as ;(semi colon), /(forward slash), {}(curly brackets), ()(parenthesis), <>(angled brackets), or +(plus) are not supported.

4.11.4.2 Editing an External Group

You can edit an external group to modify fields such as **Description**, **Mode**, **Roles**, or **Group Properties**. If any updates are made to the roles of the users in the external groups, the modifications are applicable immediately to the users existing in the local LDAP.

Note:

Ensure that you synchronize with the source directory service if you update the **Group DN** or the search filter.

► To edit an External Group:

1. In the ESA Web UI, navigate to **Settings > Users > External Groups**.
2. Select the required external group.
3. Edit the required fields.
4. Click **Save**.
5. **Enter your password** prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

The changes to the external group are updated.

4.11.4.3 Deleting an External Group

When you delete an external group, the following scenarios are considered while removing a user from an external group:

- If the users are not part of other external groups, the users are removed from the local LDAP.
- If the users are a part of multiple external groups, only the association with the deleted external group and roles is removed.

► To remove an External Group:

1. In the ESA Web UI, navigate to **Settings > Users > External Groups**.
2. Select the required external group and click the Delete () icon.
3. **Enter your password** prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

The external group is deleted.

4.11.4.4 Synchronizing the External Group

When the proxy authentication is enabled, the **External Groups Sync Service** is started. This service is responsible for the automatic synchronization of the external groups with the directory services. The time interval for automatic synchronization is 24 hours.

Note:

In an HA setup, ensure that you start the **External Groups Sync Service** after you restart the appliances in the setup.

You can manually synchronize the external groups with the directory services using the Synchronize (⌚) icon.

After clicking the Synchronize (⌚) icon, **Enter your password** prompt appears. Enter the password and click **Ok**.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information about Password Policy, refer to [Password Policy for the LDAP Users](#).

The following scenarios occur when synchronization is performed between the external groups and the directory services.

- Users are added to ESA and roles are assigned
- Roles of existing users in ESA are updated
- Users are deleted from the ESA if they are associated with any external groups

Based on the scenarios, the messages appearing in the Web UI, when synchronization is performed, are described in the following table.

Message	Description
Added	Users are added to the ESA the roles mentioned in the external groups are assigned to the user
Updated	Roles pertaining to the users are updated ESA
Removed	Roles corresponding to the deleted external group is removed for the users. Users are not deleted from ESA.
Deleted	Users are deleted from ESA as they are not associated to any external group.
Failed	Updates to the user fail. Note: The reason for the failure in update appears in the Web UI.

If a GroupDN for an external group is not available during synchronization, the users are removed or deleted. The following log appears in the Insight Analytics screen:

Appliance Warning: GroupDN is missing in external Source.

Also, in the Appliance logs, the following message appears:

External Group: <Group name>, GroupDN: <domain name> could not be found on the external source

4.11.5 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.

Note: For more information about configuring Azure AD Settings from the CLI Manager, refer to section [Working with Azure AD](#).

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.

Azure AD Settings

Tenant ID: [redacted] ⓘ

Client ID: [redacted] ⓘ

Auth Type: Secret ⓘ

Client Secret: [redacted] ⓘ

Test **Apply**

Figure 4-45: Azure AD configuration

- Enter the data in the fields as shown in the following table:

Table 4-15: Azure AD Settings

Setting	Description
Tenant ID	Unique identifier of the Azure AD instance
Client ID	Unique identifier of an application created in Azure AD
Auth Type	<p>Select one of the Auth Type:</p> <ul style="list-style-type: none"> 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 <p>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.</p>
Client Secret/Thumbprint	<p>The client secret/thumbprint is the password of the Azure AD application.</p> <ul style="list-style-type: none"> 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/>

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

4.11.5.1 Importing Azure Users

Before you begin

Before importing Azure users, ensure that the following prerequisites are considered:

- Ensure that the user is not present in the nested group. If the user is present in the nested group, then the nested group will not be synced on the appliance.
- Ensure to check the user status before importing them to the appliance. If a user with the *Disabled* status is imported, then that user will not be able to login to the appliance.

- Ensure that an external user is not added to the group. If an external user is added to the group, then that user will not be synced on the appliance.
- Ensure that the special character # (hash) is not used while creating the username. If you are importing users from the Azure AD, then the usernames containing the special character # (hash) will not be able to login to the appliance. The usernames containing the following special characters are supported in the appliance.
 - ' (single quote)
 - . (period)
 - ^ (caret)
 - ! (exclamation)
 - ~ (tilde)
 - - (minus)
 - _ (underscore)

You can import users from the Azure AD to the appliance, on the **User Management** screen.

Note: Ensure that the Azure AD settings are enabled before importing the users.

For more information about Azure AD settings, refer to section [Configuring the Azure AD Settings](#).

► To import Azure users:

1. On the Web UI, navigate to **Settings > Users > User Management**.
2. Click **Import Azure Users**.
3. The **Enter your password** prompt appears. Enter the password and click **OK**.

Note: If the number of unsuccessful password attempts exceed the defined value in the password policy, then the user account gets locked.

For more information about Password Policy, refer to section [Password Policy for the LDAP Users](#).

The **Import Users** screen appears.

4. Search a user by entering the name in the **Username/Filter** box.
5. If required, toggle the **Overwrite Existing Users** option to ON to overwrite users that are already imported to the appliance.
6. Click **Next**.
The users matching the search criteria appear on the screen.
7. Select the required users and click **Next**.
The screen to select the roles appears.
8. Select the required roles for the selected users and click **Next**.
The screen displaying the imported users appears.
9. Click **Close**.
The users, with their roles, are imported to the appliance.

4.11.5.2 Working with External Azure Groups

The Azure AD is an identity management system that contains information about the enterprise users. You can map the users in the Azure AD to the various roles defined in the Appliances. The External Azure Groups feature enables you to associate users or groups to the roles.

You can import users from the Azure AD to assign roles for performing various security and administrative operations on the appliances. Using External Azure Groups, you connect to Azure AD, import the required users or groups, and assign the Appliance-specific roles to them.

Note: Ensure that **Azure AD** is enabled to use external Azure group.

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

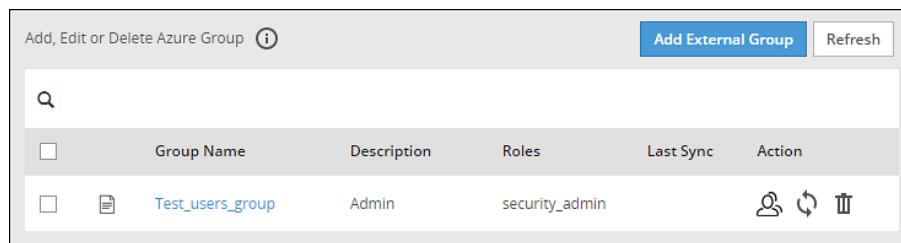


Figure 4-46: External Azure Groups Screen

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

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

Table 4-16: External Groups Icons

Icon	Description
👤	List the users present for the Azure External Group
⟳	Synchronize with the Azure External Group to update the users
ⓧ	Delete the Azure External Group

4.11.5.2.1 Adding an Azure External Group

You can add an Azure External Group to assign roles for a group of users.

► To add an External Group:

1. On the ESA Web UI, navigate to **Settings > Users > Azure External Groups**.
2. Click **Add External Group**.
3. Enter the group name in the **Groupname/Filter** field.

The screenshot shows the 'External Group' creation dialog. At the top right are 'Save' and 'Cancel' buttons. Below them is a search bar with 'test' entered and a 'Search Groups' button. A 'Description' field is empty. A 'Roles' tab is selected, showing a list of roles with checkboxes:

<input type="checkbox"/>	Title	Description	Permission
<input type="checkbox"/>	Shell Accounts	Accounts that have shell access	Shell (non-CLI) Acce...
<input type="checkbox"/>	Security Administrat...	Security Administrator Role	Appliance web manage...
<input type="checkbox"/>	Policy Proxy User	Grant Application-Protector B2B Proxy-lo...	Proxy-User
<input type="checkbox"/>	Security Administrat...	Security Administrator Viewer Role	Appliance CLI Viewer...
<input type="checkbox"/>	Directory Administrat...	Local LDAP Administrator Role	Directory Manager
<input type="checkbox"/>	Policy User	Grant Application-Protector access	Policy-User

Figure 4-47: Creating an External Group

4. Click **Search Groups** to view the list of groups.
 5. Select one group from the list, and click **Submit**.
 6. Enter a description in the **Description** field.
 7. Select the required roles from the **Roles** tab.
 8. Click **Save**.
- The *External Group has been created successfully* message appears.

4.11.5.2.2 Editing an Azure External Group

You can edit an Azure external group to modify **Description** and **Roles**. If any updates are made to the roles of the users in the Azure External Groups, then the modifications are applicable immediately to the users existing on the Appliance.

► To edit an External Group:

1. On the ESA Web UI, navigate to **Settings > Users > Azure External Groups**.
2. Select the required external group.
3. Edit the required fields.
4. Click **Save**.
5. **Enter your password** prompt appears. Enter the password and click **Ok**.

Note: If the number of unsuccessful password attempts exceed the defined value in the password policy, then the user account gets locked.

For more information about Password Policy, refer to section [Password Policy for the LDAP Users](#).

The changes to the external group are updated.

4.11.5.2.3 Synchronizing the Azure External Group

When the Azure AD is enabled, the **Azure External Groups** is started. You can manually synchronize the Azure External Groups using the Synchronize (⌚) icon.

After clicking the Synchronize (⌚) icon, the **Enter your password** prompt appears. Enter the password and click **Ok**.

Note: If the number of unsuccessful password attempts exceed the defined value in the password policy, then the user account gets locked. For more information about Password Policy, refer to section [Password Policy for the LDAP Users](#).

The messages appearing on the Web UI, when synchronization is performed between Azure External Groups and the appliance, are described in the following table.

Message	Description
Success	<ul style="list-style-type: none"> Users are added to the ESA and roles are assigned Roles of existing users in the ESA are updated Users are deleted from the ESA if they are associated with any external Azure Groups
Failed	<p>Updates to the user failed</p> <p>Note: The reason for the failure in updating the user appears on the Web UI.</p>

4.11.5.2.4 Deleting an Azure External Group

When you delete an Azure External Group, the following scenarios are considered while removing a user from the Azure External Group:

- If the users are not part of other external groups, then the users are removed from the Appliance.
- If the users are a part of multiple external groups, the only the association with the deleted Azure External Group and roles is removed.

► To remove an Azure External Group:

- On the ESA Web UI, navigate to **Settings > Users > Azure External Groups**.
- Select the required external group and click the Delete (🗑) icon.
- Enter your password** prompt appears. Enter the password and click **Ok**.

Note: If the number of unsuccessful password attempts exceed the defined value in the password policy, then the user account gets locked.

For more information about Password Policy, refer to section [Password Policy for the LDAP Users](#).

The Azure External Group is deleted.

Chapter 5

Trusted Appliances Cluster (TAC)

[*5.1 TAC Topology*](#)

[*5.2 Cluster Configuration Files*](#)

[*5.3 Deploying Appliances in a Cluster*](#)

[*5.4 Cluster Security*](#)

[*5.5 Reinstalling Cluster Services*](#)

[*5.6 Uninstalling Cluster Services*](#)

[*5.7 FAQs on TAC*](#)

[*5.8 Creating a TAC using the Web UI*](#)

[*5.9 Joining an Existing Cluster using the Web UI*](#)

[*5.10 Connection Settings*](#)

[*5.11 Managing Communication Methods for Local Node*](#)

[*5.12 Viewing Cluster Information*](#)

[*5.13 Removing a Node from the Cluster using the Web UI*](#)

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.

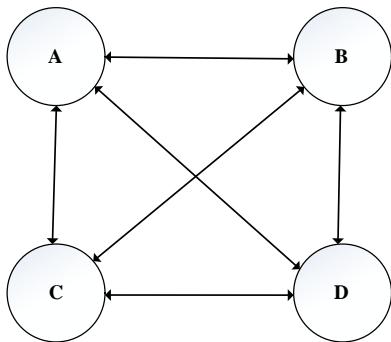
A Trusted Appliances cluster (TAC) is a tool, where appliances, such as, ESA or DSG replicate and maintain information. In a TAC, multiple appliances are connected using SSH. A trusted channel is created to transfer data between the appliances in a cluster. You can also run remote commands, backup data, 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.

5.1 TAC Topology

The TAC is a connected graph with a fully connected cluster. In a fully connected cluster, every node directly communicates with other nodes in the cluster.

The following figure shows a connected graph with four nodes A, B, C, and D that are directly connected to each other.



In a TAC, each appliance is classified either as a client or a server.

- Client: A client is a stateless agent that requests information from a server.
- Server: A server maintains information about all the appliances in the cluster, performs regular health checks, and responds to queries from the clients.

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 to the cluster is the leader. The other appliances added to the cluster are followers.

It is important to maintain the number of servers to keep the cluster available. For a cluster to be available, 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.

5.2 Cluster Configuration Files

In a cluster, you can deploy an appliance as a server or a client by modifying the cluster configuration files. For deploying an appliance on a cluster, the following configuration files are available for an appliance.

agent.json

This file specifies the role of an appliance in the cluster. The *agent.json* file is available in the */opt/cluster-consul-integration/configure* directory.

The following table describes the attributes that can be configured in the *agent.json* file.

Attribute	Description	Values
type	The role of the appliance in the cluster.	<ul style="list-style-type: none"> • auto (default) – Role of the appliance is determined based on state of the TAC and the parameters of the <i>auto_agent.json</i> file. • client – Appliance is added to cluster as a client • server – Appliance is added to cluster as a server <p>For more information about the deployment scenarios, refer to section Deploying Appliances in a cluster.</p>

agent_auto.json

This file is considered only if the *type* attribute in the *agent.json* file is set to *auto*. The *agent_auto.json* file 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.

The *agent_auto.json* file is available in the */opt/cluster-consul-integration/configure* directory.

The following table describes the attributes that can be configured in the `agent_auto.json` file.

Attribute	Description	Values
maximum_servers	The maximum number of servers that can be deployed in a cluster.	<p>5 (default)</p> <p>Note:</p> <ul style="list-style-type: none"> 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.
PAP_eligible_servers	The list of appliances that can be deployed as servers.	<ul style="list-style-type: none"> ESA (default) - ESA appliance CG – DSG appliance

config.json

This file contains the cluster-related information for an appliance, such as, data center, ports, Consul certificates, bind address, and so on. The `config.json` file is available in the `/opt/consul/configure` directory.

5.3 Deploying Appliances in a Cluster

You can deploy the appliances in a cluster as a server or a client. The `type` attribute in the `agent.json` file and the `PAP_eligible_servers` and `maximum_servers` attribute in the `auto_agent.json` file determine how the appliance is deployed in the cluster.

The following flowchart illustrates how an appliance is deployed in a cluster.

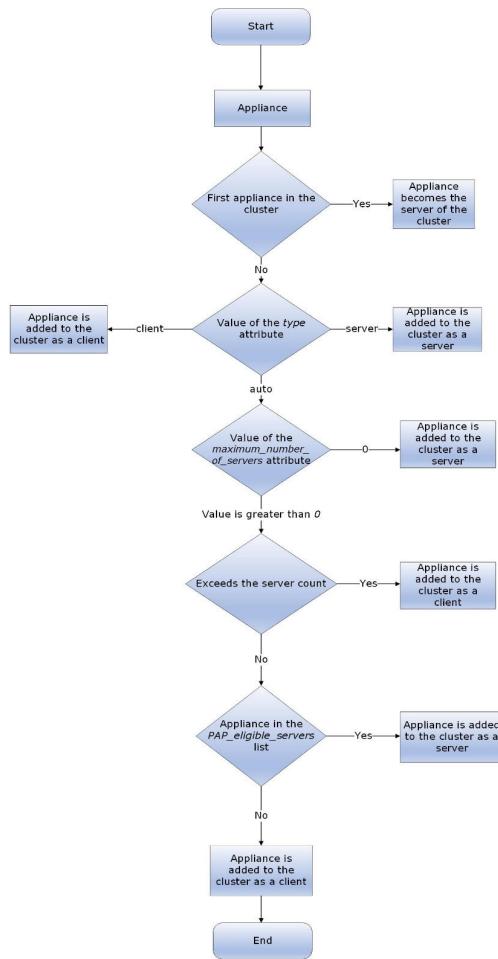


Figure 5-1: Flowchart for Deploying Appliances in a Cluster

The following example describes a scenario of deploying appliances in a cluster.

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`

The screenshot shows the 'Cluster Status' interface. At the top, there are tabs for 'Status' and 'Saved Files'. Below that is a 'Management' dropdown showing 'Online: 1 Failure: 0 Current Master Site: site1'. There are also 'Filter' and 'Display' dropdowns. The main area displays a single node entry: 'protegility-esa001'. To the right of the node name is a table with the following data:

Name	protegility-esa001(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

Now, you want to add another ESA appliance, ESA002, to this cluster as a server. In this case, you must ensure that the `type` attribute in the `agent.json` file of ESA002 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	Description	Labels	Status	Status Message
protegrity-esa001	Created on Mon Oct	_all_ESA.Enterprise-Security-Administrator.site1.Consul Server	Online	No messages
protegrity-esa002	Created on Wed Oct	_all_ESA.Enterprise-Security-Administrator.site1.Consul Server	Online	No messages
protegrity-esa003	Created on Wed Oct	_all_ESA.Enterprise-Security-Administrator.site1.Consul Client	Online	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
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, consider the cluster with five servers, ESA001, ESA002, ESA003, ESA004, and ESA006 as shown in the following figure.

Name	protegility-cg001(.....)
Description	Created on Wed Oct
Labels	__all___ESA.Enterprise-Security-Administrator.site1.Consul Server
Status	Online
Status Message	No messages

Name	protegility-es004(.....)
Description	Created on Wed Oct
Labels	__all___ESA.Enterprise-Security-Administrator.site1.Consul Server
Status	Online
Status Message	No messages

Name	protegility-es006(.....)
Description	Created on Wed Oct
Labels	__all___ESA.Enterprise-Security-Administrator.site1.Consul Server
Status	Online
Status Message	No messages

Name	protegility-es003(.....)
Description	Created on Wed Oct
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.

Name	protegility-es007(.....)
Description	Created on Wed Oct
Labels	__all___ESA.Enterprise-Security-Administrator.site1.Consul Client
Status	Online
Status Message	No messages

Name	protegility-es001(.....)
Description	Created on Mon Oct
Labels	__all___ESA.Enterprise-Security-Administrator.site1.Consul Server
Status	Online
Status Message	No messages

Name	protegility-es004(.....)
Description	Created on Wed Oct
Labels	__all___ESA.Enterprise-Security-Administrator.site1.Consul Server
Status	Online
Status Message	No messages

Name	protegility-es006(.....)
Description	Created on Wed Oct
Labels	__all___ESA.Enterprise-Security-Administrator.site1.Consul Server
Status	Online
Status Message	No messages

Name	protegility-cg001(.....)
Description	Created on Wed Oct
Labels	__all___ESA.Enterprise-Security-Administrator.site1.Consul Server
Status	Online
Status Message	No messages

5.4 Cluster Security

This section describes about the Cluster Security.



Gossip Key

In the cluster, the appliances communicate using the Gossip protocol. The cluster supports encrypting the communication using the gossip key. This key is generated during the creation of the cluster. The gossip key is then shared across all the appliances in the cluster.

SSL Certificates

The certificates are used to authenticate the appliances on the cluster. Every appliance contains the following default cluster certificates in the certificate repository:

- Server certificate and key for Consul
- CA certificate and key for Consul

In a cluster, the server certificates of the appliances are validated by the CA certificate of the appliance that initiated the cluster. This CA certificate is shared across all the appliances on the cluster for SSL communication.

You can also upload your custom CA and server certificates to the appliances on the cluster. The CA.key file is not mandatory when you deploy custom certificates for an appliance.

Note: Ensure that you apply a single CA certificate on all the appliances in the cluster.

If the CA.key is available, the appliances that are added to the cluster download the CA certificate and key. The new server certificate for the appliance are generated using the CA key file.

If the CA.key is not available, all the keys and certificates are shared among the appliances in the cluster.

Ensure that the custom certificates match the following requirements:

- The CN attribute of the server certificate is set in the following format:
server.<datacenter name>.<domain>

For example, server.ptydatacenter.protegrity

Note: The domain and datacenter name must be equal to the value mentioned in the config.json file.

- The custom certificates contain the following entries:
 - localhost
 - 127.0.0.1
 - FQDN of the local servers in the cluster

For example, an SSL Certificate with SAN extension of servers ESA1, ESA2, and ESA3 in a cluster has the following entries:

- localhost
- 127.0.0.1
- ESA1.protegrity.com
- ESA2.protegrity.com
- ESA3.protegrity.com

The following figure illustrates the certificates.



Certificate Repository					
ID	Type	Archive Time	Status	Description	Action
78773ee5.0	certificate, key	February 01 2022, 16:13:59	In use	Audit Store Client Cert and Key for plug	
59a91e26.0	certificate, key	February 01 2022, 15:49:21	In use	System initial server certificate and key.	
f7320cdf.0	certificate, key	February 01 2022, 15:49:21	In use	System initial client certificate and key.	
6f2e6d24.0	certificate, key	February 01 2022, 16:10:11	In use	Audit Store Client Cert and Key for es_cluster	
c043178a.0	certificate, key	February 01 2022, 16:16:51	In use	Audit Store Client Cert and Key for ian	
<input type="checkbox"/> 6c78352b.2	certificate, key	February 02 2022, 15:19:45	Expired	Client Certificate and Key.	
<input type="checkbox"/> 6c78352b.1	certificate, key	February 02 2022, 10:38:10	Expired	Audit Cert & Key	
<input type="checkbox"/> 6c78352b.0	certificate, key	February 02 2022, 10:37:14	Expired	Client Key	

Show entries

Figure 5-2: Cluster Certificates

Ports

The following ports are used for enabling communication between appliances:

- TCP port of 8300 – Used by servers to handle incoming request
- TCP and UDP ports of 8301 – Used by appliances to gossip on LAN
- TCP and UDP ports of 8302 – Used by appliances to gossip on WAN

5.5 Reinstalling Cluster Services

If the configuration files for TAC are corrupted, you can reinstall the consul service.

Before you begin

Ensure that Cluster-Consul-Integration v0.2 service is uninstalled before reinstalling Consul v1.0 service.

► To view TAC certificates:

1. In the CLI Manager, navigate to **Administration> Add/Remove Services**.
2. Press **ENTER**.
3. Select **Install applications**.
4. Select only **Consul v1.0** and select **OK**.
5. Select **Yes**.
The Consul product is reinstalled on your appliance.
6. Install the **Cluster-Consul-Integration v0.2** service.
For more information about installing services, refer to the *Protegility Installation Guide 9.1.0.5*.

5.6 Uninstalling Cluster Services

If you are using a cluster with a maximum of ten nodes in a cluster and do not want to continue with the integrated cluster services, you can uninstall the services as shown in the following steps.

Before you begin

Note:

If the node contains scheduled tasks associated with it, then you cannot uninstall the cluster services on it. Ensure that you delete all the scheduled tasks before uninstalling the cluster services.

► To uninstall cluster services:

1. Remove the appliance from the TAC.
2. In the CLI Manager, navigate to **Administration> Add/Remove Services**.
3. Press **ENTER**.
4. Select **Remove already installed applications**.
5. Select **Cluster-Consul-Integration v0.2** and select **OK**.
The integration service is uninstalled.
6. Select **Consul v1.0** and select **OK**.
The Consul product is uninstalled from your appliance.

5.7 FAQs on TAC

This section lists the FAQs on TAC.

Question	Answer
Can I block communication between appliances?	No. Blocking communication between appliances is disabled from release v7.1.0 MR2.
What is the recommended minimum quorum of servers required in a cluster?	The recommended minimum quorum of servers required in a cluster is three.
How to determine which appliance is the leader of the cluster?	In the OS Console of an appliance, run the following command: <pre>/usr/local/consul operator raft list-peers -http-addr https://localhost:9000 -ca-file /opt/consul/ssl/ca.pem -client-cert /opt/consul/ssl/cert.pem -client-key /opt/consul/ssl/cert.key</pre>
Can I change the certificates of an appliance that is added to a cluster?	Yes. Ensure that the certificates are valid. For more information about the validity of the certificates, refer to the <i>Protegity Certificate Management Guide 9.1.0.5</i> .
Can I remove the last server from the cluster?	No, you cannot remove the last server from the cluster. The clients depend on this server for cluster related information. If you remove this server, then you risk de-stabilizing the cluster.
How to determine the role of an appliance in a cluster?	In the Web UI, navigate to the Trusted Appliance Cluster. On the screen, the labels for the appliances appear. The label for the server is <i>Consul Server</i> and that of the client is <i>Consul Client</i> .
Can I add an appliance other than ESA as server?	Yes. Ensure that the value of the type attribute in the <i>agent.json</i> file under the <i>/opt/cluster-consul-integration/configure</i> directory is set as server.

5.8 Creating a TAC using the Web UI

You can create a TAC, where you add an appliance to the cluster.

Before you begin

Note: When setting up or adding appliances to your cluster, you may be required to request a license for new nodes from Protegility.

For more information about licensing, refer to the [Protegility Data Security Platform Licensing Guide 9.0.0.0](#) and your license agreement with Protegility.

Important:

Before creating a TAC, ensure that the [SSH](#) Authentication type is set to **Public key** or **Password + PublicKey**.

► To create a cluster using the Web UI:

1. In the ESA Web UI, navigate to **System > Trusted Appliances Cluster**.
The **Join Cluster** screen appears.
2. Select **Create a new cluster**.
The following screen appears.

Create Cluster

A Trusted Appliances Cluster can be used to transfer data from one node to other nodes. Setting up a trusted appliances cluster allows you to synchronize files and configurations across multiple sites.

Communication Methods [i](#)

<input checked="" type="radio"/> 10.91.2.48	
<input type="radio"/> protegrity-framework310.protegrity.com	

[Add New](#)

[Create](#)

[Join a Cluster](#)

Figure 5-3: Create Cluster Screen

3. Select the preferred communication method.

Note: Select **Add New** to add, edit, or delete a communication method.

For more information about managing communication methods, refer to [Managing Communication Methods for Local Node](#).

4. Click **Create**.
A cluster is created.

5.9 Joining an Existing Cluster using the Web UI

If your appliance is not a part of any trusted appliances cluster, then you can add it to an existing cluster. This section describes the steps to join a TAC using the Web UI.

- To join a cluster using the Web UI:

1. On the ESA Web UI, navigate to **System > Trusted Appliances Cluster**.
The following screen appears.

Join Cluster

Provide the IP of the target node along with credentials of the user with administrative privileges to connect with the target node. Then select a site and a preferred method to join a cluster.

Node

Username

Password

Connect **Clear**

[Create a new Cluster](#)

Figure 5-4: Join Cluster

2. Enter the IP address of the target node in the **Node** text box.
3. Enter the credentials of the user of the target node in the **Username** and **Password** text boxes.
4. Click **Connect**.

The **Site** drop-down list and the **Communication Methods** options appear.

Note: Click **Add New** to add a new communication method

5. Select the site and the preferred communication method.

6. Click **Join**.

The node is added to the cluster and the following screen appears.

Name	protegrity-esa710(10.31.1.110)
Description	Created on Tue Aug 30 11:18:35 2022
Labels	__all__,ESA,Enterprise-Security-Administrator,site1,Consul Server
Status	Online
Status Message	No messages

Name	protegrity-esa585(10.31.1.94)
Description	Created on Tue Aug 30 11:20:32 2022
Labels	__all__,ESA,Enterprise-Security-Administrator,site1
Status	Online
Status Message	No messages

Figure 5-5: New Node Added to the Cluster

Note:

After joining an appliance to the cluster, during replication, the Consul certificates are copied from the source to the target appliance. In this case, it is recommended to delete the Consul certificates pertaining to the target node from the Certificate Management screen. Navigate to **Settings > Network > Certificate Repository**. Click the delete icon next to **Server certificate and key for Consul**.

c043178a.0	certificate, key	In use	 ⓘ
d0af2d7c.1	certificate, key	Server certificate and key for Consul.	 ⓘ ⚡ 

Figure 5-6: Server Certificate and Key

5.10 Connection Settings

In a TAC, you can create a partially connected cluster using the Connecting Setting feature. In a partially connected cluster, the nodes selectively communicate with other nodes in the cluster without disconnecting the graph. If you want to avoid redundant information between certain nodes in the cluster, you can block the direct communication between them.

Note: This feature is only supported if the *Cluster-Consul-Integration v0.2* and *Consul* components are not installed on your system.

The following figure shows a partially connected cluster connected graph with four nodes, where the nodes selectively communicate with some nodes in the cluster.

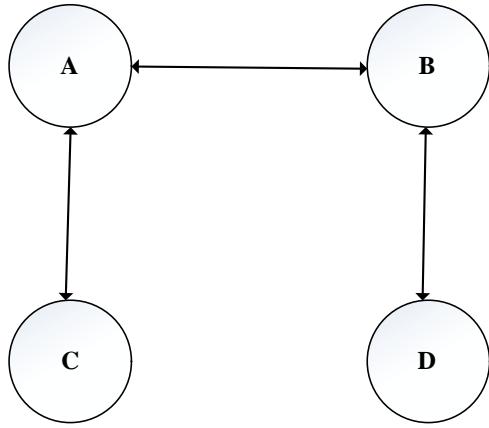


Figure 5-7: Partially Connected Cluster

As shown in the figure, the direct communication between nodes C and D, A and D, B and C are blocked. If node B requires information about node C, it receives information from node A. The cluster is a fully connected graph where you can communicate directly or indirectly with every node in the cluster.

Note: In a disconnected graph, there is no communication path between one node and other nodes in the cluster. You cannot create a TAC with a disconnected graph.

Note: In a partially connected cluster, as some nodes are not connected to each other directly, there might be a delay in propagating data, depending on the path that the data needs to traverse.

5.10.1 Connection Settings for Nodes

This section describes the steps to set the connection settings for nodes in a cluster.

- To set connection settings for nodes in the cluster:

- In the CLI Manager, navigate to **Tools > Trusted Appliances Cluster > Connection Management: Set connection settings for cluster nodes**.

The following screen appears.

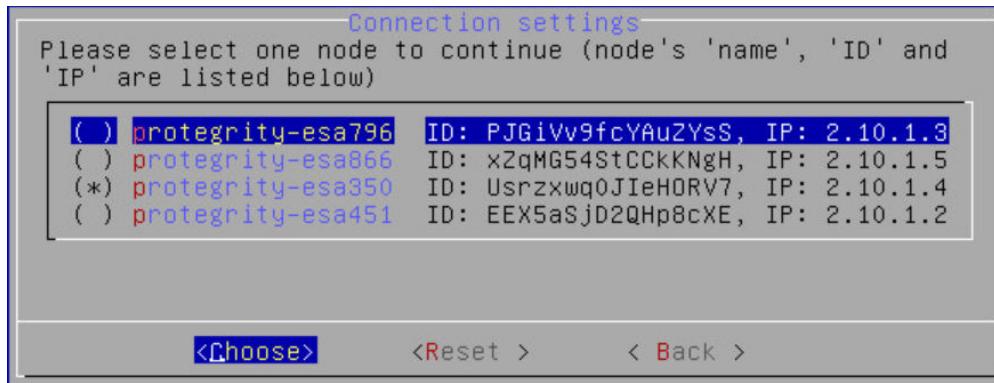


Figure 5-8: Connection Settings

- Select the required node in the cluster.
- Select **Choose**.

The list of connection settings between the node and other nodes in the cluster appears.

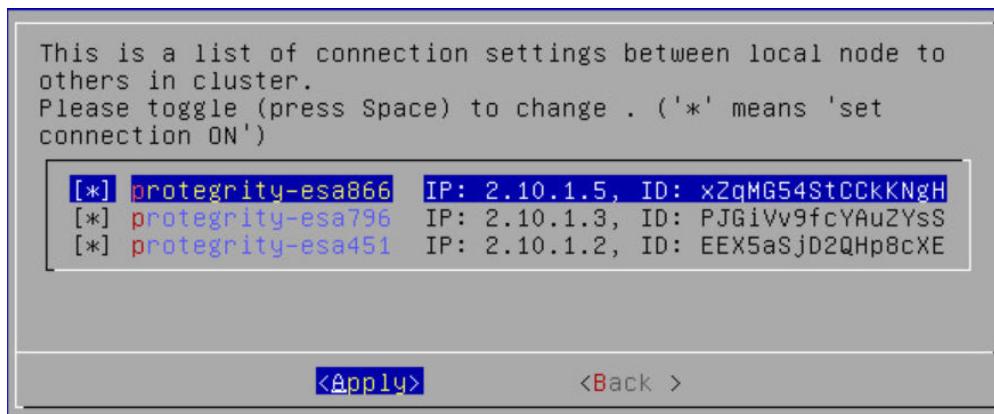


Figure 5-9: Select Connection Settings

- Press **SPACEBAR** to toggle the connection setting for a particular node.
- Select **Apply**.

The connection settings for the node are saved.

Caution: You can only create cluster export tasks between nodes that are directly connected to each other.

5.11 Managing Communication Methods for Local Node

Every node in a network is identified using a unique identifier. A communication method is a qualifier for the remote nodes in the network to communicate with the local node.

There are two standard methods by which a node is identified:

- Local IP Address of the system (ethMNG)
- Host name

The nodes joining a cluster use the communication method to communicate with each other. The communication between nodes in a cluster occur over one of the accessible communication methods.

5.11.1 Adding a Communication Method from the Web UI

This section describes the steps to add a communication method from the Web UI.

► To add a communication method from the Web UI:

1. In the Web UI, navigate to **System > Trusted Appliances Cluster**.
The **Join Cluster** Screen appears.

Note:

In the Web UI, you can add a communication method only before creating a cluster.

2. Click **Add New Cluster**.
3. Click **Add New**.
The **Add Communication Method** text box appears.
4. Type the communication method and select **OK**.

The communication method is added.

5.11.2 Editing a Communication Method from the Web UI

This section describes the steps to edit a communication method from the Web UI.

► To edit a communication method from the Web UI:

1. In the Web UI, navigate to **System > Trusted Appliances Cluster**.
The **Join Cluster** Screen appears.

Note:

In the Web UI, you can edit a communication method only when you create a cluster.

2. Click **Add a new cluster**.
The **Create New Cluster** screen appears.
3. Click the **Edit** (edit icon) corresponding to the communication method to be edited.
The **Edit Communication Method** text box appears.
4. Type the communication method and select **OK**.

The communication method is edited.

5.11.3 Deleting a Communication Method from the Web UI

This section describes the steps to delete a communication method from the Web UI.

► To delete a communication method from the Web UI:

1. In the Web UI, navigate to **System > Trusted Appliances Cluster**.
The **Join Cluster** Screen appears.

Note:

In the Web UI, you can delete a communication method when you create a cluster.

2. Click **Add a new cluster**.
The **Create New Cluster** screen appears.
3. Click the **Delete** (trash bin) icon corresponding to the communication method to be deleted.
A message confirming the delete operation appears.
4. Select **OK**.

The communication method is deleted.

5.12 Viewing Cluster Information

This section describes the how to view cluster information using the Web UI.

► To execute commands using Web UI:

1. In the Web UI, navigate to **System > Trusted Appliances Cluster**.
The screen with the appliances connected to the cluster appears.
2. Select **All** drop-down list.
The following options appear:
 - Top 10 CPU
 - Network
 - System Info
 - Node Summary
 - MemoryFree
 - Top 10 memory
 - Disk Free
 - Cluster tasks
3. Select the required option.
The selected information for the appliances appears in the right pane.

5.13 Removing a Node from the Cluster using the Web UI

This section describes the steps to remove a node from a cluster using the Web UI.

Before you begin

Note:

If a node is associated with a cluster task that is based on the hostname or IP address, then the *Leave Cluster* operation will not remove the node from the cluster. Ensure that you delete all such tasks before removing any node from the cluster.

► To remove a node from a cluster using the Web UI:

1. On the Web UI of the node that you want to remove from the cluster, navigate to **System > Trusted Appliances Cluster**.
The screen displaying the cluster nodes appears.
2. Navigate to **Management > Leave Cluster**.
The following screen appears.

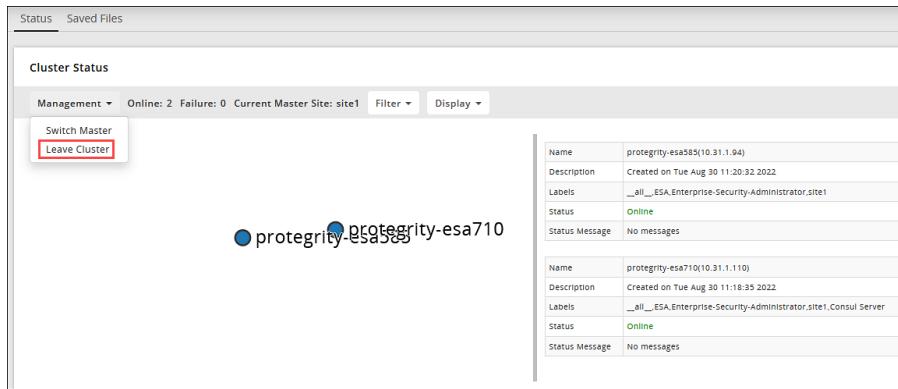


Figure 5-10: Node Selection for Removal

A confirmation message appears.

3. Select **Ok**.
The node is removed from the cluster.

Note:

If the scheduled tasks are created between the nodes in a cluster, then ensure that after you remove a node from the cluster, all the scheduled tasks related to the node are disabled or deleted.

Chapter 6

Appliance Virtualization

- [6.1 Xen Paravirtualization Setup](#)
 - [6.2 Xen Server Configuration](#)
 - [6.3 Installing Xen Tools](#)
 - [6.4 Xen Source – Xen Community Version](#)
-

The information in this section provides low-level details on appliance virtualization and requires some Xen knowledge and technical skills.

The default installation of Protegity appliance uses hardware virtualization mode (HVM). The appliance can be reconfigured to use parallel virtualization mode (PVM) to optimize the performance of virtual guest machines. Protegity supports the following virtual servers:

- Xen®
- Microsoft Hyper-VP™
- Linux KVM Hypervisor

This section describes how to switch from HVM to PVM. The following two main tasks are involved:

- Configuration changes on the guest machine (the appliance)
- Configuration changes on the virtual server

The appliance configuration changes are facilitated by the Xen Paravirtualization tool, which is available in the appliance Tools menu, in the CLI Manager.

The virtual server configuration is done with its own tools. The examples used in this section are for using paravirtualization with Xen. The Xen hypervisor changes are facilitated by the Xen Paravirtualization Tool. Xen hypervisor is a thin software layer that is inserted between the server hardware and the operating system. This provides an abstraction layer that allows each physical server to run one or more virtual servers, effectively decoupling the operating system and its applications from the underlying physical server.

For more information about Xen hypervisor, refer to <http://www.xen.org/>.

6.1 Xen Paravirtualization Setup

This section describes the paravirtualization process, from preparation to running the tools and rebooting into PVM mode.

The paravirtualization tool provides an easy way to convert HVM to PVM and back again. It automates changes to configuration files and XenServer parameter.

This section describes the actual configuration changes on both the Appliance and XenServer in case you need or want to understand the low-level mechanisms involved.

Note: It is recommended that you consult Protegity Support before using the information in this Technical Reference section to manually change your configurations.

6.1.1 Pre-Conversion Tasks

Before switching from HVM to PVM you should perform a system check, interface check, and system backup.

6.1.1.1 System Check

The Protegity software appliance is installed with HVM. This means the appliance operating system does not know that it is running on a hypervisor.

► To check the system:

Use the following Linux command to check whether the Linux kernel supports paravirtualization and examine the hypervisor.

`# dmesg | grep -i boot`

If the following message does not appear, then the kernel does not support paravirtualization:

Booting paravirtualized kernel

The rest of the output shows the hypervisor name (for example, *Xen*). If you are running on a physical hardware, or the hypervisor was not configured to use PVM, then the following output appears:

bare hardware

6.1.1.2 Interface Check

The conversion tools and tasks assume that the Protegity Appliance virtual hard disk is using the IDE interface, which is the default interface. Check that the device name used by the Linux Operating System is *hda*, and not *sda* or other devices.

6.1.1.3 System Backup

Switching from HVM to PVM requires changes in many configuration files, so it is very important to back up the system before applying the changes. Use the XenServer snapshot functionality to back up the system.

For more information about the snapshot functionality, refer to the XenServer documentation.

It is also recommended that you back up the appliance data and configuration files using the standard appliance backup mechanisms.

For more information about backing up from CLI Manager, refer to section [Managing Local OS Users](#).

Managing local OS user option provides you the ability to create users that need direct OS shell access and are allowed to perform non-standard functions, such as schedule remote operations, backup agents, run health monitoring, etc. This option also lets you manage passwords and permissions for the *jasperdbuser* and *dpsdbuser*, which are available by default when ESA is installed.

6.1.1.3.1 Managing Local OS Users

This section describes the steps to manage the local OS users.

► To manage local OS users:

1. Navigate to **Administration > Accounts and Passwords > Manage Passwords and Local-Accounts > Manage local OS users**.
2. In the dialog displayed, enter the root password and confirm selection.
3. Add a new user or select an existing user as explained in following steps.
 - a. Select **Add** to create a new local OS user.
 - i. In the dialog box displayed, enter a User name and Password for the new user.

Note:

The **&** character is not supported in the **Username** field.

- ii. Confirm the password in the required text boxes.
 - iii. Select **OK** and press **Enter** to save the user.
- b. Select an existing user from the list displayed.

- i. You can select one of the following options from the displayed menu.

Options	Description	Procedure
Check password	Validate entered password.	In the dialog box displayed, enter the password for the local OS user. A <i>Validation succeeded</i> message appears.
Update password	Change password for the user.	<ol style="list-style-type: none"> 1. In the dialog box displayed, enter the Old password for the local OS user. This step is optional. 2. Enter the New Password and confirm it in the required text boxes.
Update shell	Define shell access for the user.	In the dialog box displayed, select one of the following options: <ul style="list-style-type: none"> • No login access • Linux Shell - <i>/bin/sh</i> • Custom <p>Note: The default shell is set as No login access (<i>/bin/false</i>).</p>
Toggle SSH access	Set SSH access for the user.	Select the Toggle SSH access option and press Enter to set SSH access to Yes .
		Note: The default is set as No when a user is created.

Options	Description	Procedure
Delete user	Delete the local OS user and related home directory.	Select the Delete user option and confirm the selection.

4. Select Close to exit the option.

6.1.1.4 Backup and Restore

This section discusses about Appliance Virtualization backup and restore.

For more information about backing up from the Web UI, refer to section [System Backup and Restore](#). If you backed up the OS in HVM/PVM mode, then you will be able to restore only in the mode in which you backed it up.

6.1.2 Paravirtualization Process

There are several tasks you must perform to switch from HVM to PVM.

The following figure shows the overall task flow.

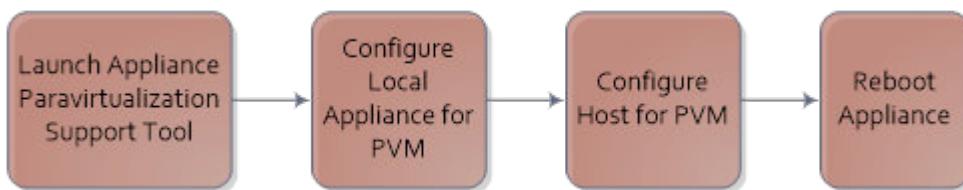


Figure 6-1: HVM to PVM Conversion Task Flow

The installed Appliance comes with the Appliance Paravirtualization Support Tool, which is equipped with the following:

- Displays the current paravirtualization status of the appliance
- Displays Next Boot paravirtualization status of the appliance
- Converts from HVM to PVM and back again
- Connects to the XenServer and configures the Xen hypervisor for HVM or PVM.

6.1.2.1 Starting Appliance Paravirtualization Support Tool

You can use Appliance Paravirtualization Support Tool to configure the local appliance for PVM.

► To start the Appliance Paravirtualization Support Tool:

In the ESA CLI Manager, navigate to **Tools > Xen ParaVirtualization** screen.

The root permission is required for entering the tool menu.

When you launch the tool, the main screen shows the current system status and provides options for managing virtualization.

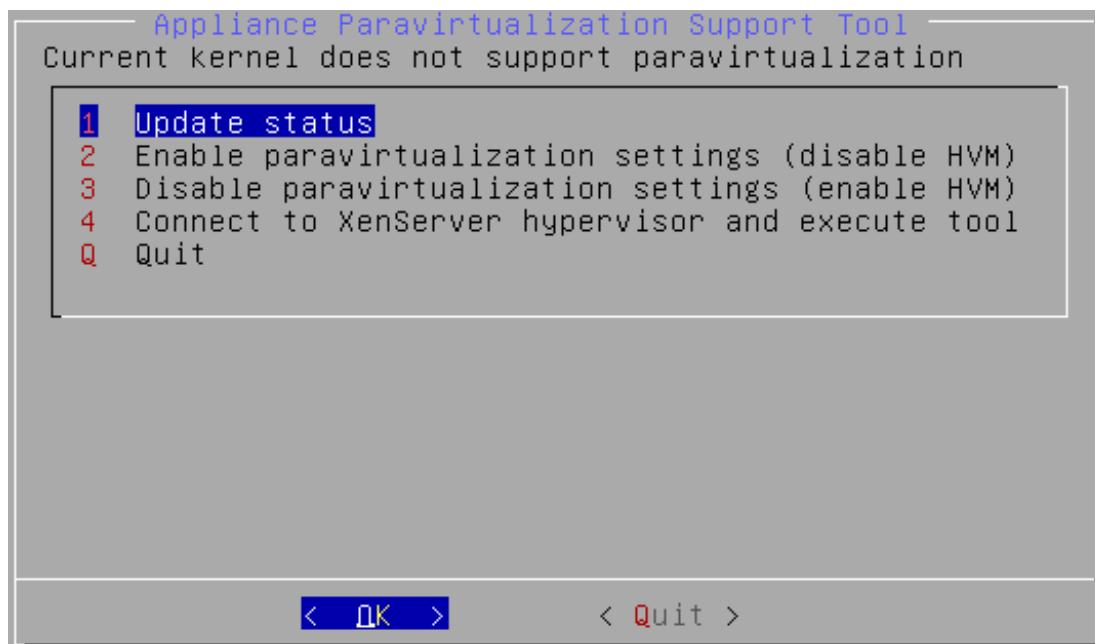


Figure 6-2: Appliance Paravirtualization Support Tool Main Screen

6.1.2.2 Enabling Paravirtualization

When you convert your appliance to the PVM mode, the internal configuration is modified and the Next Boot status changes to support paravirtualization. Both the virtual block device and virtual console support is enabled as well.

► To enable Paravirtualization:

1. To enable PVM on the appliance, you need to configure both XenServer and the appliance. You can configure XenServer in two ways:
 - Copy the tool to the XenServer and execute it locally (not using the appliance).
 - Execute the commands manually using the `xe` command of Xen console.
2. To configure the local appliance for PVM from the Appliance Paravirtualization Support Tool main screen, select **Enable paravirtualization settings**.

The status indicators in the **Next boot configuration** section of the main screen change from *Disabled* to *Enabled*.

6.1.2.3 Configuring Host for PVM

This section describes the steps to configure the Host for PVM.

Before you begin

To configure the Host for PVM, you need to have access to the XenServer machine.

Once the local Appliance is configured to use PVM, you connect to the XenServer to run the Xen ParaVirtualization Support Tool to configure changes on the Xen hypervisor so that it runs in Host PVM mode. You will be asked for a root password upon launching the tool.

The following figure shows the main screen of the Xen Paravirtualization Support Tool.

```
[leave empty to the list of virtual-machines]
ESA_DEMO

Virtual Machine Information:
  Name:....."ESA_DEMO"
  UUID:....."a22dbc11-3f2e-b021-a98e-3b8d372e4854"
  VBD-UUID:....."0b911be6-816d-18a7-1a7a-0e6bdfbaeacb"

Current settings for ESA_DEMO:
  Power-state:....."running"
  HVM-boot-policy:...."BIOS order"
  PV-bootloader:.....""
  VBD Bootable:....."false"
  Conclusion: Current VM configuration does NOT supports XEN paravirtualization

Main Menu (VM:ESA_DEMO):
-----
1. Change target VM
2. Query settings
3. Backup settings
4. Enable paravirtualization settings (disable HVM)
5. Disable paravirtualization settings (enable HVM)
Q. Quit
?
```

Figure 6-3: Xen ParaVirtualization Support Tool Main Screen

► To configure the Host for PVM:

1. From the Appliance ParaVirtualization Support Tool main screen, select **Connect to XenServer hypervisor and execute tool**.
2. Select **OK**.
The XenServer hypervisor interface appears.
3. At the prompt, type the IP or host name of the XenServer.
4. Press **ENTER**.
5. At the prompt, type the user name for SCP/SSH connection.
6. Press **ENTER**.
7. At the prompt, type the password to upload the file.
The tool is uploaded to the `/tmp` directory.
8. Press **ENTER**.
An introduction message appears.
9. At the prompt, type the password to remotely run the tool.
10. Press **ENTER**.
Alternatively, press **ENTER** to list available virtual machines.
The Xen ParaVirtualization Support Tool Main Screen appears and shows the current virtual machine information and status.
11. Type **4** to enable paravirtualization settings.
12. Press **ENTER**.
The following screen appears.

```
-----
1. Change target VM
2. Query settings
3. Backup settings
4. Enable paravirtualization settings (disable HVM)
5. Disable paravirtualization settings (enable HVM)
q. Quit
? 4

New settings to apply :
    HVM-boot-policy:.......
    PV-bootloader:....."pygrub"
    VBD Bootable:....."true"

The following commands will be executed to apply the new para-virtualization settings:

    xe vm-param-set uuid=a22dbc11-3f2e-b021-a98e-3b8d372e4854 HVM-boot-policy=""
    xe vm-param-set uuid=a22dbc11-3f2e-b021-a98e-3b8d372e4854 PV-bootloader="pygrub"
    xe vbd-param-set uuid=0b911be6-816d-18a7-1a7a-0e6bdfbaeacb bootable="true"
Apply settings ? Enter YES to save or N to cancel....
```

Figure 6-4: Xen Paravirtualization Settings Screen

14. At the prompt, type **Y** to save the configuration.
15. Press ENTER.
16. Type **q** to exit the Appliance Paravirtualization Support Tool.

Note:

You can use option **3** to back up the entries that will be modified.

The backup is stored in the `/tmp` directory on the XenServer machine as a rollback script that can be executed later on to revert the configuration back from PVM to HVM.

6.1.2.4 Rebooting Appliance for PVM

You reboot the Appliance after configuring it and the Host for PVM so that the appliance starts and runs in PVM mode.

Before you begin

Caution:

Before rebooting, exit both local and remote Paravirtualization tools before rebooting the appliance.

If you encounter console issues after reboot, then close the XenCenter and restart a new session.

In the PVM, the system might not boot if there are two bootable devices. Be sure to eject any bootable CD/DVD on the guest machine.

You cannot boot in the System Restore mode when in the Xen Server PVM mode, because it does not show up during appliance launching and appears only if you have previously backed up the OS. However, you can boot in the System Restore mode when in the Xen Server HVM mode.

► To reboot appliance for PVM:

1. To reboot the appliance for PVM, navigate to **Administration > Reboot and Shutdown > Reboot**.
2. Restart the Appliance Paravirtualization Support Tool and check the main screen to verify the current mode.

6.1.2.5 Disabling Paravirtualization

This section describes the steps to disable Paravirtualization.

► **To disable Paravirtualization:**

1. To revert the appliance back to HVM, you need to disable paravirtualization on the guest appliance OS and on the XenServer.
 2. To return the appliance to HVM, use the Disable Paravirtualization Settings option, available in the Appliance Paravirtualization Support Tool.
- The status indicators in the Next boot configuration section on the main screen change from *Enabled* to *Disabled*.
3. To return the XenServer to HVM, perform one of the following tasks to revert the XenServer configuration to HVM:

If...	Then...
You backed up the XenServer configuration by creating a rollback script while switching from HVM to PVM (using option 3 on the Xen Paravirtualization Support Tool)	Execute the rollback script.
You want to use the Xen Paravirtualization Support Tool	Use the Xen Paravirtualization Support Tool to connect to the XenServer, and then type 5 to select Disable paravirtualization Setting (enable HVM) . For more information about connecting to the XenServer, refer to section Configure Host for PVM .
You want to perform a manual conversion	Manually convert from PVM to HVM. For more information about converting from PVM to HVM, refer to section Manual Configuration of Xen Server .

6.2 Xen Server Configuration

This section describes about configuring the Xen Server.

6.2.1 Appliance Configuration Files for PVM

This section lists the appliance configuration files for PVM.

The following table describes the appliance configuration files that are affected by the appliance Xen Paravirtualization tool.

Table 6-1: Appliance Configuration Files for PVM

File Name	Description	HVM	PVM
/boot/grub/menu.lst	Boot Manager. The root partition is affected and the console parameters.	root=/dev/hda1	root=/dev/xvda1 console=hvc0 xencons=hvc0
/etc/fstab	Mounting table	Using the hda device name (/dev/hda1,/dev/hda2,...)	Using the xvda device-name (/dev/xvda1,...)
/etc/inittab	Console	tty1	hvc0



6.2.2 Xen Server Parameters for PVM

This section lists the Xen Server Parameters for PVM.

The following settings are affected by the Appliance Paravirtualization Support Tool.

Table 6-2: XenServer Parameters for PVM

Parameter Name	Description	HVM	PVM
HVM-boot-policy	VM parameter: boot-loader	BIOS Order	“” (empty)
PV-bootloader	VM Parameter: paravirtualization loader	“” (empty)	Pygrub
Bootable	Virtual Block Device parameter	false	“true”

6.2.3 Manual Configuration of Xen Server

This section describes about configuring the Xen Server manually.

It is recommended that you use the Xen Paravirtualization Support Tool to switch between HVM and PVM. However, you sometimes might need to manually configure the XenServer. This section describes the commands you use to switch between the two modes.

Note: It is recommended that you consult Protegity Support before manually applying the commands. Back up your data prior to configuration changes. Read the XenServer documentation to avoid errors.

6.2.3.1 Converting HVM to PVM

This section describes the steps to convert HVM to PVM.

► To convert HVM to PVM:

Use the following commands to convert from HVM to PVM, where *NAME_OF_VM_MACHINE* is the name of the virtual machine.

```
TARGET_VM_NAME="NAME_OF_VM_MACHINE"
TARGET_VM_UUID=$(xe vm-list name-label="$TARGET_VM_NAME" params=uuid --minimal)
TARGET_VM_VBD=$(xe vm-disk-list uuid=$TARGET_VM_UUID | grep -A1 VBD | tail -n 1 | cut -f2 - | sed "s/ *//g")
xe vm-param-set uuid=$TARGET_VM_UUID HVM-boot-policy=""
xe vm-param-set uuid=$TARGET_VM_UUID PV-bootloader="pygrub"
xe vbd-param-set uuid=$TARGET_VM_VBD bootable="true"
```

6.2.3.2 Converting PVM to HVM

This section describes the steps to convert PVM to HVM.

► To convert PVM to HVM:

Use the following commands to convert from PVM to HVM, where *NAME_OF_VM_MACHINE* is the name of the virtual machine.

```
TARGET_VM_NAME="NAME_OF_VM_MACHINE"
TARGET_VM_UUID=$(xe vm-list name-label="$TARGET_VM_NAME" params=uuid --minimal)
TARGET_VM_VBD=$(xe vm-disk-list uuid=$TARGET_VM_UUID | grep -A1 VBD | tail -n 1 | cut -f2 - | sed "s/ *//g")
```

```
- | sed "s/ *//g")
xe vm-param-set uuid=$TARGET_VM_UUID HVM-boot-policy="BIOS order"
xe vm-param-set uuid=$TARGET_VM_UUID PV-bootloader=""
xe vbd-param-set uuid=$TARGET_VM_VBD bootable="false"
```

6.3 Installing Xen Tools

Protegility uses Xen tools to enhance and improve the virtualization environment with better management and performance monitoring. The appliance is a hardened machine, so you must send the Xen tools (*.deb*) package to Protegility, which in turn provides you with an installable package for your Xen Server environment. You must upload the package to the appliance and install it from within the OS Console.

► To install Xen tools:

1. Mount the Xen tools CDROM to the guest machine:
 - a. Using the XenCenter, mount the XenTools (*xs-tools.iso* file) as a CD to the VM.
 - b. Log in to the appliance, and then switch to OS Console.
 - c. To manually mount the device, run the following command:
`# Mount /dev/xvdd /cdrom`
2. Copy the XEN tools *.deb* package to your (desktop) machine. You can do that:
 - Using *scp* to copy the file to a Linux machine, for example:
`# scp -F /dev/null /cdrom/Linux/*_i386.deb YOUR_TARGET_MACHINE:/tmp`
 - Using Web UI, download the following package:
`# ln -s /cdrom/Linux /var/www/xentools`
 - Downloading the file from https://YOUR_IP/xentools.

When you are done, delete the soft link (/var/www/xentools).
3. Send the *xe-guest-utilities_XXXXXX_i386.deb* file to Protegility.
 Protegility will provide you with this package in *.tgz* file.
4. Upload the package to the appliance using the Web UI.
5. Extract the package and execute the installation:


```
# cd /products/uploads
# tar xvfz xe-guest-utilities_XXXXXX_i386.tgz
# cd xe-guest-utilities_XXXXXX_i386
# ./install.sh
```
6. Unmount the */cdrom* on the appliance.
7. Eject the mounted ISO.
8. Reboot the Appliance to clean up references to temporary files and processes.

6.4 Xen Source – Xen Community Version

Unlike XenServer, which provides an integrated UI to configure the virtual machines, Xen Source® does not provide one. Therefore, the third step of switching from HVM to PVM must be done manually by changing configuration files.

This section provides examples of minimum Xen configuration files that you can use to initialize Protegity Appliance on Xen Source hypervisor.

Note: For more information about Xen Source, refer to Protegity Support, Xen Source documentation, and forums.

6.4.1 HVM Configuration

This section discusses about HVM Configuration.

The following commands are used to manually configure the appliance for full virtualization.

```
import os, re
arch_libdir = 'lib'
arch = os.uname()[4]
if os.uname()[0] == 'Linux' and re.search('64', arch):
    arch_libdir = 'lib64'
kernel = "/usr/lib/xen/boot/hvmloader"
builder='hvm'
boot="cda"
memory = 1024
name = "ESA"
vif = [ 'type=ioemu, bridge=xenbr0' ]
disk = [ 'file:/etc/xen/ESA.img,hda,w', 'file:/media/ESA.iso,hdc:cdrom,r' ]
device_model = '/usr/' + arch_libdir + '/xen/bin/qemu-dm'
sdl=0
opengl=0
vnc=1
vncunused=0
vncpasswd=''
stdvga=0
serial='pty'
```

6.4.2 PVM Configuration

This section discusses about PVM Configuration.

The following commands are used to manually configure the appliance for paravirtualization.

```
kernel = "/usr/lib/xen/boot/pv-grub-x86_64.tgz"
extra = "(hd0,0)/boot/grub/menu.lst"
memory = 1024
name = "ESA"
vif = [ 'bridge=xenbr0' ]
disk = [ 'file:/etc/xen/ESA.img,xvda,w' ]
#vfb = [ 'vnc=1' ]# Enable this for graphical GRUB splash-screen
```

Modify the configuration file (names, locations, and resources) to suit your own environment and requirements.

6.4.3 Virtual Appliance

This section discusses about Virtual Appliance.

Create a new (minimum) virtual appliance on XEN Source after creating the configuration files as */etc/xen/ESA.hvm.cfg* and */etc/xen/ESA.pv.cfg*.

```
# xm info
# dd if=/dev/zero of=/etc/xen/ESA.img bs=1 count=1 seek=15G
# xm create -c /etc/xen/ESA.hvm.cfg
... Install machine... configure PVM ...
# xm shutdown ESA
# xm create -c /etc/xen/ESA.pv.cfg
```

6.4.4 Paravirtualization FAQ and Troubleshooting

This section lists some Paravirtualization Frequently Asked Questions and Answers.

Frequently Asked Questions	Answers
Why are XenTools not provided with the appliance?	In addition to the distribution issues, the XenTools depends on the exact version of your XenServer.
I cannot boot the virtual machine in PVM mode.	<p>Ensure that no CD/DVD (ISO image) is inserted to the machine. Eject all CD/DVDs, and then reboot.</p> <p>Make sure that PVM is enabled on the hypervisor itself.</p> <p>For more information about PVM, refer to section Manual Configuration of Xen Server.</p> <p>The last resort would be to use a Live-CD, for example, Knoppix, in order modify the appliance files.</p>
I cannot initialize High-Availability.	Probably you have installed the XenTools but you have not rebooted the system after the XenTools installation. Reboot the system and retry.
I need to set up a cloned virtual machine as soon as possible.	<p>Currently cloning a virtual appliance is a risk which is not recommended.</p> <p>Perform the following steps. 1. 2.</p> <ol style="list-style-type: none"> 1. Clone a machine. 2. Log onto to the cloned machine. 3. Modify the hostname and the IP address. 4. Manually execute the following scripts: <pre><code>#/etc/opt/scripts/first-boot/5_mk_ssh_keys.sh #/etc/opt/scripts/first-boot/ 5_mk_web_certificate.sh</code></pre>
After switching to PVM mode, I cannot use the XenCenter.	Close the XenCenter and open a new instance.



Chapter 7

Appliance Hardening

- [7.1 Linux Kernel](#)
- [7.2 Restricted Logins](#)
- [7.3 Enhanced Logging](#)
- [7.4 Open Listening Ports](#)
- [7.5 Configuring User Limits](#)
- [7.6 Packages and Services](#)

The Protegrity Appliance provides the framework for its appliance-based products. The base Operating System (OS) used for Protegrity Appliances is 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 management. Linux is widely accepted as the preferred base OS for many customized solutions, such as in firewalls and embedded systems, among others.

Linux was selected for the following reasons:

- **Open Source:** Linux is an Open Source solution.
- **Stable:** The OS is a stable platform due to its R&D and QA cycles.
- **Customizable:** The OS can be customized up to a high level.
- **Proven system:** The OS has already been proven in many production environments and systems.

For a list of installed components, refer to the *Contractual.htm* document available in the appliance Web UI under **Settings > System > Files** pane.

Protegrity takes several measures to harden this Linux-based system and make it more secure. For example, many non-essential packages and components are removed. If you want to install external packages on the appliances, the packages must be certified by Protegrity.

For more information about installing external packages, contact *Protegrity Support*.

The following additional hardening measures are described in this section:

- Linux Kernel
- Restricted Logins
- Enhances Logging
- Open Listening TCP Ports
- Packages and Services

7.1 Linux Kernel

The appliance kernels are optimized for hardening. The Protegity appliances are currently equipped with a modular patched Linux Kernel version 4.19.304. These kernel are patched to enhance some capabilities as well as optimize it for server-side usage. Standard server-side features such as scheduler and TCP settings are available.

7.2 Restricted Logins

Every Protegity Appliance is equipped with an internal LDAP directory service, OpenLDAP. Appliances may use this internal LDAP for authentication, or an external one.

The ESA Server provides directory services to all the other appliances. However, to avoid single point of failure you can use multiple directory services.

Four users are predefined and available after the appliance is installed. Unlike in standard Linux, the root user is blocked from and cannot access the system without permission from the admin user. The admin user cannot access the Linux Shell Console without permission from the root user. This design provides extra security to ensure that in order to perform any OS-related or security-related operations (for example, High Availability, upgrade, and patches) both root and admin users must cooperate. The same design applies to SSH connectivity.

The main characteristics of the four users are described here.

root user

- Local OS user
- By default, can only access machine's console
- All other access requires additional *admin* user login to ensure isolation of duties
- If required, then login using SSH can be allowed, which is blocked by default
- No Web UI access

admin user

- LDAP directory management user
- Usually this user is the Chief Security Officer
- Can access and manage Web UI or CLI menu using machine's console or SSH
- Can create additional users
- If required, then root user login for OS related activities can be allowed

viewer user

- LDAP directory user
- By default, has read-only access to Appliance features
- Can access Web UI and CLI menu using machine's console or SSH but cannot modify settings/server

local_admin user

- Local OS user
- Emergency or maintenance user with limited *admin user* permission
- Handles cases where the directory server is not accessible
- By default, has SSH and Web UI blocked, and only machine's console is accessible

The appliance login design facilitates appliance hardening. The following two OS users are defined:

- root: The standard system administrator user
- local_admin: Administrative OS user for maintenance (in case the LDAP is not accessible)

By default, has SSH and Web UI blocked, and only machine's console is accessible

These are the basic login rules:

- The root user will never be able to login directly.
- The admin user can connect to the CLI Manager (locally or through SSH).
- A root shell can be accessed from within the admin CLI Manager.

7.3 Enhanced Logging

The logging capabilities are enhanced for appliance hardening. In addition to the standard OS logs or syslogs that are available by default, many other operations are logged as well.

Logs that are considered important are sent to the Protegity ESA logging facility, which can be local or remote. This means that in addition to the standard syslog repository, Protegity provides a secured repository for important system logs.

You can find these events from within the logs that are escalated to the ESA logging facility:

- System startup logs
- Protegity product or service is started or stopped
- System backup and restore operations
- High Availability events
- User logins
- Configuration changes

7.4 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 Protegity appliances.

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

Table 7-1: 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 be configured for the system users to access Insight.

Table 7-2: Ports for Insight Users

Port Number	Protocol	Source	Destination	NIC	Description
22	TCP	System User	Insight	Management NIC (ethMNG)	Access to CLI Manager

Port Number	Protocol	Source	Destination	NIC	Description
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 7-3: 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)	<ul style="list-style-type: none"> Downloading certificates and policies from ESA Sending audit logs from the protectors to ESA 	
6379	TCP	ESA	BDP Lead Node	Management NIC (ethMNG)	Communication between ESA and BDP lead node.	<p>If HDFSFP is used, this port must be opened.</p> <p>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.</p> <p>Note: If a port other than 6379 is configured while installing BDP, ensure that the configured port is open.</p>
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 7-4: 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 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



Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
						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 7-5: 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



Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
						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 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 7-6: 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 7-7: Ports for Communication with ESA

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
22	TCP	ESA	DSG	Management NIC (ethMNG)	<ul style="list-style-type: none"> Replication or Rulesets from DSG to ESA DSG Patching from ESA 	



Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
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)	<ul style="list-style-type: none"> 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)	<p>Messages sent from DSG to ESA</p> <p>This port is required to support backward compatibility, where ESA v7.2.1 communicates with the earlier versions of appliances other than ESA.</p> <p>For example, port 5671 is required for user notifications from a DSG system to appear on the ESA v7.2.1 Dashboard.</p>	
10100	UDP	DSG	ESA	Management NIC (ethMNG)	<ul style="list-style-type: none"> Establishing communication with ESA Communication in TAC 	<p>This port is optional. If the appliance heartbeat services are stopped, this port can be disabled.</p>

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

Table 7-8: 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	



Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
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)	<ul style="list-style-type: none"> 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.
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

Port Number	Protocol	Source	Destination	NIC	Description	Notes (If any)
						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 7-9: 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 7-10: 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 7-11: 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 7-12: 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 <i>td-agent</i> 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 <i>td-agent</i>	This port can be configured according to your use case when forwarding logs to an external Security information and event management (SIEM).

7.5 Configuring User Limits

In Linux, a user utilizes the system resources to perform different operations. When a user with minimal privileges runs operations that use most system resources, it can result in unavailability of resources to other users. This introduces a Denial-of-Service (DoS) attack on the system. To mitigate this attack, you can restrict users or groups utilizing the system resources. For Protegity appliances, using the ulimit functionality, you can limit the number of processes that a user can create.

Note: The ulimit functionality cannot be applied on usernames that contain the space character.

7.6 Packages and Services

Several major components, services, or packages are disabled or removed for appliance hardening. The following table lists the removed packages.

Table 7-13: Removed Objects

Removed Object	Examples
Network Services (except SSH/Apache)	telnet client/server client/server
Package Managers	apt
Additional Packages	Man Pages Documents

Chapter 8

VMware Tools in Appliances

The VMware tools are used access to the utilities that enable you to monitor and improve management of the virtual machines that are part of your environment. The version of VMware tools installed on the appliance is 2:10.3.10-1+deb10u6.

Chapter 9

System Requirements

The compatibility settings for your products to run smoothly are listed in the following table.

Table 9-1: Compatibility of Appliances Components

Component	Compatibility
Application Protocols	HTTP 1.0, HTTP 1.1, SSL/TLS
WebServices	SOAP 1.1 and WSDL 1.1
Web Browsers	Minimum supported Web Browser versions are as follows: <ul style="list-style-type: none">• 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 minimum hardware configuration recommended is as follows:

Hardware Components	Configuration
CPU	Multicore Processor, with minimum 8 CPUs
RAM	32 GB
Hard Disk	320 GB
CPU Architecture	x86

Chapter 10

Increasing the Appliance Disk Size

[10.1 Configuration of Appliance for Adding More Disks](#)

[10.2 Installation of Additional Hard Disks](#)

[10.3 Rolling Back Addition of New Hard Disks](#)

If you need to increase the total disk size of the Appliance, then you can add additional hard disks to the Appliance. The Appliance refers to the added hard disks as logical volumes, or partitions, which offer additional disk capacity.

As required, partitions can be added, removed, or moved from one hard disk to another. It is possible to create smaller partitions on a hard disk and combine multiple hard disks to form a single large partition.

10.1 Configuration of Appliance for Adding More Disks

Hard disks or volumes can be added to the appliance at two different times:

- Add the hard disk during installation of the Appliance.

For more information about adding and configuring the hard disk, refer to the [Protegity Installation Guide 9.1.0.5](#).

- Add the hard disks later when required.

Steps have been separately provided for a single hard disk installation and more than one hard disk installation later in this section.

10.2 Installation of Additional Hard Disks

Before you begin

Ensure that the Appliance is installed and working and the hard disks to be added are readily available.

► To install one or more hard disks:

1. If the Appliance is working, then log out of the Appliance and turn it off.
2. Add the required hard disk.
3. Turn on the appliance.
4. Login to the CLI console with *admin* credentials.
5. Navigate to **Tools > Disk Management**.

6. Search for the new device name, for example, `/dev/sda`, and note down the capacity and the partitions in the device.
7. Select **Refresh**.
The system recognizes any added hard disks.
8. Select **Extend** to add more hard disks to the existing disk size.
9. Select the newly added hard disk.
10. Click **Extend** again to confirm that the newly added hard disk has been added to the Appliance disk size.
A dialog appears asking for confirmation with the following message.
Warning! All data on the /dev/sda will be removed! Press YES to continue...
11. Select **Continue**.
The newly added hard disk is added to the existing disk size of the Appliance.
12. Navigate to **Tools > Disk Management**.
The following screen appears confirming addition of the hard disk to the Appliance disk size.

Summary			
Device: /dev/nvme0n1 29GiB			
Partition	Type	VG	Details
/dev/nvme0n1	LVM2_member	PTYVG_DATA	[<29.00GiB]
Device: /dev/nvme1n1 60GiB			
Partition	Type	VG	Details
/dev/nvme1n1p1	ARTUUID="3ff66a37-01"	N/A	
/dev/nvme1n1p2	ARTUUID="3ff66a37-02"	PTYVG	[16.09GiB]
/dev/nvme1n1p3	ARTUUID="3ff66a37-03"	PTYVG_DATA	[<13.51GiB]
/dev/nvme1n1p4	ARTUUID="3ff66a37-04"	PTYVG_DATA	[<30.00GiB]
/dev/nvme1n1	dos	N/A	
No additional disks found.			
Refresh		< Exit >	

Figure 10-1: Disk Addition Confirmation Screen

10.3 Rolling Back Addition of New Hard Disks

If the Appliance has been upgraded, then roll back to the setup of the previous version is possible. Roll back option is unavailable if you have upgraded your system to Appliance v8.0.0 and have not finalized the upgrade. When you finalize the upgrade, you confirm that the system is functional. Only then the rolling back feature becomes available.

For more information about upgrade, refer to the [Protegility Upgrade Guide 9.1.0.5](#).

Chapter 11

Extending the Size of the OS Partition

[11.1 Starting in Single User Mode](#)

[11.2 Creating a Partition](#)

[11.3 Extending the OS and the Backup Volume](#)

[11.4 Extending the Logs Volume](#)

Depending on the requirements, you can extend the size of the partitions in a physical volume to accommodate all the logs and other appliance related data. You can utilize the Logical Volume Manager (LVM) to increase the partitions in the physical volume. Using LVM, you can manage hard disk storage to allocate, mirror, or resize volumes.

In an appliance, the physical volume is divided into the following three logical volume groups:

Table 11-1: Logical Volumes

Partition	Description
Boot	Contains the boot information
PTYVG	Contains the files and information about OS and logs
Data Volume Group	Contains the data that in the /opt directory

The PTYVG volume partition contains the OS information. You must increase the PTYVG volume group to extend the root partition. The following table describes the different logical volumes in the PTYVG volume group.

Table 11-2: PTYVG Volume Partition

Logical Volume	Description	Default Size
OS	The root partition	8 GB
OS-bak	The backup for the root partition	8 GB
LOGS	The logs that are in the /var/log directory	6 GB
SWAP	The swap partition	8 GB

The following table illustrates the partitioning of all the logical volume groups in a single hard disk system.

Table 11-3: Partition of Logical Volume Groups

Partition	Partition Name	Physical Volume	Volume Group	Directory	Directory Path	Size
/dev/sda	sda1	Physical Volume 1	PTYVG		/boot	400M
	sda2			OS	/	8G
				OS_bak		8G
				logs	/var/log	6G
	sda3	Physical Volume 2	PTYVG_DATA	opt		50% of rest



Partition	Partition Name	Physical Volume	Volume Group	Directory	Directory Path	Size
				opt_bak		50% of rest

As shown in the table, the boot partition contains information for 400 MB. The *PTYVG* partition uses 24.1 GB of hard disk space to store information about the OS and the logs. The remaining partition is allotted for the data volume group.

Note:

For Cloud-based platforms, the *OS_bak* directory is not available in the data volume group. The data in the *PTYVG* partition is available in the *OS* directory only.

For Cloud-based platforms, the *opt_bak* directory is not available in the data volume group. The data in the *PTYVG_DATA* partition is available in the *opt* directory only.

If multiple hard disks installed on an appliance, then you can select the required hard disks for configuring the OS volume and the data volume. You can also, extend the OS partition or the disk partition across the hard disks that are installed on the appliance.

The following table illustrates an example of partitioning in multiple hard disks.

Table 11-4: Partitioning in Multiple Hard Drives

Partition	Partition Name	Physical Volume	Volume Group	Directory	Directory Path	Size
/dev/sda	sda1				/boot	400M
	sda2	Physical Volume 1	PTYVG	OS	/	8G
				OS_bak		8G
				logs	/var/log	6G
				swap	[SWAP]	2.1G
	sda3	Physical Volume 2	PTYVG_DATA	opt		50% of rest
				opt_bak		50% of rest

Partition	Physical Volume	Volume Group	Directory	Directory Path	Size
/dev/sdb	Physical Volume 1	PTYVG_DATA	opt	/opt	50%
			opt_bak		50%

Note:

For Cloud-based platforms, the *OS_bak* directory is not available in the data volume group. The data in the *PTYVG* partition is available in the *OS* directory only.

For Cloud-based platforms, the *opt_bak* directory is not available in the data volume group. The data in the *PTYVG_DATA* partition is available in the *opt* directory only.

The hard disk, *sda*, contains the partitions for the root and the *PTYVG* volumes. The hard disk, *sdb* contains the partition for the data volume group.

The following sections describe the procedures to extend the OS partition.

Note: Before extending the OS partition, it is recommended to back up your appliance. It ensures that you can roll back your changes in case of an error.



When you add a new hard disk to the partition, you should restart the system. This ensures that all the hard disks appear.

Caution: For the Cloud-based platforms, the names of the hard disks may get updated after restarting the system. Ensure that you verify the names of the hard disks before proceeding further.

11.1 Starting in Single User Mode

You must load in the Single User Mode to change the kernel command line.

Note:

For Cloud-based platforms, the *Single User Mode* is unavailable. It is recommended to perform the following operations from the OS Console. While performing these operations, ensure that the system is accessible by only a single user.

► To boot into Single User Mode:

1. Install a new hard disk on the appliance.
For more information about installing a new hard disk, refer to section [Increasing the Appliance Disk Size](#).
2. Boot the appliance in *Single User Mode*.
3. If the GRUB Credentials are enabled, the screen to enter the GRUB credentials appears. Enter the credentials and press **ENTER**.

The following screen appears.



4. Select **Normal** and press **E**.
The following screen appears.



GNU GRUB version [REDACTED]

```
setparams 'Normal'
load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
linux /generic-4.19.200-bzImage.img root=/dev/mapper/PTYVG-OS dolvm quiet
t apic=off net.ifnames=0 ipv6.disable=1 apparmor=1 security=apparmor audit=1 audit_backlog_limit=8192
initrd /generic-4.19.200-initrd.img
```

PROTEGRITY

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.

5. Select the *linux/generic* line and append <SPACE>**S** to the end of the line as shown in the following figure.



GNU GRUB version [REDACTED]

```
setparams 'Normal'
load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
linux /generic-4.19.200-bzImage.img root=/dev/mapper/PTYVG-OS dolvm quiet
t apic=off net.ifnames=0 ipv6.disable=1 apparmor=1 security=apparmor audit=1 audit_backlog_limit=8192 S_ ←
initrd /generic-4.19.200-initrd.img
```

PROTEGRITY

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.

6. Press **F10** to restart the appliance.

After the appliance is restarted, a prompt to enter the root password appears.

7. Enter the root password and press **ENTER**.

11.2 Creating a Partition

After editing the kernel command line, you must create the required partitions.

The following procedure describes how to create a partition on a new hard disk, *sdb*. You can add multiple hard disks to the appliance.

Note: If you add multiple hard disks to the appliance, then the devices are created as */dev/sdb*, */dev/sdc*, */dev/sdd*, and so on. You can select the required hard disk based on the storage space available.

Note: For Cloud-based platforms, the names of the hard disk might differ. Based on the cloud platform, the hard disk names may appear as *nvme1n1*, *xvdb*, or so on.

► To create a partition:

1. Run the following command to list the hard disks that are available.

`lsblk`

2. Run the following command to format the partition.

`fdisk /dev/sdb`

3. Type *o* to create a partition table and press **ENTER**.

4. Type *n* to create a new partition and press **ENTER**.

5. Type *p* to create a primary partition and press **ENTER**.

6. In the following prompt, assign a partition number to the new partition.

If you want to enter the default number for the partition, then press **ENTER**.

7. Type the required starting partition sector for the partition.

If you want to enter the default sector for the partition, then press **ENTER**.

8. Type the last sector for the partition and press **ENTER**.

If you want to enter the default sector for the partition, then press **ENTER**.

9. Type *t* to change the type of the new partition and press **ENTER**.

10. Type *8e* to convert the disk partition to Linux LVM and press **ENTER**.

11. Type *w* to save the changes and press **ENTER**.

A message *The partition table has been altered!* appears.

12. Run the following command to initialize the disk partition that is used with LVM.

`pvcreate /dev/sdb1`

Note: For Cloud-based platforms, you should use the name of the disk partition only. For instance, if the name of the hard disk on the Cloud-based platform is *nvme0n1*, then run the following command to initialize the disk partition that is used with LVM.

`pvcreate /dev/nvme0n1`

If the following confirmation message appears, then press *y*.

```
WARNING: dos signature detected on /dev/sdb1 at offset 510. Wipe it? [y/n]: y
```

A message *Physical volume “/dev/sdb1” is created successfully created appears.*

13. Run the following command to extend the PTYVG volume.



```
vgextend PTYVG /dev/sdb1
```

A message *Volume group “PTYVG” successfully extended* appears.

11.3 Extending the OS and the Backup Volume

After extending the PTYVG volume you can resize the OS and the OS_bak volumes using the *lvextend* and *resize* commands.

Before you begin

Ensure that you consider the following points before extending the partitions in the PTYVG volume group:

- Back up the OS partition before extending the partition
- Back up the policy, LDAP, and other required data to the /opt directory before extending the volume.

The following procedure describes how to extend the *OS* and the *OS_bak* volumes by 4 GB.

Note:

Ensure that there is enough free space available while extending the size of the OS, the OS_bak, and the log volumes. For instance, if you extend the hard disk by 1 GB and if the space is less than the required level, then the following error arrears.

```
Insufficient free space: 1024 extents needed, but only 1023 available
```

To resolve this error, you must increase the partition size by 0.9 GB.

► To create a partition:

1. Run the following commands to extend the *OS-bak* and *OS* volume.

```
# lvextend -L +4G /dev/PTYVG/OS_bak
```

A message *Logical Volume OS_bak successfully resized* appears.

2. Run the following command to resize the file system in the *OS_bak* volume.

```
# resize2fs /dev/mapper/PTYVG-OS_bak
```

A message *resize2fs: On-Line resizing finished successfully* appears.

3. Run the following commands to extend the *OS* volume.

```
# lvextend -L +4G /dev/PTYVG/OS
```

A message *Logical Volume OS successfully resized* appears.

4. Run the following command to resize the file system in the *OS* volume.

```
# resize2fs /dev/mapper/PTYVG-OS
```

A message *resize2fs: On-Line resizing finished successfully* appears.

5. Restart the appliance.

Note: Ensure that you extend the size of the *OS* and the *OS_bak* volumes to the same value.

11.4 Extending the Logs Volume

You can resize the logs volumes using the *lwestend* and *resize* commands. This ensures that you provision the required space for the logs that are generated. You must back up the current logs to the */opt* directory before extending the logs volume.

Before you begin

Before extending the logs volume, ensure that you start the appliance in Single User Mode and create a partition.

For more information about Single User Mode, refer to section [Starting in Single User Mode](#).

For more information about creating a partition, refer to section [Creating a Partition](#).

The following procedure describes how to extend the *logs* volume by 4 GB.

► To extend the logs volume:

1. Run the following commands to create a temporary folder in the */opt* directory.

```
# mkdir /opt/tmp/logs
```

2. Run the following command to copy the files from the logs volume to the */opt* directory.

```
# /usr/bin/rsync -axzHS --delete-before /var/log/ /opt/tmp/logs/
```

Note: While copying the logs from the */var/log* directory to the */opt* directory, ensure that the space available in the */opt* directory is more than the size of the logs.

3. Run the following commands to extend the logs volume.

```
# lwestend -L +4G /dev/PTYVG/logs
```

A message *Logical Volume logs successfully resized* appears.

4. Run the following command to resize the file system in the logs volume.

```
# resize2fs /dev/mapper/PTYVG-logs
```

A message *resize2fs: On-Line resizing finished successfully* appears.

5. Run the following command to copy the files from */opt* directory to the logs volume.

```
# /usr/bin/rsync -axzHS --delete-before /opt/tmp/logs/ /var/log/
```

6. Run the following command to remove the temporary folder created in the */opt* directory.

```
# rm -r /opt/tmp/logs
```

7. Restart the appliance.

Chapter 12

Mandatory Access Control (MAC)

[12.1 Viewing Status of Profiles](#)

[12.2 Creating a Profile](#)

[12.3 Setting a Profile on Complain Mode](#)

[12.4 Setting a Profile on Enforce Mode](#)

[12.5 Analyzing Events](#)

[12.6 Modifying an Existing Profile](#)

[12.7 AppArmor Permissions](#)

[12.8 Troubleshooting for AppArmor](#)

Mandatory Access Control (MAC) is a security approach that allows or denies an individual to access resources in a system. With MAC, you can set policies that can be enforced on the resources. The policies are defined by the administrator and cannot be overridden by other users.

Among many implementations of MAC, Application Armor (AppArmor) is a CIS recommended Linux security module that protects the operating system and its applications from threats. It implements MAC for constraining the ability of a process or user on the operating system resources.

AppArmor allows you to define policies for protecting the executable files and directories present in the system. It applies these policies to the profiles. Profiles are groups, where restriction on specific actions for the files or directories are defined. The following are the two modes of applying policies on profiles:

- **Enforce:** The profiles are monitored to either permit or deny a specific action.
- **Complain:** The profiles are monitored, but actions are not restricted. Instead, actions are logged in the audit events.

For more information about AppArmor, refer to the following link.

<http://wiki.apparmor.net>

AppArmor in Protegity appliances

AppArmor increases security by restricting actions on the executable files in the system. It is added as another layer of security to protect custom scripts and prevent information leaks in case of any security breach. On the Protegity appliances, AppArmor is enabled to protect the different OS features, such as, antivirus, firewall, scheduled tasks, trusted appliances cluster, proxy authentication, and so on. Separate profiles are created for the appliance-specific features. For more information about the list of profiles, refer to [Viewing profiles](#). In an unprecedented case of a security breach on the appliances, any attempt to modify the protected profiles are foiled by AppArmor. The logs for the denials are generated and appear under system logs where they can be [analyzed](#).

After AppArmor is enabled, all profiles that are defined in it are protected. Although it is enabled, if a new executable script is introduced in the appliance, AppArmor does not automatically protect this script. For every new script or file to be protected, a separate AppArmor profile must be *created* and permissions must be assigned to it.

The following sections describe the various tasks that you can perform on the Protegity appliances using AppArmor.

12.1 Viewing Status of Profiles

Using the **aa-status** command, AppArmor loads and displays all the profiles that are configured in the system. It displays all the profiles that are in *enforce* and *complain* modes.

► To view the status for the profiles:

1. Login to the CLI Manager of the appliance.
2. Navigate to **Administration > OS Console**.
3. Run the status command as follows:

aa-status

The screen with the list of all profiles appears.

```
root@protegity-esas66:/var/www# aa-status
apparmor module is loaded.
76 profiles are loaded.
76 profiles are in enforce mode.
/etc/opt/2FA/2fa.sh
/etc/opt/2FA/qrencode
/etc/opt/2FA/web_help.html
/etc/opt/AntiVirus/AntiVirus
/etc/opt/AntiVirus/config.xml
/etc/opt/AntiVirus/history.xml
/etc/opt/AntiVirus/menu_av.py
/etc/opt/Cluster/clusterConnection.pyc
/etc/opt/Cluster/clusterFileConfig.pyc
/etc/opt/Cluster/clusterFileManager.pyc
/etc/opt/Cluster/clusterLog.pyc
/etc/opt/Cluster/clusterMenu.pyc
/etc/opt/Cluster/cluster_config.status.xml
/etc/opt/Cluster/cluster_config.xml
/etc/opt/Cluster/cluster_helper
/etc/opt/Cluster/clustermgr.pyc
/etc/opt/Cluster/commands.xml
/etc/opt/Cluster/root_scripts/cluster_task.py
/etc/opt/Cluster/root_scripts/cluster_tasks.pyc
/etc/opt/Cluster/root_scripts/disable_cluster_as_root.sh
/etc/opt/Cluster/root_scripts/enable_cluster_as_root.sh
/etc/opt/Cluster/root_scripts/network_summary.sh
/etc/opt/Cluster/root_scripts/top_cpu.sh
/etc/opt/Cluster/root_scripts/top_mem.sh
/etc/opt/Firewall/firewall.py
/etc/opt/Firewall/firewall_help.txt
/etc/opt/Firewall/menu.py
```

Figure 12-1: Profiles

12.2 Creating a Profile

In addition to the existing profiles in the appliances, AppArmor allows creating profiles for other executable files present in the system. Using the `aa-genprof` command, you can create a profile to protect a file. When this command is run, AppArmor loads that file in *complain* mode and provides an option to analyze all the activities that might arise. It learns about all the activities that are present in the file and suggests the permissions that can be applied on them. After the permissions are assigned to the file, the profile is created and set in the *enforce* mode.

As an example, consider an executable file `apparmor_example.sh` in your system for which you want to create a profile. The script is copied in the `/etc/opt` directory and contains the following actions:

- Creating a file `sample1.txt` in the `/etc/opt` directory
- Changing permissions for the `sample1.txt` file
- Removing `sample1.txt` file

Note:

Ensure that `apparmor_example.sh` file has a `755` permission set to it.

The following steps describe how to generate a profile for the `apparmor_example.sh` file.

► To create a profile:

1. Login to the CLI Manager of the appliance.
2. Navigate to **Administration > OS Console**.
3. Navigate to the `/etc/opt` directory.
4. Run the following command to view the commands in the `apparmor_example.sh` file.

`cat apparmor_example.sh`

The following commands appear.

```
#!/bin/bash
touch /etc/opt/sample1.txt
chmod 400 /etc/opt/sample1.txt
rm /etc/opt/sample1.txt
```

5. Replicate the SSH session. Navigate to the OS Console and run the following command

`aa-genprof /etc/opt/apparmor_example.sh`

The following screen appears.

```
Writing updated profile for /etc/opt/apparmor_example.sh.
Setting /etc/opt/apparmor_example.sh to complain mode.

Before you begin, you may wish to check if a
profile already exists for the application you
wish to confine. See the following wiki page for
more information:
http://wiki.apparmor.net/index.php/Profiles

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

Profiling: /etc/opt/apparmor_example.sh

[(S)can system log for AppArmor events] / (F)inish
```

Figure 12-2: Loading AppArmor

- Switch to the first SSH session and run the following script.

```
./apparmor_example.sh
```

The commands are run successfully.

- Switch to the second SSH session. Type **S** to scan and create a profile for the *apparmor_example.sh* file.

AppArmor reads the first command. It provides different *permissions* based on what the command does, and assigns a severity to it.

```
Profile: /etc/opt/apparmor_example.sh
Execute: /bin/touch
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X) ix On / (D)eny / Abo(r)t / (F)inish
```

- Type **I** to assign the inherit *permissions*.

- After selecting the option for the first command, AppArmor reads each action and provides a list of *permissions* for each action. Type the required character that needs to be assigned for the *permissions*.

- Type **F** to finish the scanning and **S** to save the change to the profile.

The following message appears.

```
Setting /etc/opt/apparmor_example.sh to enforce mode.

Reloaded AppArmor profiles in enforce mode.

Please consider contributing your new profile!
See the following wiki page for more information:
http://wiki.apparmor.net/index.php/Profiles

Finished generating profile for /etc/opt/apparmor_example.sh.
```

- Restart the AppArmor service using the following command.

```
/etc/init.d/apparmor restart
```

- Navigate to the */etc/apparmor.d* directory to view the profile.

The profile appears as follows.

```
etc.opt.apparmor_example.sh
```

12.3 Setting a Profile on Complain Mode

For easing the restrictions applied to the a profile, you can apply the *complain* mode on it. AppArmor allows actions to be performed, but logs all the activities that occur for that profile. AppArmor provides the ***aa-complain*** command to perform this task. The following task describe the steps to set the *apparmor_example.sh* file in the *complain* mode.

► To set a profile in complain mode:

1. Login to the CLI Manager of the appliance.
2. Navigate to **Administration > OS Console**.
3. Run the enforce command as follows:

```
aa-complain /etc/apparmor.d/etc.opt.apparmor_example.sh
```

4. Run the ***./apparmor_example.sh*** script.
5. Navigate to the */var/log/syslog* directory to view the logs.

The logs display that, even though an event has certain restriction, AppArmor allowed it to occur and has logged it for the *apparmor_example.sh* script.

```
May 5 23:25:18 protegrity-es544 /usr/local/sbin/LogInfo: Shell #60572: User root executed "./apparmor_example.sh" exitcode=0
May 5 23:25:17 protegrity-es544 kernel: audit: type=1400 audit(1588701317.779:151): apparmor="ALLOWED" operation="open" profile="/etc/opt/apparmor_example.sh" name="/etc/op
tr" pid=25506 comm="ls" requested_mask="r" denied_mask="r" fsuid=0 ouid=0
May 5 23:25:17 protegrity-es544 kernel: audit: type=1400 audit(1588701317.779:150): apparmor="ALLOWED" operation="open" profile="/etc/opt/apparmor_example.sh" name="/dev/tt
y" pid=25504 comm="apparmor_exampl" requested_mask="wr" denied_mask="wr" fsuid=0 ouid=0
May 5 23:25:13 protegrity-es544 /usr/local/sbin/LogInfo: Shell #60572: User root executed "vi apparmor_example.sh" exitcode=0
```

Figure 12-3: Logs in Complain Mode

12.4 Setting a Profile on Enforce Mode

When the appliance is installed in your system, the *enforce* mode is applied on the profiles by default. If you want to add a profile in *enforce* mode, AppArmor provides the ***aa-enforce*** command to perform this task. The following task describe the steps to set the *apparmor_example.sh* file in the *enforce* mode.

► To set a profile in enforce mode:

1. Login to the CLI Manager of the appliance.
2. Navigate to **Administration > OS Console**.
3. Run the enforce command as follows:

```
aa-enforce /etc/apparmor.d/etc.opt.apparmor_example.sh
```

4. Run the ***./apparmor_example.sh*** script.

Based on the permissions that are assigned while creating the profile for the script, the following message is displayed on the screen.

```
root@protegrity-esa544:/etc/opt# ./apparmor_example2.sh
touch: cannot touch '/etc/opt/sample1.txt': Permission denied
chmod: cannot access '/etc/opt/sample1.txt': No such file or directory
rm: cannot remove '/etc/opt/sample1.txt': No such file or directory
root@protegrity-esa544:/etc/opt#
```

Figure 12-4: Enforce Mode

Note:

The *Deny* permission is assigned to all the commands in this script.

12.5 Analyzing Events

AppArmor provides an interactive tool to analyze the events occurring in the system. The [**aa-logprof**](#) is one such utility that scans the logs for the events in your system. The [**aa-logprof**](#) command scans the logs and provides a set actions for modifying a profile.

Consider the *apparmor_example.sh* script that is in the *enforce* mode. After a certain period of time, you modify the script and insert a command to list all the files in the directory. When you run the *apparmor_example.sh* script, a *Permission denied* error appears on the screen. As a new command is added to this script and *permissions* are not assigned to the updated entry, AppArmor does not allow the script to run. The permissions must be assigned before the script is executed. To evaluate the permissions that can be applied to the new entries, you can view the logs for details. On the appliance CLI Manager, the logs are available in the *audit.log* file in the */var/log*/directory. The following figure displays the logs that appear for the *apparmor_example.sh* script.

```
2 /etc/init.d/appliance-queues-server: {"origin": {"time_utc": 1589365539, "ip": "2.10.1.6", "hostname": "protegrity-esa982"}, "level": "Low", "process": {"version": "7.2.2.1832", "name": "ESAPAP"}, "logtype": "System", "client": {"ip": "2.10.1.6"}, "additional_info": {"description": "2020-05-13T15:55:39.780595+05:30 protegrity-esa982 audispd: node=protegrity-esa982 type=AVC msg=audit(1589365539.770:5582): apparmor=\\DENIED\\ operation=\"open\" profile=\"/etc/opt/apparmor_example.sh\\\" name=\"\\'/etc/opt/\\'\" pid=2568 comm=\"\\ls\\\" requested_mask=\"r\" denied_mask=\"r\" fsuid=0 ouid=0", "title": "Apppliance Warning:2020-05-13T15:55:39.780595+05:30 protegrity-esa982 audispd: node=protegrity-esa982 type=AVC msg=audit(1589...\"}}
```

Figure 12-5: System Logs

In the figure, the logs describe the profile for *apparmor_example.sh*. The logs contain the following information:

- AppArmor has denied an *open* operation for the profile that contains a new command.
- The script does not have access to */dev/tty* directory with the *requested_mask="r"* permission as it is not defined for the new command.

Thus, the logs provide an insight on the different operations that occur when the script is executed. After analyzing the logs and evaluating the permissions, you can run the [**aa-logprof**](#) command to update the permissions for the script.

Note:

The changes that are applied on the profiles are audited and logs are generated for it. For more information about the audit logs, refer to System Auditing

Important:

It is not recommended to use the [**aa-logprof**](#) command for profiles defined by Protegrity. If you want to modify an existing profile, refer to [Modifying an existing Profile](#).

► To update profile permissions:

1. Login to the CLI Manager of the appliance.
2. Navigate to **Administration > OS Console**.
3. Run the ***aa-logprof*** command.

```
Reading log entries from /var/log/syslog.
Updating AppArmor profiles in /etc/apparmor.d.
Complain-mode changes:

Profile: /etc/opt/apparmor_examples.sh
Path: /bin/rm
Old Mode: r
New Mode: mr
Severity: unknown

[1 - /bin/rm mr,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audit(t) /
Abo(r)t / (F)inish
```

4. Type the required permissions. Type **F** to finish scanning.
5. After the permissions are granted, the following screen appears.

```
= Changed Local Profiles =
The following local profiles were changed. Would you like to save them?

[1 - /etc/opt/apparmor_examples.sh]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean
profiles / Abo(r)t
```

6. Type **S** to save the changes.
7. Navigate to the **/etc/apparmor.d** directory to view the profile.

12.6 Modifying an Existing Profile

In an appliance, Protegility provides a **default set of profiles** for the appliance-specific features. These include profiles for Two-factor authentication, Antivirus, TAC, Networking, and so on. The profiles contain appropriate permissions that require the feature to run smoothly without compromising its security. However, access-denial logs for some permissions may appear when these features are run. This calls for modifying the profile of a feature by appending the permissions to it.

Consider the ***usr.sbin.apache2*** profile that is related to the networking services. When this feature is executed, based on the permissions that are defined, AppArmor allows to run the required operations. If it encounters a new action on this profile, it generates a **Denied** error and halts the task from proceeding.

For example, the following log appears for the ***usr.sbin.apache2*** profile after the host name of the system is changed from the **Networking** screen on the CLI Manager.

```
type=AVC msg=audit(1593004864.290:2492): apparmor="DENIED" operation="exec"
profile="/usr/sbin/apache2" name="/sbin/ethtool" pid=32518 comm="sh"
requested_mask="x" denied_mask="x" fsuid=0 ouid=0FSUID="root" OUID="root"
```

As described in the log, AppArmor denied an execute permission for this profile. Every time you change the host name from the CLI manager, AppArmor will not permit the operation to be performed. This can be mitigated by modifying the profile from the **/etc/apparmor.d/custom** directory. Thus, the additional permission must be added to the ***usr.sbin.apache2*** profile that is present in the **/etc/apparmor.d/custom** directory. This ensures that the new permissions to the profile are considered and existing

permissions are not overwritten when the feature is executed. If you get a permission error log on the **Appliance Logs** screen, then perform the following steps to update the *usr.sbin.apache2* profile with a new permission.

Note:

The following steps are also applicable for permission denial logs that appear for other default profiles provided by Protegity. Based on the permissions that are denied, update the respective profiles with the new operations.

► To update profile permissions:

1. On the CLI Manager, navigate to **Administration > OS Console**.
2. Navigate to the */etc/apparmor.d/custom* directory.
3. Open the required profile on the editor.
For example, open the *usr.sbin.apache2* profile in the editor.
4. Add the following permission.

```
<Value in the name parameter of the denial log> rix,
```

For example, the command for *usr.sbin.apache2* denial log is as follows.

```
/sbin/ethtool rix,
```

5. Save the changes and exit the editor.
6. Run the following command to update the changes to the AppArmor profile.

```
apparmor_parser -r /etc/apparmor.d/<Profile>
```

For example,

```
apparmor_parser -r /etc/apparmor.d/usr.sbin.apache2
```

7. Now, change the host name of the system from the CLI Manager. The denial logs are not observed.

12.7 AppArmor Permissions

The following table describes the different permissions that AppArmor lists when creating a profile or analyzing events.

Table 12-1: AppArmor Permissions

Permission	Description
(I)nherit	Inherit the permissions from the parent profile
(A)llow	Allow access to a path
(I)gnore	Ignore the prompt
(D)eny	Deny access to a path
(N)ew	Create a new profile
(G)lob	Select a specific path or create a general rule using wild cards that match a broader set of paths
Glob with (E)xtension	Modify the original directory path while retaining the filename extension
(C)hild	Creates a rule in a profile, requires a sub-profile to be created in the parent profile, and rules must be separately generated for this child



Permission	Description
Abo(r)	Exit AppArmor without saving the changes
(F)inish	Finish scanning for the profile
(S)ave	Save the changes for the profile

12.8 Troubleshooting for AppArmor

The following table describes solutions to issues that you might encounter while using AppArmor.

Table 12-2: AppArmor Troubleshooting

Issue	Reason	Solution
After you run the File Export or File Import operation in the appliance, the following message appears in the logs:	<pre>type=AVC msg=audit(1594813145.658:730 6): apparmor="DENIED" operation="exec" profile="/usr/sbin/apache2" name="/usr/lib/sftp-server" pid=58379 comm="bash" requested_mask="x" * denied_mask="x" *fsuid=0 ouid=0FSUID="root" OUID="root"</pre>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> On the CLI Manager, navigate to Administration > OS Console Navigate to the <i>/etc/apparmor.d/custom</i> directory. Edit the <i>usr.sbin.apache2</i> profile. Insert the following line. <code>/usr/lib/sftp-server rix,</code> Restart the AppArmor service using the following command. <code>/etc/init.d/apparmor restart</code>
If a scheduler task containing a customized script is run, then the scheduled task is not executed and a denial message appears in the log. For example, if a task scheduler contains the <i>/demo.sh</i> script in the command line, the following message appears in the logs.	<pre>type=AVC msg=audit(1598429205.615:352 53): apparmor="DENIED" operation="exec" profile="/usr/sbin/apache2" name="/demo.sh" pid=32684 comm=".taskV5FLVl.tmp" requested_mask="x" denied_mask="x" fsuid=0 ouid=0FSUID="root" OUID="root"</pre>	<p>AppArmor restricts running any custom scripts from the scheduled task</p> <p>Perform the following steps.</p> <ol style="list-style-type: none"> On the CLI Manager, navigate to Administration > OS Console Navigate to the <i>/etc/apparmor.d/custom</i> directory. Edit the <i>usr.sbin.apache2</i> profile. Insert the following line. <code>/demo.sh rix,</code> Restart the AppArmor service using the following command. <code>/etc/init.d/apparmor restart</code>
If you run the Put Files operation between two machines in a TAC, the following messages appear as logs in the source and target appliances.	<p>Source appliance</p> <pre>type=AVC msg=audit(1598288495.530:516 8): apparmor="DENIED" operation="mknod" profile="/etc/opt/Cluster/ cluster_helper" name="/ dummyfilefortest.sh" pid=62621</pre>	<p>Perform the following steps.</p> <ol style="list-style-type: none"> On the CLI Manager, navigate to Administration > OS Console Navigate to the <i>/etc/apparmor.d/custom</i> directory. Edit the <i>etc.opt.Cluster.cluster_helper</i> profile. Insert the following line on the source appliance <code>/<filename> cix,</code>



Issue	Reason	Solution
<pre>comm="mv" requested_mask="c" denied_mask="c" fsuid=0 ouid=0FSUID="root" OUID="root"</pre> <p>Target appliance</p> <pre>type=AVC msg=audit(1598288495.950:211 6): apparmor="DENIED" operation="chown" profile="/etc/opt/Cluster/ cluster_helper" name="/ dummyfilefortest.sh" pid=17413 comm="chown" requested_mask="w" denied_mask="w" fsuid=0 ouid=0FSUID="root" OUID="root"</pre>		<p>5. Insert the following line on the target appliance</p> <pre style="background-color: #f0f0f0; padding: 5px;">/<filename> wix,</pre> <p>6. Restart the AppArmor service on the source and target appliances using the following command:</p> <pre style="background-color: #f0f0f0; padding: 5px;">/etc/init.d/apparmor restart</pre>

Chapter 13

Accessing Appliances using Single Sign-On (SSO)

[13.1 What is Kerberos](#)

[13.2 What is SAML](#)

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/>

13.1 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).

13.1.1 Implementing Kerberos SSO for Protegity Appliances

In the Protegity 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 Protegity appliances, only Microsoft AD is supported.

13.1.1.1 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).

13.1.1.2 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 Protegity appliances.

Table 13-1: 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

13.1.1.2.1 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](#).
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](#).
8. Assign the role with the SSO Login permissions to the required users.

13.1.1.2.2 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 Protegility, 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 Protegility appliances, only Microsoft AD is supported.

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

13.1.1.2.3 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
```

13.1.1.2.4 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.

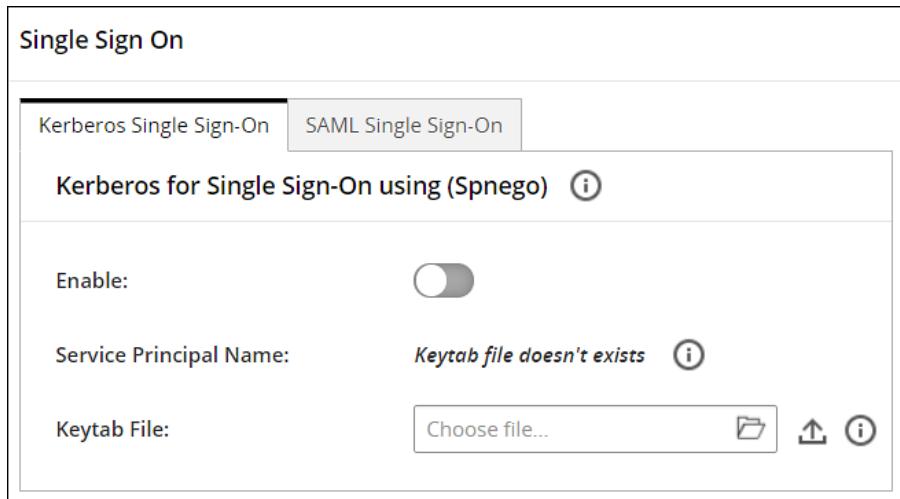


Figure 13-1: Uploading Keytab

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.

13.1.1.2.5 Configuring SPNEGO Authentication on the Web Browser

Before implementing Kerberos SSO for Protegity 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.

13.1.1.2.5.1 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.

13.1.1.2.5.2 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.

13.1.1.3 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.

13.1.1.4 Scenarios for Implementing Kerberos SSO

This section describes the different scenarios for implementing Kerberos SSO.

13.1.1.4.1 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.

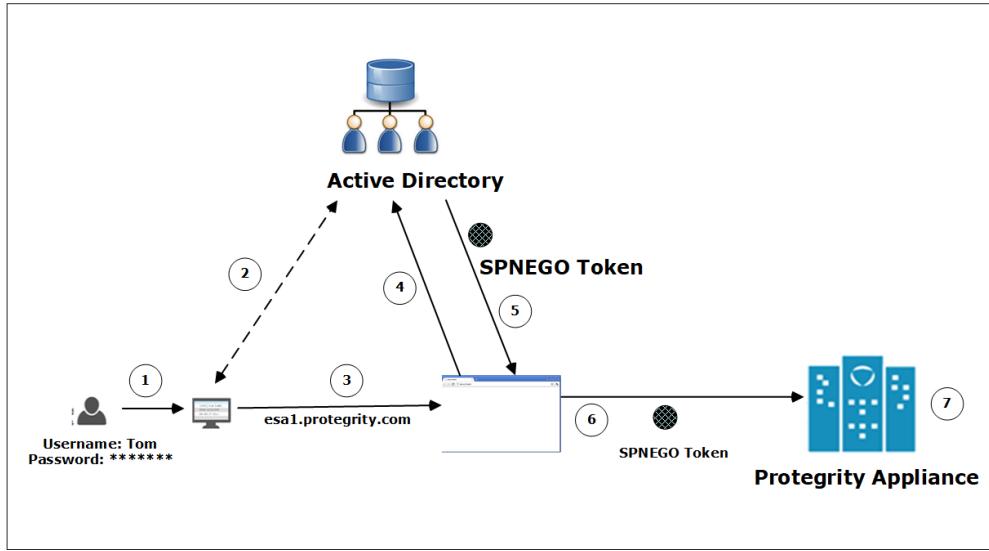


Figure 13-2: SSO Implementation

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.protegity.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.

13.1.1.4.2 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.

13.1.1.4.2.1 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.

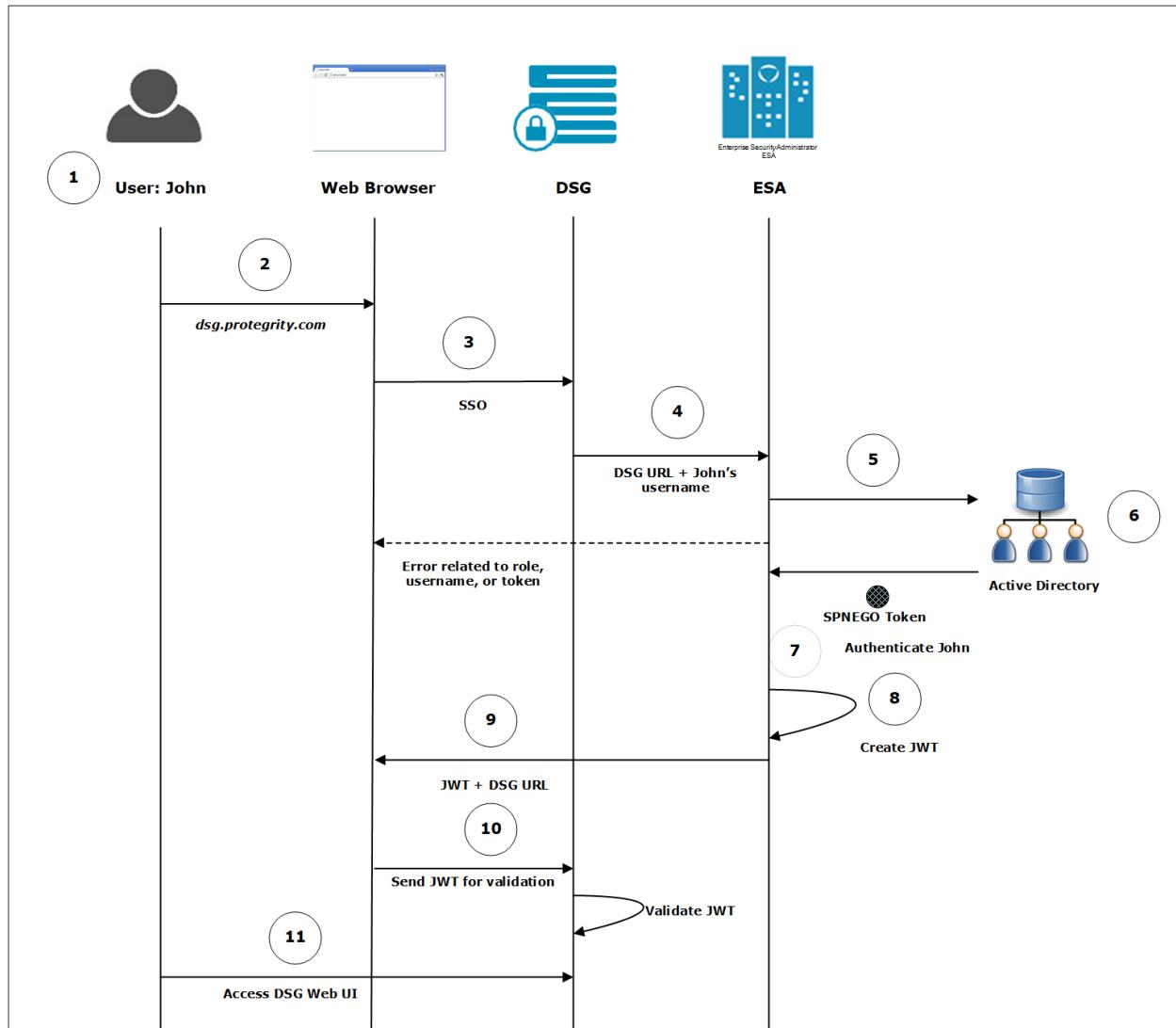


Figure 13-3: SSO with External LDAP

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.protegity.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 [Protegity 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 [Protegity Data Security Gateway User Guide 3.1.0.5](#).

13.1.1.4.2.1.1 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**.

- On the **Data to import** tab, select **Appliance JWT Configuration**, and click **Next**.

Note:

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

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

13.1.1.4.3 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.

- Import users from an external directory* on the $L1$ and $L2$ and assign SSO login permissions.
- Ensure that the FQDN is resolved to the IP address of the load balancer.
- Configure SPN* for the load balancer.
- Create and upload* the keytab file on $L1$ and $L2$.
- 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.

13.1.1.5 Viewing Logs

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

The screenshot shows a web-based log viewer titled "Enterprise-Security-Administrator - Event Logs". At the top, there is a message "New logs will appear on top ①" and a timestamp "Server Time: Wed, Oct 13 2021 17:08:58 +0530GMT". Below this are several log entries:

- Oct 13 17:00:56 protegility-esa726 /mod_wsgi: User admin logged into the web-interface from [REDACTED]
- Oct 13 16:52:33 protegility-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 protegility-esa726 /mod_wsgi: Reset web session timeout (web-user 'admin' , IP: ' [REDACTED] ')
- Oct 13 16:23:45 protegility-esa726 /mod_wsgi: User admin logged into the web-interface from [REDACTED]
- Oct 13 16:23:32 protegility-esa726 CLI: [INFO] User admin (web/local user) logged-out from the CLI-Manager
- Oct 13 16:19:11 protegility-esa726 CLI: [INFO] User admin (web/local user) logged-in to the CLI-Manager

At the bottom of the interface, there are buttons for "Print", "Download", "Refresh", "Save a copy", and a red "Purge log" button.

Figure 13-4: Appliance Logs

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

13.1.1.6 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.

13.1.1.7 Troubleshooting

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

Table 13-2: 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 configured 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.	<ul style="list-style-type: none"> 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 	<p>Ensure that the following points are considered:</p> <ul style="list-style-type: none"> The user is imported to the internal LDAP. Role assigned to the user has SSO Login permission enabled. <p>For more information about configuring user role, refer to section Importing Users and assigning role.</p>
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.
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 <i>Service not available</i> message appears on the Web browser.	<ul style="list-style-type: none"> Active Directory is not reachable Appliance on which the LDAP services are utilized is not reachable 	<p>Ensure the following points are considered:</p> <ul style="list-style-type: none"> The active directory is up and running. The appliance on which the LDAP services are utilized is up and running.

13.2 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:** A file containing information for connecting an SP to an IdP

13.2.1 Implementing SAML SSO for Protegity Appliances

In the Protegity 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.

13.2.2 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)

13.2.3 Setting up SAML SSO

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

Table 13-3: 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.	<ul style="list-style-type: none"> • Adding Users • Adding Roles <p>Note: For more information, refer to section <i>Adding Users to Internal LDAP and Managing Roles</i> in the <i>Protegity Appliances Overview Guide 9.1.0.5</i>.</p>
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.	Configuring Service Provider (SP) Settings
3	Appliance Web UI	Provide the metadata information that is generated on the IdP.	Configuring IdP Settings



13.2.3.1 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.

13.2.3.2 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.

13.2.4 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

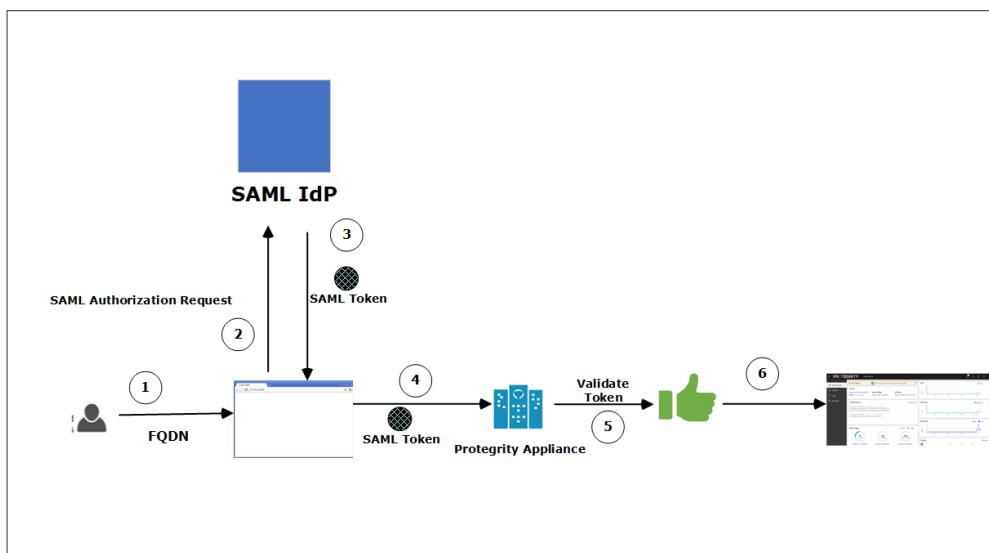


Figure 13-5: SAML SSO Workflow

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

For example, the user enters `esa.protegity.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.

13.2.5 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.

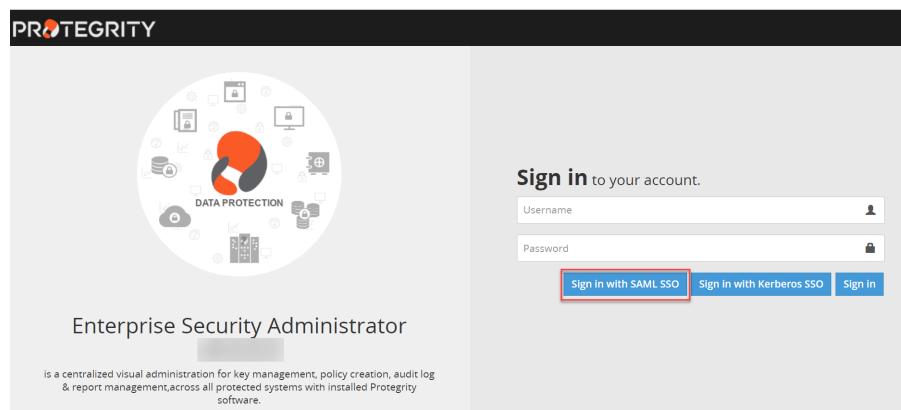


Figure 13-6: Login Screen

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.

13.2.6 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.protegity.com*.

- On the Azure IdP, perform the following steps to retrieve the entity ID and metadata.
 - 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/>.
 - 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*
 - 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

- 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.

- 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**.
- 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**.
- Select the **Enable** option to enable SAML SSO.
- If you want to allow access to User Management screen, enable the **Access User Management screen** option.
- Log out from ESA.
- Open a new Web browser session. Log in to the Azure portal as *Sam* with the IdP credentials.
- 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.

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

13.2.7 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.

13.2.8 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.

The screenshot shows a web-based log viewer titled "Enterprise-Security-Administrator - Event Logs". At the top, there is a message "New logs will appear on top" with a help icon. To the right, the server time is displayed as "Wed, Oct 13 2021 17:08:58 +0530GMT". Below the header are several buttons: "Current Event Log" (dropdown), "Print", "Download", "Refresh", "Save a copy", and a red "Purge log" button. The main area contains a list of log entries with timestamps and log messages. Some log entries contain redacted IP addresses.

Timestamp	Log Message
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 13-7: Appliance Logs

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

13.2.9 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.
- 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.

13.2.10 Troubleshooting

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

Table 13-4: SAML SSO Troubleshooting

Issue	Reason	Solution
<p>The following message appears while logging in with SSO.</p> <p style="background-color: #e0e0e0; padding: 5px;">Login Failure: Unauthorized to SSO Login.</p>	<ul style="list-style-type: none"> • 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 • 	<p>Ensure that the following points are considered:</p> <ul style="list-style-type: none"> • The user is imported to the internal LDAP. • The role assigned to the user has SSO Login permission enabled. <p>For more information about configuring user role, refer to section Importing Users and assigning role.</p>

Chapter 14

Appendix: Sample External Directory Configurations

- [14.1 Sample AD configuration](#)
- [14.2 Sample ODSEE configuration](#)
- [14.3 Sample SAML Configuration](#)
- [14.4 Sample Kerberos Configuration](#)
- [14.5 Sample Azure AD Configuration](#)

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 describe the parameters that you must configure to connect with an external directory.

14.1 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.

14.2 Sample ODSEE configuration

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

Note:

Protegility 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.

14.3 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/4b1c35a8-5a82-4cb4-9b03-7b818fa58cf/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:



14.4 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>.keytab`

14.5 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`

Appendix

Installing Protegrity Appliances on Cloud Platforms

[15.1 Installing Protegrity Appliances on Amazon Web Services \(AWS\)](#)

[15.2 Installing Protegrity Appliances on Azure](#)

[15.3 Installing Protegrity Appliances on Google Cloud Platform \(GCP\)](#)

This section describes the procedure for installing appliances on cloud platforms, such as, Amazon Web Services (AWS), Google Cloud Platform (GCP), and Azure.

Appendix A

Installing Protegility Appliances on Amazon Web Services (AWS)

[15.1.1 Verifying Prerequisites](#)

[15.1.2 Obtaining the AMI](#)

[15.1.3 Loading the Protegility Appliance from an Amazon Machine Image \(AMI\)](#)

[15.1.4 Backing up and Restoring Data on AWS](#)

[15.1.5 Increasing Disk Space on the Appliance](#)

[15.1.6 Best Practices for Using Protegility Appliances on AWS](#)

[15.1.7 Running the Appliance-Rotation-Tool](#)

[15.1.8 Working with Cloud-based Applications](#)

Amazon Web Services (AWS) is a cloud-based computing service, which provides several services, such as computing power through Amazon Elastic Compute Cloud (EC2), storage through Amazon Simple Storage Service (S3), and so on.

The AWS stores Amazon Machine Images (AMIs), which are templates or virtual images containing an operating system, applications, and configuration settings.

Protegility appliances offer flexibility and can run in the following environments:

- **On-premise:** The appliance is installed and runs on dedicated hardware.
- **Virtualized:** The appliance is installed and runs on a virtual machine.
- **Cloud:** The appliance is installed and runs on or as part of a Cloud-based service.

Protegility provides AMIs that contain the appliance image, running on a customized and hardened Linux distribution.

This section describes the prerequisites and tasks for installing Protegility appliances on AWS. In addition, it describes some best practices for using the Protegility appliances on AWS effectively.

Caution:

The *Full OS Backup/Restore* features of the Protegility appliances is not available on the AWS platform.

15.1.1 Verifying Prerequisites

This section describes the prerequisites including the hardware, software, and network requirements for installing and using Protegility appliances on AWS.

15.1.1.1 Prerequisites

The following prerequisites are essential to install the Protegility appliances on AWS:

- Login URL for the AWS account
- AWS account with the authentication credentials
- Access to the *My.Protegility* portal

15.1.1.2 Hardware Requirements

As the Protegility appliances are hosted and run on AWS, the hardware requirements are dependent on the configurations provided by Amazon. However, these requirements can autoscale as per customer requirements and budget. The following table lists the minimum hardware requirements and the equivalent configuration option that is available on AWS.

Table -1:

Appliance	CPU	Memory	Disk Size	Number of network interfaces
DSG	4 cores	16 GB	64 GB	2
ESA	8 cores	32 GB	320 GB	1

The minimum recommendation for an appliance is 8 CPU cores and 32 GB memory. Based on this hardware requirement, select the required configuration for creating an AWS instance.

15.1.1.3 Network Requirements

The Protegility appliances on AWS are provided with an Amazon Virtual Private Cloud (VPC) networking environment. The Amazon VPC enables you to access other AWS resources, such as other instances of Protegility appliances on AWS.

You can configure the Amazon VPC by specifying its usable IP address range. You can also create and configure subnets, network gateways, and the security settings.

For more information about the Amazon VPC, refer to the Amazon VPC documentation at: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html.

If you are using the ESA or the DSG appliance with AWS, then ensure that the inbound and outbound ports of the appliances are configured in the Amazon Virtual Private Cloud (VPC), as described in this section, to ensure that they are able to interact with the other required components.

For more information about the list of inbound and outbound ports to be configured based on the appliance, refer to section [Open Listening Ports](#) [Open Listening Ports](#).

15.1.1.3.1 Accessing the Internet

The following points list the ways in which you can provide or limit Internet access for an appliance instance in the VPC:

- If you need to connect the appliance to the Internet, then ensure that the appliance is on the default subnet so that it uses the Internet gateway that is included in the VPC.

- If you need to allow the appliance to initiate outbound connections to, and prevent inbound connections from the Internet, then ensure that you use a Network Address Translation (NAT) device.
- If you want to block the connection of the appliance to the Internet, then ensure that the appliance is on a private subnet.

15.1.1.3.2 Accessing a Corporate Network

If you need to connect the appliance to a corporate network, then ensure that you use an IPSec hardware VPN connection.

15.1.2 Obtaining the AMI

Before creating the instance on AWS, you must obtain the image from the [My.Protegility](#) portal. On the portal, you select the required ESA version and choose AWS as the target cloud platform. You then share the product to your cloud account. The following steps describe how to share the AMI to your cloud account.

To obtain and share the AMI:

1. Log in to the [My.Protegility](#) portal with your user account.
2. Click **Product Management > Explore Products > Data Protection**.
3. Select the required ESA Platform Version.

The **Product Family** table will update based on the selected ESA Platform Version.

Note: The ESA Platform Versions listed in the drop-down menu reflect all versions that were either previously downloaded or shipped within the organization along with any newer versions available thereafter. You can check the list of products previously downloaded from **Product Management > My Product Inventory**.

4. Select the **Product Family**.
The description box will populate with the **Product Family** details.
5. Click **View Products** to advance to the **Product List** screen.

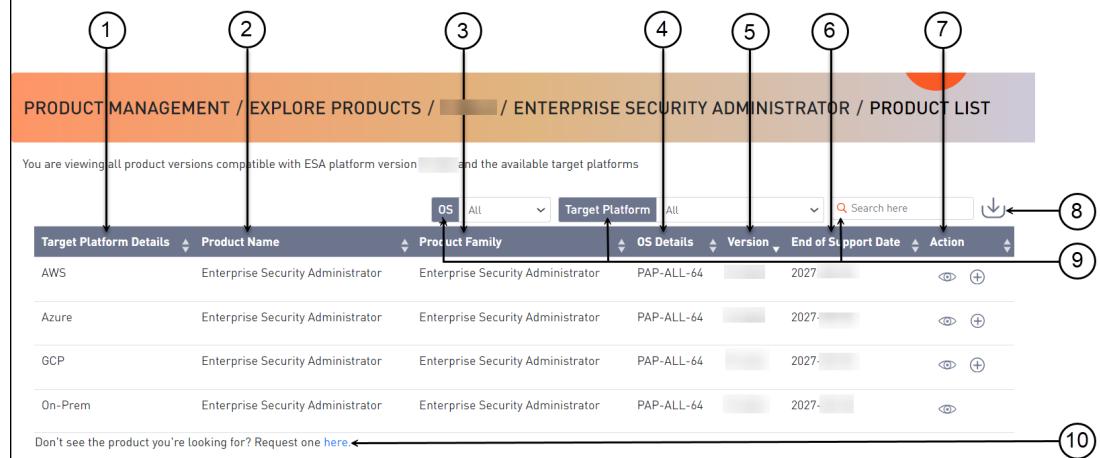


Figure -1: Product List Screen

Table -2: Product List Screen Description

Callout	Element Name	Description
1	Target Platform Details	Shows details about the target platform.
2	Product Name	Shows the product name.

Callout	Element Name	Description
3	Product Family	Shows the product family name.
4	OS Details	Shows the operating system name.
5	Version	Shows the product version.
6	End of Support Date	Shows the final date that Protegility will provide support for the product.
7	Action	Click the View icon () to open the Product Detail screen.
8	Export as CSV	Downloads a .csv file with the results displayed on the screen.
9	Search Criteria	Type text in the search field to specify the search filter criteria or filter the entries using the following options: <ul style="list-style-type: none"> • OS • Target Platform
10	Request one here	Opens the Create Certification screen for a certification request.

6. Select the AWS cloud target platform you require and click the **View** icon () from the **Action** column. The **Product Detail** screen appears.

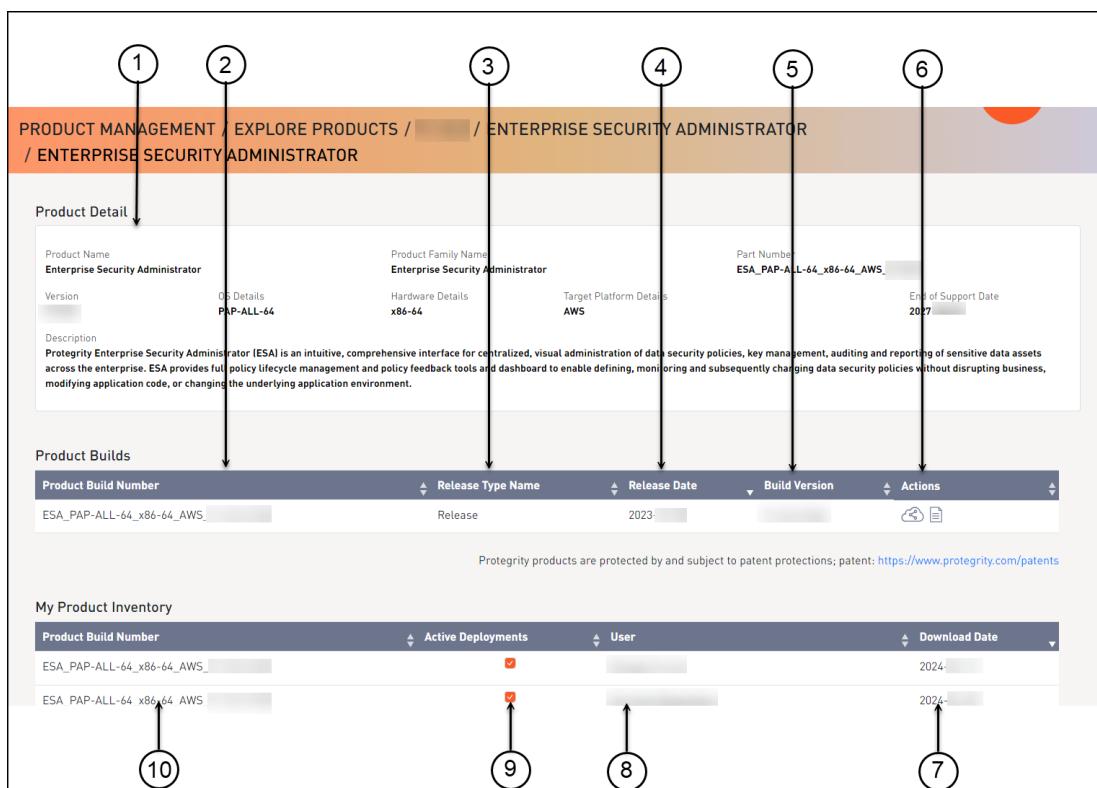


Figure -2: Product Detail Screen

Table -3: Product Details Screen Description

Callout	Element Name	Description
1	Product Detail	Shows the following information about the product: <ul style="list-style-type: none"> • Product name • Family name • Part number • Version • OS details • Hardware details

Callout	Element Name	Description
		<ul style="list-style-type: none"> • Target platform details • End of support date • Description
2	Product Build Number	Shows the product build number.
3	Release Type Name	Shows the type of build, such as, release, hotfix, or patch.
4	Release Date	Shows the release date for the build.
5	Build Version	Shows the build version.
6	Actions	<p>Shows the following options for download:</p> <ul style="list-style-type: none"> • Click the Share Product icon () to share the product through the cloud. • Click the Download Signature icon () to download the product signature file. • Click the Download Readme icon () to download the Release Notes.
7	Download Date	Shows the date when the file was downloaded.
8	User	Shows the user name who downloaded the build.
9	Active Deployment	<p>Select the check box to mark the software as active. Clear the check box to mark the software as inactive.</p> <p>Note: This option is available only after you download a product.</p>
10	Product Build Number	Shows the product build number.

7. Click the **Share Product** icon () to share the desired cloud product.

Note:

If the user does not have access to cloud products or has access to cloud products and the Customer Cloud Account details are not available, then a message appears with the information that is required and the contact information for obtaining access to cloud share.

A dialog box appears and your available cloud accounts will be displayed.

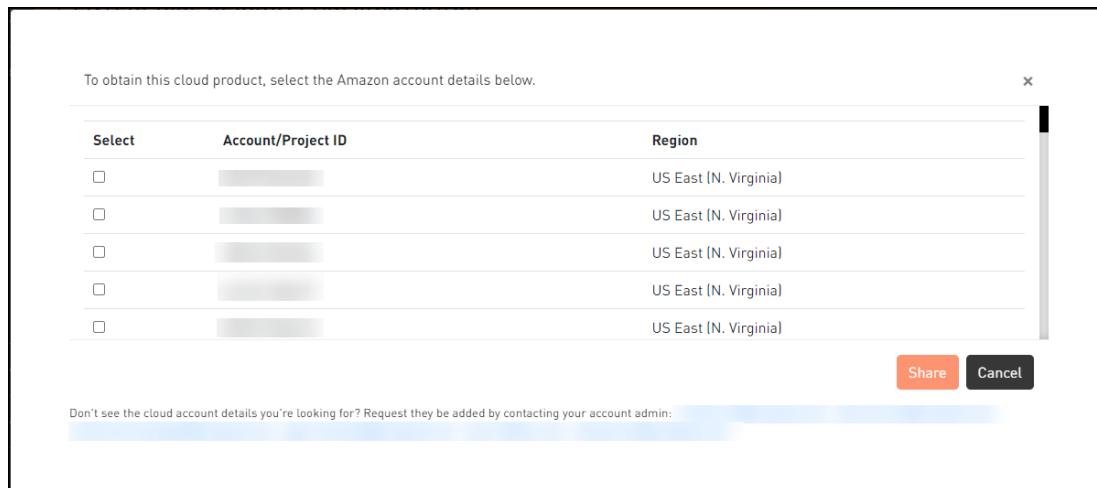


Figure -3: Account Selection Screen

8. Select your required cloud account in which to share the Protegility product.
9. Click **Share**.

A message box is displayed with the command line interface (CLI) instructions with the option to download a detailed PDF containing the cloud web interface instructions. Additionally, the instructions for sharing the cloud product are sent to your registered email address and to your notification inbox in [My.Protegility](#).

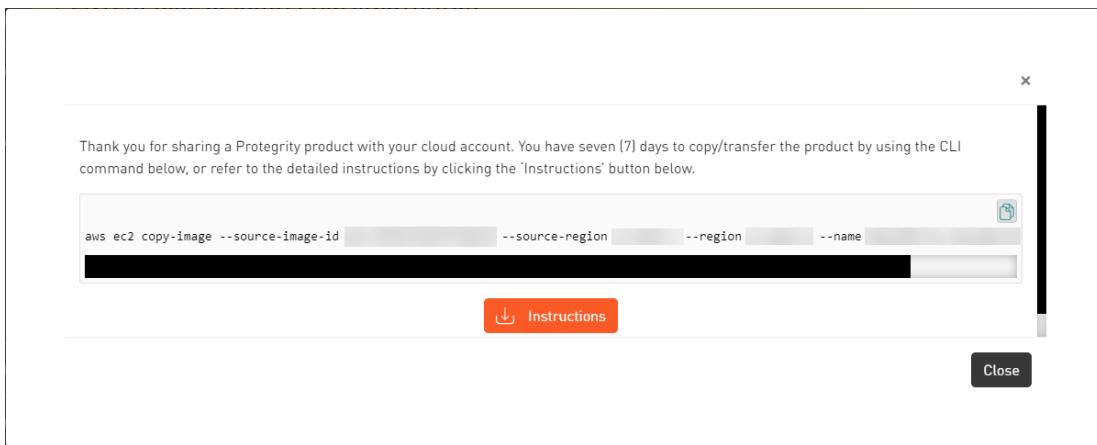


Figure -4: Sharing Command

10. Click the **Copy** icon () to copy the command for sharing the cloud product and run the command in CLI. Alternatively, click **Instructions** to download the detailed PDF instructions for cloud sharing using the CLI or the web interface.

Note:

The cloud sharing instruction file is saved in a `.pdf` format. You need a reader, such as, Acrobat Reader to view the file.

The Cloud Product will be shared with your cloud account for seven (7) days from the original share date in the [My.Protegility](#) portal.

After the seven (7) day time period, you need to request a new share of the cloud product through [My.Protegility](#).

15.1.3 Loading the Protegility Appliance from an Amazon Machine Image (AMI)

This section describes the tasks that need to be performed for loading the Protegility appliance from an AMI, which is provided by Protegility.

15.1.3.1 Creating an Instance of the Protegility Appliance from the AMI

Perform the following steps to create an instance of the Protegility appliance using an AMI.

► To create an instance of the Protegility appliance:

1. Access AWS at the following URL:
<https://aws.amazon.com/>
The AWS home screen appears.
2. Click the **Sign In to the Console** button.
The AWS login screen appears.
3. On the AWS login screen, enter the following details:

- Account Number
 - User Name
 - Password
4. Click the **Sign in** button.
- After successful authentication, the AWS Management Console screen appears.
5. Click **Services**.
6. Navigate to **Compute > EC2**
- The EC2 Dashboard screen appears.
7. Contact Protegity Support and provide your Amazon Account Number so that the required Protegity AMIs can be made accessible to the account.
8. Click on **AMIs** under the Images section.
- The AMIs that are accessible to the user account appear in the right pane.
9. Select the AMI of the required Protegity appliance in the right pane.
10. Click the **Launch** button to launch the selected Protegity appliance.
- The Choose an Instance screen appears.
11. Depending on the performance requirements, choose the required instance type.
For the ESA appliance, an instance with 32 GB RAM is recommended.
12. If you need to configure the details of the instance, then click the **Next: Configure Instance Details** button.
The Configure Instance Details screen appears.
13. Specify the following parameters on the Configure Instance Details screen:
- **Number of Instances:** The number of instances that you want to launch at a time.
 - **Purchasing option:** The option to request Spot instances, which are unused EC2 instances. If you select this option, then you need to specify the maximum price that you are willing to pay for each instance on an hourly basis.
 - **Network:** The VPC to launch the appliance in. If you need to create a VPC, then click the Create new VPC link. For more information about creating a VPC, refer to the section [Configuring VPC](#).
 - **Subnet:** The Subnet to be used to launch the appliance. A subnet resides in one Availability zone.
If you need to create a Subnet, then click the *Create new subnet* link.
- For more information about creating a subnet, refer to the section [Adding a Subnet to the Virtual Private Cloud \(VPC\)](#).
- **Auto-assign Public IP:** The IP address from where your instance can be accessed over the Internet. You need to select Enable from the list.
 - **Availability Zone:** A location within a region that is designed to be isolated from failures in other Availability Zones.
 - **IAM role:** This option is disabled by default.
 - **Shutdown behaviour:** The behaviour of the appliance when an OS-level shut down command is initiated.
 - **Enable Termination Protection:** The option to prevent accidental termination of the appliance instance.
 - **Monitoring:** The option to monitor, collate, and analyze the metrics for the instance of your appliance.
14. If you need to add additional storage to the instance of the appliance, then click the **Next: Add Storage** button.
The Add Storage screen appears.
15. You can provision additional storage for the appliance by clicking the **Add New Volume** button. *Root* is the default volume for your instance.
Alternatively, you can provision additional storage for the appliance later too.
For more information on configuring the additional storage on the instance of the appliance, refer to the section [Increasing Disk Space on the Appliance](#).
16. If you need to create a key-value pair, then click the **Next: Add Tags** button.
The Add Tags screen appears.

Depending on your instance requirements, add the key-value pairs.

17. If you need to configure the Security Group, then click the **Next: Configure Security Group** button.
The Configure Security Group screen appears.
18. You can assign a security group from the available list.
Alternatively, you can create security group with rules for the required inbound and outbound ports.
19. Click the **Review and Launch** button.
The Review Instance Launch screen appears, listing all the details related to the instance of the appliance. You can review the required sections before you launch your instance.
20. Click the **Launch** button.
The Key Pair dialog box appears.
21. Select the **Existing Key Pair** option and choose a key from the list of available key pairs. Alternatively, you can select the **Create a new Key Pair**, to create a new key pair.

Note:

If you proceed without a key pair, then the system will not be accessible.

22. Select the confirmation check box.
23. Click the **Launch Instances** button.
The instance of the required Protegility appliance is launched and the *Launch Status* screen appears.
24. Click the **View Instances** button.
The *Instances* screen appears listing the instance of the appliance.
25. If you need to use the instance of the appliance, then access the appliance CLI Manager using the IP address of the appliance.

15.1.3.2 Configuring the Virtual Private Cloud (VPC)

If you need to connect two Protegility appliances, or to the Internet, or a corporate network using a Private IP address, then you might need to configure the VPC.

For more information about the various inbound and outbound ports to be configured in the VPC, refer to section [Open Listening Ports](#).

Perform the following steps to configure the VPC for the instance of the Protegility appliance.

► To configure the VPC for the Protegility appliance:

1. Ensure that you are logged in to AWS and at the AWS Management Console screen.
2. On the AWS Management Console, click **VPC** under the *Networking* section.
The VPC Dashboard screen appears.
3. Click on **Your VPCs** under the Virtual Private Cloud section.
The Create VPC screen appears listing all available VPCs in the right pane.
4. Click the **Create VPC** button.
The Create VPC dialog box appears.
5. Specify the following parameters on the Create VPC dialog box:
 - **Name tag:** The name of the VPC.

- **CIDR block:** The range of the IP addresses for the VPC in $x.x.x.x/y$ form where $x.x.x.x$ is the IP address and y is the /16 and /28 netmask.
 - **Tenancy:** The tenancy parameter for the VPC, which can be set to *Default* or *Dedicated*. If the value of this parameter is set to *Default*, then it will select the tenancy attribute, which is specified at the launch of the instance of the appliance for the VPC.
6. Click the **Yes, Create** button.
The VPC is created.

15.1.3.3 Adding a Subnet to the Virtual Private Cloud (VPC)

You can add Subnets to your VPC. A subnet resides in an Availability zone. When you create a subnet, you can specify the CIDR block.

Perform the following steps to create the subnet for your VPC.

► To create a Subnet:

1. Ensure that you are logged in to AWS and at the AWS Management Console screen.
2. On the AWS Management Console, click VPC under the Networking section.
The VPC Dashboard screen appears.
3. Click **Subnets** under the Virtual Private Cloud section.
The create subnet screen appears listing all available subnets in the right pane.
4. Click the **Create Subnet** button.
The Create Subnet dialog box appears.
5. Specify the following parameters on the Create Subnet dialog box.
 - **Name tag:** The name for the Subnet.
 - **VPC:** The VPC for which you want to create a subnet.
 - **Availability Zone:** The Availability zone where the subnet resides.
 - **CIDR block:** The range of the IP addresses for the VPC in $x.x.x.x/y$ form where $x.x.x.x$ is the IP address and y is the /16 and /28 netmask.
6. Click the **Yes, Create** button.
The Subnet is created.

15.1.3.4 Finalizing the Installation of Protegility Appliance on the Instance

When you install the appliance, it generates multiple security identifiers such as, keys, certificates, secrets, passwords, and so on. These identifiers ensure that sensitive data is unique between two appliances in a network. When you receive a Protegility appliance image, the identifiers are generated with certain values. If you use the security identifiers without changing their values, then security is compromised and the system might be vulnerable to attacks. Using the **Rotate Appliance OS Keys**, you can randomize the values of these security identifiers for an appliance. During the finalization process, you run the key rotation tool to secure your appliance.

Note:

If you do not complete the finalization process, then some features of the appliance may not be functional including the Web UI.

For example, if the OS keys are not rotated, then you might not be able to add appliances to a Trusted Appliances Cluster (TAC).

Note:

For information about the default passwords, refer to the section *Launching the ESA instance on Amazon Web Services* in the *Release Notes 9.0.0.0*.

15.1.3.4.1 Logging in and Finalising the AWS Instance using the SSH Client

After installing the Protegility Appliance on AWS, you must log in to the AWS instance using the SSH Client.

► To login to the AWS instance using the SSH Client:

1. Start the local SSH Client.
2. Perform the SSH operation on the AWS instance using the key pair utilizing the following command.

```
ssh -i <path of the private key pair> local_admin@<IP address of the AWS instance>
```

Note:

Ensure that you use the *local_admin* user to perform the SSH operation.

3. Press **Enter**.

The following screen appears.

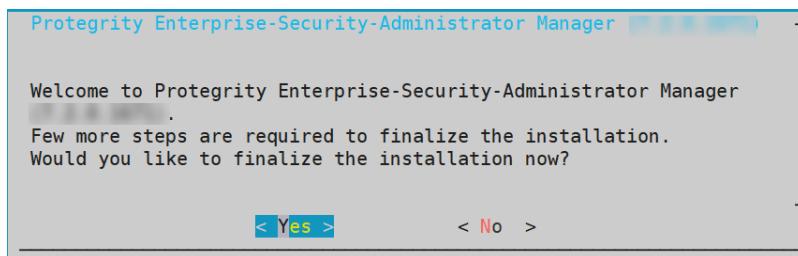


Figure -5: Finalizing Installation Confirmation screen

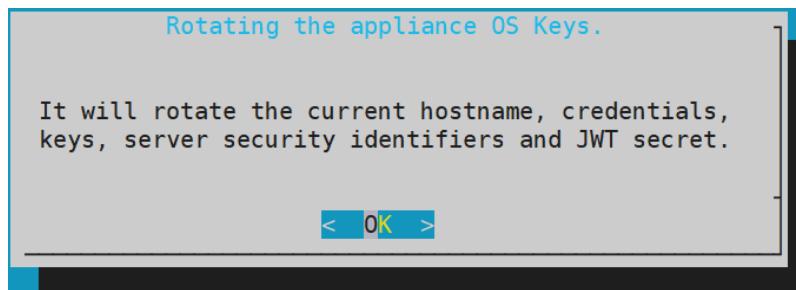
Caution:

Ensure that the finalization process is initiated from a single session only. If you start finalization simultaneously from a different session, then the "*Finalization is already in progress.*" message appears. You must wait until the finalization of the instance is successfully completed.

Additionally, ensure that the appliance session is not interrupted. If the session is interrupted, then the instance becomes unstable and the finalization process is not completed on that instance.

4. Select **Yes** to initiate the finalization process.

A confirmation screen to rotate the appliance OS keys appears.

**Note:**

If you select **No** in the **Finalizing Installation Confirmation** screen in Step 3, then the finalization process is not initiated.

To manually initiate the finalization process, navigate to **Tools > Finalize Installation** and press **ENTER**.

5. Select **OK** to rotate the appliance OS keys.

The following screen appears.

User's Passwords	
Please provide user's passwords	
root password	[Redacted]
root password verification	[Redacted]
admin password	[Redacted]
admin password verification	[Redacted]
viewer password	[Redacted]
viewer password verification	[Redacted]
local_admin password	[Redacted]
local_admin password verification	[Redacted]

<Apply> **<Help >**

- To update the user passwords, provide the credentials for the following users:

- root
- admin
- viewer
- local_admin

- Select **Apply**.

The user passwords are updated and the appliance OS keys are rotated.

The finalization process is completed.

Note: The *SSH Authentication Type* by default, is set to *Publickey*. Ensure that you use the *Password + Publickey* for accessing the CLI. You can change the authentication type from the ESA Web UI, once the finalization is completed.

Note:

The appliance comes with some products installed by default. If you want to verify the installed products or install additional products, then navigate to **Administration > -- Installations and Patches -- > Add/Remove Services**.

For more information about installing products, refer to the section *Installing Products* in the [Protegility Installation Guide 9.1.0.5](#).

15.1.3.5 Connecting to an ESA instance (for DSG deployment)

If you are using an instance of the DSG appliance, then you need to provide the connectivity details related to an instance of the ESA appliance in the DSG appliance using the CLI Manager.

Note:

Ensure that you run the *Appliance-rotation-tool* on the ESA before you setup the communication of the DSG appliance with the ESA appliance.

For more information about running the Appliance-rotation-tool on the ESA, refer to section [Running the Appliance-Rotation-Tool](#).

For more information about connecting to an instance of the ESA appliance, refer to the section *Setting up ESA Communication* in the [Protegility Data Security Gateway User Guide 3.1.0.5](#).

15.1.3.5.1 Deploying the Instance of the Protegility Appliance with the Protectors

You can configure the various protectors that are a part of the Protegility Data Security Platform with the instance of the ESA appliance running on AWS.

Depending on the Cloud-based environment which hosts the protectors, the protectors can be configured with the instance of the ESA appliance in one of the following ways:

- If the protectors are running on the same VPC as the instance of the ESA appliance, then the protectors need to be configured using the internal IP address of the appliance within the VPC.
- If the protectors are running on a different VPC than that of the instance of the ESA appliance, then the VPC of the instance of the ESA needs to be configured to connect to the VPC of the protectors.

15.1.4 Backing up and Restoring Data on AWS

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup or restore information in case of failures.

15.1.4.1 Creating a Snapshot of a Volume on AWS

In AWS, you can create a snapshot of a volume by performing the following steps:

► To create a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Volumes** under the Elastic Block Store section.
The screen with all the volumes appears.

2. Right click on the required volume and select **Create Snapshot**.
The **Create Snapshot** screen for the selected volume appears.
3. Enter the required description for the snapshot in the **Description** text box.
4. Select **click to add a Name tag** to add a tag.
5. Enter the tag in the **Key** and **Value** text boxes.
6. Click **Add Tag** to add additional tags.
7. Click **Create Snapshot**.

A message *Create Snapshot Request Succeeded* along with the snapshot id appears.

Note:

Ensure that you note the snapshot id.

Note: Ensure that the status of the snapshot is **Completed**.

15.1.4.2 Restoring a Snapshot on AWS

On AWS, you can restore data by creating a volume of a snapshot. You then attach the volume to an EC2 instance.

Note:

Ensure that the status of the instance is **Stopped**.

Note:

Ensure that you detach an existing volume on the instance.

► To restore a snapshot on AWS:

1. On the EC2 Dashboard screen, click **Snapshots** under the **Elastic Block Store** section.
The screen with all the snapshots appears.
2. Right-click on the required snapshot and select **Create Volume from snapshot**.
The **Create Volume** screen form appears.
3. Select the type of volume from the **Volume Type** drop-down list.
4. Enter the size of the volume in the **Size (GiB)** textbox.
5. Select the availability zone from the **Availability Zone** drop-down list.
6. Click **Add Tag** to add tags.
7. Click **Create Volume**.

A message *Create Volume Request Succeeded* along with the volume id appears. The volume with the snapshot is created.

Note:

Ensure that you note the *volume id*.

8. Under the **EBS** section, click **Volume**.
The screen displaying all the volumes appears.
9. Right-click on the volume that is created.
The pop-up menu appears.
10. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
11. Enter the Instance ID or name of the instance in the **Instance** text box.
12. Enter `/dev/xvda` in the **Device** text box.
13. Click the **Attach** to add the volume to an instance.
The snapshot is added to the EC2 instance as a volume.

15.1.5 Increasing Disk Space on the Appliance

After an instance of the appliance is created, you can increase the disk space on the appliance.

Perform the following steps to increase the disk space for the appliance on AWS.

► To increase disk space for the Appliance on AWS:

1. On the EC2 Dashboard screen, click **Volumes** under the *Elastic Block Store* section.
The Create Volume screen appears.
 2. Click the **Create Volume** button.
The **Create Volume** dialog box appears.
 3. Enter the required size of the additional disk space in the **Size (GiB)** text box.
 4. Enter the snapshot ID of the instance, for which the additional disk space is required in the **Snapshot ID** text box.
 5. Click the **Create** button.
The required additional disk space is created as a volume.
 6. Right-click on the additional disk, which is created.
The pop-up menu appears.
 7. Select **Attach Volume**.
The **Attach Volume** dialog box appears.
 8. Enter the Instance ID or name tag of the appliance to add the disk space in the **Instance** text box.
 9. Click the **Attach** button to add the disk space to the required appliance instance.
The disk space is added to the appliance instance.
 10. After the disk space on the appliance instance is added, navigate to Instances under the *Instances* section.
 11. Right-click on the appliance instance in which the disk space was added.
The popup menu appears.
 12. Select **Instance State > Stop**.
The appliance instance is stopped.
 13. Select **Instance State > Start**.
The appliance instance is started.
 14. After the appliance instance is started, configure the additional storage on the appliance using the CLI Manager on the appliance.
- For more information on configuring the additional storage on the appliance, refer to section [Installation of Additional Hard Disks](#).

15.1.6 Best Practices for Using Protegity Appliances on AWS

The following table lists some best practices for using Protegity appliances on AWS.

Table -4: Best Practices for using Protegity Appliances with AWS

Practice	Description
Force SSH Keys	<p>Configure the appliance to enable SSH keys and disable SSH passwords for all users.</p> <p>If you need to create or join a Trusted Appliance cluster, then ensure that SSH passwords are enabled when you are creating or joining the cluster, and then disabled.</p> <p>For more information about the SSH keys, refer to section Working with Secure Shell (SSH) Keys.</p>
Install Upgrades	<p>After you run the Appliance-rotation tool, it is recommended that you install all the latest Protegity updates .</p>
Configure your VPC or Security Group	<p>To ensure successful communication between the appliance and the other entities connected to it.</p> <p>For more information about the list of inbound and outbound ports for the appliances, refer to section Open Listening Ports.</p>

15.1.7 Running the Appliance-Rotation-Tool

The *Appliance-rotation-tool* modifies the required keys, certificates, credentials, and passwords for the appliance to differentiate the sensitive data on the appliance from other similar instances.

Note:

If you are configuring an ESA appliance instance, then you must run the Appliance-rotation-tool after creating the instance of the appliance.

Note:

Ensure that you do not run the appliance rotation tool when the appliance OS keys are in use.

For example, you must not run the appliance rotation tool when a cluster is enabled, two-factor authentication is enabled, external users are enabled, or there are custom certificates in the Audit Store cluster.

Perform the following steps to rotate the required keys, certificates, credentials, and passwords for the appliance.

► To rotate keys, certificates, credentials, and passwords for the Protegity appliance:

1. On the ESA, navigate to **CLI Manager > Tools > Rotate Appliance OS Keys**.
The root password dialog box appears.

2. Enter the appliance root password.
 3. Press ENTER.

The **Appliance OS Key Rotation** dialog box appears.

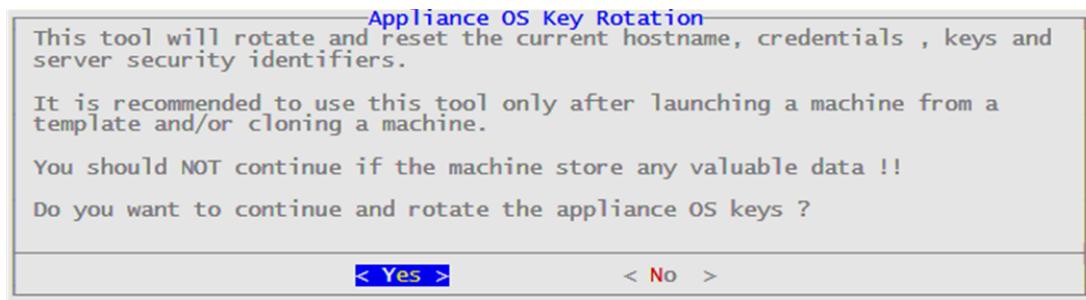


Figure -6: Appliance OS Key Rotation Dialog box

4. Select Yes.
 5. Press ENTER.

The administrative credentials dialog box appears.

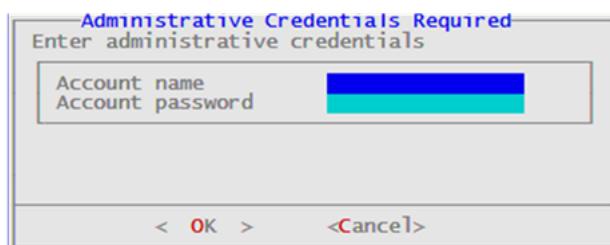


Figure -7: Administrative Credentials Dialog box

6. Enter the required Account name on the appliance.
 7. Enter the required Account password on the appliance.
 8. Select OK.
 9. Press ENTER.

The process to rotate the required keys, certificates, credentials, and other identifiers on the appliance starts.

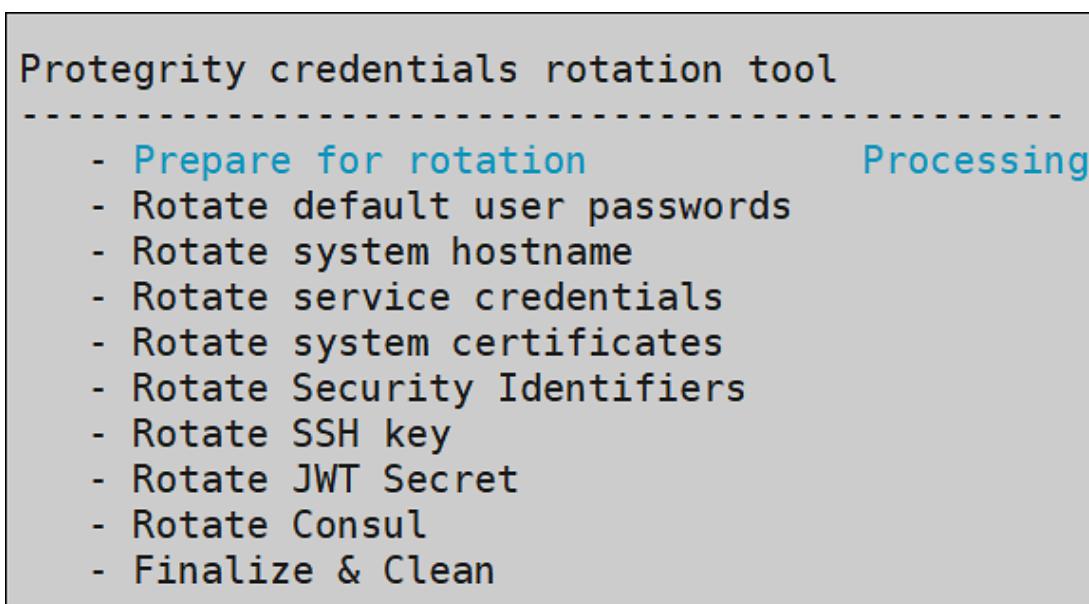


Figure -8: Protegrity Credentials Rotation Tool Status screen

10. To update the user passwords, provide the credentials for the following users.

- root
- admin
- viewer
- local_admin

Note:

If you have manually deleted any of the default users, such as, *admin* or *viewer*, then that user is not listed on the **User's Passwords** screen.

User's Passwords

Please provide user's passwords

root password	[Redacted]
root password verification	[Redacted]
admin password	[Redacted]
admin password verification	[Redacted]
viewer password	[Redacted]
viewer password verification	[Redacted]
local_admin password	[Redacted]
local_admin password verification	[Redacted]

<Apply> **<Help >**

11. Select **Apply**.

The user passwords are updated and the appliance OS keys are rotated.

15.1.8 Working with Cloud-based Applications

Cloud-based applications are products or services for storing data on the cloud. In cloud-based applications, the computing and processing of data is handled on the cloud. Local applications interact with the cloud services for various purposes, such as, data storage, data computing, and so on. Cloud-based applications are allocated resources dynamically and aim at reducing infrastructure cost, improving network performance, easing information access, and scaling of resources.

AWS offers a variety of cloud-based products for computing, storage, analytics, networking, and management. Using the Cloud Utility product, services such as, CloudWatch and AWS CLI are leveraged by the Protegity appliances.

15.1.8.1 Prerequisites

The following prerequisites are essential for AWS Cloud Utility.

- The **Cloud Utility AWS v2.0** product must be installed.

Note:

From 8.0.0.0, if an instance is created on the AWS using the cloud image, then **Cloud Utility AWS** is preinstalled on this instance.

For more information about installing the Cloud Utility AWS v2.0, refer to the *Protegity Installation Guide 9.1.0.5*.

- If you are launching a Protegity appliance on an AWS EC2 instance, then you must have a valid **IAM Role**.

For more information about IAM Role, refer to *Configuring Access for AWS Resources*.

- If you are launching a Protegity appliance on a non-AWS instance, such as on-premise, Microsoft Azure, or GCP instance, then the **AWS Configure** option must be set up.

For more information about configuring AWS credentials, refer to *AWS Configure*.

- The user accessing the **Cloud Utility AWS Tools** must have **AWS Admin** role assigned.

For more information about AWS admin, refer to *Managing Roles*.

15.1.8.2 Configuring Access for AWS Resources

A server might contain resources that only the authorized users can access. For accessing a protected resource, you must provide valid credentials to utilize the services of the resource. Similarly, on the AWS platform, only privileged users can access and utilize the AWS cloud applications. The Identity and Access Management (IAM) is the mechanism for securing access to your resources on AWS.

The two types of IAM mechanisms are as follows:

- **IAM user** is an entity that represents users on AWS. To access the resources or services on AWS, the IAM user must have the privileges to access these resources. By default, you have to set up all required permissions for a user. Each IAM user can have specific defined policies. An IAM user account is beneficial as it can have special permissions or privileges associated for a user.

For more information about creating an IAM user, refer to the following link:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html

An IAM user can access the AWS services on the required Protegity appliance instances with the access keys. The access keys are the authentication mechanisms that authorize AWS CLI requests. The access keys can be generated when you create the IAM user account. Similar to the username and password, the access keys consist of access key ID and the secret access key. The access keys validate a user to access the required AWS services.

For more information about setting up an IAM user to use AWS Configure, refer to *AWS Configure*.

- **IAM role** is the role for your AWS account and has specific permissions associated with it. An IAM role has defined permissions and privileges which can be given to multiple IAM users. For users that need same permissions to access the AWS services, you should associate an IAM role with the given user account.

If you want a Protegity appliance instance to utilize the AWS resources, the instance must be provided with the required privileges. This is achieved by attaching an IAM role to the instance. The IAM role must have the required privileges to access the AWS resources.

For more information about creating an IAM role, refer to the following link:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create.html

For more information about IAM, refer to the following link.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

15.1.8.2.1 AWS Configure

The **AWS Configure** operation is a process for configuring an IAM user to access the AWS services on the Protegity appliance instance. These AWS services include CloudWatch, CloudTrail, S3 bucket, and so on.

To utilize AWS resources and services, you must set up **AWS Configure** if you have an **IAM User**.

To set up **AWS Configure** on a non-AWS instance, such as on-premise, Microsoft Azure, or GCP instance, you must have the following:

1. A valid IAM User
2. Secret key associated with the IAM User
3. Access key ID for the IAM User
4. The AWS Region on whose servers you want to send the default service requests

For more information about the default region name, refer to the following link.

<https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html>

If the access keys or the IAM role do not have the required privileges, then the user cannot utilize the corresponding AWS resources.

Note:

For **AWS Configure**, only one IAM user can be configured for an appliance at a time.

15.1.8.2.2 Configuring AWS Services

Note:

It is recommended to configure the AWS services from the **Tools > Cloud Utility AWS Tools > AWS Configure** menu.

► To configure the AWS services:

1. Login to the Appliance CLI Manager.

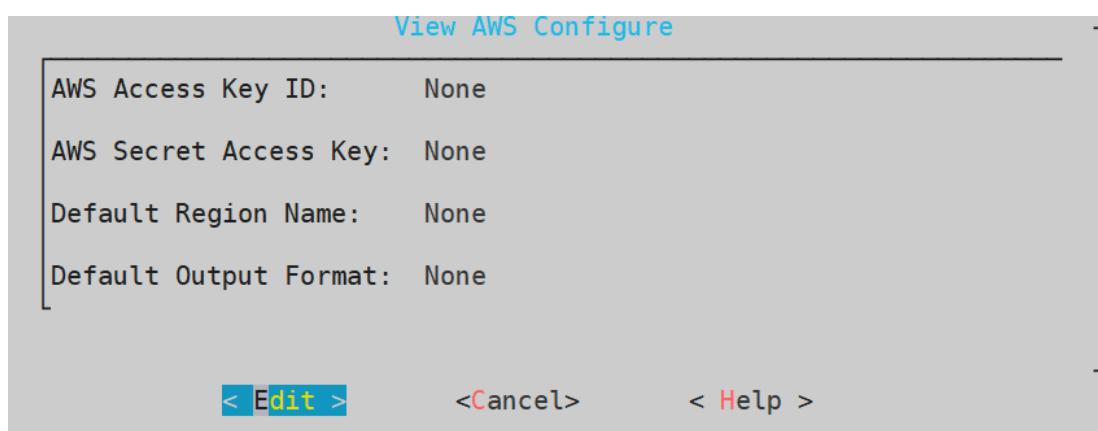
Note:

On the Appliance Web UI, ensure that the **AWS Admin** privilege is assigned to the user role for configuring AWS on non-AWS instance.

2. To configure the AWS services, navigate to **Tools > Cloud Utility AWS Tools > AWS Configure**.

3. Enter the *root* credentials.

The following screen appears.



4. Select **Edit** and press **ENTER**.
5. Enter the AWS credentials associated with your IAM user in the **AWS Access Key ID** and **AWS Secret Access Key** text boxes.
6. Enter the region name in the **Default Region Name** text box.

Note:

This field is case sensitive. Ensure that the values are entered in small-case.

For more information about the default region name, refer to the following link:

<https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html>

7. Enter the output format in the **Default Output Format** text box.

If the field is left empty, the **Default Output Format** is *json*. However, the supported **Default Output Formats** are *json*, *table*, and *text*.

Note:

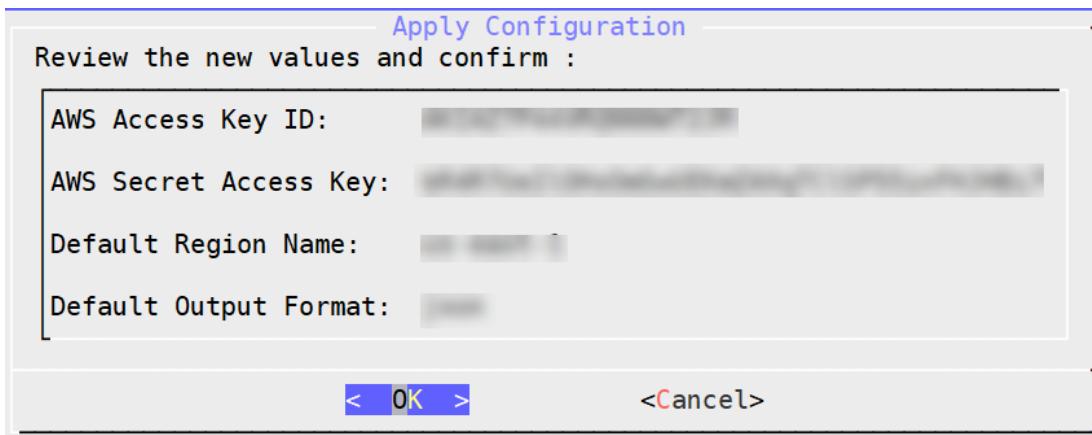
This field is case sensitive. Ensure that the values are entered in small-case.

For more information about the default output format, refer to the following link:

<https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html>

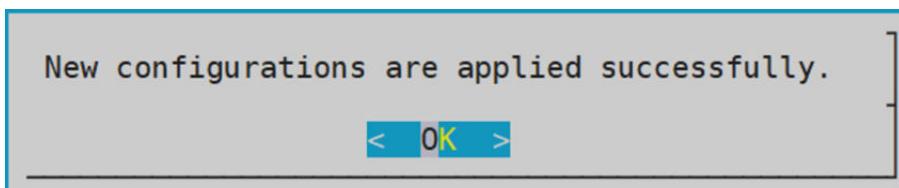
8. Select **OK** and press **ENTER**.

A validation screen appears.



9. Select **OK** and press **ENTER**.

A confirmation screen appears.



10. Select **OK**.

The configurations are applied successfully.

15.1.8.3 Working with CloudWatch Console

AWS CloudWatch tool is utilized for monitoring applications. Using CloudWatch, you can monitor and store the metrics and logs for analyzing the resources and applications.

CloudWatch allows you to collect metrics and track them in real-time. Using this service you can configure alarms for the metrics. CloudWatch provides visibility into the various aspects of your services including the operational health of your device, performance of the applications, and resource utilization.

For more information about AWS CloudWatch, refer to the following link:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html>

CloudWatch logs helps you to monitor a cumulative list of all the logs from different applications on a single dashboard. This provides a central point to view and search the logs which are displayed in the order of the time when they were generated. Using CloudWatch you can store and access your log files from various sources. CloudWatch allows you to query your log data, monitor the logs which are originating from the instances and events, and retain and archive the logs.

For more information about CloudWatch logs, refer to the following link:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

15.1.8.3.1 Prerequisites

For using AWS CloudWatch console, ensure that the IAM role or IAM user that you want to integrate with the appliance must have *CloudWatchAgentServerPolicy* policy assigned to it.

For more information about using the policies with the IAM Role or IAM User, refer to the following link:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-iam-roles-for-cloudwatch-agent.html>

15.1.8.3.2 Integrating CloudWatch with Protegity Appliance

You must enable CloudWatch integration to use the AWS CloudWatch services. This helps you to send the metrics and the logs from the appliances to the AWS CloudWatch Console.

The following section describes the steps to enable CloudWatch integration on Protegity appliances.

► To enable AWS CloudWatch integration:

1. Login to the ESA CLI Manager.
2. To enable AWS CloudWatch integration, navigate to **Tools > Cloud Utility AWS Tools > CloudWatch Integration**.
3. Enter the *root* credentials.

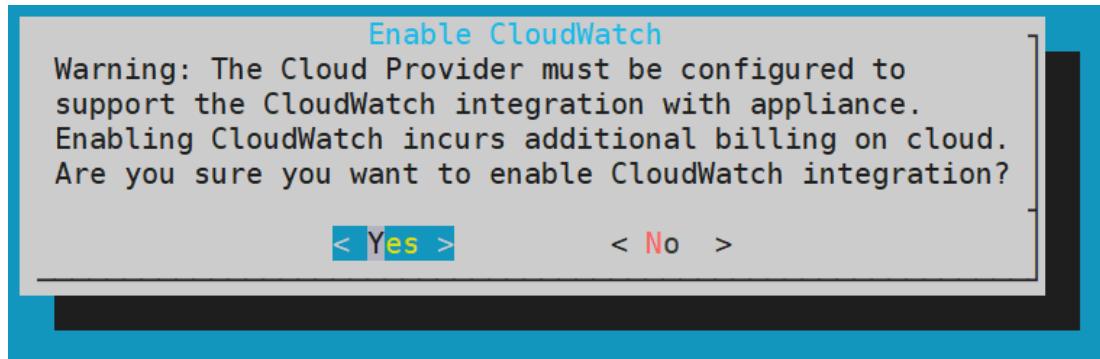
The following screen appears.

Note:

The warning message is displayed due to the cost involved from AWS.

For more information about the cost of integrating CloudWatch, refer to the following link:

<https://aws.amazon.com/cloudwatch/pricing/>



4. Select **Yes** and press **ENTER**.

A screen listing the logs that are being sent to the CloudWatch Console appears.

```
Following logs will be sent to CloudWatch :  
Appliance Logs:  
/var/log/syslog  
/var/log/user.log  
/var/log/apache2/error.log  
/var/log/apache2-service_dispatcher/error.log  
/var/log/apache2-webservices/error.log
```

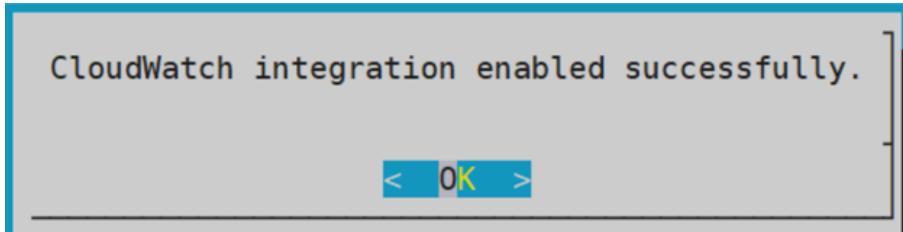
Do you wish to continue with above log files?

< Yes >

< No >

5. Select **OK**.

Wait till the following screen appears.



CloudWatch integration enabled successfully.

< OK >

6. Select **OK**.

CloudWatch integration is enabled successfully.

Note:

CloudWatch service is added on the Web UI and CLI.

15.1.8.3.3 Configuring Custom Logs on AWS CloudWatch Console

You can send logs from an appliance which is on-premise or launched on any of the cloud platforms, such as, AWS, GCP, or Azure. The logs are sent from the appliances and stored on the AWS CloudWatch Console. By default, the following logs are sent from the appliances:

- Syslogs
- Current events logs
- Apache2 error logs
- Service dispatcher error logs
- Web services error logs

You can send custom log files to the AWS CloudWatch Console. To send custom log files to the AWS CloudWatch Console, you must create a file in the `/opt/aws/pty/cloudwatch/config.d` directory. You can add or edit the log streams in this file to generate the custom logs with the following parameters.

Note:

You must not edit the default configuration file, `appliance.conf`, in the `/opt/aws/pty/cloudwatch/config.d` directory.

If you want to configure a new log stream, then you must use the following syntax:

```
[  
  {  
    "file_path": "<path_of_the_first_log_file>",  
    "log_stream_name": "<Name_of_the_log_stream_to_be_displayed_in_CloudWatch>",  
    "log_group_name": "{hostname}"  
  },  
  .  
  .  
  {  
    "file_path": "<path_of_the_nth_log_file>",  
    "log_stream_name": "<Name_of_the_log_stream_to_be_displayed_in_CloudWatch>",  
    "log_group_name": "{hostname}"  
  }  
]
```

The following table explains the parameters that you must use to configure the log streams.

Parameter	Description	Example
file_path	Location where the file or log is stored	“/var/log/appliance.log”
log_stream_name	Name of the log that will appear on the AWS CloudWatch Console	“Appliance_Logs”
log_group_name	Name under which the logs are displayed on the CloudWatch Console Note: On the CloudWatch Console, the logs appear under the hostname of the ESA instance. Caution: Ensure that you must not modify the parameter <code>log_group_name</code> and its value <code>{hostname}</code> .	

The following snippet displays the sample configuration file, `configuration_filename.conf`, that sends appliance logs to the AWS CloudWatch Console.

```
[  
  {  
    "file_path": "/var/log/syslog",  
    "log_stream_name": "Syslog",  
    "log_group_name": "{hostname}"  
}
```



```

        },
        "file_path": "/var/log/user.log",
        "log_stream_name": "Current_Event_Logs",
        "log_group_name": "{hostname}"
    }
]

```

Note:

If you configure custom log files to send to CloudWatch Console, then you must reload the CloudWatch integration or restart the CloudWatch service. Also, ensure that the CloudWatch integration is enabled and running.

For more information about Reloading AWS CloudWatch Integration, refer to [Reloading AWS CloudWatch Integration](#).

15.1.8.3.4 Toggling the CloudWatch Service

In the Protegity appliances, the **Cloudwatch** service enables the transmission of logs from the appliances to the AWS CloudWatch Console. Enabling the AWS Cloudwatch Integration also enables this service with which you can start or stop the logs from being sent to the AWS CloudWatch Console. The following sections describe how to toggle the **CloudWatch** service for pausing or continuing log transmission.

Note:

To toggle the CloudWatch service, ensure that the valid AWS credentials are configured.

15.1.8.3.4.1 Starting/Stopping the CloudWatch Service from the Web UI

If you want to temporarily stop the transmission of logs from the appliance to the AWS Console, then you can stop the CloudWatch Service from the CLI Manager or the Web UI.

► To start/stop the AWS CloudWatch service from the Web Ui:

1. Login to the Appliance Web UI.
2. Navigate to **System > Services**.
3. Select the **Stop** icon corresponding to the CloudWatch service for stopping the transmission of logs and metrics.

Note:

Similarly, select the **Start** icon to start and the **Restart** icon to restart the CloudWatch service.

15.1.8.3.4.2 Starting/Stopping the CloudWatch Service from the CLI Manager

If you want to temporarily stop the transmission of logs from the appliance to the AWS Console, then you can stop the CloudWatch Service from the CLI Manager or the Web UI.

► To start/stop the AWS CloudWatch service from the CLI Manager:

1. Login to the appliance CLI Manager.
2. Navigate to **Administration > Services**.
3. Select the CloudWatch service and choose **Stop** for stopping the transmission of logs and metrics.

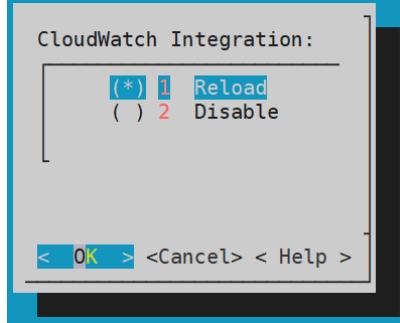
15.1.8.3.5 Reloading the AWS CloudWatch Integration

If you want to update the existing configurations in the `/opt/aws/pty/cloudwatch/config.d` directory, then you must reload the CloudWatch integration.

► To reload the AWS CloudWatch integration:

1. Login to the ESA CLI Manager.
2. To reload CloudWatch, navigate to **Tools > Cloud Utility AWS Tools > CloudWatch Integration**.
3. Enter the *root* credentials.

The following screen appears.



4. Select **Reload** and press **ENTER**.
The logs are updated and sent to the AWS CloudWatch Console.

15.1.8.3.6 Viewing Logs on AWS CloudWatch Console

After performing the required changes on the CLI Manager, the logs are visible on the CloudWatch Console.

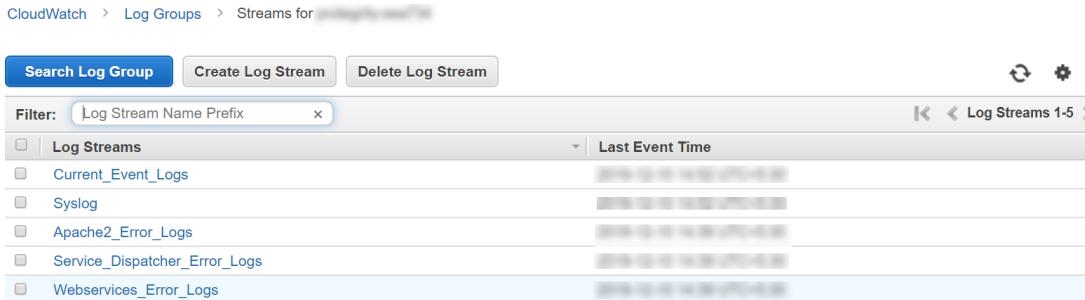
► To view the logs on the CloudWatch console:

1. Login to the AWS Web UI.
2. From the **Services** tab, navigate to **Management & Governance > CloudWatch**.
3. To view the logs, from the left pane navigate to **Logs > Log groups**.
4. Select the required log group.

Note:

The log group name is the same as the hostname of the appliance.

5. To view the logs, select the required log stream from the following screen.



15.1.8.3.7 Working with AWS CloudWatch Metrics

The metrics for the following entities in the appliances are sent to the AWS CloudWatch Console.

Metrics	Description
Memory Use Percent	Percentage of the memory that is consumed by the appliance.
Disk I/O	<p>Bytes and packets read and written by the appliance.</p> <p>You can view the following parameters:</p> <ul style="list-style-type: none"> • write_bytes • read_bytes • writes • reads
Network	<p>Bytes and packets sent and received by the appliance.</p> <p>You can view the following parameters:</p> <ul style="list-style-type: none"> • bytes_sent • bytes_received • packets_sent • packets_received
Disk Used Percent	Percentage of the disk space that is consumed by the appliance.
CPU Idle	Percentage of time for which the CPU is idle.
Swap Memory Use Percent	Percentage of the swap memory that is consumed by the appliance.

Unlike logs, you cannot customize the metrics that you want to send to CloudWatch. If you want to customize these metrics, then contact Protegility Support.

15.1.8.3.8 Viewing Metrics on AWS CloudWatch Console

► To view the metrics on the CloudWatch console:

1. Login to the AWS Web UI.
2. From the **Services** tab, navigate to **Management & Governance > CloudWatch**.

3. To view the metrics, from the left pane navigate to **Metrics**.

4. Navigate to **AWS namespace**.

The following screen appears.

The screenshot shows the AWS CloudWatch Metrics console. At the top, there are tabs: All metrics (selected), Graphed metrics, Graph options, and Source. Below the tabs is a search bar with placeholder text "Search for any metric, dimension or resource id" and a "Graph search" button. A summary section displays "2,422 Metrics". Under "Custom Namespaces", there is a single entry for "CWAgent" with "1,413 Metrics". Under "AWS Namespaces", there are nine entries arranged in three rows of three: Billing (12 Metrics), DynamoDB (14 Metrics), EBS (294 Metrics); EC2 (572 Metrics), Firehose (3 Metrics), Logs (60 Metrics); NATGateway (13 Metrics), S3 (18 Metrics), Usage (11 Metrics); and VPN (12 Metrics). A vertical scrollbar is visible on the right side of the list.

5. Select **EC2**.

6. Select the required metrics from the following screen.

The screenshot shows the AWS CloudWatch Metrics console with the path "All > EC2" selected. At the top, there are tabs: All metrics (selected), Graphed metrics, Graph options, and Source. Below the tabs is a search bar with placeholder text "Search for any metric, dimension or resource id". A summary section displays "572 Metrics". There are four entries under "EC2": "By Image (AMI) Id" (8 Metrics), "Per-Instance Metrics" (548 Metrics), "Aggregated by Instance Type" (8 Metrics), and "Across All Instances" (8 Metrics).

7. To view metrics of the Protegity appliances that are on-premise or other cloud platforms, such as Azure or GCP, navigate to **Custom namespace > CWAgent**.

The configured metrics appear.

15.1.8.3.9 Disabling AWS CloudWatch Integration

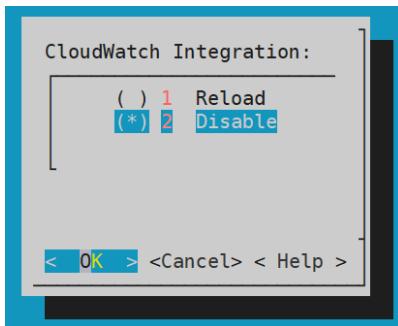
If you want stop the logs and metrics that are being sent to the AWS CloudWatch Console by disintegrating the CloudWatch service from the appliance, then disable the AWS CloudWatch integration from the appliance. As a result, the **CloudWatch** service is removed from the **Services** screen of the Web UI and the CLI Manager.

► To disable the AWS CloudWatch integration:

1. Login to the ESA CLI Manager.

2. To disable CloudWatch, navigate to **Tools > Cloud Utility AWS Tools > CloudWatch Integration**.

The following screen appears.



3. Select **Disable** and press **ENTER**.

The logs from the appliances are not updated in the AWS CloudWatch Console and the CloudWatch Integration is disabled.

Note:

After disabling CloudWatch integration, you must delete the **Log groups** and **Log streams** from the AWS CloudWatch console.

15.1.8.4 Working with the AWS Cloud Utility

You can work with the AWS Cloud Utility in various ways. This section contains some scenarios using Cloud Utility product. However, the scope of working with the Cloud Utility is not limited to the scenarios covered in this section.

The following scenarios are explained in this section:

1. Encrypting and storing the backed up files on the AWS S3 bucket.
2. Setting metrics-based alarms using the AWS Management Console.

Note: The *Security Administrator* role must have the *AWS Admin* permission to work with the AWS Cloud Utility.

15.1.8.4.1 Storing Backup Files on the AWS S3 Bucket

If you want to store backed up files on the AWS S3 bucket, you can use the Cloud Utility feature. You can transit these files from the Protegity appliance to the AWS S3 bucket.

The following tasks are completed in this section:

1. Encrypting the backed up *.tgz* files using the AWS Key Management Services (KMS).
2. Storing the encrypted files in the AWS S3 bucket.
3. Retrieving the encrypted files stored in the S3 bucket.
4. Decrypting the retrieved files using the AWS KMS.
5. Importing the decrypted files on the Protegity appliance.

The AWS S3 bucket is a cloud resource which helps you to securely store your data. It enables you to keep the data backup at multiple locations, such as, on-premise and on cloud. For easy accessibility, you can backup and store data of one machine and import the same data to another machine, using the AWS S3 bucket. It also provides an additional layer of security by helping you encrypt the data before uploading it to the cloud.

Using the *OS Console* option in the CLI Manager, you can store your backed up files in the AWS S3 bucket. You can encrypt your files using the the AWS Key Management Services (KMS) before storing it in the AWS S3 bucket.

The following figure shows the flow for storing your data on the AWS S3 bucket.



Figure -9: Encrypting and storing files on the AWS S3 bucket

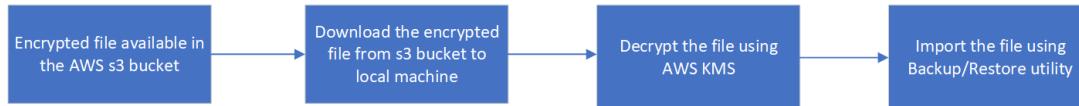


Figure -10: Retrieving and decrypting files from the AWS S3 bucket

15.1.8.4.1.1 Prerequisites

Ensure that you complete the following prerequisites for uploading the backed up files to the S3 bucket:

- The *Configured AWS user* or the attached *IAM role* must have access to the S3 bucket.

For more information about configuring access to the AWS resources, refer to [Configuring access for AWS resources](#).

- The *Configured AWS user* or the attached *IAM role* must have **AWSKeyManagementServicePowerUser** permission to use the KMS.

For more information about configuring AWS resources, refer to [Configuring access for AWS resources](#).

For more information about KMS, refer to the following link.

<https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html>

- The backed up *.tgz* file should be present in the */products/exports* folder.

For more information about exporting the files, refer to [Export Data Configuration to Local File](#).

- You must have the KMS keys present in the AWS Key Management Service.

For more information about KMS keys, refer to the following link:

<https://docs.aws.amazon.com/kms/latest/developerguide/getting-started.html>.

15.1.8.4.1.2 Encrypting and Storing Files

► To encrypt and upload the exported file from */products/exports* to the S3 bucket:

1. Login to the Appliance CLI manager.
2. To encrypt and upload files, navigate to **Administration > OS Console**.
3. Enter the *root* credentials.
4. Change the directory to */products/exports* using the following command.

```
cd /products/exports
```

5. Encrypt the required file using the *aws-encryption-cli* command.

```
aws-encryption-cli --encrypt --input <file_to_encrypt> --master-keys key=<Key_ID>
region=<region-name> --output <encrypted_output_filename> --metadata-output
<metadata_filename> --encryption-context purpose=<purpose_for_performing encryption>
```

Parameter	Description
file_to_encrypt	The backed up file that needs to be encrypted before uploading to the S3 bucket.
Key_ID	The key ID of the KMS key that needs to be used for encrypting the file.
region-name	The region where the KMS key is stored
encrypted_output_filename	The name of the file after encryption.
metadata_filename	The name of the file where the metadata needs to be stored.
purpose_for_performing encryption	The purpose of encrypting the file.

For more information about encrypting data using the KMS, refer to the following link.

<https://docs.aws.amazon.com/cli/latest/reference/kms/encrypt.html>

The file is encrypted.

6. Upload the encrypted file to the S3 bucket using the following command.

The file is uploaded in the S3 bucket.

```
aws s3 cp <encrypted_output_filename> <s3Uri>
```

For example, if you have an encrypted file *test.enc* and you want to upload it to your personal bucket, *mybucket*, in s3 bucket, then use the following command:

```
aws s3 cp test.enc s3://mybucket/test.enc
```

For more information about the S3 bucket, refer to the following link:

<https://docs.aws.amazon.com/cli/latest/reference/s3/>

15.1.8.4.1.3 Decrypting and Importing Files

► To decrypt and import the files from the S3 bucket:

1. Login to the Appliance CLI manager.
2. To decrypt and import the file, navigate to **Administration > OS Console**.
3. Enter the *root* credentials.
4. Change the directory to */products/exports* using the following command:

```
cd /products/exports
```

5. Download the encrypted file using the following command.

```
aws s3 cp <s3Uri> <local_file_name(path)>
```

For example, if you want to download the file *test.txt* to your local machine as *test2.txt*, then use the following command:

```
aws s3 cp s3://mybucket/test.txt test2.txt
```

6. Decrypt the downloaded file using the following command.

```
aws-encryption-cli --decrypt --input <file_to_decrypt> --output <decrypted_file_name>
--metadata-output <metadata_filename>
```

Parameter	Description
file_to_decrypt	The backed up file that needs to be decrypted after downloading from the S3 bucket.
decrypted_output_filename	The name with which the file is saved after decryption.
metadata_filename	The name of the file where the metadata needs to be stored.

Note:

Ensure that the *metadata_filename* must be the same filename which is used during encryption of the file.

The file is decrypted.

For more information about decrypting the downloaded file, refer to the following link.

<https://aws.amazon.com/blogs/security/how-to-encrypt-and-decrypt-your-data-with-the-aws-encryption-cli/>

7. Import the decrypted file to the local machine.

For more information about importing the decrypted file, refer to [Import Data/Configurations from a File](#).

15.1.8.4.2 Set Metrics Based Alarms Using the AWS Management Console

If you want to set alarms and alerts for your machine, using the Protegity appliances, you can send logs and metrics to the AWS Console. The AWS Management Console enables you to set alerts and configure SNS events as per your requirements.

You can create alerts based on the following metrics:

- Memory Use Percent
- Disk I/O
- Network
- Disk Used Percent
- CPU Idle
- Swap Memory Use Percent

15.1.8.4.2.1 Prerequisite

Ensure that the CloudWatch integration is enabled.

For more information about enabling the CloudWatch integration, refer to [Enabling AWS CloudWatch Integration](#).

15.1.8.4.2.2 Creating an SNS Event

The following steps explain how to create an SNS event for an email-based notification.

► To create an SNS event:

1. Login to the Amazon Management Console.
2. To create an SNS event, navigate to **Services > Application Integration > Simple Notification Services > Topics**.
3. Select **Create topic**.

The following screen appears.

The screenshot shows the 'Create topic' wizard in the Amazon SNS console. The top navigation bar shows 'Amazon SNS > Topics > Create topic'. The main title is 'Create topic'. A 'Details' tab is selected. Under 'Name', the value 'MyTopic' is entered. A note below says 'Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_.)'. Under 'Display name - optional', the value 'My Topic' is entered. A note below says 'Maximum 100 characters, including hyphens (-) and underscores (_.)'. A note at the bottom right of the 'Details' section states: '► Encryption - optional' and 'Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.'.

4. Enter the required **Details**.

5. Click **Create topic**.

The following screen appears.

The screenshot shows the 'Details' tab of an AWS SNS topic configuration. It includes fields for Name, ARN, Display name, and Topic owner. Action buttons for Edit, Delete, and Publish message are at the top right. Below the tabs are links for Subscriptions, Access policy, Delivery retry policy (HTTP/S), Delivery status logging, and Encryption.

Note:

Ensure that you remember the Amazon Resource Name (ARN) associated to your topic.

For more information about the ARN, refer to the following link.

<https://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html>

The topic is created.

6. From the left pane, click **Subscriptions**.
7. Click **Create subscription**.
8. Enter the **Topic ARN** of the topic created in the above step.
9. From the **Protocol** field, select **Email**.
10. In the **Endpoint**, enter the required email address where you want to receive the alerts.

Create subscription

Details

Topic ARN

 MyTopic

Protocol

The type of endpoint to subscribe

 Email

Endpoint

An email address that can receive notifications from Amazon SNS.

 test@example.com

After your subscription is created, you must confirm it. [Info](#)

11. Enter the optional details.

12. Click **Create subscription**.

An SNS event is created and a confirmation email is sent to the subscribed email address.

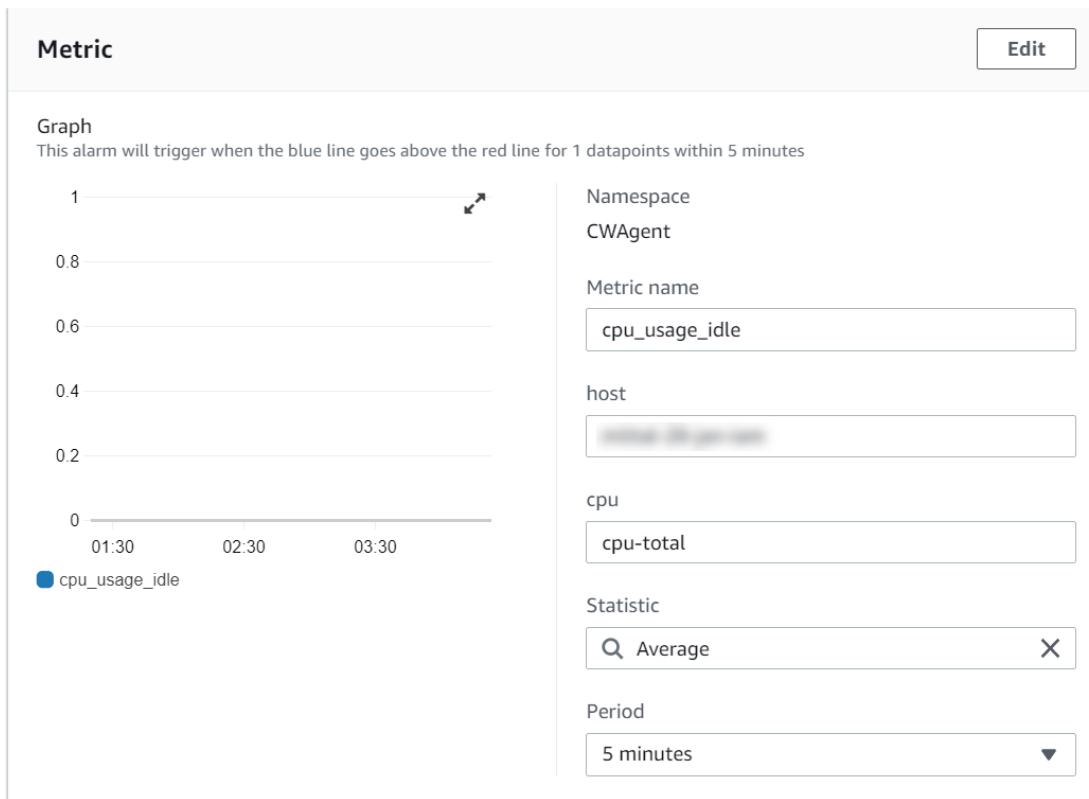
13. To confirm the email subscription, click the **Confirm Subscription** link from the email received on the registered email address.

15.1.8.4.2.3 Creating Alarms

The following steps explain the procedure to set an alarm for CPU usage.

To create an alarm:

1. Login to the Amazon Management Console.
2. To create an alarm, navigate to **Services > Management & Governance > Cloud Watch**.
3. From the left pane, select **Alarms**.
4. Select **Create alarm**.
5. Click **Select metric**.
The **Select metric** window appears.
6. From the **Custom Namespaces**, select **CWAgent**.
7. Select **cpu, host**.
8. Select the required metric and click **Select metric**.
9. Configure the required metrics.



10. Configure the required conditions.

The figure shows the 'Conditions' configuration screen. It includes the following sections:

- Threshold type:** Static (selected) vs Anomaly detection (disabled).
- Whenever cpu_usage_idle is...**: Define the alarm condition.
 - Greater > threshold (selected)
 - Greater/Equal >= threshold
 - Lower/Equal <= threshold
 - Lower < threshold
- than...**: Define the threshold value (10000).
- Additional configuration**: A link to further configuration.

[Cancel](#) [Next](#)

11. Click **Next**.

The **Notification** screen appears.

12. Select the *alarm state*.
13. From **Select SNS topic**, choose **Select an existing SNS topic**.
14. Enter the required email type in *Send a notification to...* dialog box.
15. Select **Next**.
16. Enter the **Name** and **Description**.
17. Select **Next**.
18. Preview the configuration details and click **Create alarm**.
An alarm is created.

15.1.8.5 FAQs for AWS Cloud Utility

This section lists the FAQs for the AWS Cloud Utility.

Question	Answer
Where can I install the AWS Cloud/CloudWatch/Cloud Utilities?	<p>AWS Cloud Utility can be installed on any appliance-based products. It is compatible with the ESA and the DSG that are installed on-premise or on cloud platforms, such as, AWS, Azure, or GCP.</p> <p>From v8.0.0.0, if an instance is created on the AWS using the cloud image, then Cloud Utility AWS is preinstalled on this instance.</p>
Which version of AWS CLI is supported by the AWS Cloud Utility product v2.0?	AWS CLI 2.2.8 is supported by the Cloud Utility AWS product v2.0.
What version of appliances are compatible with the AWS Cloud Utility?	<p>The compatible versions are:</p> <p>ESA v7.2.1 and above</p> <p>DSG v2.4.0 and above</p>
What is the Default Region Name while configuring AWS services?	<p>The Default Region Name on whose servers you want to send the default service requests. For more information about Default Region Name, refer to the following link:</p> <p>https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html</p>
Can I configure multiple accounts for AWS on a single appliance?	No, you cannot configure multiple accounts for AWS on a single appliance.
How to determine the Log group name ?	The Log group name is same as the <i>hostname</i> of the appliance.
Can I change the Log group name ?	No, you cannot change the Log group name .
Can I change the appliance <i>hostname</i> after enabling CloudWatch integration?	<p>If you change the appliance <i>hostname</i> after enabling CloudWatch integration, then:</p> <ul style="list-style-type: none"> • A new Log Group is created with the updated <i>hostname</i>. • Only the new logs will be present in the updated Log Group. • The new Log Group consists of only the updated logs files. • It is recommended to manually delete the previous Log Group from the AWS CloudWatch Console.
Are there any configuration files for AWS CloudWatch?	<p>Yes, there are configuration files for CloudWatch.</p> <p>The configuration files are present in <i>/opt/aws/pty/cloudwatch/config.d/</i> directory.</p> <p>The <i>config.json</i> file for cloud watch is present in <i>/opt/aws/pty/cloudwatch/config.json</i> file.</p> <div style="background-color: #e0f2e0; padding: 10px;"> <p>Note:</p> <p>It is recommended not to edit the default configuration files.</p> </div>
What happens if I enable CloudWatch integration with a corrupt file?	<p>The invalid configuration file is listed in a dialog box.</p> <p>The logs corresponding to all other valid configurations will be sent to the AWS CloudWatch Console.</p>
What happens if I edit the only default configuration files, such as, <i>/opt/aws/pty/cloudwatch/</i>	In this case, only metrics will be sent to the AWS CloudWatch Console.

Question	Answer
<code>config.d/</code> , with invalid data for CloudWatch integration?	
How can I export or import the CloudWatch configuration files?	<p>You can export or import the CloudWatch configuration files either through the CLI Manager or through the Web UI.</p> <p>For more information about exporting or importing the configuration files through the CLI manager, refer to Exporting Data Configuration to Local File.</p> <p>For more information about exporting or importing the configuration files through the Web UI, refer to Backing Up Data.</p>
What are the compatible Output Formats while configuring the AWS?	<p>The following Default Output Formats are compatible:</p> <ul style="list-style-type: none"> • json • table • text
If I use an <i>IAM role</i> , what is the Default Output Formats ?	The Default Output Format is <i>json</i> .
If I disable the CloudWatch integration, why do I need to delete Log Groups and Log Streams manually?	<p>You should delete Log Groups and Log Streams manually because this relates to the billing cost.</p> <p>Protegity will only disable sending logs and metrics to the CloudWatch Console.</p>
How can I check the status of the CloudWatch agent service?	<p>You can view the status of the CloudWatch service using one of the following.</p> <ul style="list-style-type: none"> • On the Web UI, navigate to System > Services Console. • On the CLI Manager, navigate to Administration > Services. • On the CLI Manager, navigate to Administration > OS Console and run the following command: <pre>/etc/init.d/cloudwatch_service status</pre>
Can I customize the metrics that i want to send to the CloudWatch console?	<p>No, you cannot customize the metrics to send to the CloudWatch console.</p> <p>If you want to customize the metrics, then contact Protegity Support.</p>
How often are the metrics collected from the appliances?	The metrics are collected at 60 seconds intervals from the appliance.
How much does Amazon CloudWatch cost?	For information about the billing and pricing details, refer to https://aws.amazon.com/cloudwatch/pricing/ .
Can I provide the file path as <i>filename/*</i> to send logs to the folder?	<p>No, you can not provide the file path as <i><filename/*></i>.</p> <p>Regex is not allowed in the CloudWatch configuration file. You must specify the absolute file path.</p>
Can I configure AWS from OS Console ?	<p>No, you can not.</p> <p>If you configure AWS from the OS Console it will change the expected behaviour of the AWS Cloud Utility.</p>
What happens to the custom configurations if I uninstall/ remove the AWS Cloud Utility product?	The custom configurations are retained.
What happens to CloudWatch if I delete AWS credentials from ESA after enabling CloudWatch integration?	<p>You can not change the status of the CloudWatch service.</p> <p>You must reconfigure the ESA with valid AWS credentials to perform the CloudWatch-related operations.</p>

Question	Answer
Why some of the log files are world readable?	The files with the <code>.log</code> extension present in the <code>/opt/aws/pty/cloudwatch/logs/state</code> folder are not log files. These files are used by the CloudWatch utility to monitor the logs.
Why the CloudWatch service is stopped when the patch is installed. How to restart this service?	As the CloudWatch service is stopped when the patch is installed, it remains in the stopped state after the Cloud Utility Patch (CUP) installation. So, we must restart the CloudWatch service manually. To restart the CloudWatch service manually, perform the following steps. <ol style="list-style-type: none"> 1. Login to the OS Console. 2. Restart the CloudWatch service using the following command. <code>/etc/init.d/cloudwatch_service restart</code>

15.1.8.6 Working with AWS Systems Manager

AWS Systems Manager allows you to manage and operate the infrastructure on AWS. Using the Systems Manager console, you can view operational data from multiple AWS services and automate operational tasks across the AWS services.

For more information about AWS Systems Manager, refer to the following link:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html>

15.1.8.6.1 Prerequisites

For using AWS Systems Manager, ensure that the IAM role or IAM user that you want to integrate with the appliance must have a policy assigned to it. You can attach one or more IAM policies that define the required permissions for a particular IAM role.

For more information about the IAM role, refer to section Configuring Access for AWS Instances.

For more information about creating an IAM instance profile for Systems Manager, refer to the following link:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>

15.1.8.6.2 Setting up AWS Systems Manager

You must set up AWS Systems Manager to use the SSM Agent (Systems Manager Agent).

You can set up Systems Manager for:

- An AWS instance
- A non-AWS instance or an on-premise platform

Note:

After the SSM Agent is installed in an instance, ensure that the auto-update option is disabled, as we do not support auto-update. If the SSM Agent gets auto updated, the service will get corrupted.

For more information about automatic updates for SSM Agent, refer to the following link:

SSM Agent Automatic Updates

15.1.8.6.2.1 Setting up Systems Manager for AWS Instance

► To set up Systems Manager for an AWS instance:

1. Assign the IAM Role created in the section [Prerequisites](#).

For more information about attaching an IAM role to an instance, refer to the following link:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html#attach-iam-role>

2. Start the Amazon SSM Agent service.

Note: When you restart the AWS instance, the Amazon SSM-Agent service will be in the stopped state. This is the default behavior. Ensure that you manually start the service after attaching the IAM role.

For more information about starting a service, refer to the section [Working with Services](#).

Note:

Ensure that the Amazon SSM Agent is always *Running* in the *Automatic* mode.

15.1.8.6.2.2 Setting up Systems Manager for non-AWS Instance

► To set up Systems Manager for non-AWS instance:

1. Create a hybrid activation for the Linux instances.

For more information about creating a managed instance activation for a hybrid environment, refer to the following link:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-managed-instance-activation.html>

Important: After you successfully complete the activation, an Activation Code and Activation ID appears. Copy this information and save it. If you lose this information, then you must create a new activation.

2. Login to the CLI as an admin user and open the OS Console.

3. Using the Activation Code and Activation ID obtained in Step 1 and run the following command to activate and register the SSM-Agent.

```
amazon-ssm-agent -register -code <activation-code> -id <activation-id> -region <region>
```

Here `<region>` is the identifier of the instance region.

Note:

Note the instance-id. This will be used to perform operations from SSM-Agent.

For more information on how to register a managed instance, refer to the following link:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-install-managed-linux.html#systems-manager-install-managed-linux-deregister-reregister>

- Start the Amazon SSM-Agent from the Services menu or run the following command to start the SSM-Agent.

`/etc/init.d/amazon-ssm-agent start`

15.1.8.6.3 FAQs on AWS Systems Manager

This section lists the FAQs on AWS Systems Manager.

Question	Answer
What can I do when there is a problem with starting the service or the service is automatically updated?	Uninstall and reinstall the Cloud Utility AWS product. For more information on installing and uninstalling the services, refer to the section Add/Remove Services.
What is the name of the service?	The service name is Amazon SSM-Agent.
What can I do if the AWS Systems Manager shows permission denied message after attaching the correct IAM Role?	Restart the service after attaching the IAM role for new permissions to take effect.
Is the Amazon SSM-Agent service available in the Services menu in the Web UI and the CLI?	Yes.
Can I manage the Amazon SSM-Agent service from the Menu option in the Web UI?	Yes, you can start/stop and restart the Amazon SSM Agent service from the Menu option in the Web UI.
After reinstalling the Cloud Utility patch, the Amazon SSM Agent service is <i>Running</i> in the <i>Manual</i> mode. How can I change it to <i>Automatic</i> mode?	To change the status of the service from <i>Manual</i> to <i>Automatic</i> mode, perform the following steps. <ol style="list-style-type: none"> Login to the ESA Web UI using the administrative credentials. Navigate to Systems > Services. Toggle the mode of the service from <i>Manual</i> to <i>Automatic</i>.

15.1.8.7 Troubleshooting for the AWS Cloud Utility

This section lists the troubleshooting for the AWS Cloud Utility.

Error/ Problem	This may happen because...	Recovery
While using AWS services the following error appears: <code>UnknownRegionError("No default region found . . .")</code>	The service is unable to retrieve the <i>AWS Region</i> from the system.	The service is region specific. Include the region name in the command. <code>region=<region-name></code>
The CloudWatch service was running and the service has stopped after restarting the system.	The CloudWatch <i>Service Mode</i> is set to <i>Manual</i>	You should restart the service manually. Note:



Error/ Problem	This may happen because...	Recovery
		If the CloudWatch <i>Service Mode</i> is set to <i>Automatic</i> , then wait until all the services start.
The CloudWatch integration is enabled, but the log group/log stream is not created or logs are not being updated. To verify the error, check the log file by using the following command in the <i>OS Console</i> . <pre>vi /var/log/amazon/amazon-cloudwatch-agent/amazon-cloudwatch-agent.log</pre>	The associated IAM Role or IAM User does not have required permissions to perform CloudWatch-related operations.	Assign <i>CloudWatchAgentServerPolicy</i> permissions to the associated IAM Role or IAM User and restart the service.
You can see one of the following errors: <ul style="list-style-type: none">• <i>E! WriteToCloudWatch failure, err: AccessDenied: User: arn:aws:sts:**** is not authorized to perform: cloudwatch:PutMetricData</i>• <i>E! cloudwatchlogs: code: AccessDeniedException, message: User: arn:aws:sts:**** is not authorized to perform: logs:PutLogEvents</i>• <i>E! CreateLogStream / CreateLogGroup AccessDeniedException: User: arn:aws:sts:**** is not authorized to perform: logs>CreateLogStream</i>		
I can see the following error message: <pre>Unable to locate valid credentials for CloudWatch</pre>	The error message can be because of one of the following reasons: <ul style="list-style-type: none">• If you are using an AWS instance, then the IAM Role is not configured for the AWS instance.• If you are using a non-AWS instance, then the IAM User is configured with invalid AWS credentials on the appliance.	On AWS instance, navigate to the AWS console and attach the IAM role to the instance. For more information about attaching the IAM role, refer to the following link. https://aws.amazon.com/blogs/security/easily-replace-or-attach-an-iam-role-to-an-existing-ec2-instance-by-using-the-ec2-console/ On non-AWS instance, to configure the IAM user with valid credentials, navigate to Tools > CloudWatch Utility AWS Tools > AWS Configure .
I am unable to see AWS Tools section under Tools in the CLI Manager	The AWS Admin role is not assigned to the instance.	For more information about the AWS Admin role, refer to Managing Roles

Error/ Problem	This may happen because...	Recovery
I have installed v7.2.1 patch. However, I am unable to view the AWS Tools menu in the CLI Manager.	The Cloud Utility Product is not installed.	For more information about adding the Cloud Utility Product, refer to the <i>Protegility Installation Guide 9.1.0.5</i> .
I can see one of the following error messages: CloudWatch Service started failed CloudWatch Service stopped failed	The ESA is configured with invalid AWS credentials.	You must reconfigure the ESA with valid AWS credentials.

Appendix

B

Installing Protegility Appliances on Azure

[*15.2.1 Prerequisites*](#)

[*15.2.2 Azure Cloud Utility*](#)

[*15.2.3 Setting up Azure Virtual Network*](#)

[*15.2.4 Creating a Resource Group*](#)

[*15.2.5 Creating a Storage Account*](#)

[*15.2.6 Creating a Container*](#)

[*15.2.7 Obtaining the Azure BLOB*](#)

[*15.2.8 Creating Image from the Azure BLOB*](#)

[*15.2.9 Creating a VM from the Image*](#)

[*15.2.10 Accessing the Appliance*](#)

[*15.2.11 Finalizing the Installation of Protegility Appliance on the Instance*](#)

[*15.2.12 Accelerated Networking*](#)

[*15.2.13 Backing up and Restoring VMs on Azure*](#)

[*15.2.14 Connecting to an ESA Instance*](#)

[*15.2.15 Deploying the Protegility Appliance Instance with the Protectors*](#)

Azure is a cloud computing service offered by Microsoft, which provides services for compute, storage, and networking. It also provides software, platform, and infrastructure services along with support for different programming languages, tools, and frameworks.

The Azure cloud platform includes the following components:

- **Resource groups:** Resource groups in Azure are a collection of multiple Azure resources, such as virtual machines, storage accounts, virtual networks, and so on. The resource groups enable you to manage and maintain the resources as a single entity.
- **Storage accounts:** Azure storage accounts contain all the Azure storage data objects, such as disks, blobs, files, queues, and tables. The data in the storage accounts are scalable, secure, and highly available.
- **BLOB storage:** The BLOB storage is used to store unstructured data on the Azure cloud platform.

15.2.1 Prerequisites

This section describes the prerequisites, including the hardware and network requirements, for installing and using Protegility appliances on Azure.

The following prerequisites are essential to install the Protegility appliances on Azure:

- Sign in URL for the Azure account
- Authentication credentials for the Azure account
- Working knowledge of Azure
- Access to the [My.Protegility](#) portal

Before you begin:

Ensure that you use the following order to create a virtual machine on Azure:

Order	Description
1	Create a Resource Group
2	Create a Storage Account
3	Create a Container
4	Obtain the Azure BLOB
5	Create an image from the BLOB
6	Create a VM from the image

15.2.1.1 Hardware Requirements

As the Protegility appliances are hosted and run on Azure, the hardware requirements are dependent on the configurations provided by Microsoft. However, these requirements can change based on the customer requirements and budget.

The minimum recommendation for an appliance is 8 CPU cores and 32 GB memory. Based on this hardware requirement, select the required configuration for creating the Azure Virtual Machine

For more information about the hardware requirements of ESA, refer to section [System Requirements](#).

Note:

The actual hardware configuration depends on the actual usage or amount of data and logs expected.

15.2.1.2 Network Requirements

The Protegility appliances on Azure are provided with an Azure virtual networking environment. The virtual network enables you to access other instances of Protegility resources in your project.

For more information about configuring Azure virtual network, refer to section [Setting up Azure Virtual Network](#).

15.2.2 Azure Cloud Utility

The Azure Cloud Utility is an appliance component that is available for supporting features specific to Azure Cloud Platform. For Protegility appliances, this component must be installed to utilize the services of Azure Accelerated Networking and Azure

Linux VM agent. When you upgrade or install the appliance from an Azure v9.0.0 blob, the **Azure Cloud Utility** is installed automatically in the appliance.

Note:

If you are utilizing the Azure Accelerated Networking or Azure Linux VM agent, then it is recommended to not uninstall this component.

15.2.3 Setting up Azure Virtual Network

The Azure virtual network is a service that provides connectivity to the virtual machine and services on Azure. You can configure the Azure virtual network by specifying the usable IP addresses. You can also create and configure subnets, network gateways, and security settings.

For more information about setting up Azure virtual network, refer to the Azure virtual network documentation at:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>

If you are using the ESA or the DSG appliance with Azure, ensure that the inbound and outbound ports of the appliances are configured in the virtual network.

For more information about the list of inbound and outbound ports, refer to section [Open Listening Ports](#).

15.2.4 Creating a Resource Group

Resource Groups in Azure are a collection of multiple Azure resources, such as virtual machines, storage accounts, virtual networks, and so on. The resource groups enable to manage and maintain the resources as a single entity.

For more information about creating resource groups, refer to the Azure resource group documentation at,

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-portal>

15.2.5 Creating a Storage Account

Azure storage accounts contain all the Azure storage data objects, such as disks, blobs, files, queues, and tables. The data in the storage accounts are scalable, secure, and highly available.

For more information about creating storage accounts, refer to the Azure storage accounts documentation at,

<https://docs.microsoft.com/en-us/azure/storage/common/storage-quickstart-create-account>

15.2.6 Creating a Container

The data storage objects in a storage account are stored in a container. Similar to directories in a file system, the container in Azure contain BLOBS. You add a container in Azure to store the ESA BLOB.

For more information about creating a container, refer to the following link.

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-quickstart-blobs-portal>



15.2.7 Obtaining the Azure BLOB

In Azure, you can share files across different storage accounts. The ESA that is packaged as a BLOB, is shared across storage accounts on Azure. A BLOB is a data type that is used to store unstructured file formats. Azure supports BLOB storage to store unstructured data, such as audio, text, images, and so on. The BLOB of the appliance is shared by Protegility to the client's storage account.

Before creating the instance on Azure, you must obtain the BLOB from the [My.Protegility](#) portal. On the portal, you select the required ESA version and choose **Azure** as the target cloud platform. You then share the product to your cloud account. The following steps describe how to share the BLOB to your cloud account.

► To obtain and share the BLOB:

1. Log in to the [My.Protegility](#) portal with your user account.
2. Click **Product Management > Explore Products > Data Protection**.
3. Select the required ESA Platform Version.

The **Product Family** table will update based on the selected ESA Platform Version.

Note: The ESA Platform Versions listed in the drop-down menu reflect all versions that were either previously downloaded or shipped within the organization along with any newer versions available thereafter. You can check the list of products previously downloaded from **Product Management > My Product Inventory**.

4. Select the **Product Family**.
The description box will populate with the **Product Family** details.

The screenshot shows the 'PRODUCT MANAGEMENT / EXPLORE PRODUCTS' interface. At the top left, there is a dropdown menu labeled 'ESA Platform Version'. Below it, a sidebar titled 'Product Family' lists several options: Cloud Protect, Gateway Protector, Application Protector, Big Data Protector, Database Protector, Data Warehouse Protector, File Protector, and Mainframe Protector. The 'Enterprise Security Administrator' option is highlighted with a blue background and white text. To the right of the sidebar, a main content area has a title 'Enterprise Security Administrator'. Underneath the title is a 'Description' section containing a detailed paragraph about the product. At the bottom of this section are two buttons: 'View Products' and 'View Compatability Matrix'.

Figure -11: Product Family Screen

5. Click **View Products** to advance to the **Product List** screen.

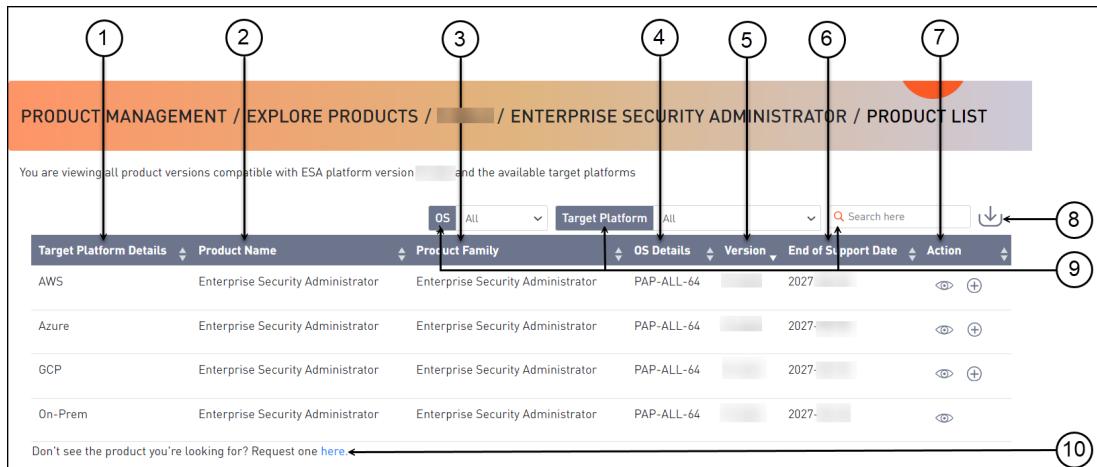


Figure -12: Product List Screen

Table -5: Product List Screen Description

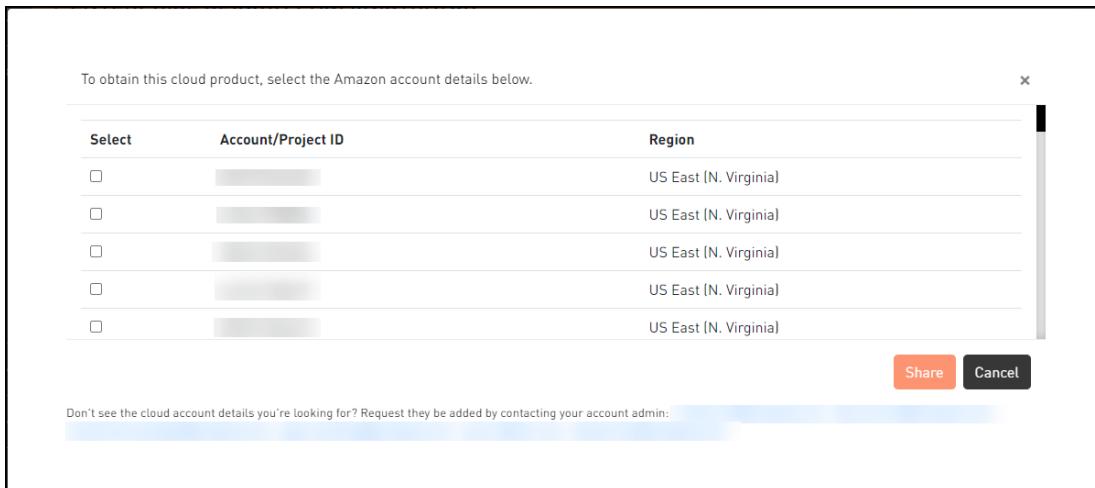
Callout	Element Name	Description
1	Target Platform Details	Shows details about the target platform.
2	Product Name	Shows the product name.
3	Product Family	Shows the product family name.
4	OS Details	Shows the operating system name.
5	Version	Shows the product version.
6	End of Support Date	Shows the final date that Protegity will provide support for the product.
7	Action	Click the View icon (ocular icon) to open the Product Detail screen.
8	Export as CSV	Downloads a .csv file with the results displayed on the screen.
9	Search Criteria	Type text in the search field to specify the search filter criteria or filter the entries using the following options: <ul style="list-style-type: none">• OS• Target Platform
10	Request one here	Opens the Create Certification screen for a certification request.

- Select the **Azure** cloud target platform you require and click the **View** icon (ocular icon) from the **Action** column. The **Product Detail** screen appears.
- Click the **Share Product** icon (cloud icon) to share the Azure cloud product.

Note:

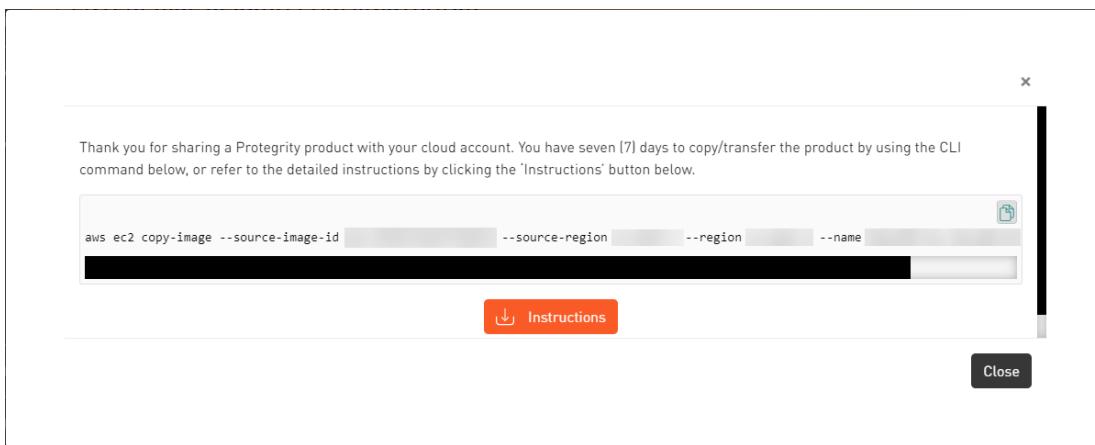
If the user does not have access to cloud products or has access to cloud products and the Customer Cloud Account details are not available, then a message appears with the information that is required and the contact information for obtaining access to cloud share.

A dialog box appears and your available cloud accounts will be displayed.

*Figure -13: Account Selection Screen*

8. Select your required cloud account in which to share the Protegility product.
9. Click **Share**.

A message box is displayed with the command line interface (CLI) instructions with the option to download a detailed PDF containing cloud web interface instructions. Additionally, the instructions for sharing the cloud product are sent to your registered email address and to your notification inbox in [My.Protegility](#).

*Figure -14: Sharing Command*

10. Click the **Copy** icon () to copy the command for sharing the cloud product and run the command in CLI. Alternatively, click **Instructions** to download the detailed PDF instructions for cloud sharing using the CLI or the web interface.

Note:

The cloud sharing instruction file is saved in a `.pdf` format. You need a reader, such as, Acrobat Reader to view the file.

The Cloud Product will be shared with your cloud account for seven (7) days from the original share date in the [My.Protegility](#) portal.

After the seven (7) day time period, you need to request a new share of the cloud product through [My.Protegility](#).

15.2.8 Creating Image from the Azure BLOB

After you obtain the BLOB from Protegility, you must create an image from the BLOB. The following steps describe the parameters that must be selected to create an image.

► To create an image from the BLOB:

1. Log in to the Azure portal.
2. Select **Images** and click **Create**.
3. Enter the details in the **Resource Group**, **Name**, and **Region** text boxes.
4. In the **OS disk** option, select **Linux**.
5. In the **VM generation** option, select **Gen 1**.
6. In the **Storage blob** drop-down list, select the Protegity Azure BLOB.
7. Enter the appropriate information in the required fields and click **Review + create**.
The image is created from the BLOB.

15.2.9 Creating a VM from the Image

After obtaining the image, you can create a VM from it. For more information about creating a VM from the image, refer to the following link.

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/quick-create-portal#create-virtual-machine>

► To create a VM:

1. Login in to the Azure homepage.
2. Click **Images**.
The list of all the images appear.
3. Select the required image.
4. Click **Create VM**.
5. Enter details in the required fields.
6. Select **SSH public key** in the **Authentication type** option.

Note:

As a security measure for the appliances, it is recommended to not use the **Password based mechanism** as an authentication type.

7. In the **Username** text box, enter the name of a user.

Note:

This user is added as an OS level user in the appliance. Ensure that the following usernames are not provided in the **Username** text box:

- [Appliance OS users](#)
- [Appliance LDAP users](#)

8. Select the required SSH public key source.
9. Enter the required information in the *Disks*, *Networking*, *Management*, and *Tags* sections.
10. Click **Review + Create**.



The VM is created from the image.

- After the VM is created, you can access the appliance from the CLI Manager or Web UI.

Note:

The OS user that is created in step 7 does not have SSH access to the appliance. If you want to provide SSH access to this user, login to the appliance as another administrative user and [toggle SSH access](#). In addition, update the user to permit [Linux shell access](#) (`/bin/sh`).

15.2.10 Accessing the Appliance

After setting up the virtual machine, you can access the appliance through the IP address that is assigned to the virtual machine. It is recommended to access the appliance with the administrative credentials.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, then the account gets locked.

For more information on the password policy for the admin and viewer users, refer the section [Password Policy for the LDAP Users](#), and for the `root` and `local_admin` OS users, refer the section [Managing Local OS Users](#).

15.2.11 Finalizing the Installation of Protegility Appliance on the Instance

When you install the appliance, it generates multiple security identifiers such as, keys, certificates, secrets, passwords, and so on. These identifiers ensure that sensitive data is unique between two appliances in a network. When you receive a Protegility appliance image, the identifiers are generated with certain values. If you use the security identifiers without changing their values, then security is compromised and the system might be vulnerable to attacks. Using the **Rotate Appliance OS Keys**, you can randomize the values of these security identifiers for an appliance. During the finalization process, you run the key rotation tool to secure your appliance.

Note:

If you do not complete the finalization process, then some features of the appliance may not be functional including the Web UI.

For example, if the OS keys are not rotated, then you might not be able to add appliances to a Trusted Appliances Cluster (TAC).

Note:

For information about the default passwords, refer to the section [Launching the ESA instance on Microsoft Azure](#) in the [Release Notes 9.0.0](#).

15.2.11.1 Finalizing ESA Installation

You can finalize the installation of the ESA after signing in to the CLI Manager.

Caution:



Ensure that the finalization process is initiated from a single session only. If you start finalization simultaneously from a different session, then the *"Finalization is already in progress."* message appears. You must wait until the finalization of the instance is successfully completed.

Additionally, ensure that the appliance session is not interrupted. If the session is interrupted, then the instance becomes unstable and the finalization process is not completed on that instance.

► To finalize ESA installation:

1. Sign in to the ESA CLI Manager of the instance created using the default administrator credentials.
The following screen appears.

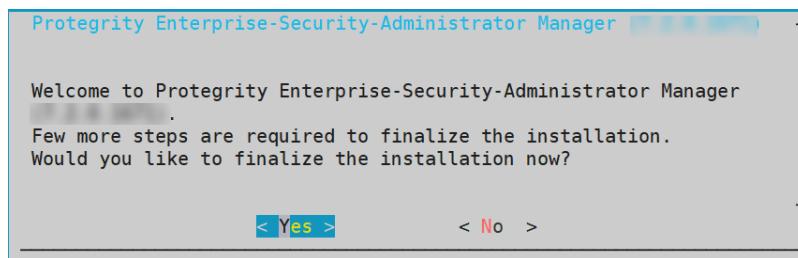


Figure -15: Finalizing Installation Confirmation screen

2. Select **Yes** to initiate the finalization process.
The screen to enter the administrative credentials appears.

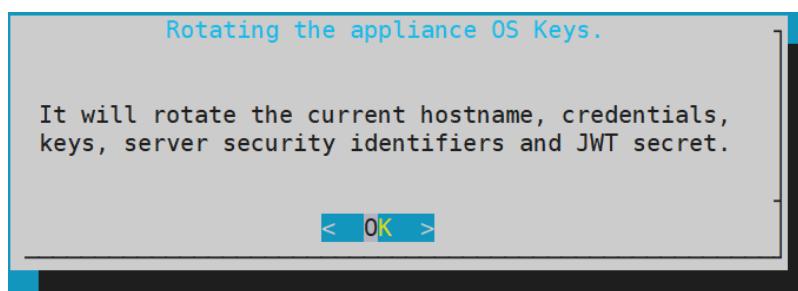
Note:

If you select **No**, then the finalization process is not initiated.

To manually initiate the finalization process, navigate to **Tools > Finalize Installation** and press **ENTER**.

3. Enter the credentials for the *admin* user and select **OK**.

A confirmation screen to rotate the appliance OS keys appears.



4. Select **OK** to rotate the appliance OS keys.

The following screen appears.

User's Passwords

Please provide user's passwords

root password	
root password verification	
admin password	
admin password verification	
viewer password	
viewer password verification	
local_admin password	
local_admin password verification	

[<Apply>](#)

[<Help >](#)

- a. To update the user passwords, provide the credentials for the following users:

- root
- admin
- viewer
- local_admin

- b. Select **Apply**.

The user passwords are updated and the appliance OS keys are rotated.

The finalization process is completed.

Note:

The appliance comes with some products installed by default. If you want to verify the installed products or install additional products, then navigate to **Administration > -- Installations and Patches -- > Add/Remove Services**.

For more information about installing products, refer the section *Working with Installation and Packages* in *Protegility Installation Guide 9.1.0.5*.

15.2.12 Accelerated Networking

Accelerated networking is a feature provided by Microsoft Azure which enables the user to improve the performance of the network. This is achieved by enabling the Single-root input/output virtualization to a virtual machine.

In a virtual environment, SR-IOV specifies the isolation of the PCIe resources to improve the manageability and performance. The SR-IOV interface helps to virtualize, access, and share the PCIe resources, such as, the connection ports for graphic cards, hard drives, and so on. This successfully reduces the latency, network jitters and CPU utilization.

As shown in *figure 16-9*, the virtual switch is an integral part of a network for connecting the hardware and the virtual machine. The virtual switch helps in enforcing the policies on the virtual machine. These policies include access control lists, isolation, network security controls, and so on, and are implemented on the virtual switch. The network traffic routes through the virtual

switch and the policies are implemented on the virtual machine. This results in higher latency, network jitters, and higher CPU utilization.

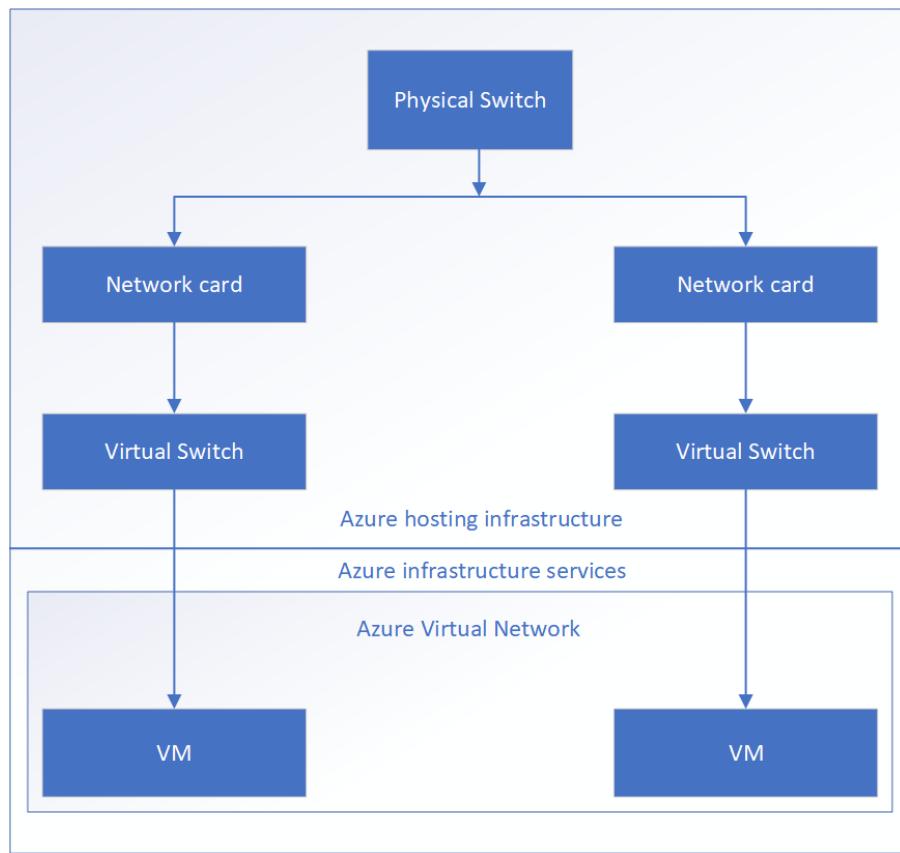


Figure -16: Without Accelerated Networking

However, in an accelerated network, the policies are applied on the hardware. The network traffic only routes through the network cards directly forwarding it to the virtual machine. The policies are applied on the hardware instead of the virtual switch. This helps the network traffic to bypass the virtual switch and the host while maintaining the policies applied at the host. Reducing the layers of communication between the hardware and the virtual machine helps to improve the network performance.

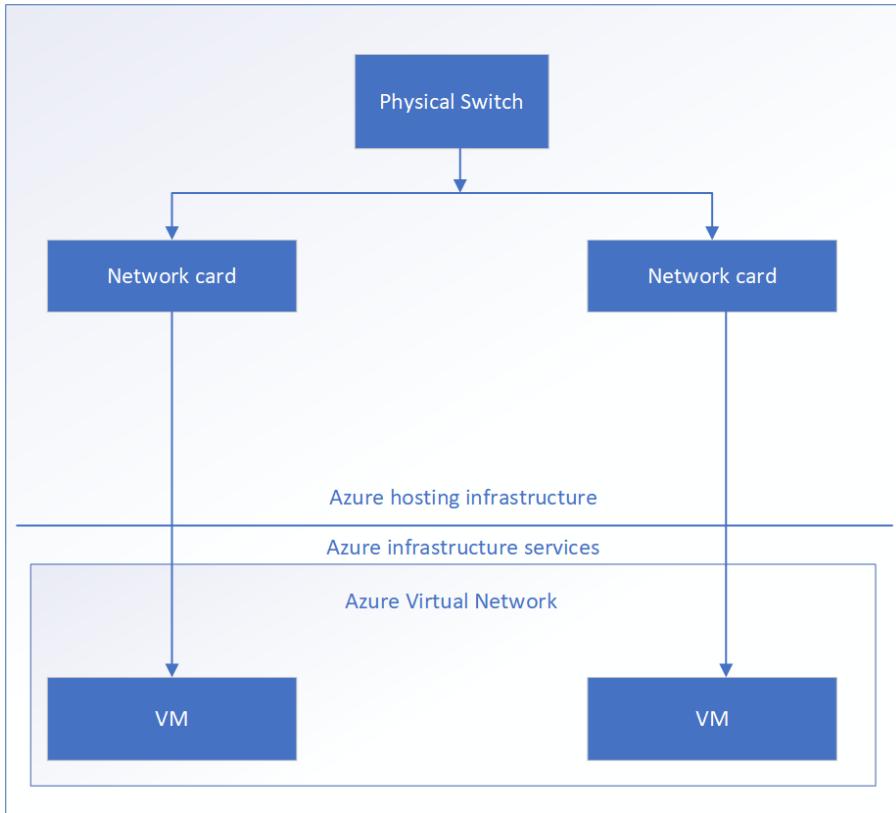


Figure -17: With Accelerated Networking

Following are the benefits of accelerated networking:

- **Reduced Latency:** Bypassing the virtual switch from the data path increases the number of packets which are processed in the virtual machine.
- **Reduced Jitter:** Bypassing the virtual switch and host from the network reduces the processing time for the policies. The policies are directly implemented on the virtual machine thereby reducing the network jitters caused by the virtual switch.
- **CPU Utilization:** Applying the policies to the hardware and implementing them directly on the virtual machine reduces the workload on the CPU to process these policies.

15.2.12.1 Prerequisites

The following prerequisites are essential to enable or disable the Azure Accelerated Networking feature.

- A machine with the Azure CLI should be configured.

Note:

This must be a separate Windows or Linux machine.

For more information about installing the Azure CLI, refer to the following link.

<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest>

- The Protegity appliance must be in the *stop (deallocated)* state.
- The virtual machine must use the supported instance size.

For more information about the supported series of virtual machines for the accelerated networking feature, refer to the [Supported Instance Sizes for Accelerated Networking](#).

15.2.12.2 Supported Instance Sizes for Accelerated Networking

There are several series of instance sizes used on the virtual machines that support the accelerated networking feature.

These include the following:

- D/DSv2
- D/DSv3
- E/ESv3
- F/FS
- FSv2
- Ms/Mms

The most generic and compute-optimized instance sizes for the accelerated networking feature is with 2 or more vCPUs. However, on the systems with supported hyperthreading features, the accelerated networking feature must have instance sizes with 4 or more vCPUs.

For more information about the supported instance sizes, refer to the following link.

<https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli#limitations-and-constraints>

15.2.12.3 Creating a Virtual Machine with Accelerated Networking Enabled

If you want to enable accelerated networking while creating the instance, then it is achieved only from the Azure CLI. The Azure portal does not provide the option to create an instance with accelerated networking enabled.

For more information about creating a virtual machine with accelerated networking, refer to the following link.

<https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli#create-a-linux-vm-with-azure-accelerated-networking>

Perform the following steps to create a virtual machine with the accelerated networking feature enabled.

► To create a virtual machine with the accelerated networking feature enabled:

1. From the machine on which the Azure CLI is installed, login to Azure using the following command.

```
az login
```

2. Create a virtual machine using the following command.

```
az vm create --image <name of the Image> --resource-group <name of the resource group>
--name <name of the new instance> --size <configuration of the instance> --admin-username
<administrator username> --ssh-key-values <SSH key path> --public-ip-address "" --nsg
<Azure virtual network> --accelerated-networking true
```

For example, the to create a virtual machine with the following parameters.

Parameter	Value
Name of the image	ProtegityESAAzure
name-of-resource-group	MyResourcegroup
size	Standard_DS3_v2
admin-username	admin
nsg	TierpointAccessDev
ssh-key-value	/testkey.pub

The virtual machine is created with the accelerated networking feature enabled.

15.2.12.4 Enabling Accelerated Networking

Perform the following steps to enable the Azure Accelerated Networking feature on the Protegity appliance.

► To enable accelerated networking:

- From the machine on which the Azure CLI is installed, login to Azure using the following command.

```
az login
```

- Stop the Protegity appliance using the following command.

```
az vm deallocate --resource-group <ResourceGroupName> --name <InstanceName>
```

Parameter	Description
ResourceGroupName	Name of the resource group where the instance is located
InstanceName	Name of the instance that you want to stop

- Enable accelerated networking on your virtual machine's network card using the following command.

```
az network nic update --name <nic-name> --resource-group <ResourceGroupName> --accelerated-networking true
```

Parameter	Description
nic-name	Name of the network interface card attached to the instance where you want to enable accelerated networking
ResourceGroupName	Name of the resource group where the instance is located

- Start the Protegity appliance.

15.2.12.5 Disabling Accelerated Networking

Perform the following steps to disable the Azure Accelerated Networking features on the Protegity appliance.

► To disable accelerated networking:

- From the machine on which the Azure CLI is installed, login to Azure using the following command.

```
az login
```

- Stop the Protegity appliance using the following command.

```
az vm deallocate --resource-group <ResourceGroupName> --name <InstanceName>
```

Parameter	Description
ResourceGroupName	Name of the resource group where the instance is located
InstanceName	Name of the instance that you want to stop

- Disable accelerated networking on your virtual machine's network card using the following command.

```
az network nic update --name <nic-name> --resource-group <ResourceGroupName> --accelerated-networking false
```

Parameter	Description
nic-name	Name of the network interface card attached to the instance where you want to enable accelerated networking
ResourceGroupName	Name of the resource group where the instance is located

- Start the Protegity appliance.

15.2.12.6 Troubleshooting and FAQs for Azure Accelerated Networking

This section lists the Troubleshooting and FAQs for the Azure Accelerated Networking feature.

Question	Answer
What is the recommended number of virtual machines required in the Azure virtual network?	It is recommended to have at least two or more virtual machines in the Azure virtual network.
Can I stop/deallocate my machine from the Web UI?	Yes. You can stop/deallocate your machine from the Web UI. Navigate to the Azure instance details page and click Stop from the top ribbon.
Can I uninstall the Cloud Utility Azure if the accelerated networking feature is enabled?	It is recommended to disable the accelerated networking feature before uninstalling the Cloud Utility Azure.
How do I verify that the accelerated networking is enabled on my machine?	<p>Perform the following steps.</p> <ol style="list-style-type: none"> Login to the CLI manager. Navigate to Administration > OS Console. Enter the <i>root</i> credentials. <p>Verify that the Azure Accelerated Networking feature is enabled by using the following commands.</p> <pre># lspci grep "Virtual Function"</pre> <p><i>Confirm the Mellanox VF device is exposed to the VM with the lspci command.</i></p> <p>The following is a sample output:</p>

Question	Answer
	<p><i>001:00:02.0 Ethernet controller: Mellanox Technologies MT27500/MT27520 Family [ConnectX-3/ConnectX-3 Pro Virtual Function]</i></p> <pre># ethtool -S ethMNG grep vf</pre> <p><i>Check for activity on the VF (virtual function) with the ethtool -S eth0 / grep vf_ command. If you receive an output similar to the following sample output, accelerated networking is enabled and working. The value of the packets and bytes should not be zero</i></p> <p><i>vf_rx_packets: 992956</i></p> <p><i>vf_rx_bytes: 2749784180</i></p> <p><i>vf_tx_packets: 2656684</i></p> <p><i>vf_tx_bytes: 1099443970</i></p> <p><i>vf_tx_dropped: 0</i></p>
How do I verify from the Azure Web portal that the accelerated networking is enabled on my machine?	<p>Perform the following steps.</p> <ol style="list-style-type: none"> From the Azure Web portal, navigate to the virtual machine's details page. From the left pane, navigate to Networking. If there are multiple NICs, then select the required NIC. Verify that the accelerated networking feature is enabled from the Accelerated Networking field.
Can I use the <i>Cloud Shell</i> on the Azure portal for enabling or disabling the accelerated networking feature?	<p>Yes, you can use the <i>Cloud Shell</i> for enabling or disabling the accelerated networking. For more information about the pricing of the cloud shell, refer to the following link.</p> <p>https://azure.microsoft.com/en-in/pricing/details/cloud-shell</p>
How can I enable the accelerated networking feature using the <i>Cloud Shell</i> ?	<p>Perform the following steps to enable the accelerated networking feature using the <i>Cloud Shell</i>.</p> <ol style="list-style-type: none"> From the Microsoft Azure portal, launch the Cloud Shell. Stop the Protegity appliance using the following command. <pre>az vm deallocate --resource-group <ResourceGroupName> --name <InstanceName></pre> <ol style="list-style-type: none"> Enable accelerated networking on your virtual machine's network card using the following command: <pre>az network nic update --name <nic-name> --resource-group <ResourceGroupName> --accelerated-networking true</pre> <ol style="list-style-type: none"> Start the Protegity appliance.
How can I disable the accelerated networking feature using the <i>Cloud Shell</i> ?	<p>Perform the following steps to disable the accelerated networking feature using the <i>Cloud Shell</i>.</p> <ol style="list-style-type: none"> From the Microsoft Azure portal, launch the Cloud Shell.

Question	Answer
	<p>2. Stop the Protegity appliance using the following command.</p> <pre>az vm deallocate --resource-group <ResourceGroupName> --name <InstanceName></pre> <p>3. Enable accelerated networking on your virtual machine's network card using the following command:</p> <pre>az network nic update --name <nic-name> --resource-group <ResourceGroupName> --accelerated-networking false</pre> <p>4. Start the Protegity appliance.</p>
Are there any specific regions where the accelerated networking feature is supported?	<p>The accelerated networking feature is supported in all public Azure regions and Azure government clouds.</p> <p>For more information about the supported regions, refer to the following link:</p> <p>https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli#regions</p>
Is it necessary to stop (deallocate) the machine to enable/disable the accelerated networking feature?	<p>Yes. It is necessary to <i>stop (deallocate)</i> the machine to enable/disable the accelerated networking feature.</p> <p>This is because if the machine is not in the <i>stop (deallocate)</i> state, then it may cause the value of the vf packets to freeze. This results in an unexpected behaviour of the machine.</p>
Is there any additional cost for using the accelerated networking feature?	<p>No. There is no additional cost required for using the accelerated networking feature.</p> <p>For more information about the costing, contact <i>Protegity Support</i>.</p>

15.2.13 Backing up and Restoring VMs on Azure

On Azure, you can prevent unintended loss of data by backing up your virtual machines. Azure allows you to optimize your backup by providing different levels of consistency. Similarly, the data on the virtual machines can be easily restored to a stable state. You can back up a virtual machine using the following two methods:

- Creating snapshots of the disk
- Using recovery services vaults

This following sections describe how to create and restore backups using the two mentioned methods.

15.2.13.1 Backing up and Restoring using Snapshots of Disks

The following sections describe how to create snapshots of disks and recover them on virtual machines. This procedure of backup and recovery is applicable for virtual machines that are created from disks and custom images.

15.2.13.1.1 Creating a Snapshot of a Virtual Machine on Azure

► To create a snapshot of a virtual machine:

1. Sign in to the Azure homepage.
2. On the left pane, select **Virtual machines**.

The **Virtual machines** screen appears.



3. Select the required virtual machine and click **Disks**.

The details of the disk appear.

4. Select the disk and click **Create Snapshot**.

The **Create Snapshot** screen appears.

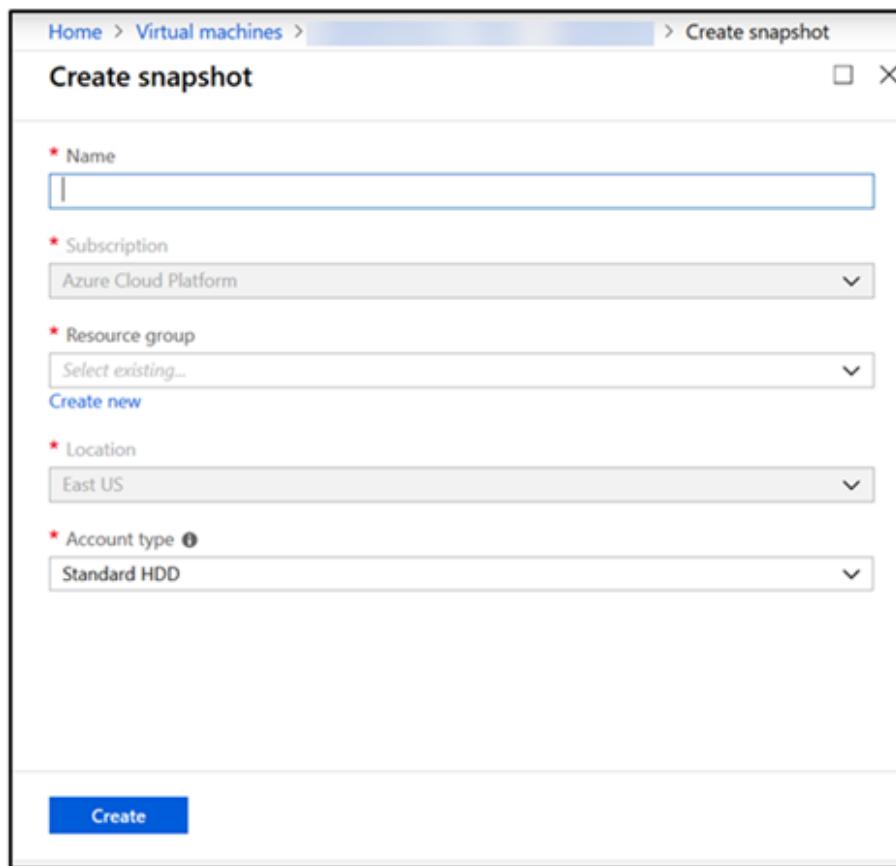


Figure -18: Create Snapshot Screen

5. Enter the following information:

- **Name:** Name of the snapshot
- **Subscription:** Subscription account for Azure

6. Select the required resource group from the **Resource group** drop-down list.

7. Select the required account type from the **Account type** drop-down list.

8. Click **Create**.

The snapshot of the disk is created.

15.2.13.1.2 Restoring from a Snapshot on Azure

This section describes the steps to restore a snapshot of a virtual machine on Azure.

Note:

Ensure that the snapshot of the machine is taken.

- To restore a virtual machine from a snapshot:

1. On the Azure Dashboard screen, select **Virtual Machine**.
The screen displaying the list of all the Azure virtual machines appears.
2. Select the required virtual machine.
The screen displaying the details of the virtual machine appears.
3. On the left pane, under **Settings**, click **Disk**.
4. Click **Swap OS Disk**.
The **Swap OS Disk** screen appears.
5. Click the **Choose disk** drop-down list and select the snapshot created.
6. Enter the confirmation text and click **OK**.
The machine is stopped and the disk is successfully swapped.
7. Restart the virtual machine to verify whether the snapshot is available.

15.2.13.2 Backing up and Restoring using Recovery Services Vaults

Recovery services vault is an entity that stores backup and recovery points. They enable you to copy the configuration and data from virtual machines. The benefit of using recovery services vaults is that it helps organize your backups and minimize the overhead of management. It comes with enhanced capabilities of backing up data without compromising on data security. These vaults also allow you to create backup policies for virtual machines, thus ensuring integrity and protection. Using recovery services vaults, you can retain recovery points of protected virtual machines to restore them at a later point in time.

For more information about Recovery services vaults, refer to the following link:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview>

Note:

This process of backup and restore is applicable only for virtual machines that are created from a custom image.

15.2.13.2.1 Creating Recovery Services Vaults

Before starting with the backup procedure, you must create a recovery services vault.

► To create a recovery services vault:

Before you begin

Ensure that you are aware about the pricing and role-based access before proceeding with the backup.

For more information about the pricing and role-based access, refer to the following links:

<https://azure.microsoft.com/en-us/pricing/details/backup/>

<https://docs.microsoft.com/en-us/azure/backup/backup-rbac-roles#mapping-backup-built-in-roles-to-backup-management-actions>

1. Sign in to the Azure homepage.
2. On the Azure Dashboard screen, search **Recovery Services vaults**.
The screen displaying all the services vaults appears.

3. Click **Add**.
The **Create Recovery Services vault** screen appears.
4. Populate the following fields:
 - **Subscription:** Account name under which the recovery services vault is created
 - **Resource group:** Associate a resource group to the vault
 - **Vault name:** Name of the vault
 - **Region:** Location where the data for recovery vault must be stored
 The **Welcome to Azure Backup** screen appears on the right pane.
5. Click **Review + create**.
The recovery services vault is created.

15.2.13.2.2 Backing up Virtual Machine using Recovery Services Vault

This section describes how to create a backup of a virtual machine using a Recovery Services Vault. For more information about the backup, refer to the link, <https://docs.microsoft.com/en-us/azure/backup/backup-azure-vm-backup-faq>

► To create a backup of a virtual machine:

1. Sign in to the Azure homepage.
2. On the left pane, select **Virtual machines**.
The **Virtual machines** screen appears.
3. Select the required virtual machine.
4. On the left pane, under **Operations** tab, click **Backup**.
The **Welcome to Azure Backup** screen appears on the right pane.
5. From the **Recovery Services vault** option, choose **Select existing** and select the required vault.
6. In the backup policy, you specify the frequency, backup schedule, and so on. From the **Choose backup policy** option, select a policy from the following options:
 - **DailyPolicy:** Retain the daily backup taken at 9.00 AM UTC for 180 days
 - **DefaultPolicy:** Retain the daily backup taken at 10.30 AM UTC for 30 days
 - **Create backup policy:** Customize the backup policy as per your requirements
7. Click **Enable backup**.
A notification stating that backup is initiated appears.
8. On the Azure Dashboard screen, search **Recovery Services vaults**.
The screen displaying all the services vaults appears.
9. Select the required services vault.
The screen displaying the details of the virtual machine appears.
10. On the center pane, under **Protected items**, click **Backup items**.
The screen displaying the different management types vault appears.
11. Select the required management type.
After the backup is completed, the list displays the virtual machine for which the backup was initiated.

15.2.13.2.3 Restoring a Virtual Machine using Recovery Services Vaults

In Azure, when restoring a virtual machine using Recovery Services vaults, you have the following two options:

- **Creating a virtual machine:** Create a virtual machine with the backed up information.
- **Replacing an existing:** Replace an existing disk on the virtual machine with the backed up information.

15.2.13.2.3.1 Restoring by Creating a Virtual Machine

This section describes how to restore a backup on a virtual machine by creating a virtual machine.

Note:

Ensure that the backup process for the virtual machine is completed.

► To restore a virtual machine by creating a virtual machine:

1. On the Azure Dashboard screen, search **Recovery Services vaults**.
The screen displaying all the services vaults appears.
2. Select the required services vault.
The screen displaying the details of the services vault appears.
3. On the center pane, under **Protected items**, click **Backup items**.
The screen displaying the different management types vault appears.
4. Select the required management type.
The virtual machines for which backup has been initiated appears.
5. Select the virtual machine.
The screen displaying the backup details, and restore points appear.
6. Click **Restore VM**.
The **Select Restore point** screen appears.
7. Choose the required restore point and click **OK**.
The **Restore Configuration** screen appears.
8. If you want to create a virtual machine, click **Create new**.
 - a. Populate the following fields for the respective options:
 - **Restore type**: Create a new virtual machine without overwriting an existing backup
 - **Virtual machine name**: Name for the virtual machine
 - **Resource group**: Associate vault to a resource group
 - **Virtual network**: Associate vault to a virtual network
 - **Storage account**: Associate vault to a storage account
 - b. Click **OK**.
9. Click **Restore**.
The restore process is initiated. A virtual machine is created with the backed up information.

15.2.13.2.3.2 Restoring a Virtual Machine using by Restoring a Disk

This section describes how to restore a backup on a virtual machine by restoring a disk on a virtual machine.

Note:

Ensure that the backup process for the virtual machine is completed. Also, ensure that the VM is stopped before performing the restore process.

► To restore a virtual machine by creating a virtual machine:

1. On the Azure Dashboard screen, search **Recovery Services vaults**.
The screen displaying all the services vaults appears.
2. Select the required services vault.
The screen displaying the details of the services vault appears.
3. On the center pane, under **Protected items**, click **Backup items**.
The screen displaying the different management types vault appears.
4. Select the required management type.
The virtual machines for which backup has been initiated appears.
5. Select the virtual machine.
The screen displaying the backup details, and restore points appear.
6. Click **Restore VM**.
The **Select Restore point** screen appears.
7. Choose the required restore point and click **OK**.
The **Restore Configuration** screen appears.
8. Click **Replace existing**.
 - a. Populate the following fields:
 - **Restore type**: Replace the disk from a selected restore point.
 - **Staging location**: Temporary location used during the restore process.
 - b. Click **OK**.
9. Click **Restore**.
The restore process is initiated. The backup is restored by replacing an existing disk on the machine with the disk containing the backed up information.

15.2.14 Connecting to an ESA Instance

If you are using an instance of the DSG appliance on Azure, you must connect it to an instance of the ESA appliance. Using the CLI manager, you must provide the connectivity details of the ESA appliance in the DSG appliance.

For more information about connecting a DSG instance with ESA, refer to the section *Setting up ESA Communication* in the [*Protegility Data Security Gateway User Guide 3.1.0.5*](#).

15.2.15 Deploying the Protegility Appliance Instance with the Protectors

You can configure the various protectors that are a part of the Protegility Data Security Platform with an instance of the ESA appliance running on Azure.

Depending on the cloud-based environment that hosts the protectors, the protectors can be configured with the instance of the ESA appliance in one of the following ways:

- If the protectors are running on the same virtual network as the instance of the ESA appliance, then the protectors need to be configured using the internal IP address of the ESA appliance within the virtual network.
- If the protectors are running on a different virtual network than that of the ESA appliance, then the virtual network of the ESA instance needs to be configured to connect to the virtual network of the protectors.

Appendix

C

Installing Protegity Appliances on Google Cloud Platform (GCP)

[*15.3.1 Verifying Prerequisites*](#)

[*15.3.2 Configuring the Virtual Private Cloud \(VPC\)*](#)

[*15.3.3 Obtaining the GCP Image*](#)

[*15.3.4 Converting the Raw Disk to a GCP Image*](#)

[*15.3.5 Loading the Protegity Appliance from a GCP Image*](#)

[*15.3.6 Finalizing the Installation of Protegity Appliance on the Instance*](#)

[*15.3.7 Connecting to an ESA instance \(for DSG deployment\)*](#)

[*15.3.8 Deploying the Instance of the Protegity Appliance with the Protectors*](#)

[*15.3.9 Backing up and Restoring Data on GCP*](#)

[*15.3.10 Increasing Disk Space on the Appliance*](#)

The Google Cloud Platform (GCP) is a cloud computing service offered by Google, which provides services for compute, storage, networking, cloud management, security, and so on. The following products are available on GCP:

- **Google Compute Engine** provides virtual machines for instances
- **Google App Engine** provides a Software Developer Kit (SDK) to develop products
- **Google Cloud Storage** is a storage platform to store large data sets
- **Google Container Engine** is a cluster-oriented container to develop and manage Docker containers

Protegity provides the images for GCP that contain either the Enterprise Security Administrator (ESA), or the Data Security Gateway (DSG).

This section describes the prerequisites and tasks for installing Protegity appliances on GCP. In addition, it describes some best practices for using the Protegity appliances on GCP effectively.

15.3.1 Verifying Prerequisites

This section describes the prerequisites including the hardware, software, and network requirements for installing and using Protegity appliances on GCP.

15.3.1.1 Prerequisites

The following prerequisite is essential to install the Protegility appliances on GCP:

- A GCP account and the following information:
 - Login URL for the GCP account
 - Authentication credentials for the GCP account
 - Access to the [My.Protegility](#) portal

15.3.1.2 Hardware Requirements

As the Protegility appliances are hosted and run on GCP, the hardware requirements are dependent on the configurations provided by GCP. However, these requirements can autoscale as per customer requirements and budget.

The minimum recommendation for an appliance is 8 CPU cores and 32 GB memory. Based on this hardware requirement, select the required configuration for creating the GCP instance.

For more information about the hardware requirements of ESA, refer to section [System Requirements](#).

Note:

The actual hardware configuration depends on the actual usage or amount of data and logs expected.

15.3.1.3 Network Requirements

The Protegility appliances on GCP are provided with a Google Virtual Private Cloud (VPC) networking environment. The Google VPC enables you to access other instances of Protegility resources in your project.

You can configure the Google VPC by specifying the IP address range. You can also create and configure subnets, network gateways, and the security settings.

For more information about the Google VPC, refer to the VPC documentation at: <https://cloud.google.com/vpc/docs/vpc>

If you are using the ESA or the DSG appliance with GCP, then ensure that the inbound and outbound ports of the appliances are configured in the VPC.

For more information about the list of inbound and outbound ports, refer to the section [Open Listening Ports](#).

15.3.2 Configuring the Virtual Private Cloud (VPC)

You must configure your Virtual Private Cloud (VPC) to connect to different Protegility appliances.

► To configure a VPC:

1. Ensure that you are logged in to the GCP Console.
2. Navigate to the **Home** screen.
3. Click the navigation menu on the Home screen.

4. Under Networking, navigate to **VPC network > VPC networks**.
The *VPC networks* screen appears.
5. Click **CREATE VPC NETWORK**.
The *Create a VPC network* screen appears.
6. Enter the name and description of the VPC network in the **Name** and **Description** text boxes.
7. Under the Subnets area, Click **Custom** to add a subnet.
 - a. Enter the name of the subnet in the **Name** text box.
 - b. Click **Add a Description** to enter a description for the subnet.
 - c. Select the region where the subnet is placed from the **Region** drop-down menu.
 - d. Enter the IP address range for the subnet in the **IP address range** text box.
For example, *10.0.0.0/99*.
- e. Select **On** or **Off** from the Private Google Access options to set access for VMs on the subnet to access Google services without assigning external IP addresses.
- f. Click **Done**.

Note:

Click **Add Subnet** to add another subnet.

8. Select **Regional** from the Dynamic routing mode option.

9. Click **Create** to create the VPC.

The VPC is added to the network.

15.3.2.1 Adding a Subnet to the Virtual Private Cloud (VPC)

You can add a subnet to your VPC.

► To add a subnet:

1. Ensure that you are logged in to the GCP Console.
2. Under Networking, navigate to **VPC network > VPC networks**.
The *VPC networks* screen appears.
3. Select the VPC.
The *VPC network details* screen appears.
4. Click **EDIT**.
5. Under Subnets area, click **Add Subnet**.
The **Add a subnet** screen appears.
6. Enter the subnet details.
7. Click **ADD**.
8. Click **Save**.

The subnet is added to the VPC.

15.3.3 Obtaining the GCP Image

Before creating the instance on GCP, you must obtain the image from the [My.Protegility](#) portal. On the portal, you select the required ESA version and choose **GCP** as the target cloud platform. You then share the product to your cloud account. The following steps describe how to share the image to your cloud account.

► To obtain and share the image:

1. Log in to the [My.Protegility](#) portal with your user account.
2. Click **Product Management > Explore Products > Data Protection**.
3. Select the required ESA Platform Version.

The **Product Family** table will update based on the selected ESA Platform Version.

Note: The ESA Platform Versions listed in the drop-down menu reflect all versions that were either previously downloaded or shipped within the organization along with any newer versions available thereafter. You can check the list of products previously downloaded from **Product Management > My Product Inventory**.

4. Select the **Product Family**.
The description box will populate with the **Product Family** details.

The screenshot shows the 'PRODUCT MANAGEMENT / EXPLORE PRODUCTS' interface. A dropdown menu labeled 'ESA Platform Version' is open. On the left, a sidebar titled 'Product Family' lists several options under 'Enterprise Security Administrator': Cloud Protect, Gateway Protector, Application Protector, Big Data Protector, Database Protector, Data Warehouse Protector, File Protector, and Mainframe Protector. The 'Enterprise Security Administrator' section on the right contains a title, a description, and two buttons: 'View Products' and 'View Compatability Matrix'. The description text reads: 'Protegility Enterprise Security Administrator (ESA) is an intuitive, comprehensive interface for centralized, visual administration of data security policies, key management, auditing and reporting of sensitive data assets across the enterprise. ESA provides full policy lifecycle management and policy feedback tools and dashboard to enable defining, monitoring and subsequently changing data security policies without disrupting business, modifying application code, or changing the underlying application environment.'

Figure -19: Product Family Screen

5. Click **View Products** to advance to the **Product List** screen.

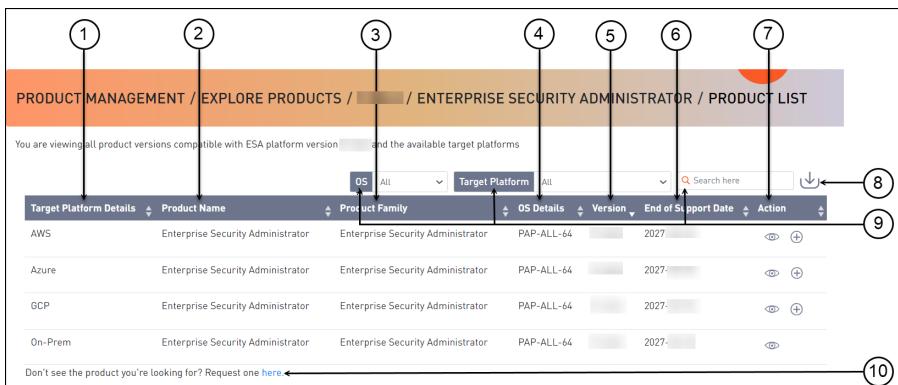


Figure -20: Product List Screen

Table -6: Product List Screen Description

Callout	Element Name	Description
1	Target Platform Details	Shows details about the target platform.
2	Product Name	Shows the product name.
3	Product Family	Shows the product family name.
4	OS Details	Shows the operating system name.
5	Version	Shows the product version.
6	End of Support Date	Shows the final date that Protegility will provide support for the product.
7	Action	Click the View icon (eye icon) to open the Product Detail screen.
8	Export as CSV	Downloads a .csv file with the results displayed on the screen.
9	Search Criteria	Type text in the search field to specify the search filter criteria or filter the entries using the following options: <ul style="list-style-type: none">• OS• Target Platform
10	Request one here	Opens the Create Certification screen for a certification request.

- Select the GCP cloud target platform you require and click the **View** icon (eye icon) from the **Action** column. The **Product Detail** screen appears.
- Click the **Share Product** icon (cloud icon) to share the GCP cloud product.

Note:

If the user does not have access to cloud products or has access to cloud products and the Customer Cloud Account details are not available, then a message appears with the information that is required and the contact information for obtaining access to cloud share.

A dialog box appears and your available cloud accounts will be displayed.

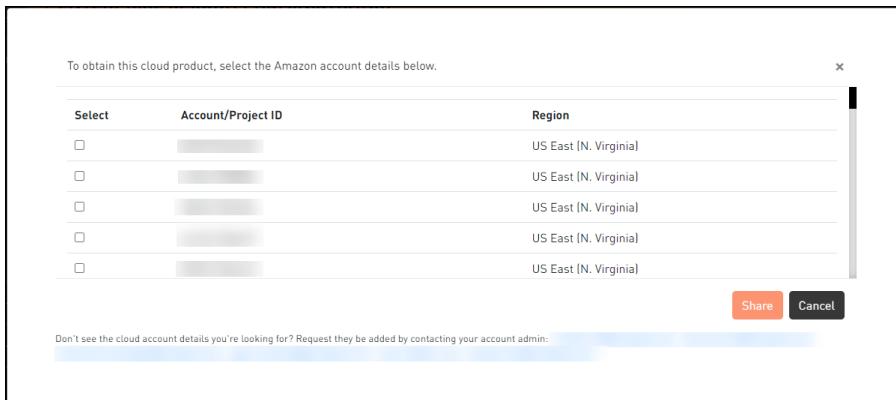


Figure -21: Account Selection Screen

8. Select your required cloud account in which to share the Protegility product.

9. Click **Share**.

A message box is displayed with the command line interface (CLI) instructions with the option to download a detailed PDF containing cloud web interface instructions. Additionally, the instructions for sharing the cloud product are sent to your registered email address and to your notification inbox in [My.Protegility](#).

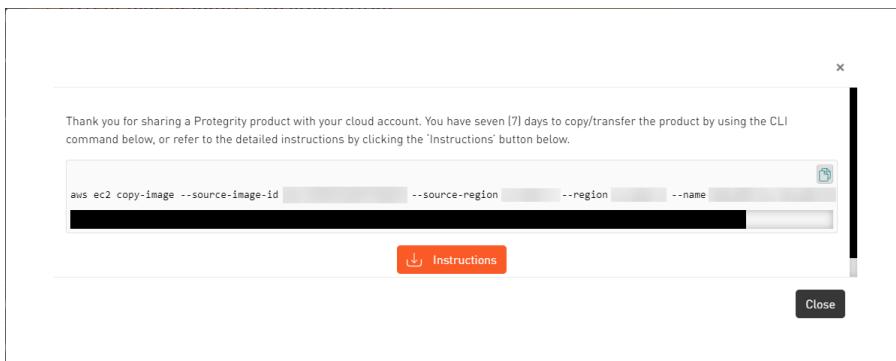


Figure -22: Sharing Command

10. Click the **Copy** icon () to copy the command for sharing the cloud product and run the command in CLI. Alternatively, click **Instructions** to download the detailed PDF instructions for cloud sharing using the CLI or the web interface.

Note:

The cloud sharing instruction file is saved in a `.pdf` format. You need a reader, such as, Acrobat Reader to view the file.

The Cloud Product will be shared with your cloud account for seven (7) days from the original share date in the [My.Protegility](#) portal.

After the seven (7) day time period, you need to request a new share of the cloud product through [My.Protegility](#).

15.3.4 Converting the Raw Disk to a GCP Image

After obtaining the image from Protegility, you can proceed to create a virtual image. However, the image provided is available as disk in a raw format. This must be converted to a GCP specific image before you create an instance. The following steps provide the details of converting the image in a raw format to a GCP-specific image.

- To convert the image:

1. Login to the GCP Console.
2. Run the following command.

```
gcloud compute images create <Name for the new GCP Image> --source-uri gs://<Name of the storage location where the raw image is obtained>/<Name of the GCP image>
```

For example,

```
gcloud compute images create esa80 --source-uri gs://stglocation80/esa-pap-all-64-x86-64-gcp-8-0-0-0-1924.tar.gz
```

The raw image is converted to a GCP-specific image. You can now create an instance using this image

15.3.5 Loading the Protegility Appliance from a GCP Image

This section describes the tasks that you must perform to load the Protegility appliance from an image that is provided by Protegility. You must create a VM instance using the image provided in the following two methods:

- Creating a VM instance from the Protegility appliance image provided
- Creating a VM instance from a disk that is created with an image of the Protegility appliance

15.3.5.1 Creating a VM Instance from an Image

This section describes how to create a VM instance from an appliance image provided to you.

 To create a VM instance from an image:

1. Ensure that you are logged in to the GCP.
2. Click **VM instances**.
The *VM instances* screen appears.
3. Click **CREATE INSTANCE**.
The *Create an instance* screen appears.
4. Enter the following information:
 - **Name:** Name of the instance
 - **Description:** Description for the instance
5. Select the region and zone from the **Region** and **Zone** drop-down menus respectively.
6. Under the **Machine Type** area, select the processor and memory configurations based on the requirements.

Note:

Click **Customize** to customize the memory, processor, and core configuration.

7. Under the Boot disk area, click **Change** to configure the boot disk.
The *Boot disk* screen appears.
 - a. Click **Custom Images**.
 - b. Under the **Show images from** drop-down menu, select the project where the image of the appliance is provided.
 - c. Select the image for the root partition.
 - d. Select the required disk type from the **Boot disk type** drop-down list.

e. Enter the size of the disk in the **Size (GB)** text box.

f. Click **Select**.

The disk is configured.

8. Under the *Identity and API access* area, select the account from the **Service Account** drop-down menu to access the Cloud APIs.

Depending on the selection, select the access scope from the **Access Scope** option.

9. Under the *Firewall* area, select the **Allow HTTP traffic** or **Allow HTTPS traffic** checkboxes to permit HTTP or HTTPS requests.

10. Click **Networking** to set the networking options.

a. Enter data in the **Network tags** text box.

b. Click **Add network interface** to add a network interface.

If you want to edit a network interface, then click the edit icon ().

11. Click **Create** to create and start the instance.

15.3.5.2 Creating a VM Instance from a Disk

You can create disks using the image provided for your account. You must create a boot disk using the OS image. After creating the disk, you can attach it to an instance.

This section describes how to create a disk using an image. Using this disk, you then create a VM instance.

15.3.5.2.1 Creating a Disk from the GCP Image

Perform the following steps to create a disk using an image.

► To create a disk of the Protegility appliance:

1. Access the GCP domain at the following URL:

<https://cloud.google.com/>

The GCP home screen appears.

2. Click **Console**.

The GCP login screen appears.

3. On the GCP login screen, enter the following details:

- User Name
- Password

4. Click **Sign in**.

After successful authentication, the GCP management console screen appears.

5. Click **Go to the Compute Engine dashboard** under the *Compute Engine* area.

The *Dashboard* screen appears

6. Click **Disks** on the left pane.

The *Disks* screen appears.

7. Click **CREATE DISK** to create a new disk.

The *Create a disk* screen appears.

8. Enter the following details:
 - **Name:** Name of the disk
 - **Description:** Description for the disk
9. Select one of the following options from the **Type** drop-down menu:
 - **Standard persistent disk**
 - **SSD persistent disk**
10. Select the region and zone from the **Region** and **Zone** drop-down menus respectively.
11. Select one of the following options from the **Source Type** option:
 - **Image:** The image of the Protegility appliance that is provided.
Select the image from the Source Image drop-down menu.

Note:

Ensure that you have access to the Protegility appliance images.

- **Snapshot:** The snapshot of a disk
 - **Blank:** Create a blank disk
12. Enter the size of the disk in the **Size (GB)** text box.
 13. Select **Google-managed** key from the **Encryption** option.
 14. Click **Create**.

The disk is created.

15.3.5.2.2 Creating a VM Instance from a Disk

This section describes how to create a VM instance from a disk that is created from an image.

For more information about creating a disk, refer to section [Creating a Disk from the GCP Image](#).

► To create a VM instance from a disk:

1. Ensure that you are logged in to the GCP Console.
2. Click **VM instances**.
The *VM instances* screen appears.
3. Click **CREATE INSTANCE**.
The *Create an instance* screen appears.
4. Enter information in the following text boxes:
 - **Name**
 - **Description**
5. Select the region and zone from the **Region** and **Zone** drop-down menus respectively.
6. Under the **Machine Type** section, select the processor and memory configuration based on the requirements.
Click **Customize** to customize your memory, processor and core configuration.
7. Under *Boot disk* area, click **Change** to configure the boot disk.
The *Boot disk* screen appears.
 - Click **Existing Disks**.

- Select the required disk created with the Protegility appliance image.
 - Click **Select**.
8. Under Firewall area, select the **Allow HTTP traffic** or **Allow HTTPS traffic** checkboxes to permit HTTP or HTTPS requests.
9. Click **Create** to create and start the instance.

15.3.5.3 Accessing the Appliance

After setting up the virtual machine, you can access the appliance through the IP address that is assigned to the virtual machine. It is recommended to access the appliance with the administrative credentials.

Note:

If the number of unsuccessful password attempts exceed the defined value in the password policy, the account gets locked.

For more information on the password policy for the admin and viewer users, refer to the section [Password Policy for the LDAP Users](#), and for the *root* and *local_admin* OS users, refer to the section [Managing Local OS Users](#).

15.3.6 Finalizing the Installation of Protegility Appliance on the Instance

When you install the appliance, it generates multiple security identifiers such as, keys, certificates, secrets, passwords, and so on. These identifiers ensure that sensitive data is unique between two appliances in a network. When you receive a Protegility appliance image, the identifiers are generated with certain values. If you use the security identifiers without changing their values, then security is compromised and the system might be vulnerable to attacks. Using the **Rotate Appliance OS Keys**, you can randomize the values of these security identifiers for an appliance. During the finalization process, you run the key rotation tool to secure your appliance.

Note:

If you do not complete the finalization process, then some features of the appliance may not be functional including the Web UI.

For example, if the OS keys are not rotated, then you might not be able to add appliances to a Trusted Appliances Cluster (TAC).

Note:

For information about the default passwords, refer to the section [Launching the ESA instance on Google Cloud Platform](#) in the [Release Notes 9.0.0.0](#).

15.3.6.1 Finalizing ESA Installation

You can finalize the installation of the ESA after signing in to the CLI Manager.

Caution:

Ensure that the finalization process is initiated from a single session only. If you start finalization simultaneously from a different session, then the "*Finalization is already in progress.*" message appears. You must wait until the finalization of the instance is successfully completed.

Additionally, ensure that the appliance session is not interrupted. If the session is interrupted, then the instance becomes unstable and the finalization process is not completed on that instance.

► To finalize ESA installation:

1. Sign in to the ESA CLI Manager of the instance created using the default administrator credentials.
The following screen appears.

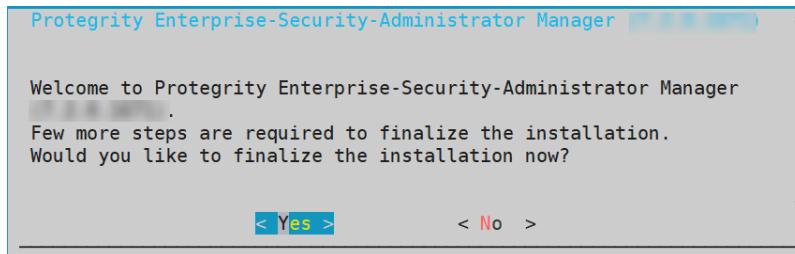


Figure -23: Finalizing Installation Confirmation screen

2. Select **Yes** to initiate the finalization process.

The screen to enter the administrative credentials appears.

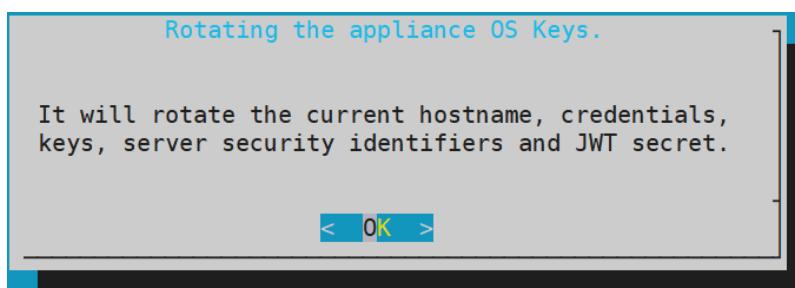
Note:

If you select **No**, then the finalization process is not initiated.

To manually initiate the finalization process, navigate to **Tools > Finalize Installation** and press **ENTER**.

3. Enter the credentials for the *admin* user and select **OK**.

A confirmation screen to rotate the appliance OS keys appears.



4. Select **OK** to rotate the appliance OS keys.

The following screen appears.

User's Passwords

Please provide user's passwords

root password	
root password verification	
admin password	
admin password verification	
viewer password	
viewer password verification	
local_admin password	
local_admin password verification	

[<Apply>](#)
[<Help >](#)

- a. To update the user passwords, provide the credentials for the following users:

- root
- admin
- viewer
- local_admin

- b. Select **Apply**.

The user passwords are updated and the appliance OS keys are rotated.

The finalization process is completed.

Note:

The appliance comes with some products installed by default. If you want to verify the installed products or install additional products, then navigate to **Administration > -- Installations and Patches -- > Add/Remove Services**.

For more information about installing products, refer the section *Working with Installation and Packages* in *Protegility Installation Guide 9.1.0.5*.

15.3.7 Connecting to an ESA instance (for DSG deployment)

If you are using an instance of the DSG appliance on GCP, you must connect it to the instance of the ESA appliance. Using the CLI manager, you must provide the connectivity details of the ESA appliance in the DSG appliance.

For more information about connecting to an instance of the ESA appliance, refer to the section *Setting up ESA Communication* in the *Data Security Gateway Guide 3.0.0.0*.

15.3.8 Deploying the Instance of the Protegity Appliance with the Protectors

You can configure the various protectors that are a part of the Protegity Data Security Platform with the instance of the ESA appliance running on AWS.

Depending on the Cloud-based environment which hosts the protectors, the protectors can be configured with the instance of the ESA appliance in one of the following ways:

- If the protectors are running on the same VPC as the instance of the ESA appliance, then the protectors need to be configured using the internal IP address of the appliance within the VPC.
- If the protectors are running on a different VPC than that of the instance of the ESA appliance, then the VPC of the instance of the ESA needs to be configured to connect to the VPC of the protectors.

15.3.9 Backing up and Restoring Data on GCP

A snapshot represents a state of an instance or disk at a point in time. You can use a snapshot of an instance or a disk to backup or restore information in case of failures.

15.3.9.1 Creating a Snapshot of a Disk on GCP

This section describes the steps to create a snapshot of a disk.

► To create a snapshot on GCP:

1. On the **Compute Engine** dashboard, click **Snapshots**.
The *Snapshots* screen appears.
2. Click **Create Snapshot**.
The *Create a snapshot* screen appears.
3. Enter information in the following text boxes.
 - Name - Name of the snapshot
 - Description – Description for the snapshot
4. Select the required disk for which the snapshot is to be created from the **Source Disk** drop-down list.
5. Click **Add Label** to add a label to the snapshot.
6. Enter the label in the **Key** and **Value** text boxes.
7. Click **Add Label** to add additional tags.
8. Click **Create**.

Note: Ensure that the status of the snapshot is set to **completed**.

Note: Ensure that you note the snapshot id.

15.3.9.2 Restoring from a snapshot on GCP

This section describes the steps to restore data using a snapshot.

Note: Ensure that the snapshot of the disk is created.

► To restore data using a snapshot on GCP:

1. Navigate to **Compute Engine > VM instances**.
The *VM instances* screen appears.
2. Select the required instance.
The screen with instance details appears.
3. Stop the instance.
4. After the instance is stopped, click **EDIT**.
5. Under the **Boot Disk** area, remove the **Existing disk**.
6. Click **Add New Disk**.
7. Enter information in the following text boxes:
 - Name - Name of the snapshot
 - Description – Description for the snapshot
8. From the **Disk source type** drop-down list, select the **Snapshot** option.
9. Select the snapshot from the **Source snapshot** drop-down list.
10. Under the **Disk settings** area, click the **Disk type** drop-down list, and select the **Standard persistent disk**.
11. Enter the size of the disk in the **Size** text box.
12. Click **Add Label** to add a label to the snapshot.
13. Enter the label in the **Key** and **Value** text boxes.
14. Click **Save**.
The instance is updated with the new snapshot.

15.3.10 Increasing Disk Space on the Appliance

After creating an instance on GCP, you can add a disk to your appliance.

► To add a disk to a VM instance:

1. Ensure that you are logged in to the GCP Console.
2. Click **VM instances**.
The *VM instances* screen appears.
3. Select the instance.
The *VM instance* details screen appears.
4. Click **EDIT**.
5. Under **Additional disks**, click **Add new disk**.

6. Enter the disk name in the **Name** field box.
7. Select the disk permissions from the **Mode** option.
8. If you want to delete the disk or keep the disk after the instance is created, select the required option from the **Deletion rule** option.
9. Enter the disk size in GB in the **Size (GB)** field box.
10. Click **Done**.
11. Click **Save**.

The disk is added to the VM instance.