AlgoSec Security Management Suite

Software Version: A30.10

Installation and Setup Guide

View our most recent updates in our online ASMS Tech Docs.

Document Release Date: 4 May, 2020 | **Software Release Date**: April 2020

Legal Notices

AlgoSec, FireFlow, AppViz and AppChange are registered trademarks of AlgoSec Systems Ltd. and/or its affiliates in the U.S. and certain other countries.

Check Point, the Check Point logo, ClusterXL, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, INSPECT, INSPECT XL, OPSEC, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UserAuthority, VPN-1, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Cisco, the Cisco Logo, Cisco IOS, IOS, PIX, and ACI are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Specifications subject to change without notice.

Proprietary & Confidential Information

This document contains proprietary information. Neither this document nor said proprietary information shall be published, reproduced, copied, disclosed, or used for any purpose other than the review and consideration of this material without written approval from AlgoSec, 65 Challenger Rd., Suite 310, Ridgefield Park, NJ 07660 USA.

The software contains proprietary information of AlgoSec; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between AlgoSec and the client and remains the exclusive property of AlgoSec If you find any problems in the documentation, please report them to us in writing. AlgoSec does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of AlgoSec Systems Ltd.

Contents

Introduction 7
ASMS products 7
Server installation options 8
ASMS deployment checklist 10
Infrastructure and analytics 10
AlgoSec Firewall Analyzer deployment tasks 11
Network visibility and awareness 12
Intelligent policy change automation 12
Application discovery and management 13
System requirements 13
Hardware minimum requirements 13
Software requirements 15
Networking requirements and recommendations 16
Supported deployments per architecture structure 18
Prepare an AlgoSec hardware appliance 18
Shipping carton contents 19
Device name mapping 20
Generation 9 technical specifications and elements 20
Generation 10 technical specifications and elements 22
ASMS system security 24
Additional hardening procedures 25
Connecting securely to the AFA server 25
Connecting securely from the AFA server 26
Download ASMS software packages 27
Download installation files 27
Required software packages per deployment 28
FIPS 140-2 compliance 28
Deploy standalone appliances 30
Deploy clusters and distributed architectures 32
Deploy clusters and distributed architecture nodes 32

Deploy ASMS on the cloud **35**
Deploy ASMS on AWS 35
Deploy ASMS on Microsoft Azure 36
Configure ASMS machines **45**
Connect to the Administration Interface 45
Perform basic configurations 47
Configure NAS storage 48
Deconfigure NAS storage 51
Manage clusters **53**
Cluster roles and modes 53
High availability clusters 54
Disaster recovery clusters 55
Build a cluster 56
Verify cluster connectivity 56
HA clusters only: Add a second interface 57
Build an ASMS HA or DR cluster 58
Configure HA/DR parameters 60
Break a cluster 61
Switch appliance roles 63
Troubleshoot HA/DR clusters 64
DR clusters: primary appliance failed 64
DR clusters: secondary appliance failed 64
Split-brain situations 65
Current synchronization operation canceled 65
Manage nodes automatically removed from clusters 65
Forcibly remove a node from a cluster 66
Collect cluster logs for AlgoSec technical support 67
Set up the ASMS environment **68**
Define the first ASMS Administrator 68
Run the FireFlow setup program 71
Additional optional configurations 72

Configure a distributed architecture **74**
Configure load distribution 74
Configure geographic distribution 75
Enabling distributed processing 76
Add or edit Load Units 77
Add or edit Remote Agents 80
Delete Load Units or Remote Agents 82
Disable distributed processes 83
Basic sanity checks **84**
ASMS basic functionality 84
Test machine installation and configuration 85
Test basic ASMS processes 86
Test basic AFA functionality 87
Test basic FireFlow functionality 88
Test basic AppViz functionality 89
Populate your environment **91**
Upgrade ASMS **92**
Licensing during upgrade 92
Enabling new features after upgrade 92
Upgrade prerequisites 92
Mandatory upgrade prerequisites 92
Disk space requirements for upgrades 94
Recommended upgrade prerequisites 94
Upgrade your system 96
Perform an automated ASMS upgrade 96
Troubleshoot your automated upgrade 99
General system maintenance **101**
Reboot the appliance 101
Reset the appliance to factory defaults 102
Migrate the Central Manager 103
Relocate devices 105

Use case scenario: Migrating an entire ASMS system 109
Contact AlgoSec technical support 111
Backup and restore **113**
Backup and restore prerequisites 113
Access backup and restore from FireFlow or AppViz 113
ASMS licensing **115**
Obtain a license 115
Online license requirements 116
Install a license 117
HA/DR clusters 119
License usage 120
Virtual router licensing 121
Public cloud licensing 121
View license usage statistics 121
Update licenses 124
Logins and other basics **125**
Supported browsers 125
Log in to ASMS 125
View ASMS product details 128
Log out of ASMS 129
Send us feedback **131**

Introduction

This guide describes how to deploy the AlgoSec Security Management Suite (ASMS), upgrade to new versions, or reconfigure deployment options on existing environments.

This section includes:

- ASMS products
- Server installation options
- Introduction

ASMS products

ASMS installations can include the following products, depending on your license:

AlgoSec Firewall Analyzer (AFA)	Analyze security devices across your network, including both on-premises and cloud devices.
FireFlow	Manage your network security life cycles on devices managed by AFA.
AppViz	Manage application-centric security policy management tasks on devices managed by AFA. AppViz is powered by FireFlow.

An ASMS environment can use AFA alone, AFA with FireFlow, or AFA with both FireFlow and AppViz. Each product in use must be enabled on the ASMS license.

AlgoSec also provides the following additional software for use with ASMS:

AlgoSec AppViz AutoDiscovery	Installed on top of AlgoSecAppViz, AutoDiscovery enables you to import business services as AppViz applications. For more details, see *the AlgoSecAutoDiscovery User Guide*.
AlgoSec AlgoBot	Provides quick access to core ASMS functionality and data from the comfort of your existing chat platforms, including desktop, web, and mobile options. For more details, see AlgoBot: The First Intelligent Chatbot for Network Security Policy Management.

Server installation options

ASMS products can be deployed using the following server installation options:

AlgoSec Hardware Appliances	AlgoSec can provide you with hardware appliances that are pre-installed with AlgoSec software. No software installations are required for the initial setup, although you may need to perform upgrades for new versions. For details, see Deploy standalone appliances.
Virtual Appliances	AlgoSec can provide you with a pre-installed VM image for you to deploy on your own system. No software installations are required for the initial setup, although you may need to perform upgrades for new versions. For details, see Deploy standalone appliances.
Cloud deployments	Deploy ASMS on Amazon AWS or Microsoft Azure to manage your devices from the cloud. For details, see Deploy ASMS on the cloud.

Advanced options

Advanced server configuration options include:

- **High Availability / Disaster Recovery (HA/DR) clusters**

  Prevent data loss or downtime using cluster environments.

- **Distributed architectures**

  AlgoSec supports the following distributed architecture options:

Geographic distribution	Manage devices across multiple geographic locations using Remote Agents that are managed by a Central Manager AlgoSec appliance. Geographic distributions enhance both performance and security because you only need one connection to manage firewalls in multiple locations.

Load distribution	Increase computing power with Load Unit machines that are managed by an ASMS Central Manager appliance. In this configuration, all Load Units must be in the same geographical location as the Central Manager.

For more details, see Deploy clusters and distributed architectures.

ASMS deployment checklist

If you are deploying a full ASMS system out-of-the box, use the following list to prepare for deployment and ensure that you've configured your system as recommended.

For more details, see also Download ASMS software packages and ASMS system security.

For details not included in this guide, see the online ASMS Tech Docs.

Infrastructure and analytics

Deploy ASMS infrastructure

Step	Description
AlgoSec architecture recommendation review	Work with AlgoSec to understand our architecture recommendations for your needs.
Infrastructure component provisioning	Ensure that your hardware or virtual components meet our system requirements. For details, see System requirements.
Standalone appliances	Deploy your pre-installed, standalone VMware virtual appliance or AlgoSec hardware appliance. For details, see Deploy standalone appliances.
High-availability / Disaster recovery configuration	Set up your environment, including high availability or disaster recovery clusters, as well as load or geographic distribution. For details, see: • Deploy clusters and distributed architectures • Manage clusters • Configure a distributed architecture
Load distribution / remote distribution configuration	

AlgoSec Firewall Analyzer deployment tasks

Step	Description
Licensing application	Install your license. For details, see: • Obtain a license • Install a license
Networking estate provisioning	Populate AFA with your devices.
Environment visibility and accuracy validation	View your network map in AFA and confirm that it displays as expected.
Authentication and authorization configuration	Define how AFA handles user authentication and authorization. **Best practice:** Whenever possible, leverage LDAP/LDAPS for authentication. This enables all ASMS users to log in easily, including change requestors, application owners, auditors, and so on. Configuring LDAP/LDAPS for ASMS also enables auto-provisioning, which means that users are automatically created and assigned to their appropriate roles based on their LDAP group membership, without any additional configuration.
User and role configuration	Define AFA users and their roles.
Outbound mail integration configuration	Configure AFA to send email notifications.
Storage and retention configuration	Configure AFA settings for data storage.

Step	Description
Infrastructure component monitoring	Configure monitoring systems for each ASMS product. **Best practice:** Deploy WatchDog monitoring to provide the broadest and most up-to-date set of system parameters to be monitored. Direct syslog messages WatchDog to your enterprise NOC.
Schedule AFA analysis	Configure AFA settings for scheduled analysis jobs.

Network visibility and awareness

Build your ASMS network topology

Step	Description
Sanity end-to-end traffic simulation	Run an end-to-end traffic simulation query to ensure that the data presents as expected.
Network topology modeling & adjustment	After viewing default reports and query results, you may want to adjust the way AFA displays your data.

Intelligent policy change automation

Deploy AlgoSec FireFlow

Step	Description
FireFlow initial setup	FireFlow templates and workflows are fully configurable. We recommend using the default configuration to get started, and then customizing FireFlow as needed.
FireFlow sanity-check request	Create a sample change request and push it through the entire workflow to test each step in the process.

Application discovery and management

Deploy AlgoSecAppViz

Step	Description
AppViz initial setup	Set up AppViz to view your network details from a business perspective.
AppViz sanity-check application	View data for your application from AppViz to test each feature.
AlgoSec AutoDiscovery Deployment tasks	Install and configure AutoDiscovery so that AppViz can automatically detect your flows and applications.

System requirements

ASMS's system requirements include the following:

- System requirements
- Software requirements
- Networking requirements and recommendations

Note: ASMS performance on VMs depends on the other, non-AlgoSec machines residing on the same VMware platform. To ensure performance, we recommend working with dedicated resources.

Hardware minimum requirements

We recommend that ASMS deployments meet or exceed the following minimum hardware requirements.

These requirements apply for both primary and secondary nodes, and on standalone systems, Central Managers, Remote Agents, or Load Units.

Hardware	Required
CPU	6 cores *
Memory	24 GB *
Storage	300 GB
Network	For details, see Bandwidth requirements for distributed environments

Upgraded system requirements for A30.10

System optimizations in version A30.10 require additional CPU and memory specifications than were required in earlier systems.

If you are upgrading, we highly recommend increasing your system specifications to match the updated requirements as needed. Systems that remain with legacy minimum specifications may have unexpected results.

Note: If your system specifications are already larger than the updated CPU and memory requirements, your system specifications can stay as they are. In such cases, there is no need to resize your entire system.

Note: These minimum requirements suffice for initial demo and testing environments, such as for up to 50 simple devices. For details about final sizing calculations for production environments, contact your AlgoSec partner or sales engineer.

Differences per environment configuration

Hardware requirements will differ, depending on your environment configuration and type. Main differences and considerations include:

Configuration	Description
NAS storage	If you configure AFA to store all reports on a remote NAS server, this will impact where the storage space is needed. For details, see Configure NAS storage.
HA/DR clusters	Each node in an HA/DR cluster must be identical, including the same type of installation (AlgoSec hardware or VM appliance), and have the same amount of disk space. For details, see Manage clusters
Distributed architecture	In distributed architecture environments, consider the requirements for the Central Manager and each Remote Agent (geographic distribution) or Load Unit (load distribution). Remote Agents and Load Units do not store reports. For details, see Configure a distributed architecture.
AWS deployments	If you are deploying on AWS, we recommend: • Ensuring that your machine is compatible with CentOS6. We recommend machines from the **Amazon EC2 General Purpose M4** family. • Ensuring that your AWS instance includes high performance storage, such as SSD disks For more details, see the AWS Documentation.

Software requirements

ASMS requires the following software, depending on your deployment method:

Deployment	Requirements
AlgoSec hardware appliances	AlgoSec hardware appliances comes pre-installed with all require software. No additional software is needed.
Virtual appliances	ASMS can be deployed on virtual machines that use VMWare ESX versions 5.5 and higher. For more details, see the Support page on the AlgoSec portal.

Networking requirements and recommendations

This section includes the following data:

- Networking requirements and recommendations
- Required port connections
- Bandwidth requirements for distributed environments
- Email and device connectivity requirements
- AFA server DNS name / IP address recommendations
- Security certificate recommendations

For more details, see Manage clusters and Configure a distributed architecture.

Required port connections

Deploying ASMS requires the following port connectivity between nodes:

Type	Port	Central Manager <> Load Unit	Central Manager <> Remote Agent	Load Unit <> Load Unit	HA	DR
ICMP		✔	✔	✖	✔	✔
SSH	TCP/22	✔	✔	✖	✔	✔
HTTPS	TCP/443	✔	✔	✖	✔	✔
syslog	UDP/514	✖	✖	✖	✔	✖
hazelcast	TCP/5701	✔	✖	✔	✔	✖
activemq	TCP/61616	✔	✖	✖	✔	✖
postgrsql	TCP/5432	✔	✖	✖	✔	✔
postgrsql additional port	TCP/5433	✖	✖	✖	✔	✖
HA/DR	TCP/9595	✖	✖	✖	✔	✔

Bandwidth requirements for distributed environments

Distributed environments must work with the following minimum bandwidths between nodes:

Central Manager and load distribution agents	1 Gb/s
Between High Availability nodes	1 Gb/s
Central Manager and geographic distribution agents	100 Mb/s
Between Disaster Recovery nodes	100 Mb/s

Tip: The faster your network speed, the faster your clusters will be completely synched.

Email and device connectivity requirements

Enable the following connectivity for AFA and FireFlow:

Requirement	Description
Email address	Define an e-mail address to be used by AFA and FireFlow, such as fireflow@mycorp.com, on a mail server that supports SMTP and POP3/IMAP4. Alternatively, emails can be forwarded to AFA and FireFlow as an MTA (message transfer agent).
Email access	Enable access from AFA and FireFlow to the mail server via SMTP and POP3/IMAP4
Device access	Enable access from the Central Manager, any high availability secondary nodes, and Remote Agents to devices via SSH, OPSEC, REST, or SNMP (as needed)

This connectivity configuration includes configuring the necessary passwords for FireFlow.

AFA server DNS name / IP address recommendations

The AFA server must have a fixed DNS name or IP address that can be used to access the AFA user interface.

We recommend that you do not configure the server to obtain an IP address automatically or to use DHCP.

Security certificate recommendations

To prevent warnings from appearing about security certificates, install a certificate signed by a CA instead of a self-signed certificate.

For more details, see the Centos documentation.

Note: AlgoSec recommends using a 2048-bit certificate instead of the 1024-bit certificate recommended by the Centos documentation.

Supported deployments per architecture structure

The following table lists the supported deployment models for each architecture structure.

Deployment	Standalone ASMS	High Availability	Disaster Recovery	Load Distribution	Geographic Distribution	NAS
AlgoSec Physical Appliance (2XXX series)	✔	✔	✔	✔	✔	✔
Virtual Appliance (VMWare)	✔	✔	✔	✔	✔	✔
ASMS on AWS (AMI)	✔	✖	✔	✔ *	✔	✖
ASMS on Azure	✔	✖	✖	✖	✖	✖

Note: When deployed on AWS, any Load Units must also be located in AWS, in the same subnet as the Central Manager.

➔ See also:

- *The AlgoSec AutoDiscovery User Guide*

Prepare an AlgoSec hardware appliance

This section describes how to prepare an AlgoSec hardware appliance before continuing with your deployment.

Do the following:

1. Review the contents of the shipping carton, technical specifications, and appliance elements. For details, see:
   - Shipping carton contents
   - Device name mapping
   - Generation 9 technical specifications and elements
   - Generation 10 technical specifications and elements
2. Mount the appliance on the rack, with the AlgoSec logo facing front.
3. Connect one end of the power cable supplied to the power jack on the appliance's rear panel. Plug the other end into an electrical outlet.
4. Do one of the following:

Configure the appliance directly (Recommended)	Do the following: a. Use a VGA cable to connect a monitor to the video port on the appliance's rear panel. b. Connect a keyboard to one of the USB ports on the appliance's front or rear panel.
Configure the appliance via iLO	Do the following: a. Connect one end of the network cable supplied to the iLO port on the appliance's rear panel. b. Connect the other end of the cable to a network port.

5. Remove the bezel from the front panel, and press the **Power On** button.

Shipping carton contents

Each AlgoSec hardware appliance comes in a shipping container with the following items:

A Hardware appliance	One of the following AlgoSec hardware appliances: • Generation 9 (model 2062, 2162, or 2322) • Generation 10 (model 2063, 2203, 2403)
Two power cables	Only one power cable is needed for 2062 appliances.
Two network cables	Only one network cable is needed for 2062 appliances.
License	For all models except the 2062 appliance: A Hewlett Packard Enterprise (HPE) iLO license

Note: iLO provides additional features for controlling and maintaining the appliance. For 2062 appliances, you may want to contact HPE to acquire an iLO license. For more details, see the HPE iLO documentation.

Device name mapping

For all appliances, the names of physical devices start with **1**. Corresponding OS names start with **0**.

For example, a physical device might be named **NIC1**. The OS would be **ETH0**.

Generation 9 technical specifications and elements

This section includes:

- Generation 9 technical specifications
- Generation 9 2062, 2162, and 2322 front panel elements
- Generation 9 2162, and 2322 rear panel elements

Generation 9 technical specifications

	2062	2162	2322
Dimensions (HxDxW)	429x434.6x607.6 mm	432x434.7x698.5 mm	432x434.7x698.5 mm

	2062	2162	2322
Weight (maximum)	17 kg	15.3 kg	15.3 kg
Form Factor	1U rack-mount	1U rack-mount	1U rack-mount
Voltage	110/240V	110/240V	110/240V
Power Supply	550W PSU	500W PSU redundant	800W PSU redundant
CPU	1X Intel Xeon E52603, 6 cores, 1.6GHz	2 X Intel Xeon E52630v3, 16 cores, 2.6GHz	2 X Intel Xeon E52698v3, 32 cores, 2.3GHz
Memory	16GB	64GB	128GB
Hardware Manufacturer	HPE	HPE	HPE

Generation 9 2062, 2162, and 2322 front panel elements

Element	Description
	Power On/Standby button with a LED whose state indicates the appliance's power status: ■ **Flashing**. The appliance is initializing. ■ **On**. The appliance is on. ■ **Off**. The appliance is off.
	A LED whose state indicates the appliance's hard disk status: ■ **Flashing**. The hard disk is in use. ■ **Off**. The hard disk is not in use.
	Video connector.
	USB ports.
UID	Unit ID button (activates Unit ID LED on the rear panel).
	Health LED.

Element	Description
	NIC activity LED.

Generation 9 2162, and 2322 rear panel elements

Element	Description
Power jack	Two power jacks for supplying power to the appliance (that is, redundant PSUs).
ETH2 **ETH3** **ETH4**	Ethernet ports. When a HA cluster is configured, one port can be used to connect the primary and secondary appliances.
	Four USB Ports.
	Serial connector (inactive)
	Video connector
iLO	iLO /NIC connector.
UID	Unit ID LED (activated by Unit ID button on the front panel).

Generation 10 technical specifications and elements

This section includes:

- Generation 10 technical specifications
- Generation 10 rear panel elements
- Generation 10 front panel elements

Generation 10 technical specifications

	2063	2203	2403
Dimensions (HxDxW)	4.29 x 43.46 x 70.7 cm 1.69 x 17.11 x 27.83 in	4.29 x 43.46 x 70.7 cm 1.69 x 17.11 x 27.83 in	4.29 x 43.46 x 70.7 cm 1.69 x 17.11 x 27.83 in
Weight (maximum)	8 SFF 16.27 kg (35.86 lb)	8 SFF 16.27 kg (35.86 lb)	8 SFF 16.27 kg (35.86 lb)
Chasis	HP Rack Mount Consoles	HP Rack Mount Consoles	HP Rack Mount Consoles
Storage	2 x 1200GB	5 x 1200GB	8 x 1200GB
Power Supply	500W PSU redundant	500W PSU redundant	800W PSU redundant
CPU	6 cores: Intel Xeon Bronze 3104	20 cores: Intel Xeon Silver 4114	40 cores: Intel Xeon Gold 6138
Memory	16GB	64GB	128GB
Hardware Manufacturer	HPE	HPE	HPE

Generation 10 front panel elements

Element	Description
	Power On/Standby button with a LED whose state indicates the appliance's power status: ■ **Flashing**. The appliance is initializing. ■ **On**. The appliance is on. ■ **Off**. The appliance is off.
	A LED whose state indicates the appliance's hard disk status: ■ **Flashing**. The hard disk is in use. ■ **Off**. The hard disk is not in use.

Element	Description
	Video connector.
	USB ports.
UID	Unit ID button (activates Unit ID LED on the rear panel).
	Health LED.
iLO	iLO /NIC connector.
	NIC activity LED.

Generation 10 rear panel elements

Element	Description
Power jack	Two power jacks for supplying power to the appliance (that is, redundant PSUs).
ETH2 **ETH3** **ETH4**	Ethernet ports. When a HA cluster is configured, one port can be used to connect the Primary and Secondary appliances.
	Four USB Ports.
	Serial connector (inactive)
	Video connector
UID	Unit ID LED (activated by Unit ID button on the front panel).

ASMS system security

AlgoSec products are released after a careful hardening procedure, which is also updated periodically as needed per industry standards.

We use standard vulnerability scanners, customer feedback, as well as our own security expertise to create, run, and make updates to this hardening procedure.

To ensure maximum security, make sure to routinely install any security patches released by AlgoSec. These security patches may include updates for AlgoSec Firewall Analyzer, FireFlow, AppViz, as well as appliance package updates.

Additional hardening procedures

You may wish to do additional hardening by doing the following:

- Place the AFA server in a special zone behind one of your devices.
- Write very restricted policy rules to control access to the AFA server.
- Install valid certificates properly signed by a certificate authority, replacing the pre-installed, self-signed certificates that are provided by default on AlgoSec web servers.

  For more details, see How to Install and Generate an SSL key and Certificate Signing Request (CSR) KB article on AlgoPedia.

When configuring external firewalls for your ASMS system, see the following sections:

- Connecting securely to the AFA server
- Connecting securely from the AFA server

Warning: If you want to perform additional hardening on your AlgoSec system, contact AlgoSec professional services.

Performing hardening procedures on your own may render your AlgoSec system inoperable and void your support contract.

Connecting securely to the AFA server

We recommend limiting inbound connectivity from other computers to the AFA server. Your team's computers must be able to browse the AFA reports via the internal Apache Web server, which is configured to serve pages using SSL (HTTPS) and listen on port TCP/443.

The TCP/80 port can be closed.

Connecting securely from the AFA server

Part of hardening a Linux server involves filtering network traffic to and from the server. When doing so, you must ensure that the communication ports used by AFA remain open.

AFA sends the following outgoing requests, which require no open, listening ports:

Request	Description
Outbound HTTPS requests	AFA issues output, HTTPS requests (TCP/443) only to activate licenses. These requests are sent to https://portal.algosec.com/en/support/support_home. Ensure that this traffic is not blocked, and that your outbound Web proxies do not manipulate or sanitize it.
DNS queries	AFA may need to issue DNS queries to the local DNS server (UDP/53).
SMTP communication	AFA sends email notifications if configured to do so. When configured, AFA must be able to communicate with your local mail server via SMTP (TCP/25).
POP mail retrieval	Email retrieval via "fetchmail" over POP3 must be accessible, if configured (TCP/110).
SSH device communication	If you want to enable remote access to the AFA server, we recommend using SSH. Ensure that port TCP/22 is accessible.
Authentication	LDAP authentication must be open, if relevant (TCP/389 or TCP/636) RADIUS authentication must be open, if relevant (UDP/1812)
Backup saves	AlgoSec automatic backup over FTP must be open, if relevant FTP (TCP/21) or SFTP (TCP/22)
Syslog messages	Communication must be open to send Syslog messages to a Syslog server, if AFA is configured to do so

Note: AFA will send additional requests via interfaces that differ depending on your device types.

Download ASMS software packages

This section describes how to download ASMS software packages from the AlgoSec portal.

Download installation files

Do the following:

1. Browse to the AlgoSec Portal, and navigate to **Downloads > Software > AlgoSec Security Management Suite**.

   Tip: To read about hotfix updates, click the **Hotfixes** menu.

2. Do one of the following, depending on whether you are upgrading or deploying a new installation:

New installation	Select **New Installation**, and then: a. Select your deployment type and version. b. Click **Next > Download**.
Upgrade	Select **Upgrade**, and then: a. Select your version, and click **Next**. b. On the **Update** page, select the builds you want to upgrade, and then click **Download All**. For more details, see Required software packages per deployment. **Note:** If you have FIPS deployment, click **I need the FIPS version**. Click **I need the 2xxx Series version** to return to the default page. For more details, see FIPS 140-2 compliance.

3. Continue with one of the following to install your software:
   - Deploy standalone appliances
   - Deploy clusters and distributed architectures
   - Deploy ASMS on the cloud (AWS AMI or Microsoft Azure)

Required software packages per deployment

Download the following software packages, depending on your deployment type:

Major version upgrades	When upgrading to a major version, you must download the Appliance build and the software builds for all active products, even if they are not included in your license. • AFA is always active. • FireFlow is active only when licensed and configured. In distributed architectures, FireFlow is always inactive on Remote Agents and Load Units. AFA administrators can manually activate or deactivate FireFlow: • To disable FireFlow manually, in the AFA **Administration** area, set the **FireFlow_configured parameter** to no. • To enable FireFlow again, run the FireFlow configuration process again from the **algosec_conf** menu. For details, see Run the FireFlow setup program.
Hotfix upgrades	If you are upgrading to a hotfix version, the build files required will depending on the content of the hotfix.

Note: For details about native Linux installations, see Deploy or upgrade a standalone native Linux server in AlgoPedia.

FIPS 140-2 compliance

AlgoSec supports a version of the Appliance build file that uses FIPS 140-2 compliant encryption packages.

If your environment includes a geographic or load distribution architecture, make sure to install the FIPS installation package on all Remote Agents / Load Units, as well as the Central Manager.

Warning: Using this mode of Appliance build is irreversible. Once the FIPS package is running on your system you must use FIPS installation packages for all future upgrades.

Deploy standalone appliances

This topic describes the high-level steps required to deploy pre-installed, standalone VMware virtual appliances or AlgoSec hardware appliances.

Note: Each installation package includes software for the full AlgoSec Security Management Suite. Functionality for each ASMS product is enabled via license, and not by installation.

Do the following:

1. Do one of the following:

AlgoSec hardware appliances	Starting by preparing your machine. For details, see Prepare an AlgoSec hardware appliance.
AlgoSec VMware virtual appliances	Download a VMware OVF machine. For details, see Download ASMS software packages.

2. Perform initial configurations, including configuring your machine's IP address. For details, see Configure ASMS machines.
3. Connect your machine to your organization's network. To connect an AlgoSec Hardware Appliance to the network, ensure that you use the **ETH0** on the appliance's rear panel.
4. If you configured a dynamic IP address using DHCP, verify the IP address assigned. For details, see Configure ASMS machines.
5. (Optional) Configure NAS storage. For details, see Configure NAS storage.
6. Test your installation. For details, see Test machine installation and configuration.
7. Set up your environment. For details, see Set up the ASMS environment.
8. Perform sanity checks. For details, see Basic sanity checks.

9. Continue to deploy ASMS products, including populating your environment with devices and users. For more details, see ASMS deployment checklist.

Deploy clusters and distributed architectures

This section describes how to deploy clusters and / or distributed architectures.

Note: Each installation package includes software for the full AlgoSec Security Management Suite. Functionality for each ASMS product is enabled via license, and not by installation.

Deploy clusters and distributed architecture nodes

Clusters and distributed architectures must be deployed on virtual appliances or AlgoSec hardware appliances, or as AWS or Azure instances. If you are deploying clusters, each node must be identical: either both hardware appliances, or both virtual appliances.

Both nodes must run the same version of ASMS, and must have the same amount of disk space.

Do the following:

1. Do one of the following:

AlgoSec hardware appliances	Starting by preparing your machine. For details, see Prepare an AlgoSec hardware appliance.
AlgoSec VMware virtual appliances	Download a VMware OVF machine. For details, see Download ASMS software packages.

Note: If you are reusing an appliance in a new role, you must re-set it to it's factory defaults.

For example, you might do this if you appliance was previously used as a Central Manager, and you now want to use it as a Load Unit or Remote Agent.

For details, see General system maintenance and Switch appliance roles.

2. Perform initial configurations, including configuring your machine's IP address. For details, see Configure ASMS machines.
3. Connect your machine to your organization's network. To connect an AlgoSec Hardware Appliance to the network, ensure that you use the **ETH0** on the appliance's rear panel.
4. If you configured a dynamic IP address using DHCP, verify the IP address assigned. For details, see Configure ASMS machines.
5. For NAS storage, do one of the following:

HA clusters	Configure NAS storage for the primary node of the cluster. The cluster building process automatically configures NAS on the secondary HA node.
DR clusters	If you want NAS on both nodes, you must configure NAS on both nodes. In order to achieve this, you must provide a second NAS server at the disaster recovery site.
Load distributions	Configure NAS for the Central Manager only. NAS will automatically be configured for the Load Units. **Note:** NAS support for load distribution environments is only supported with NFSV4.

Important: The user/customer is responsible for configuring the NAS server at the primary site and the NAS server at the disaster recovery site to sync with one another.

For more details, see Configure NAS storage.

6. If you are deploying clusters, build and configure the clusters. For details, see Manage clusters.
7. Test your installation. For details, see Test machine installation and configuration.
8. Set up your environment on your primary node or Central Manager / Master Appliance. For details, see Set up the ASMS environment.
9. If you are deploying an HA/DR cluster on the primary appliance or Central Manager / Master Appliance, install a license on the secondary node using the Administration Interface CLI. For details, see Connect to the Administration Interface.

   Load Units and Remote Agents do not need their own licenses installed.
10. If you are deploying a distributed architecture, configure the distribution. For details, see Configure a distributed architecture.
11. Perform sanity checks. For details, see Basic sanity checks.
12. Continue to deploy ASMS products, including populating your environment with devices and users. For more details, see ASMS deployment checklist.

➔ See also:

- Introduction
- ASMS licensing
- General system maintenance

Deploy ASMS on the cloud

This topic describes how you can deploy ASMS on Amazon AWS or Microsoft Azure to manage your devices from the cloud.

Note: Each installation package includes software for the full AlgoSec Security Management Suite. Functionality for each ASMS product is enabled via license, and not by installation.

This section includes:

- Deploy ASMS on AWS
- Deploy ASMS on Microsoft Azure

Deploy ASMS on AWS

Deploy ASMS on an AWS instance using an ASMS AMI available from the AlgoSec Portal.

If you are deploying on AWS, we recommend:

- Ensuring that your machine is compatible with CentOS6. We recommend machines from the **Amazon EC2 General Purpose M4** family.
- Ensuring that your AWS instance includes high performance storage, such as SSD disks

For more details, see the AWS Documentation.

Do the following:

1. Deploy your AWS AMI. For details, see Download ASMS software packages.

   On the **Download AlgoSecSecurity Management Suite > AMI** page, select an AWS Region and enter your AWS Account ID.

The AlgoSec AMI is shared with your account. When the setup process is complete, you are notified and provided with the details required to access your new instance with ASMS.

2. If you are deploying clusters or distributed architectures, continue with Deploy clusters and distributed architectures.

   Otherwise, continue with deploying ASMS products, including populating your environment with devices and users. For details, see ASMS deployment checklist.

Deploy ASMS on Microsoft Azure

Deploy ASMS on Microsoft Azure by converting a VHD file available from the AlgoSec portal to an Azure image.

Do the following:

1. Download the ASMS Azure files.
2. Create an Azure image from the VHD.
3. Log in to your Azure virtual machine as the **root** user.

   You may need to unlock the **root** user before logging in. If so, run:

   ```
   sudo passwd -u root
   ```

If you are deploying clusters or distributed architectures, continue with Deploy clusters and distributed architectures.

Otherwise, continue with deploying ASMS products, including populating your environment with devices and users. For details, see ASMS deployment checklist.

Download the ASMS Azure files

When you click **Download** on the **Download AlgoSecSecurity Management Suite > New Installation** page, a VHD file is downloaded to your local machine.

For more details, see Download ASMS software packages.

Create an Azure image from the VHD

The following steps describe how to convert your ASMS VHD file to an Azure image, and refer to areas of the Azure portal. For more details, see the Microsoft Azure documentation.

Note: Converting a VHD file to an Azure image has a variety of options and methods.

Use the steps described below when deploying your ASMS installation to prevent unexpected errors.

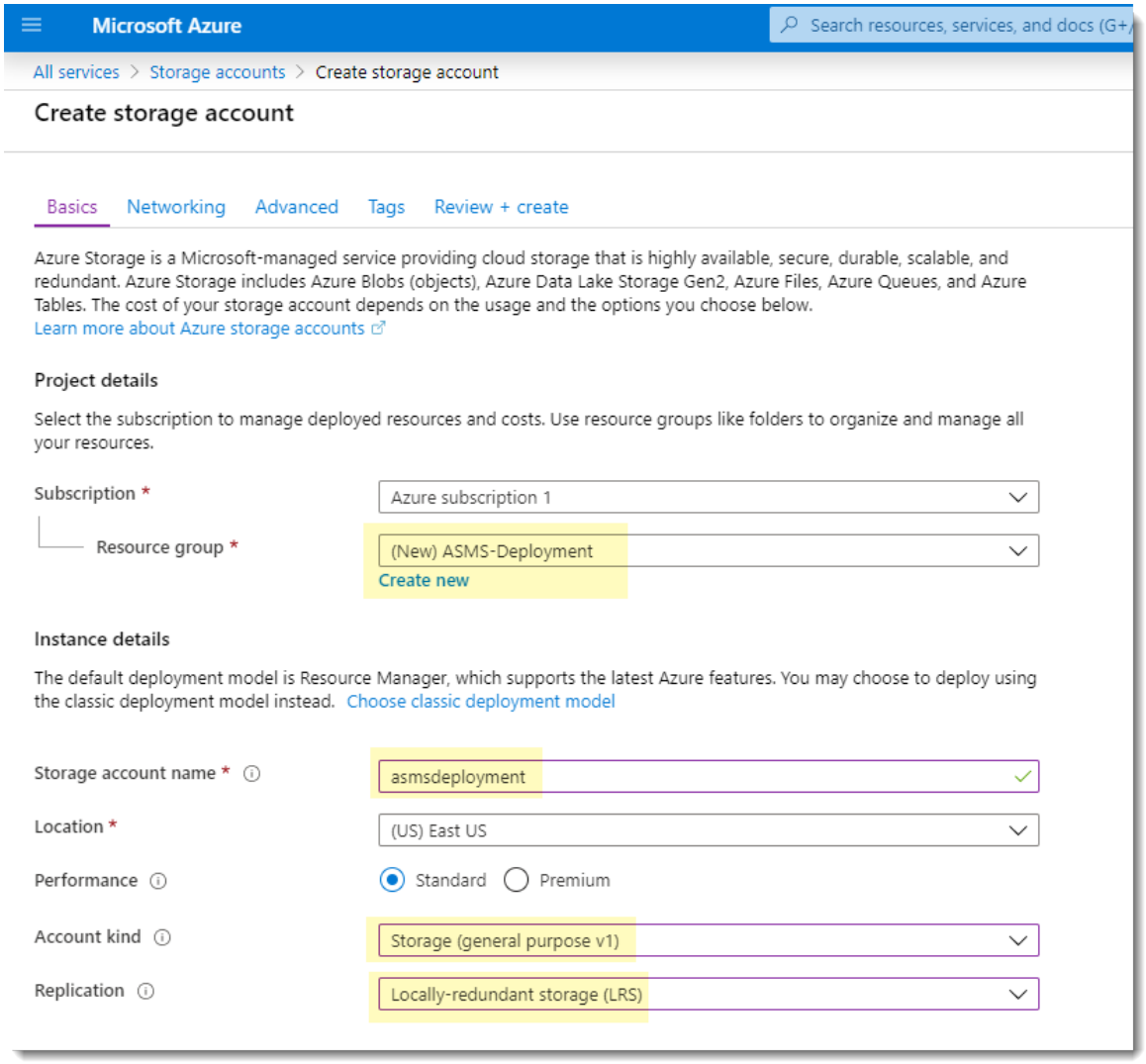
Do the following:

1. Create a new Azure storage account.

   Define your settings as follows:

Resource Group	Under the Resource Group field, click **Create new** to create a new resource group. Enter a meaningful name for your new resource group, such as **ASMS-Deployment.**
Storage account name	Enter a meaningful name for your storage account, such as **asmsdeployment**.
Account kind	Select **Storage (general purpose v1)**.
Replication	Select **LRS (Locally-redundant storage)**.

   For example:

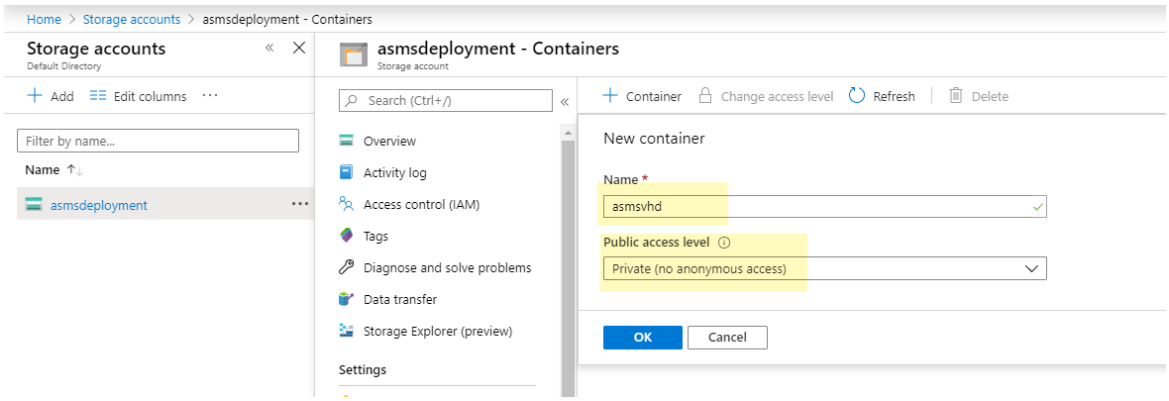


Continue in the wizard to create the new storage account and wait while it's deployed.

2. Once the new storage account is deployed, navigate to the **Storage accounts** area, and click the new storage account to view details.
3. In your new storage account, click **Containers**, and then + Container to add a new container.

   Define your new container with a meaningful name and a **Public access level** of **Private (no anonymous access).**

For example:



4. Switch to the Azure CLI, and ensure that the PowerShell **Az** module is installed.

   If it's not installed, run the following:

   ```
   Install-Module -Name Az -AllowClobber -Scope AllUsers
   ```

   Tip: You may need to configure the **Set-ExecutionPolicy** cmdlet.

   For more details, see Set-ExecutionPolicy and Install the Azure PowerShell module in the Microsoft documentation.

5. Connect to the Azure account from the CLI. Run:

   ```
   Connect-AzAccount
   ```

   When prompted, enter your credentials to log in.

6. Copy the VHD file downloaded from the AlgoSec portal to your Azure resource group.

   From the CLI, run:

   ```
   Add-AzVhd -ResourceGroupName "ASMS-Deployment" -Destination
   "https://asmsdeployment.blob.core.windows.net/asmsvhd/<VHD_NAME>.vhd"
   -LocalFilePath "<VHD_NAME>.vhd"
   ```

In this command, replace **<VHD_NAME>.vhd** with the exact name of the file you downloaded.

For example: **AlgoSec-app-3000.10.100-asms-75-co6.vhd**

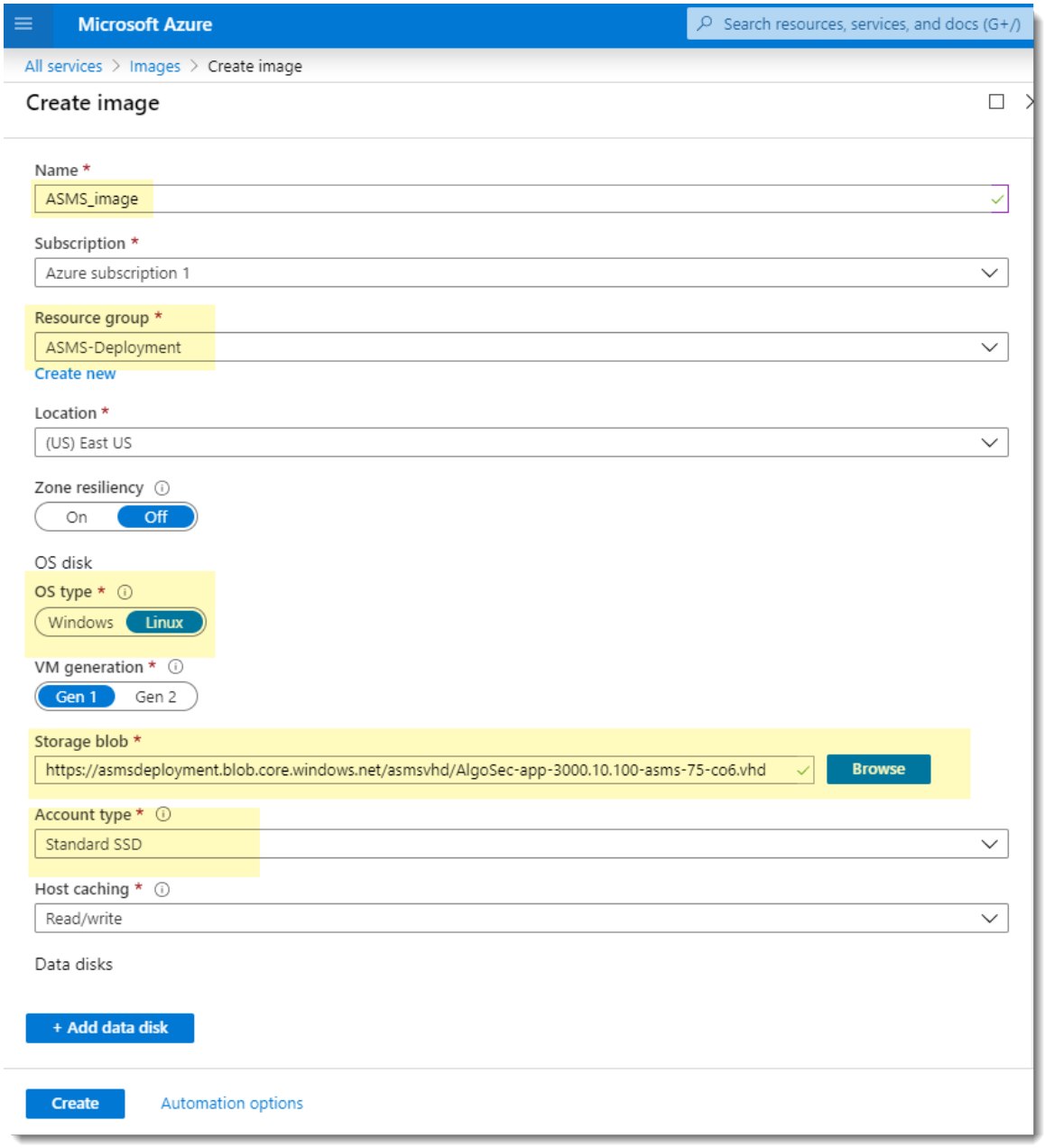
> **Note:** While the VHD that AlgoSec provides is dynamic, and the Azure requires a fixed hard disk, the upload process converts the dynamic file to a fixed file format.
>
> Additionally, while you can convert this dynamic file to a fixed file manually, this requires a very large upload, and also runs the risk of errors. We recommend using the commands provided here to perform this upload.

7. Return to the Azure portal to create your image. Navigate to **Images**, and click + Add.

   In the **Create image** pane, enter the following details:

Name	Enter a meaningful name. For example, **ASMS_image**.
Resource group	Select the new resource group you created for ASMS.
OS type	Select **Linux**.
Storage blob	Click **Browse**, and navigate to the VHD you uploaded via the CLI.
Account type	Select **Standard SSD**.

   For example:

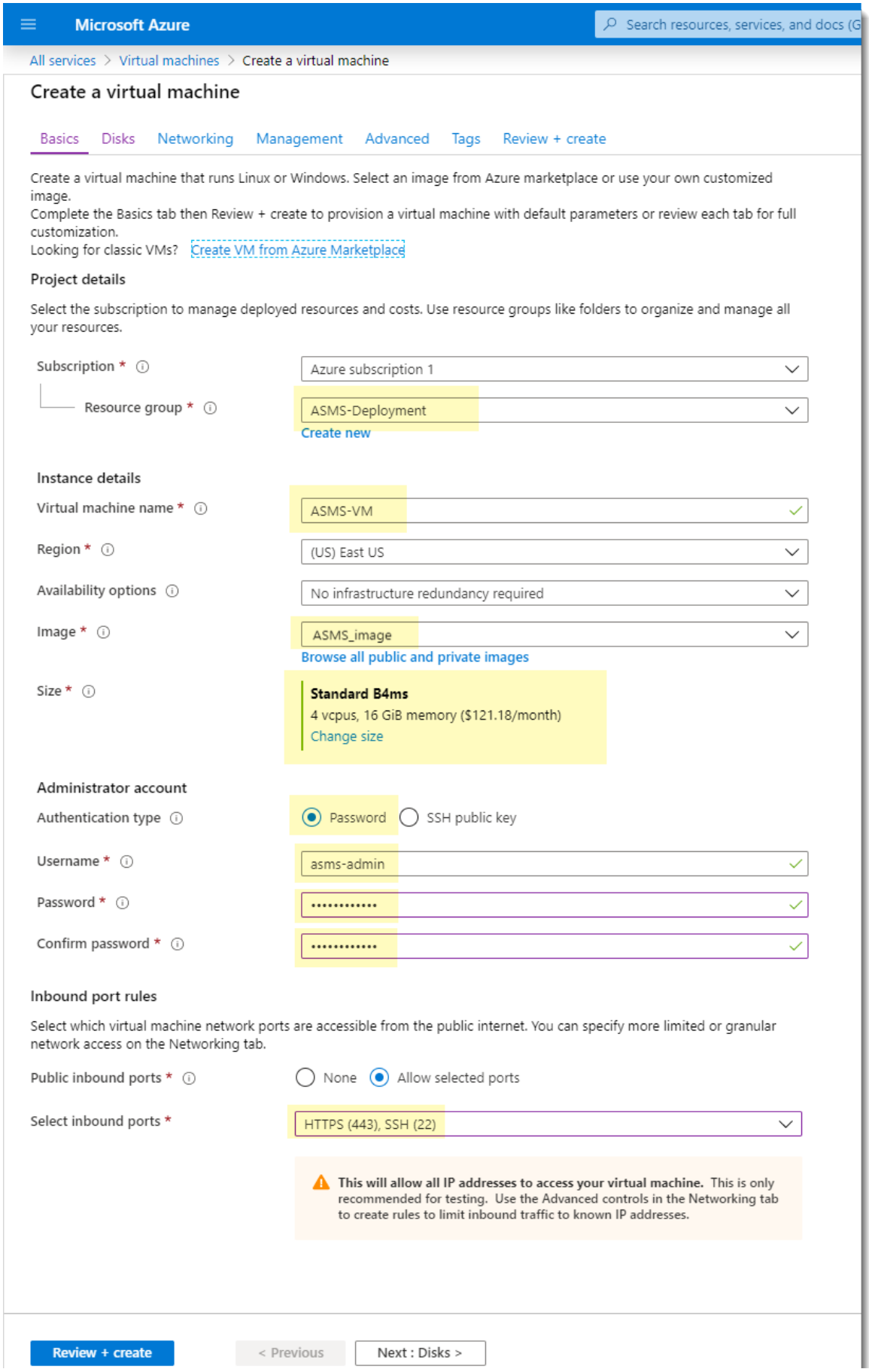


8. Navigate to the Azure **Virtual machines** area, and click + Add to create a new virtual machine.

   On the **Create a virtual machine** page, enter the following details:

Resource group	Select the resource group you created earlier.
Virtual machine name	Enter a meaningful name for your virtual machine.
Image	Navigate to and select the image you created earlier.
Size	Click **Change size**, and select a minimum of **B4ms**.
Authentication type	Select **Password**.
Username / **Password**	Enter credentials to access the new virtual machine. **Note:** Although you must set these credentials now, you'll need to log in to the machine as user **root** in order to deploy ASMS.
Select inbound ports	Select **HTTPS (443)** and **SSH (22)**.

For example:


Microsoft Azure
Search resources, services, and docs (G
All services > Virtual machines > Create a virtual machine
Create a virtual machine
Basics Disks Networking Management Advanced Tags Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.
Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription * Azure subscription 1
Resource group * ASMS-Deployment
Create new
Instance details
Virtual machine name * ASMS-VM
Region * (US) East US
Availability options No infrastructure redundancy required
Image * ASMS_image
Browse all public and private images
Size * Standard B4ms
4 vcpus, 16 GiB memory ($121.18/month)
Change size
Administrator account
Authentication type Password SSH public key
Username * asms-admin
Password * ••••••••••••
Confirm password * ••••••••••••
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports * None Allow selected ports
Select inbound ports * HTTPS (443), SSH (22)
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.
Review + create
< Previous
Next : Disks >

9. Click **Next: Disks >** to continue, and then select **Standard SSD**.
10. Continue through the wizard to create your virtual machine with ASMS installed.

When you're done, log in to your machine to deploy and set up your ASMS system. Continue with step 3 above.

➔ See also:

- Introduction
- ASMS licensing
- General system maintenance

Configure ASMS machines

This section describes how to access the ASMS Administration Interface, also known as the **algosec_conf** menu CLI, and perform basic configurations on your ASMS appliances.

Configure or de-configure NAS storage as needed for your deployment or upgrade, and test your installation and configuration after making system changes.

For details, see:

- Connect to the Administration Interface
- Configure ASMS machines
- Configure NAS storage
- Deconfigure NAS storage

Connect to the Administration Interface

Connect to the ASMS Administration Interface, or **conf** menu CLI as follows:

During initial setup	Do one of the following: • **AlgoSec Hardware Appliance**s: Connect directly (with a monitor/VGA cable) or via an iLO connection, depending on the way you prepared the appliance. For more details, see Prepare an AlgoSec hardware appliance. • **Virtual Appliance**s: Connect via a remote console.
After initial setup	Connect to the administration interface via SSH.

Do the following:

1. Open the console.

   If you are connecting via iLO, do the following:

a. In a browser, navigate to the IP address of the iLO interface. By default, this is done via DHCP.

b. Log in using the username and password printed on the sticker on top of the hardware appliance.

c. Select **Remote Console** in the menu on the left.

d. Click **Java Integrated Remote Console**.

The system prompts you for your login credentials.

2. Log in to the machine as user **root**.

   Default password: **algosec**.

   The main menu appears:

```
Please select a configuration item:
1. Configure IP address
2. Configure Time and Date
3. Configure DNS Server
4. Change DNS domain name
5. Change Hostname
6. Change root password
7. Change afa password
8. Upgrade software
9. Reset AFA admin password
10. Reset database password
11. Configure NAS
12. Install License
13. HA/DR Setup
14. Setup FireFlow configuration
15. Distributed Architecture configuration
16. Migrate ASMS units
17. Services status
```

```
18. Collect Logs
Q Logout
Press 'a' to exit to shell
Your choice:
>
```

Tip: Click the links in the sample above to jump to procedures with more details.

Perform basic configurations

This procedure describes how to configure an ASMS machine's IP address, as well as other basic settings.

Note: Configuring the IP address is mandatory during initial configuration.

Do the following:

1. Connect to the Administration interface. For details, see Connect to the Administration Interface.
2. Enter **1** to do any of the following:
   - Configure a static IP address
   - Configure DHCP
   - Look up the IP address, after configuring DHCP

Tip: We recommend using static IP addresses for Central Manager appliances, primary nodes, Load Slaves or Remote Agents, and so on.

Note: If you are working with clusters, and you change the IP address for an HA cluster, you must re-build the cluster afterward.

For details, see Build a cluster.

3. Configure any of the following options by entering the relevant number:
   - Configure the time and date
   - Configure a DNS server
   - Configure a DNS domain name
   - Change the machine's hostname
   - Change the root password
   - Change the afa password
   - Reset the AFA admin password
   - Reset the database password

   For more details, see Connect to the Administration Interface.
4. When you're done, enter **Q** to exit.

Configure NAS storage

This procedure describes how to configure AFA to store all reports on a remote NAS server.

NAS storage support

ASMS supports NAS storage configurations as follows:

Support	Description
Supported protocols	NFSv4 (default) and NFSv3, depending on the NAS server. ASMS attempts to connect first via NFSv4, and if it cannot, automatically uses NFSv3.
Deployment types	VMs with an AlgoSec-provided image deployed and AlgoSec Hardware Appliances only.

Support	Description
HA clusters	Configure NAS on the primary node. When you build the cluster, NAS is automatically configured on the secondary node.
DR clusters	Secondary nodes can have their own NAS server at the disaster recovery site. In such cases, customers are responsible for configuring the communication synchronization between the NAS servers at the primary and disaster recovery sites.
Load distribution architectures	Load distribution architectures are supported with NFSv4 only. Configuring NAS for the Central Manager automatically configures NAS for all Load Units.

Do the following:

1. Log on to the NAS server, and create a new directory in a shared space.
2. Connect to the Administration interface on your ASMS machine. For details, see Connect to the Administration Interface.
3. Enter **11** to configure NAS. The system confirms that NAS is not configured.
4. Enter **1** to set NAS for storing system reports. The system displays a message similar to the following:

```
You are about to configure a NAS server for storing system reports.
Note: No changes will take place without your final approval.
Before adding NAS configuration, your reports will be copied to
the following directory: algosec/firewalls_back_algosec/groups_back
algosec/matrices_back algosec/fwfiles_back
Once NAS configuration completes successfully, you may copy the
data back to the original directories.
```

5. Enter the NAS server IP.
6. Enter the NAS mount path. This is the directory that you created on the NAS

server in step 1.

The system confirms by displaying the NAS configuration IP, mount path, and NFS version.

For example:

```
NAS configuration details:
NAS server IP: <NAS IP you entered>
NAS Mount path: <NAS mount path you entered>
NFS version: NFSv4
```

Tip: If you specifically want to use NSFv3, change the NFS version manually.

7. The system prompts you to confirm the details. Enter **y** to confirm.

   If there is already content present in the mount path directory, the system prompts you to continue with one of the following:

   ```
   1. Abort NAS addition
   2. Delete directory content
   3. Use directory content
   ```

8. Enter **3** to use directory content.

   If you have Load Units configured, the system configures NAS on the Load Units as well.

   When the configuration is complete, the following message appears:

   ```
   NAS configured successfully
   ```

9. Copy reports from **algosec/firewalls_back_algosec/groups_back algosec/matrices_back algosec/fwfiles_back** to your newly moutned NAS directory.

   For example: **algosec/firewalls algosec/groups algosec/matrices algosec/fwfiles**

NAS storage is now enabled and ASMS can connect to the NAS server.

Note: To check NAS status at any time, connect to the Administration interface again and enter **11**.

The system confirms whether or not NAS is configured for your system.

Deconfigure NAS storage

Deconfigure NAS if needed as part of a larger process, or if you don't want reports to be stored on your remote NAS server.

Note: When NAS is deconfigured for a Master Appliance, it is automatically deconfigured for all Load Units.

Do the following:

1. Log on to the NAS server.
2. Connect to the ASMS machine's Administration Interface. For details, see Connect to the Administration Interface.
3. Back up your data by copying the reports from the mounted NAS directory. For example, copy the files from **algosec/firewalls algosec/groups algosec/matrices algosec/fwfiles** to a backup directory at **algosec/firewalls_back_algosec/groups_back algosec/matrices_back algosec/fwfiles_back**.
4. From the ASMS Administration Interface, enter **11** to deconfigure NAS.

   The system displays the NAS configuration details, and prompts you to select whether you want to check the NAS connectivity status or remove the NAS server.
5. Enter **2** to remove the server.

   The system prompts you to confirm that you want to remove the existing configuration.
6. Enter **y** to confirm.

NAS is removed from any Load Units, as needed. When NAS is fully removed, the following message appears:

```
NAS removal succeeded. Press 'Enter' to go back to main menu.
*NAS is not configured*
```

7. Copy your reports to your production directories and remove them from the remote NAS server.

NAS is deconfigured, and ASMS no longer connects to the remote NAS server.

Manage clusters

ASMS clusters prevent data loss and downtime in the event of hardware failures. Virtual Appliances and AlgoSec Hardware Appliances support both high availability and disaster recovery clusters.

Note: If you have both ASMS deployed on virtual machines and also AlgoSec Hardware Appliances in your system, each cluster must have nodes of the same type: **hardware-hardware** or **VM-VM**.

For more details, see:

- Cluster roles and modes
- High availability clusters
- Disaster recovery clusters

Cluster roles and modes

Each appliance node in the cluster is assigned one of the following roles and service statuses:

Roles	• **Primary** appliances synchronize data to the secondary appliance. • **Secondary** appliances receive data from the primary appliance.
Service modes	• **Primary** appliances currently run AlgoSec services. • **Secondary** appliances do not currently run AlgoSec services.

By default, the primary appliance is active, and the secondary appliance is in standby mode.

The primary and secondary appliances regularly verify that they can communicate with each other and that the other is alive. In the event that the primary appliance goes down, the secondary appliance will become active, in an event called *failover*.

ASMS clusters include the following types:

- High availability clusters
- Disaster recovery clusters

High availability clusters

High availability clusters both prevent downtime and protect data, as follows:

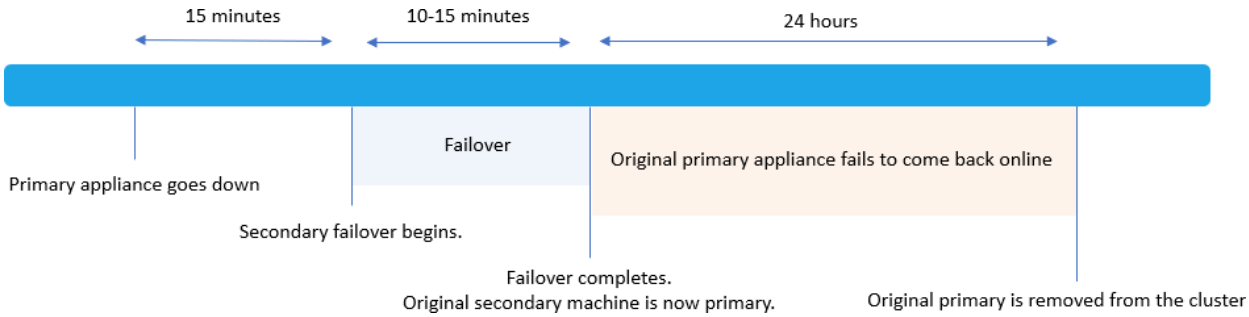
Automatic failover	**A secondary appliance automatically becomes active if the primary appliance fails.** *Ping nodes* are used to determine whether the primary appliance is connected to the network. If a ping to the node that represents the primary machine fails, the network connection on the primary appliance is considered to be down, triggering a failover to the secondary appliance. **Note:** Automatic failover occurs after a grace period of 15 minutes.
Co-location	**Both nodes are located at the same site and are physically connected.** This prevents a situation called *split-brain*, where failover might occur when the primary appliance is actually still active, such as if a ping from the primary appliance fails to reach the secondary appliance due to networking issues only.
Shared virtual IP address	**Configuring HA clusters includes configuring a virtual IP address shared by both machines.** This ensures that if or when failover occurs, AlgoSec services remain available at the same IP address.
Database permissions	In HA clusters, databases are fully active only on the secondary node, and partially active on the primary node. The secondary node also offers both read and write capabilities, while the primary node offers only read capabilities. In most cases, this does not affect your appliance configuration.

Post-failover scenarios

After failover occurs, the original secondary node becomes the new primary node.

- If the original primary node comes back online within 24 hours, it remains in the cluster as the new secondary node.
- Otherwise, the original primary node is removed from the cluster, and the original secondary node remains in the cluster as a single node.

For example:



Add FireFlow to your clusters

If FireFlow was not licensed and configured when your cluster was originally built, break and rebuild the cluster after adding FireFlow to your license and configuring it.

For details, see

- ASMS licensing
- Break a cluster
- Build a cluster

Disaster recovery clusters

Disaster recovery clusters protect data only.

The appliance nodes are located at different sites. If a primary appliance fails, the secondary appliance must be put into active mode manually. This is called *manual failover*, or *switching appliance modes*.

For more details, see Switch appliance roles.

➔ **See also**:

- Build a cluster
- Configure HA/DR parameters
- Break a cluster
- Switch appliance roles
- Troubleshoot HA/DR clusters

Build a cluster

This section describes how to build an ASMS HA or DR cluster, starting with the primary appliance. Data from the local or primary appliance is copied to the secondary or remote appliance during the build process.

For details, see;

- Verify cluster connectivity
- HA clusters only: Add a second interface
- Build an ASMS HA or DR cluster

Note: The amount of time the build process requires is dependent on the size of the database and the monitoring directory, and may be significant.

Verify cluster connectivity

If communication between the primary and secondary appliances goes through a firewall, make sure to allow traffic between their defined communication ports and services in both directions.

For more details, see Required port connections.

Important: For HA clusters, you must not make any changes to the **iptables** service.

This service is crucial to the communication between the nodes, and any manual changes may compromise the environment.

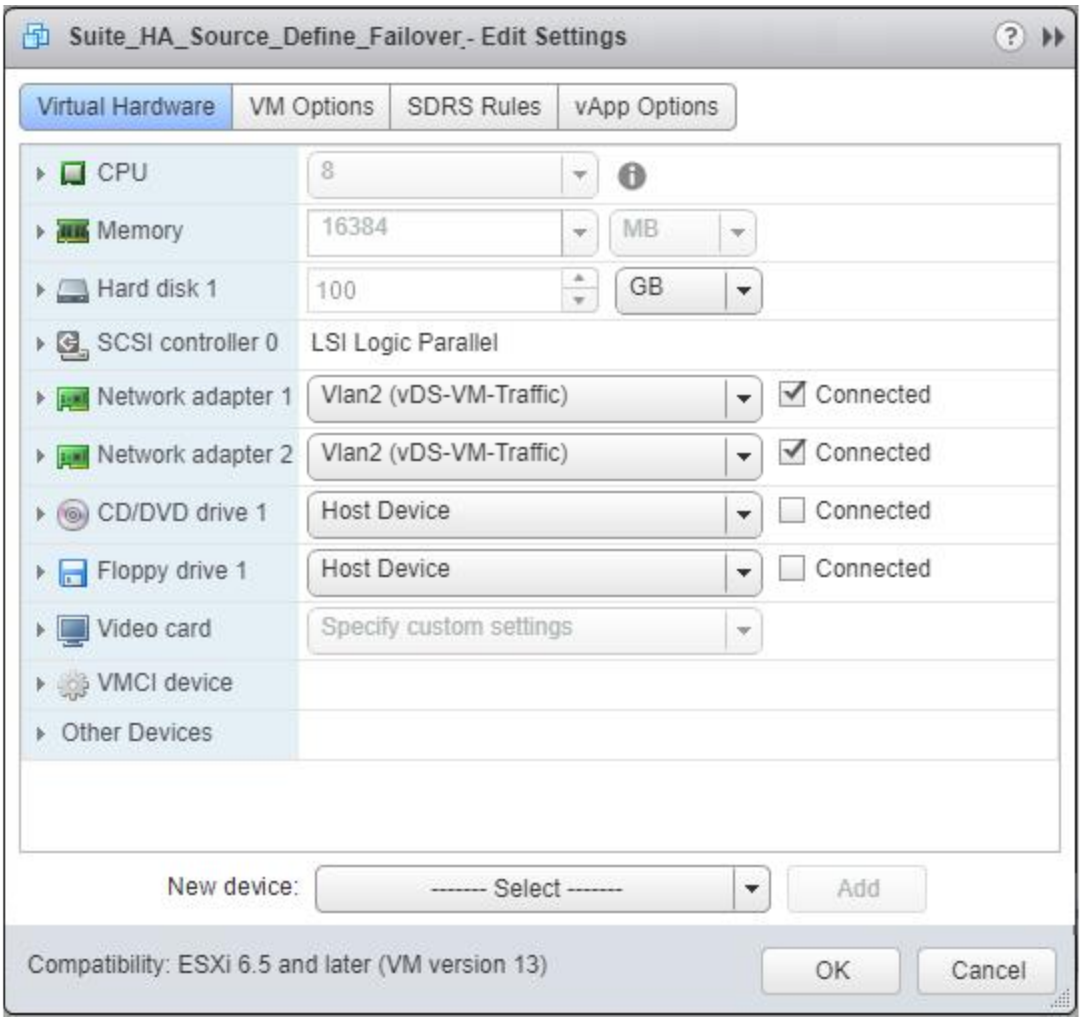
HA clusters only: Add a second interface

Before building an HA cluster deployed as a virtual appliance, configure the VM hardware to add a second interface.

Do the following:

1. Access the VM configuration for the VM hardware.
2. Add a second network adapter, and enable it as **Connected**.

   For example:



3. Verify your interface configuration.

   As user root, run: **ifconfig -a**

A list of all detected interfaces is displayed. Compare your interfaces to ensure that they are configured as needed.

Note: You do not need to configure an IP address on the second interface. This will be configured when you build the cluster.

Continue with Build an ASMS HA or DR cluster.

Build an ASMS HA or DR cluster

This procedure describes how to build an ASMS HA or DR cluster, or to rebuild one with default parameters.

Do the following:

1. If you are configuring an HA cluster on AlgoSec Hardware Appliances by connecting the appliances via network cable, connect one end of a crossover cable to the ETH1 port on each appliance.

   Tip: Connecting via network cable helps to ensure that failover does not occur due to network connection issues.

2. From the appliance that will be the primary node, connect to the ASMS Administration Interface. For details, see Connect to the Administration Interface.
3. In the Administration Interface, enter **13**. The following prompt appears:

```
*HA/DR is not configured*
Please select an item or enter "a" to abort:
1. Build HA cluster
2. Build DR cluster
3. Collect Logs
Your choice:
```

4. Enter the number for the option you want to continue with, and then continue with the wizard as prompted. The primary appliance is always the local machine.

HA clusters	Enter the following details, as prompted: • The cluster's virtual IP address and the virtual IP's subnet mask. • The primary appliance's **eth1** IP address. • The secondary appliance's IP address, ping node IP address, root password, and node name. • The secondary appliance's **eth1** IP address. • The witness machine IP address (ping node address). **Tip:** Select a ping node that reflects the local appliance's connectivity, and is reachable exclusively from that interface. We recommend selecting switches and routers for this purpose. Do not select the local or remote appliance, or a workstation. • The subnet mask for the primary and secondary appliances. • The subnet mask for the eth1 of the primary and secondary appliances.
DR clusters	Enter the following details, as prompted; The secondary appliance's IP address, ping node IP address, root password, and node name.

A summary of the primary and secondary appliances' information appears and you are prompted to confirm the details.

5. Enter **y** to confirm the summary.

   The system begins to build the cluster. This may take some time, depending on the amount of ASMS data.

   When complete, a success message appears with the cluster status, and an email confirmation is sent to the administrator email.

   Tip: If initial synchronization results in an Rsync error, we recommend selecting option 2: **Continue despite rsync failure**. Synchronization should succeed the

second time.

6. Optional: Customize HA/DR parameters. For details, see Configure HA/DR parameters.
7. If your machine is now part of an HA cluster, you'll need to update the appliance's IP address in other systems that send data to ASMS. For example, if you previously had this set to a specific IP address, you'll need to change this to a virtual IP address.

Note: Report synchronization from the primary appliance to the secondary appliance is based on NAS configuration. Reports are only synched to the secondary appliance is NAS is not configured.

Configure HA/DR parameters

This procedure describes how to configure HA/DR parameters, and can be performed any time after building an HA or DR cluster.

Changing parameter values must be done from the primary appliance only. Viewing parameter values is supported from either the primary or secondary appliance.

Do the following:

1. From the primary appliance, connect to the ASMS Administration Interface. For details, see Connect to the Administration Interface.
2. In the Administration Interface, enter **13**. A prompt similar to the following appears:

```
Cluster status:
1. Primary          |  10.10.10.14      |  Up (this appliance)  |
AFA, ABF, AFF
2. Secondary (HA)   |  10.10.10.13      |  Up                   |  DB
            10.10.10.14 <-> 10.10.10.13 : Synced
```

```
* VIP - 10.10.10.18
```

3. Enter **4** to view / edit cluster parameters.

   The parameters and their current values are displayed, and the system asks whether you want to make any changes.

4. Enter **y** to make changes.

   Each parameter appears, with the option to change the value. Make your changes as needed for each parameter, until a confirmation message appears.

   Note: When automatic failover is configured, if a ping does not arrive from the primary appliance within the configured **Failover Over Timeout** value, the secondary appliance automatically becomes active.

   Automatic failover is not supported for DR clusters. DR cluster nodes must have their roles switched manually, if needed. For details, see Switch appliance roles.

5. Enter **y** to confirm the changes.

   Your changes are applied, and a success message appears, along with the cluster status. A confirmation email is also sent to the Administrator user.

Break a cluster

This topic describes how to break a cluster. Removing an appliance from a cluster changes it to a standalone appliance, and also temporarily stops any AlgoSec services running on the appliance.

Do the following:

1. From the primary appliance, connect to the ASMS Administration Interface. For details, see Connect to the Administration Interface.
2. Enter **13**. The console displays details about the cluster, including primary and

secondary nodes and their statuses.

For example:

```
Cluster status:

1. Primary          |  10.10.10.14       |  Up (this appliance)   |
AFA, ABF, AFF

2. Secondary (HA)   |  10.10.10.13       |  Up                    |  DB

             10.10.10.14 <-> 10.10.10.13 : Synced

* VIP - 10.10.10.18
```

3. Enter **2** to remove the HA configuration. When prompted to confirm, enter **yes**.

   AlgoSec services are stopped and the appliance is removed from the cluster.

   When complete, the services are started again, and a success message appears along with the cluster status. An email notification is also sent to the Administrator user.

4. After breaking a cluster, make sure to bring down one of the appliances that used to be in the cluster. This is required to prevent duplication, as both appliances remain connected to the same Load Units / Remote Agents, as well as devices and firewalls.

5. **HA clusters only:** After breaking an HA cluster, the virtual IP remains attached to the node that used to be the primary node.

   Remove it as needed by doing the following:

   a. Connect to the ASMS Administration Interface, and enter **13** to configure HA/DR. For details, see Connect to the Administration Interface.

   b. Enter **4** to remove a VIP.

   c. At the prompt, enter **y** to confirm.

d. If you have Load Units configured, run the **Distributed Architecture configuration** from the main Administration interface. For details, see Add or edit Load Units.

Switch appliance roles

This procedure describes how to switch appliance roles, so that the primary appliance becomes the secondary, and the secondary appliance becomes primary. Perform this procedure as part of a manual failover process for DR clusters, in HA clusters as needed, if automatic failover is disabled.

Switching appliance roles may also be required as part of maintenance procedures. If you need to take the primary appliance offline, first perform a manual failover to the secondary appliance.

Do the following:

1. Connect to the ASMS Administration Interface. For details, see Connect to the Administration Interface.

   You can perform this procedure from either appliance, unless the primary appliance is already down.

2. Enter **13**. The console displays details about the cluster, including primary and secondary nodes and their statuses.

   For example:

```
AlgoSec HA cluster status:
1. Primary 10.10.0.101 - Up (this appliance)
2. Secondary 10.10.0.102 - Up
* VIP - 10.10.0.103
10.10.0.101 -> 10.10.0.102 : Synced
Please select an item or enter 'a' to abort:
1. View cluster status details
```

```
2. Remove HA configuration
3. Switch roles
4. View/Edit Cluster parameters
5. Collect Logs
```

3. Enter **3** to switch roles. The system prompts you to confirm.
4. Enter **y** to confirm that you want to switch roles.

   The manual failover begins. Data from the primary appliance is synchronized to the secondary appliance, and the secondary appliance becomes active.

   When the process is complete, a success message appears, with the cluster status. An email notification is also sent to the Administrator user.
5. Continue as instructed to do the following:
   a. Enter **algosec_conf** to return to the main menu.
   b. Enter **15** to run the Distributed Architecture configuration.
   c. Adjust your load units by doing the following:
      - Activate the DR load units
      - Disable / remove the primary load units

Troubleshoot HA/DR clusters

This topic describes common troubleshooting issues and how to solve them.

DR clusters: primary appliance failed

If you have a DR cluster and your primary appliance has failed, perform a manual failover to the secondary appliance by switching appliance roles.

For details, see Switch appliance roles.

DR clusters: secondary appliance failed

If you have a DR cluster and your secondary appliance has failed, do the following:

1. Fix the secondary appliance.
2. Re-build your cluster. For details, see Build a cluster.

Split-brain situations

If you've received an email notification that a split-brain situation was detected, do the following:

1. Break the cluster. For details, see Break a cluster.
2. Examine any FireFlow tickets and AFA reports on each appliance, and determine which appliance has the most recent data.

   Note: If the data on both appliances seem to be equally recent, we recommend choosing the primary appliance.

3. Re-build the cluster from the appliance with the most recent data. For details, see Build a cluster.

Current synchronization operation canceled

If a new synchronization starts while the previous is still running, the new synchronization is automatically canceled, and the system sends an email notification.

To resolve this issue, configure synchronizations to run less frequently. For details, see Configure HA/DR parameters.

Manage nodes automatically removed from clusters

ASMS automatically removes a secondary cluster in the following scenarios:

- If **there is less than 10% of disk space** found on the **Primary** data partition.

  In this case, a warning message will have been sent by email and to the Issues Center when the **Primary** was found to have less than 20% free disk space.
- If the **secondary node is unresponsive** for more than 12 hours.

In this case, a warning message will have been sent by email and to the Issues Center when the secondary node had been unresponsive for 6 hours.

When the node is removed, the Central Manager is left as a single-node cluster.

To continue with your cluster, first handle your disk space or connectivity issue, and then re-build the cluster as follows:

Disk space issues	If your node was removed for a disk space issue, do the following: 1. Log in to the Central Manager and access the Administration menu. 2. Enter **13** to re-build your cluster and enter the details for your secondary node. For more details, see Connect to the Administration Interface and Build a cluster.
Connectivity issues	If your node was removed for a connectivity issue, when the secondary node is available again, it will still be configured to send data to the primary node. Do the following: 1. Forcibly remove the cluster configuration from the secondary node, and from any other nodes in the cluster. For more details, see Forcibly remove a node from a cluster. 2. Access the Central Manager node to rebuild the cluster again.

Forcibly remove a node from a cluster

This procedure describes how to forcibly remove a node from a cluster, which is sometimes recommended after system or connectivity errors have occurred.

Note: Before you start, we recommend gathering any logs you may need before they are overwritten as the cluster configuration is removed.

Do the following:

If you are recommended to forcibly remove a node from a cluster, do the following:

1. Log in to the node you want to remove and access the **Administration** (**algosec_conf**) menu.
2. Enter **13** to access the HA/DR configuration.
3. Enter **1** to forcibly remove the cluster configuration from the node.

   Note: This option appears only when the system detects that an error has occurred.

   If this option does not appear, you might be trying to break the cluster using the standard procedure. For details, see Break a cluster.

4. Repeat steps 2-4 on all nodes in the cluster, including the Central Manager.
5. Log in to the Central Manager and access the **Administration** (**algosec_conf**) menu.
6. Enter **13** to access the HA/DR configuration and rebuild your cluster.

For more details, see Connect to the Administration Interface andBuild a cluster.

Collect cluster logs for AlgoSec technical support

If you've been requested to send cluster logs to AlgoSec technical support for further analysis, do the following:

1. From the primary or secondary appliance's administration interface main menu, select option **13**.
2. In the HA/DR sub-menu, select **Collect HA logs**. This is option **3** when there is no cluster configured and option **5** when a cluster is configured.

A ***.tar** file containing all of the relevant logs will be created in the appliance's `/tmp` library.

Set up the ASMS environment

This section describes the basic procedures required to set up your initial ASMS environment, and includes:

- Define the first ASMS Administrator
- Run the FireFlow setup program
- Additional optional configurations

If you are setting up AFA only, install your licenses as part of the procedure to Define the first ASMS Administrator. If you are setting up both AFA and FireFlow, install your licenses after both procedures are complete.

Define the first ASMS Administrator

This procedure describes how to define the first ASMS Administrator user, and must be performed before other users can be added to the system.

Do the following:

1. Access your AFA user interface. In your browser, browse to **https://<AFA_server>/** where **<AFA_server>** is the AFA server IP address or DNS name.

   Contact your local network administrator for this value. For more details, see AFA server DNS name / IP address recommendations .

   The **Configure the First Administrator** dialog appears.

Tip: If a warning message about the Web server's certificate appears, click **Accept** or **OK**, depending on your browser and security settings.

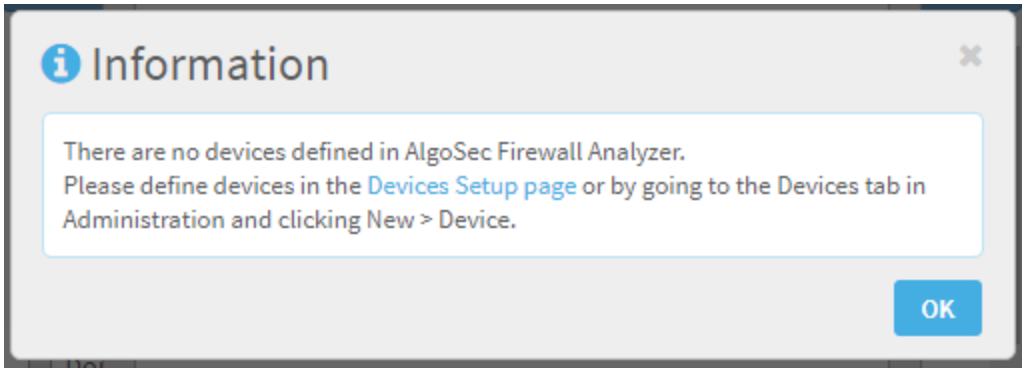
For more details, see Security certificate recommendations.

2. In the **Configure the First Administrator** dialog, enter the following values:

Username	Enter a username for the administrator.
Full name	Enter the administrator user's full name.
E-Mail Address	Enter the email address you want ASMS to use to contact the administrator.
Password	Enter a password for the administrator. The password must have a minimum of 4 characters (letters or numbers).
Repeat	Enter your password again.

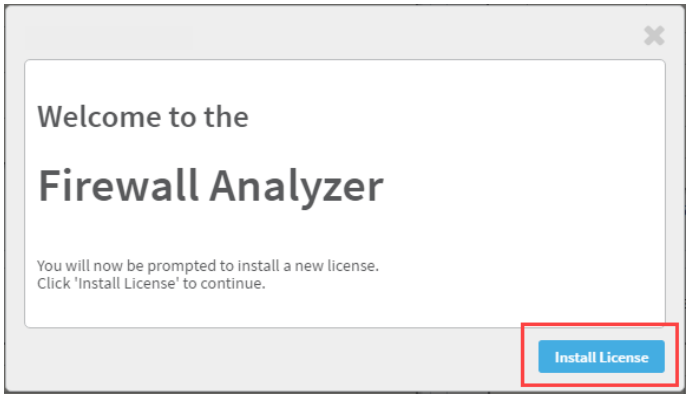
3. Click **Next** to log in to AFA as the new administrator.

Since this is your first login to ASMS, a message appears to notify you that you don't have any devices defined yet.



From here, do one of the following:

- Click the **Devices Setup page** link to start defining devices immediately.
- Click **OK** to close the window and install a license. In the **Welcome** dialog that appears, click **Install License**.

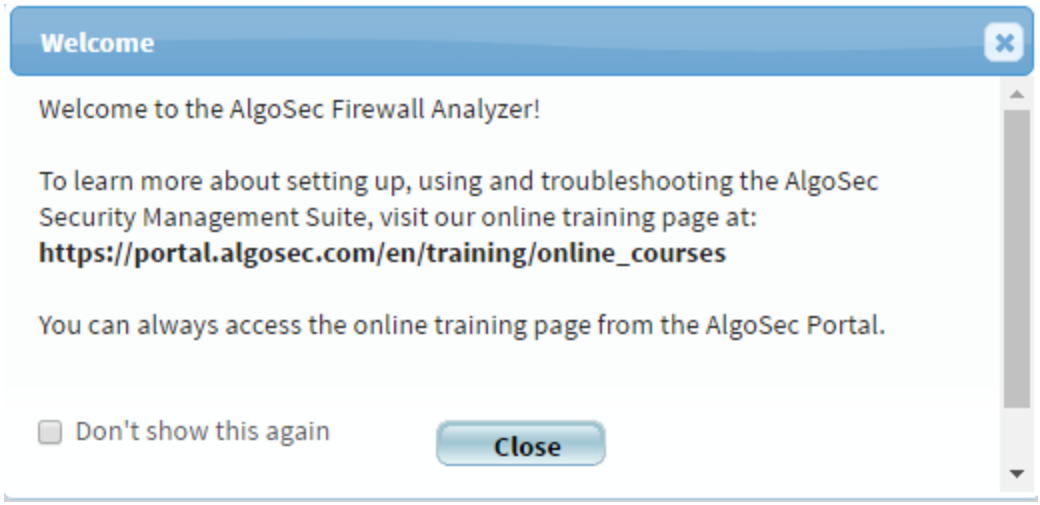


License installation

While you can define devices immediately, you cannot run an analysis until you install a license. If you are also setting up FireFlow, install your license only after that procedure is complete. For details, see:

- Run the FireFlow setup program
- ASMS licensing

When your license is installed, the **Welcome** dialog appears:



Click **Close** to access the AFA Home page.

Tip: Training courses are accessible from the AlgoSec portal.

Run the FireFlow setup program

This procedure describes how to set up FireFlow, and must be done after defining your first AFA Administrator. For more details, see Define the first ASMS Administrator.

Do the following:

1. Start a session as follows, depending on your deployment mode:

AlgoSec Hardware Appliances	Initiate an SSH session to the appliance's IP address. The default IP address is **192.168.1.1**.
ASMS deployed on virtual machines	Open the VM's console.

   The system prompts you to log in.

2. Log in as user: **root**

   If you are working with a virtual appliance or an AlgoSec Hardware Appliance, the default password is **algosec**.

3. Access the Administration Interface (the **algosec_conf** menu). For details, see Connect to the Administration Interface.
4. Enter **14** to set up the FireFlow configuration.

   For each prompt, enter the requested data, including:

Server Settings dialog	Configure the FireFlow server's email address and database password. This email address is used to send all email coming from FireFlow.
Predefined Users dialog	Configure a special user, named **FireFlow_batch**. FireFlow users this username to perform batch operations in AFA.
Outgoing Email dialog	Configure the outgoing SMTP email details for both AlgoSec Firewall Analyzer and FireFlow.
Incoming Email dialog	Configure FireFlow to fetch emails from a dedicate mail server mailbox, using POP3 or IMAP. This enables users to submit change requests to FireFlow via email, and to add comments to tickets by replying to FireFlow system-generated emails.

When complete, the **Setup Config is done** dialog appears.

Additional optional configurations

You may also want to configure the following AFA and FireFlow settings:

Device rule comments	AFA and FireFlow are configured to use the following regular expression in all device rule comments: `FireFlow #<ticket ID>` where **<ticket ID>** is the ID number of the FireFlow ticket.
Device analysis schedule	By default, automatic device analysis is scheduled for the ALL_FIREWALLS group, which includes all devices in the system, for 1:00 AM, daily.

Log in to ASMS to continue your configurations. For details, see Logins and other basics.

Configure a distributed architecture

ASMS supports the following types of distributed architectures:

- Configure load distribution
- Configure geographic distribution

Note: ASMS also support high availability (HA) distributions.

For more details, see Deploy clusters and distributed architectures and Manage clusters.

Configure load distribution

ASMS load distributions have a single Central Manager, and one or more Load Units, all in the same geographical location. Each device analysis and monitoring is assigned and processed by a specified Load Unit. All Load Units run these processes in parallel and send results back to the Central Manager.

Reports are stored on the Master Appliance only. Additionally, access the AFA web interface via the address of the Master Appliance only.

Do the following:

1. Log in to AFA from the appliance you want to define as the Master Appliance. For details, see Logins and other basics.
2. Enable distributed processes. For details, see Enabling distributed processing.
3. In AFA, add each Load Unit, and then add the new IP addresses to the AFA database. For details, see Add or edit Load Units.

Maximum concurrent analysis and query processes

The maximum number of concurrently running analysis and query processes is equal to the total number of CPU cores, on all Load Units together.

View the status of each analysis and the Load Unit it's running on, in the **Analysis Status** page in AFA. To view this, click the **Analysis Status** button next to the user menu.

Minimum and maximum numbers of Load Units

When distributed processing is enabled, a Load Unit is automatically added to the Central Manager, and half of the Central Manager's cores are used to run analysis and queries.

For example, if the Central Manager has 8 cores, 4 of them will be used for the Load Unit.

ASMS supports an unlimited number of Load Units.

Configure geographic distribution

ASMS geographic distribution configurations have a Central Manager appliance in one location, and several Remote Agent appliances in other locations. Remote Agents manage and collect data from any devices local to their locations, and send all data to the Central Manager.

The Central Manager manages the Remote Agents, and can also act as a Remote Agent for any co-located devices.

Reports are stored on the Central Manager only. Additionally, access the AFA web interface via the address of the Central Manager.

Do the following:

1. Log in to AFA from the appliance you want to define as the Central Manager. For details, see Logins and other basics.
2. Enable distributed processes. For details, see Enabling distributed processing.

3. In AFA, add each Remote Agent appliance. For details, see Add or edit Remote Agents.

Note: ASMS also supports high availability configurations for remote agents. Upon failover, the master remains connected to the cluster node that is currently active. For more details, see Manage clusters.

Two devices in the same AFA environment that are manged by different Remote Agents, cannot have the same name.

➔ See also:

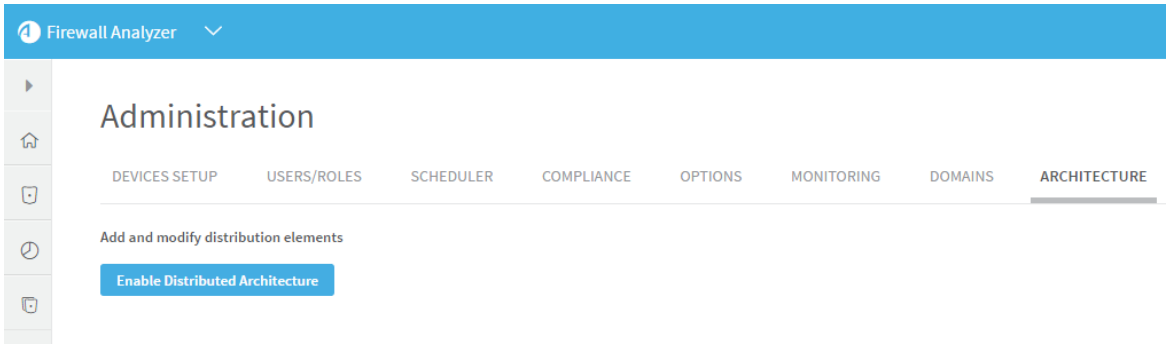
- Networking requirements and recommendations
- Delete Load Units or Remote Agents
- Disable distributed processes

Enabling distributed processing

This procedure describes how to enable distributed processing, and must be performed for both load and geographic distribution.

Do the following:

1. Ensure that you are logged in to AFA as an administrator user. For details, see Logins and other basics.
2. In AFA, click your username at the top right, and select **Administration**.
3. In the Administration area, click the **Architecture** tab.



4. Click **Enable Distributed Architecture**. When a confirmation message appears, click **OK**.

When you're done, continue with Add or edit Load Units or Add or edit Remote Agents, depending on the architecture type you're configuring.

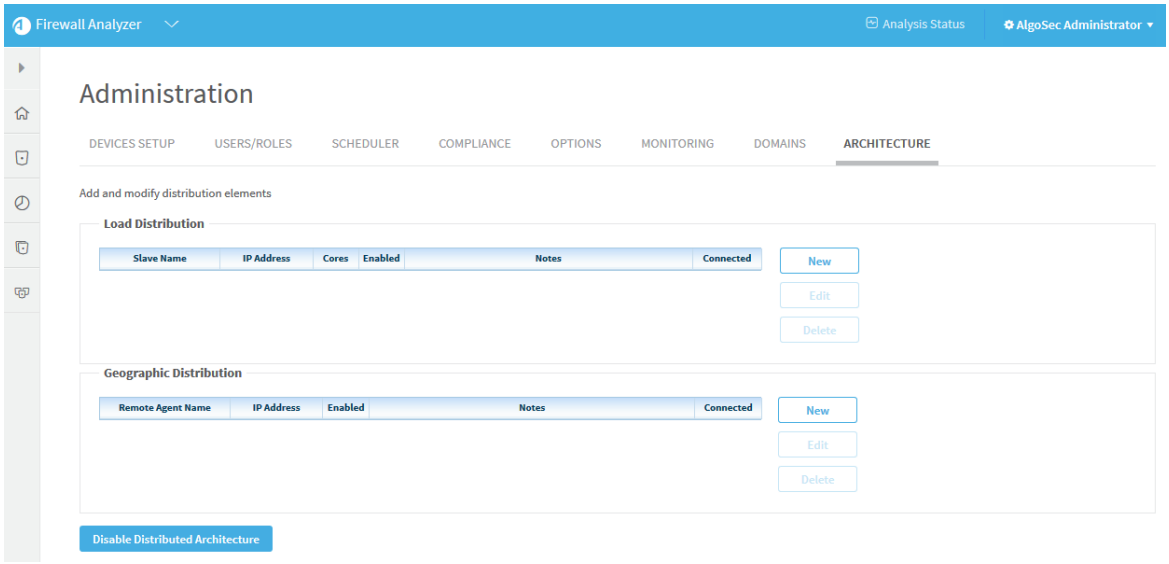
For more details, see Configure a distributed architecture.

Add or edit Load Units

This procedure describes how to add or edit Load Units to ASMS, as is part of configuring load distribution.

Do the following:

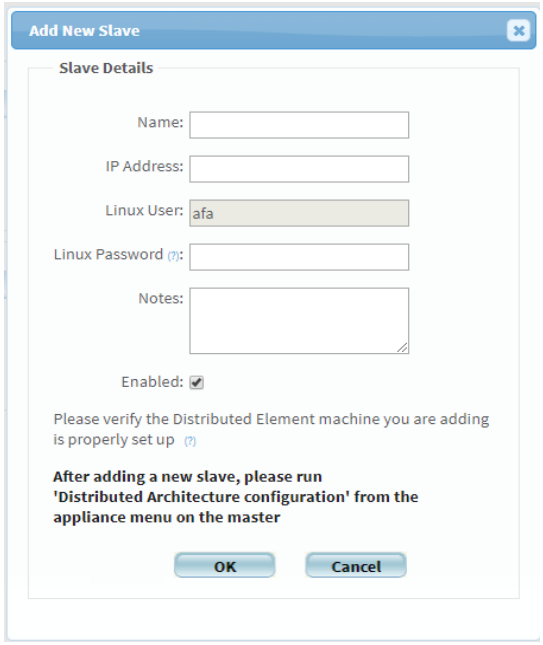
1. Ensure that you are logged in to AFA as an administrator. For details, see Logins and other basics.
2. Browse to the **Administration** area and select the **ARCHITECTURE** tab.



3. In the **Load Distribution** area, do one of the following:

   - To add a new Load Unit, click **New**.
   - To edit an existing Load Unit, click on the relevant row, and click **Edit**.

   The **Add New Slave/Edit Slave** dialog box appears.



4. Enter the following details:

Name	Enter a name for the Load Unit. Read-only when editing.
IP Address	Enter the Load Unit's IP address. Read-only when editing.
Linux User	Read only. The username of the Linux user you used to install AFA on the Load Unit. Appears only when adding a new Load Unit.
Linux Password	Enter the password of the Linux user shown. Appears only when adding a new Load Unit.
Notes	Optional. Enter any notes about this Load Unit.
Enabled	Select to enable the Load Unit.

5. Click **OK**.
6. If you added a new Load Unit, reconfigure the distributed architecture on all Load Units. Do the following:
    a. Connect to the Administration interface on the Master Appliance. If the Master Appliance is in a cluster, connect to the primary node.

       For details, see Connect to the Administration Interface.
    b. Enter **15** to configure load distribution.

If you added a new Load Unit, AFA attempts to connect to it. The **Connected** column on the **ARCHITECTURE** tab indicates whether this connection is successful. Connection statuses are indicated by the following colors:

- **Green**. Successful
- **Red**. Failed
- **Grey**. In progress

Note: If this is the first Load Unit that you've added, the number of CPU cores used by the Central Manager for running analysis is reduced by half, since the other half is now used by the Load Unit.

➔ See also:

- Delete Load Units or Remote Agents
- Disable distributed processes

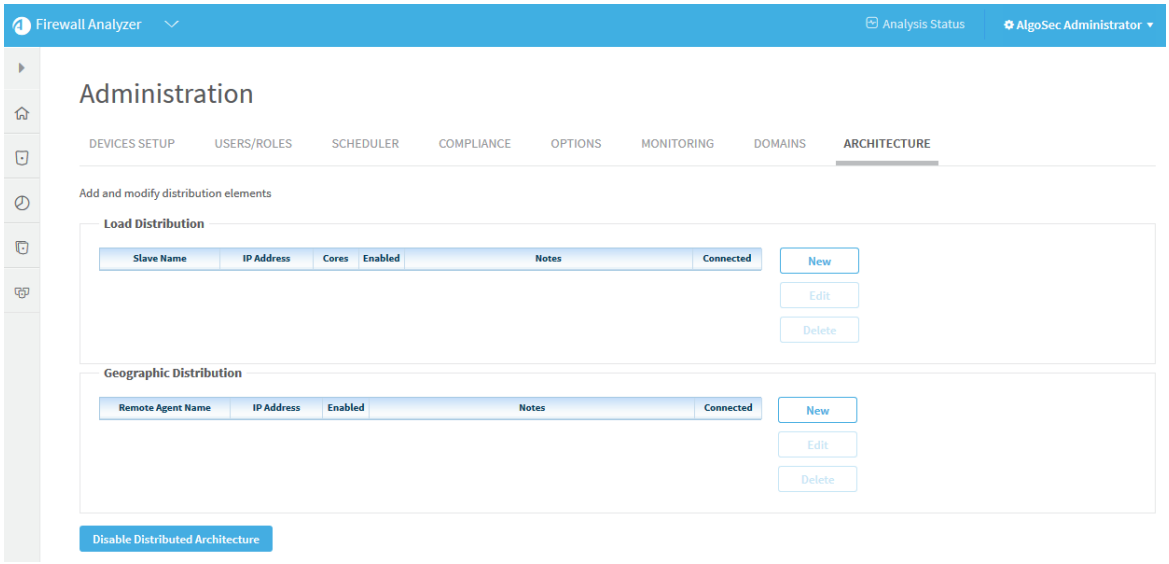
Add or edit Remote Agents

This procedure describes how to add or edit a Remote Agent, and is part of configuring geographic distribution.

If you are adding an HA cluster of appliances as a Remote Agent, you must first build the cluster. For details, see Manage clusters.

Do the following:

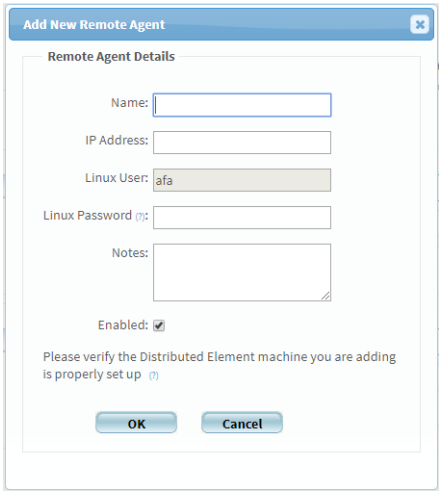
1. Ensure that you are logged in to AFA as an administrator. For details, see Logins and other basics.
2. In the toolbar, click your username, and select **Administration**.
3. In the Administration area, click the **Architecture** tab.



4. In the **Geographic Distribution** area, do one of the following:

- To add a new Remote Agent, click **New**.
- To edit an existing Remote Agent, click on the relevant row, and click **Edit**.

The **Add New Remote Agent** dialog box appears.



5. Enter the following details:

Name	Enter a unique name for the Remote Agent. Read-only when editing.
IP Address	Enter the Remote Agent's unique IP address.
Linux User	Read only. The username of the Linux user you used to install AFA on the Remote Agent.
Linux Password	Enter the password of the Linux user shown.
Notes	Optional. Enter any notes about this Remote Agent.
Enabled	Select to enable the Remote Agent.

6. Click **OK**. If you added a new Remote Agent, AFA attempts to connect to it.

The **Connected** column on the **ARCHITECTURE** tab indicates whether this connection is successful. Connection statuses are indicated by the following colors:

- **Green**. Successful
- **Red**. Failed

- **Grey**. In progress

Tip: If you are building a high availability architecture on two remote agents, continue by building a cluster.

For more details, see Build a cluster.

➔ See also:

- Delete Load Units or Remote Agents
- Disable distributed processes

Delete Load Units or Remote Agents

This procedure describes how to delete a Load Unit or Remote Agent from your ASMS environment.

Do the following:

1. Ensure that you are logged in to AFA as an administrator. For details, see Logins and other basics.
2. In the toolbar, click your username, and select **Administration**.
3. In the Administration area, click the **Architecture** tab.
4. Select the row for the Load Unit or Remote Agent you want to delete, and click **Delete**.
5. In the confirmation message that appears, click **OK**.

The Load Unit or Remote Agent is removed from your ASMS environment.

Note: After removing a Load Unit or Remote Agent from your environment, do not use it again for ASMS without restoring factory settings.

For details, see General system maintenance.

➔ See also:

- Configure a distributed architecture
- Disable distributed processes

Disable distributed processes

This procedure describes how to disable distributed processing on ASMS. This cancels all running and queued analysis, and all Remote Agents and Load Units are automatically deleted.

Do the following:

1. Ensure that you are logged in to AFA as an administrator. For details, see Logins and other basics.
2. In the toolbar, click your username, and select **Administration**.
3. In the Administration area, click the **Architecture** tab.
4. Click **Disable Distributed Architecture**.
5. In the confirmation message that appears, click **OK**.

Distributed processing is disabled.

➔ See also:

- Configure a distributed architecture
- Disable distributed processes

Basic sanity checks

This section describes how to perform basic sanity checks, which should be run after making changes to your environment, such as for clusters, distributed architectures, and upgrades.

These sanity checks also define standards for basic ASMS functionality, and enable you to verify that your environment is functioning as expected.

This section includes:

- ASMS basic functionality
- Test basic ASMS processes
- Test basic AFA functionality
- Test basic FireFlow functionality
- Test basic AppViz functionality

ASMS basic functionality

Basic functionality for ASMS is defined as follows:

Product	Description
Hardware or VM	Basic functionality on virtual machines deployed with ASMS, or on AlgoSec Hardware Appliances, includes all necessary processes running. For details, see Test basic ASMS processes.
AFA	Basic AFA functionality includes: • Add and analyze devices completely and successfully • Identify device changes correctly • Send email alerts For details, see Test basic AFA functionality.

Product	Description
FireFlow	Basic FireFlow functionality includes: • Both requestors and privileged users can successfully submit change requests • A single change request can move through all stages of the configured workflow • After changes are implemented on the device, the Validation and AutoMatching functions respond correctly For details, see Test basic FireFlow functionality.
AppViz	Basic AppViz functionality includes: • New applications can be added • Flows can be added to applications, connectivity is accurately updated, and the relevant change requests are opened • Applications can be decommissioned For details, see Test basic AppViz functionality.

Test machine installation and configuration

This section describes how to test that your ASMS machines are installed and configured correctly. Do this after making changes to your configuration, deploying a new system, or upgrading.

Do the following:

Open a browser, and browse to IP address of your AlgoSec machine.

If the AlgoSec home page appears, your machine is connected and configured correctly. For example:

If this page or another like it does not appear, check to see that your basic configurations have been done correctly. For details, see Basic sanity checks.

Test basic ASMS processes

This procedure describes how to test that basic ASMS processes are running on your machines.

Do the following:

1. Connect to the Administration Interface. For details, see Connect to the Administration Interface.
2. Enter **17** to verify service status.

   Output similar to the following should appear, confirming that all of these services are running:

```
|=====================================|
|            147.172.44.40            |
|                                     |
|   (Thu Nov 28 13:45:10 IST 2019)    |
|-------------------------------------|
```

```
| crond                 | OK          |
| httpd                 | OK          |
| postgresql            | OK          |
| activemq              | OK          |
| mongo Database        | OK          |
| syslog-ng             | OK          |
| apache-tomcat         | OK          |
| AlgoSec microservices | OK          |
| metro                 | OK          |
| map diagnostics       | OK          |
| Vulnerabilities       | OK          |
| cloudlicensing        | OK          |
| backup/restore        | OK          |
| watchdog              | OK          |
| device manager        | OK          |
| trafficlogmanager     | OK          |
| batch application     | OK          |
| configuration         | OK          |
| aff-boot              | OK          |
| ABF                   | OK          |
|=====================================|
```

Test basic AFA functionality

This procedure describes how to test basic AFA functionality.

Do the following:

1. **Prepare for your test**
    a. Define an email server.
    b. Define a user with permissions for all devices. Specify that the user receives email notifications for all reports and configuration / policy changes.

2. **Test device definition and analysis**
    a. Define a new device and assign a user with permissions for it, or use an existing device to test AFA functionality.
    b. Run a manual analysis on the device.
    c. Verify that all sections of the new report have valid results.

    In the report, on the **Policy Optimization** tab, in the **Rule Usage Statistics** area, click **All Rule Usage**.

    Check the first text line to verify that the report is based on logs collected today.
3. **Test change monitoring**
    a. Add a rule to the device's policy.
    b. Wait for the next monitoring cycle to run. By default, this runs every 20 minutes.
    c. View the device's **Monitoring** tab and verify that the change was detected.
4. **Test email alerts**
    a. Check that the user you defined back in Prepare for your test receieved an email alert about the analysis completed in Test device definition and analysis.
    b. Check that the same user received an alert about the change you made to the device in Test change monitoring.

Test basic FireFlow functionality

This procedure describes how to test basic FireFlow functionality.

Do the following:

1. **Test change request submission**

    Do the following as a Requestor user, and then again as a privileged user:

a. Log in to FireFlow and submit a change request. If your organization uses a customized template or workflow, use the custom version.

b. Verify that the change request was submitted successfully.

2. **Test workflow functionality and validation**

a. Locate one of the change requests you created in Test change request submission , and move it through the various stages of the workflow.

b. Verify that the following stages produce valid results:

- **Initial Plan:** Shows the relevant devices for the change request.
- **Risk Check**: Shows a list of risks.
- **Work Order**: Shows a valid suggestion to implemented the requested change.

c. When you get to the **Work Order** stage in the change request, implement the change on the device.

d. After the next monitoring cycle is complete, browse to the **Validation** stage of the workflow, and verify that accurate validation results are shown.

e. In AFA, run an analysis on the device. Wait 2 hours, and then browse to the **AutoMatching** FireFlow stage, and verify that the change request and change are listed in the correct section.

Test basic AppViz functionality

This procedure describes how to test basic AppViz functionality.

Do the following:

1. **Test new applications**

a. Create a new application, and add flows to it. Add at least one flow that is currently blocked by the organization's firewalls.

b. Verify that the application is created successfully.

2. **Test connectivity and change requests**
    a. Apply the application draft and check the application connectivity.
    b. Verify the connectivity for each flow, and that the connectivity of the entire application updates automatically.
    c. In the **Change Requests** tab, verify that a change request was created for the new flows.
3. **Test application decommissioning**
    a. Decommission the application you created in Test new applications.
    b. Verify that the application's status changes to **Decommissioned**.
    c. Verify that the relevant change requests were opened to drop the application's traffic.

Note: If the application contains flows that are in use by other applications, change requests for this traffic will not be opened.

Populate your environment

After your initial setup, add devices in AFA, users in FireFlow, and applications to AppViz, depending on the products supported by your licenses.

For details, see the following guides:

- **AlgoSec Firewall Analyzer Administrator Guide.** Describes how to add devices and users to AFA.
- **AlgoSecFireFlow User Guide.** Describes how to add unprivileged users, also known as Requestors, to FireFlow.
- **AlgoSecAppViz User Guide.** Describes how to add applications to AppViz.

When FireFlow and AppViz are licensed, users added to AFA automatically have access to FireFlow and AppViz, and FireFlow Requestors automatically have access to AppViz.

Upgrade ASMS

This section describes how to upgrade an ASMS environment to a new version of ASMS.

This section includes:

- Licensing during upgrade
- Enabling new features after upgrade
- Upgrade prerequisites
- Upgrade your system

Licensing during upgrade

Upgrading ASMS to a new version retains all your existing license information and configuration settings. All reports are retained as well, unless otherwise specified.

For more details, see ASMS licensing.

Enabling new features after upgrade

Some new features in our new version may only be enabled and visible after you generate new reports for all devices.

After upgrading, we recommend running a manual group report for the **ALL_FIREWALLS** group so that you can view all features.

Upgrade prerequisites

Before you start upgrading your ASMS system, read through the following prerequisites and ensure that you and the system are ready to start.

In this section:

- Mandatory upgrade prerequisites
- Recommended upgrade prerequisites

Mandatory upgrade prerequisites

The following prerequisites are required before upgrading.

- Increased system requirements in ASMS A30.10
- Upgrade prerequisites
- Downtime requirements for upgrades
- Disk space requirements for upgrades

Increased system requirements in ASMS A30.10

System optimizations in version A30.10 require additional CPU and memory specifications.

We highly recommend increasing your system specifications to match the updated requirements, if needed. Systems that remain with legacy minimum specifications may have unexpected results.

For more details, see Hardware minimum requirements.

Note: If your system specifications are already larger than the updated requirements, your system specifications can stay as they are. In such cases, there is no need to resize your entire system.

Tip: If you have a distributed architecture, make sure that you have the required system specifications on all distributed nodes to prevent errors during upgrades.

Minimum version required for upgrades

AlgoSec's upgrade process is supported only from two versions backwards. Therefore, upgrading your system to ASMS version **30.10** is supported only from **2018.2**.

If you have an ASMS version earlier than 2018.2, you must first perform any upgrades required to get to 2018.2. For details, see the upgrade procedure in the Installation and Setup Guide for 2018.2 or any other version you are upgrading to. These guides are available from the AlgoSec portal.

Note: Prerequisites and upgrade procedures will differ, depending on your system version.

Example: If you are upgrading from **6.11** to **30.10**, perform the following upgrades:

1. First, upgrade from 6.11 to 2018.2. Use the procedure in the *2018.2 Installation and Setup Guide*.
2. Then, upgrade again from 2018.2 to 30.10. For more details, see Upgrade your system.

Downtime requirements for upgrades

Downtime will be required while all of the servers in your system are upgraded. The downtime will differ depending on the number and types of servers you have. Schedule your upgrade at a time where you can afford this downtime.

Tip: Start the upgrade process to view the runtime estimation.

Disk space requirements for upgrades

5 GB of disk space is required per partition (OS and data) on all appliances:

- **If less than 5 GB of disk space is found**, the upgrade process aborts.
- **If there is less than 10 GB of disk space found**, the upgrade process presents a warning and enables you to choose whether to continue or not.

  To cancel and run the upgrade later, enter **n** at the confirmation prompt.

Recommended upgrade prerequisites

The following pre-requisites are not mandatory, but are recommended:

- Backup your system before upgrading
- VisualFlow recommendations for upgrades

- HA cluster recommendations for upgrades
- Service recommendations for upgrades

Backup your system before upgrading

If you have ASMS deployed on virtual machines, we recommend generating a fresh backup before upgrading. This isn't relevant for physical appliances, as restoring or rolling back upgrades on physical appliances is not supported.

VisualFlow recommendations for upgrades

Upgrading VisualFlow overwrites any un-applied workflow drafts, and discards all un-applied changes.

If you have un-applied workflow changes in VisualFlow, we recommend that you apply them before upgrading so that you don't lose any work.

HA cluster recommendations for upgrades

If you are upgrading AFA on HA clusters, and also have FireFlow configured, we highly recommend that you upgrade FireFlow as well.

This is not required for DR clusters.

Service recommendations for upgrades

We recommend ensuring that the following services are running when you perform the upgrade:

- psql
- metro (apache-tomcat)
- mongod

If these services are not running, the upgrade process requests that you confirm whether you would like to continue. We recommend contacting AlgoSec customer support to start these services before continuing.

Upgrade your system

This topic describes how to use the ASMS automated system upgrade on single appliances, HA/DR clusters, and distributed systems.

Note: Before you start, review the upgrade prerequisites and ensure that your system complies. For more details, see Upgrade prerequisites.

Updated system requirements for A30.10

System optimizations in version A30.10 require additional CPU and memory specifications than were required in earlier systems.

If you are upgrading, we highly recommend increasing your system specifications to match the updated requirements as needed. Systems that remain with legacy minimum specifications may have unexpected results. For details, see System requirements and Re-enable the AlgoSec Reporting Tool after upgrading.

Note: If your system specifications are already larger than the updated CPU and memory requirements, your system specifications can stay as they are. In such cases, there is no need to resize your entire system.

Perform an automated ASMS upgrade

Automated ASMS upgrades are supported for standalone hardware or VM appliances, HA/DR clusters, and distributed systems.

Do the following:

1. Determine the builds that you need to upgrade, and download the relevant software packages from the AlgoSec portal. For details, see Download ASMS software packages.
2. Access your appliance as user: **root**

   Note: If you are working on clusters or distributed nodes, access the primary

node on the master / Central Manager appliance.

The upgrade is performed across all nodes in the entire system, starting with the Central Manager.

3. Copy the downloaded software packages to the following directory: **/root/AlgoSec_Upgrade/**
4. If you aren't already connected to the ASMS Administration interface (**algosec_conf**), connect now. For details, see Connect to the Administration Interface.
5. In the administration interface main menu, enter **8** to select **Upgrade software**.

   Note: The system checks your pre-requisites to verify that your system is ready for the upgrade. If any of the pre-requisite checks fail, relevant errors are displayed to notify you. In such cases, we recommend making changes so that your system complies, and then starting the upgrade process again.

   The system lists the available builds from the files you saved in step 4, and prompts you to select the build you want to install. For example:

   ```
   ************************************
   *** Software upgrade is starting ***
   ************************************
   Select an AlgoSec build to install:
   1. algosec-appliance-3000.0.0-529-el6.x86_64.run
   2. fa-3000.0.0-891.x86_64.run
   3. Run All
   ```

   Note: The option numbering may differ depending on your system configuration.

6. Do one of the following:

Run all installations together (recommended)	Select the option to **Run All.** **Note:** The option to **Run all** does not appear at all if you have more than one build per packaged saved. In this case, to run all installations together, first remove the earlier builds.
Run each installation separately	Enter the line number for the build you want to install. When each upgrade is complete, start the process again to run the next installation. If you do this, install the builds in the following order: a. **Appliance build** b. **AFA build** c. **FireFlow** d. **AppViz build**

The system displays details about the upgrade it is about to perform, and prompts you to approve.

For example:

```
The following AlgoSec packages are going to be upgraded:
* algosec-appliance-3000.0.0-529.noarch  TO
algosec-appliance-3000.0.0-529-el6.x86_64
* fa-3000.0.0-891.x86_64  TO  fa-3000.0.0-891.x86_64
********************
*** Upgrade plan ***
********************
Local node : 10.23.0.41
Remote Agent nodes: 10.23.0.40
Runtime Estimation: Up to 80 minutes
Review the upgrade plan detailed above. Approve plan? (y/n):
```

7. Enter **y** to confirm and start the upgrade. The upgrade starts.

If you are working on a distributed system, the upgrade first starts on the local node and then continues with the distributed nodes. The system displays confirmation details as the downloaded packages are copied to the distribution nodes and installed.

When the upgrade is complete, any clusters are resumed if relevant, and the following message appears:

```
*** Software upgrade finished successfully ***
```

8. In case of a kernel upgrade on an appliance build, the system also prompts you to reboot. Reboot your system as prompted.

   Warning: Not rebooting at this stage leaves you with a legacy kernel, which may present security issues.

Re-enable the AlgoSec Reporting Tool after upgrading

If you have upgraded to A30.10, but your system does not comply with the updated system requirements, the AlgoSec Reporting Tool (ART) is automatically disabled.

To enable ART again after updating your system specifications, do the following:

1. Log in to the AFA machine as user **root**.
2. Run: **/usr/share/fa/bin/toggle_art.sh on**

The system will verify that the specifications comply and then re-enable ART.

Troubleshoot your automated upgrade

If your automated upgrade fails for any reason, the system displays an error, as well as the location of specific log files. The central upgrade log file is located at: **/var/log/algosec-software-upgrade.log**

The system also prompts you with options to start the upgrade again.

If you have a distributed system and only some nodes failed, you can select the nodes you want to reinstall, or rerun the entire upgrade from scratch. Select the option that works best for you and run through the CLI process as prompted and described above.

For more details, see the AlgoPedia article at:
https://knowledge.algosec.com/skn/c6/AlgoPedia/e14320

General system maintenance

This section describes common maintenance procedures to perform on your ASMS system.

This section includes:

- Reboot the appliance
- Reset the appliance to factory defaults
- Migrate the Central Manager
- Relocate devices
- Contact AlgoSec technical support

Reboot the appliance

This procedure describes how to reboot your appliance, which is sometimes required as part of other maintenance and configuration procedures.

Note: Perform a graceful shutdown and restart of the ASMS services to prevent unexpected behavior. For details, see ASMS graceful shutdown and startup in AlgoPedia.

Do the following:

1. Connect to the ASMS Administration Interface. For details, see Connect to the Administration Interface.
2. Press **CTRL+C** to exit the menu.
3. Run the following command:

   reboot

If needed, Hardware Appliances can also be rebooted by pressing the power button on the front panel of the appliance for 10 seconds, and then pressing it again. We do not recommend this method as part of regular operation.

Reset the appliance to factory defaults

This procedure describes how to reset the appliance to factory defaults, and must be performed if you are reusing an appliance in a new role.

For example, you might do this if you appliance was previously used as a Central Manager, and you now want to use it as a Load Unit or Remote Agent.

Note: Resetting the appliance to factory defaults erases **all** of the information on the appliance, including configurations, user data, and so on, and returns it to its initial, out-of-the-box state.

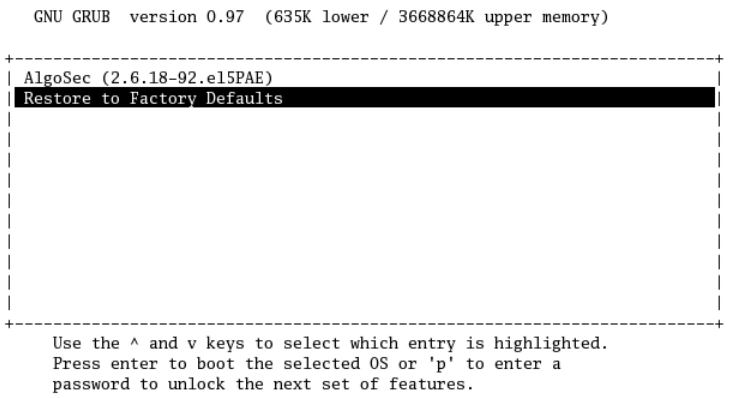
Do the following:

1. We recommend backing up your data before you reset the appliance.
2. Connect to the ASMS Administration Interface. For details, see Connect to the Administration Interface.
3. Run the following command:

   reboot

4. When the appliance reboots and a message appears, press **SPACE**. Do this within 5 seconds to prevent the appliance from fully rebooting.

   The appliance OS menu appears.



5. Use the arrow keys to select **Restore to Factory Defaults**, then press **ENTER**.

A warning message appears.

6. Enter **erase**.

   Another warning message appears.

7. Enter **YES**. Make sure you use capital letters.

   The system is formatted and re-installed, and all data is deleted. This process can take several minutes.

   At the end of the process, the system is automatically restarted.

8. Continue by configuring your machine again. For details, see Configure ASMS machines.

Migrate the Central Manager

This procedure describes how to migrate the ASMS Central Manager to another appliance, including a virtual appliance, AlgoSec hardware appliance, or an AWS/Azure instance. For example, you may want to do this while in the process of decommissioning end-of-life appliances or moving up to the cloud.

Note: Migration can be performed only from the Central Manager that is being migrated.

Additionally, if you are working with HA clusters, this procedure breaks those clusters. Rebuild them when the migration is complete.

Do the following:

1. Verify the system specifications on the source and target machines.

ASMS versions	Ensure that the ASMS version and build installed on both the source and target machines are identical.
License	Ensure that a valid ASMS license is installed on the target machine. For more details, see Install a license.
System requirements	Review the specifications on the target machine to ensure compliance. For more details, see System requirements. Additionally, verify how much storage is being used on the **/data** partition on the source machine. You must have at least the same amount of storage plus another 5% free on the target machine's **/data** partition.

2. Disable any monitoring or analysis processes any devices managed by the Central Manager. Migration may fail if there are devices currently being monitored or analyzed.
3. Connect to the Central Manager administration interface via SSH and log in as **root**.

   For details, see Connect to the Administration Interface.
4. In the main menu, enter **16** to migrate ASMS units.
5. Enter **1** to migrate a Central Manger.
6. Enter the IP address and root password of the target machine that will host the new Central Manager.
7. The migration tool runs prerequisite checks on the target machine configuration and ASMS versions. If all checks pass, confirm the details by entering **y**.

   The migration begins and displays a confirmation message when complete.
8. If you are migrating a system with HA/DR clusters, rebuild your broken clusters. For details, see Build a cluster.

After migration, the system is configured as follows:

Source machine	We recommend that you do not use the source machine after migrating without resetting it to factory settings. Therefore, all services on the source machine are disabled. For more details, see Reset the appliance to factory defaults.
Remote Agents	Remote Agents connected to the Central Manager will be automatically reconnected to the new Central Manager.

Relocate devices

This procedure describes how to relocate devices between nodes in distributed architectures, providing a full Remote Agent migration tool.

For example, you may want to do this while in the process of decommissioning end-of-life appliances or moving up to the cloud.

Relocation is performed in the background without system downtime, and supports the following options:

- From the **ASMS Central Manager** to **Remote Agents**.
- From **Remote Agents** to the **ASMS Central Manager**.
- Between different **Remote Agents**.

Relocating a device relocates all device-related data, including reports.

Do the following:

1. If you are relocating devices from a Central Manager to a Remote Agent, ensure that your devices are collected together in a device group in AFA. When relocating devices from a Central Manager, you must relocate a group, even if you are only relocating a single device.
2. Ensure that the ASMS version and build installed on both your source and target machines are identical.
3. Disable any monitoring or analysis processes for the devices you want to relocate. Relocation may fail for devices that are currently being monitored or analyzed.

4. Connect to the Central Manager administration interface via SSH and log in as **root**.

   For details, see Connect to the Administration Interface.

5. In the main menu, enter **16** to migrate ASMS units.
6. Enter **2** to relocate devices between nodes.
7. The detected nodes and their IPs are displayed. Select the following when prompted:
   - **The source node,** where the devices are currently located.

     When relocating from the Central Manager to a Remote Agent, you must also specify a device group to relocate.

   - **The target node,** where you want to move the devices.
8. Enter a time limit, in minutes, after which you want the relocation process to time-out if not completed.

   The default value is **0**, and leaves no time limit.

9. If prompted, determine whether you want to disable monitoring, scheduled analysis, and syslog messaging for all relocated devices.

   Tip: We recommend disabling these functions, especially when relocating devices to the Central Manager, to reduce CPU load on the Central Manager machine. For more details, see Default configurations for relocated devices.

10. Press **ENTER** to start the relocation process. Relocation is performed in the background and the log file location is displayed.

    Just before the relocation is complete, the system checks the connectivity to the new device. If the check passes, the relocation processes is completed. If the connectivity check fails, the devices remain on the source node.

> **Note:** If you have relocated management devices and their children, AFA runs an automatic connectivity check on the management device only. For any child, managed devices, manually verify that connectivity is active between ASMS and the device.
>
> If connectivity is down, edit the device configuration in the AFA **Administration** area.

11. After relocation is complete, edit the device configuration if needed, such as to reconfigure a syslog server or rescheduling analysis, in the AFA **Administration** area. For details, see Default configurations for relocated devices .

Default configurations for relocated devices

Relocation configures the system as follows, depending on the relocation you have performed:

From the ASMS Central Manager to Remote Agents	Monitoring, scheduled analysis, and syslog messaging is enabled for all relocated devices.
From Remote Agents to the ASMS Central Manager	Relocated devices are added to a single group on the Central Manager. This group is named after the source Remote Agent, enabling you to relocate the devices again as needed. **Note:** If you are relocating management devices, such as a Palo Alto Panorama or Juniper Space Security Director, this group includes only the management device names, although both management and managed devices are relocated as configured. Monitoring, scheduled analysis, and syslog messages is disabled for all relocated devices to reduce load on the Central Manager.*
Between different Remote Agents	Monitoring, scheduled analysis, and syslog message is kept unchanged for each relocated device.*

Local syslog configuration	When relocating devices that use a local syslog server, this configuration is also automatically relocated to the target node. No changes are made for external syslog servers.

Re-enable monitoring, scheduled analysis, and syslog messaging

If monitoring, scheduled analysis, and syslog messages are disabled on your device after relocating, use the **enableDevices** and **enableDevicesOnRemoteAgent** APIs to re-enable these again.

Relocate specific devices

If you want to relocate specific devices together, do so by creating a group and then relocating that group via API.

For example, you may want to do this if you have two Remote Agents, each with their own devices.

If the first Remote Agent is being disabled temporarily for maintenance purposes, group its devices to retain the membership details. Then use the **relocation** API call to relocate that group to the second Remote Agent. When the maintenance is complete, relocate that same group back again to the first Remote Agent.

When creating this group, verify the following:

- Verify that you include only devices that are managed by this same Remote Agent
- Verify that you include any management devices required, such as Palo Alto Panorama or Juniper Space Security Director devices.

  All devices managed by these parent devices are relocated together with their management devices, and do not need to be included in the group.
- Verify that all devices included in the group are accessible from the target machine.

Use the **relocation** REST API call and the **treeNames** parameter to define the name of the group you want to relocate.

Check Point devices with OPSEC certificates

OPSEC certificates for Check Point devices are generated per IP. Therefore, while most relocations of Check Point devices to new Remote Agents should succeed, you may have unexpected issues. In such cases, regenerate the certificate and re-install the certificate on the device.

Check or cancel relocation process

To check relocation progress or to cancel relocation, note the UUID displayed in the CLI, and use one of the following REST API requests:

- **GET device-relocation-controller**
- **DELETE device-relocation-controller**

For each of these API requests, use the UUID as the value for the **uuid** parameter.

Tip: We recommend using the ASMS Swagger API documentation to perform these API requests.

Use case scenario: Migrating an entire ASMS system

The following procedure describes a sample process for migrating your entire ASMS system to new appliances.

For example, you may want to do this if you are moving your data centers to a new location or to the cloud, moving to a new set of upgraded appliances, or if you're adding additional appliances to your system.

Tip: Migrating an entire ASMS system is a complicated process. If you are migrating a complex deployment with Remote Agents across geographic locations, consider

that the migration may required a few days.

In such cases, consider performing each Remote Agent migration and device relocation in incremental steps.

Do the following:

Step	Procedures
1. **Start by migrating your Central Manager**. Run through the entire migration and verify that everything works as expected when done.	For details, see: • Migrate the Central Manager • Basic sanity checks
2. **Migrate Load Units** by removing the existing units and adding new ones.	For details, see: • Add or edit Load Units • Delete Load Units or Remote Agents
3. **Relocate devices as needed** from legacy Remote Agents to new Remote Agents. When you're done, remote the legacy Remote Agents from your system.	For details, see: • Relocate devices • Delete Load Units or Remote Agents
4. **Run sanity checks again** to ensure that ASMS is running again as expected.	For details, see Basic sanity checks.

Contact AlgoSec technical support

This procedure describes how to contact AlgoSec support, and the files the send with your support case.

Do the following:

1. Access the Support Home page on the AlgoSec portal.
2. Click  **Submit a Support Case**.
3. Complete the fields and submit the ticket. Make sure to attach any relevant logs to your case.

   Create support logs from ASMS as follows:

   Create AFA support logs

   Do the following:

   a. In AFA, click your username at the top-right, and select **Support**.

   b. (Optional) In the **Support** dialog, enable **Debug mode** if needed, and then reproduce the issue so that the details are logged. In this case, return to the **Support** dialog again when you're done.

   c. Select either **General support file**, or the specific item you want to include in your log file.

      If you select any option other than the **General support file**, define the devices you want to generate the log file for. To add a device to the list, start entering a device name in the text box at the bottom of the dialog, and then select the device from the dropdown list displayed.

   d. Click **Generate Files**.

   e. Scroll down further to the table of support files. Click the **Details** link in the **File Path** column to access the support file you created.

   Create FireFlow support logs

Do the following:

a. In FireFlow, click your username at the top-right, and select **Support**.

b. (Optional) In the **Support** dialog, enable **Debug mode** if needed, and then reproduce the issue so that the details are logged. In this case, return to the **Support** dialog again when you're done.

c. Click the **Download General Support Zip** link to download the file.

Create a general support log file via CLI

If your UI is unavailable, generate a general support log file via CLI.

Access the **algosec_conf** CLI menu, and enter **18** to collect log files. These will be general system logs and include data for the entire system, and not per device. For more details, see Connect to the Administration Interface.

HA support logs

Create HA support logs, if the case relates to high availability issues. For more details, see Collect cluster logs for AlgoSec technical support.

➔ See also:

- Backup and restore
- ASMS licensing

Backup and restore

The AlgoSec Security Management Suite enables you to back up and restore the entire ASMS environment as needed.

This topic describes how to start a backup or restore process from FireFlow or AppViz. The actual backup and restore is handled by AlgoSec Firewall Analyzer. Starting from FireFlow or AppViz switches you to AFA to complete the process.

Backup and restore prerequisites

Note the following before starting your backup or restore procedure:

User roles	You must be an administrator to perform the backup or restore.
Version	You can only restore ASMS to the same major version from which the backup was taken. If you have upgrades to perform, upgrade your system only before the backup or after the restore. Do not attempt to upgrade your system between backup and restore processes.
System processes	Restoring your system requires some downtime. Disable any jobs scheduled to run during the restore process, such as ASMS monitoring or analysis. Reinstate the scheduling once the restore is complete.
System requirements	We recommend always restoring to an appliance with the same number of cores as the appliance from which the backup was taken.

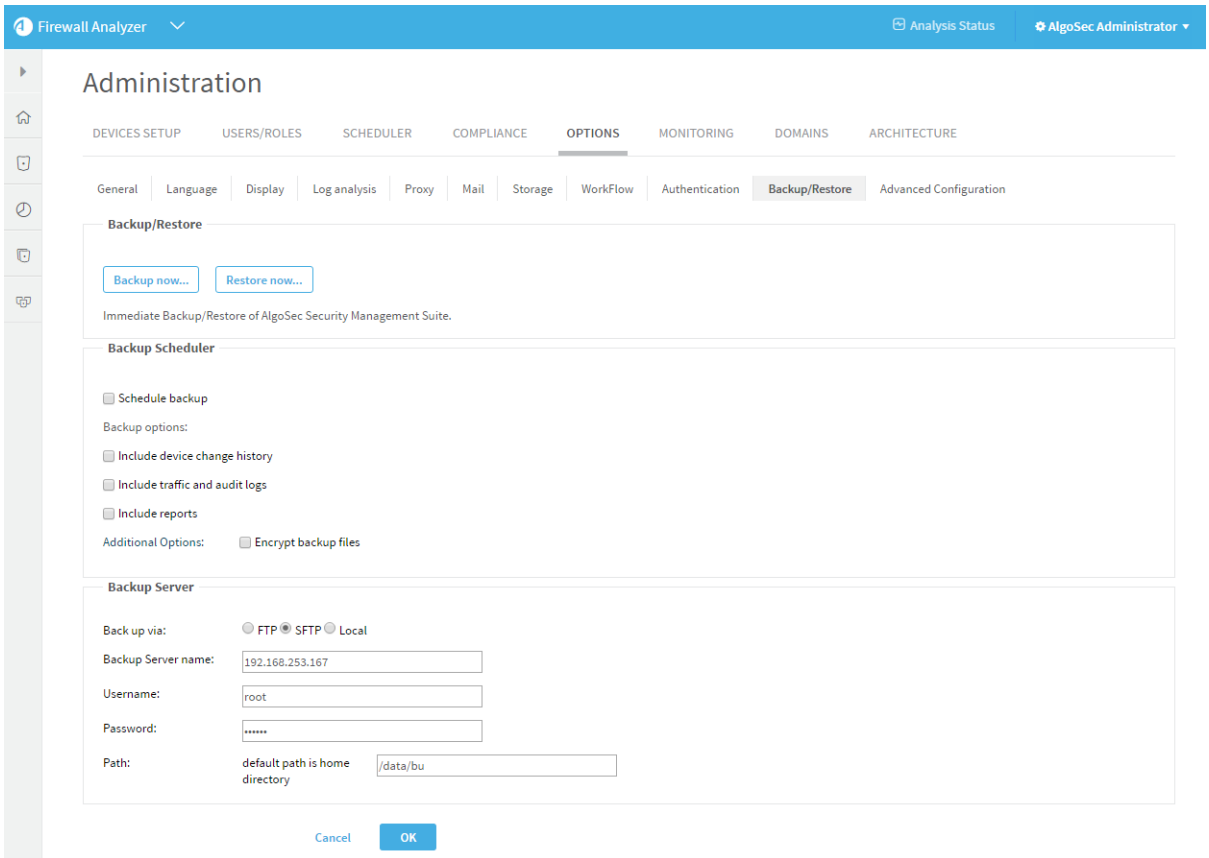
Access backup and restore from FireFlow or AppViz

Do one of the following:

FireFlow	In FireFlow, in the main menu on the left, click **Advanced Configuration**. Then, click the **Backup and Restore** tab on the right.

AppViz	In AppViz, click your username and select **Administration** from the drop-down menu. On the **Administration** page, 1. In the toolbar, click your username. From the drop-down, select **Administration**. 2. In the Administration page's **Backup and Restore** area, click **Manage Settings**.

The AFA**Backup/Restore** page appears.



Complete the fields as needed.

Note: After performing a restore, you must run a report on 'All Firewalls' to ensure a valid network map.

ASMS licensing

This topic describes how to obtain and install ASMS licenses, as well as track license usage across your devices.

AlgoSec licenses control the AFA modules available, whether FireFlow, AppViz, or AutoDiscovery are available, the number of routers supported, and more.

This section includes:

- Obtain a license
- Online license requirements
- Install a license
- License usage
- Update licenses

AlgoSec Licensing: Watch to learn about the ASMS license types available.

Obtain a license

Do the following to obtain a new license key:

1. Log in to http://portal.algosec.com using your username and password.
2. At the top of the screen, click Request License Key.
3. Populate the request form as follows:

Field	Description
Product/s	Select the product you want a license for. If you want a license for multiple products, select AlgoSec Suite. **Note:** To use AutoDiscovery, your license must also include AutoDiscovery support.

Field	Description
Internet Connection	Select whether your AFA server can connect to the internet while activating the license. For details, see Online license requirements.
AlgoSec Server MAC Address	Enter the MAC address of your AFA server. To find the MAC address, do the following: a. Browse to **https://<AFA_server>/algosec/**, where **<AFA_server>** is the AFA server URL. b. Click **AlgoSec Appliance Status**. **Note:** If your AFA server has multiple interfaces, make sure to submit the MAC address of the **eth0** interface. For details about native Linux installations, see Deploy or upgrade a standalone native Linux server in AlgoPedia.
License Key For	Select your customer status.
Number of Firewalls	Enter the number of firewalls you want to manage with AFA
Comments	Enter any additional comments required. • If you need an offline license, enter: **Please provide an offline license** • If the license will be used for a prospect, name the account

4. Click **Submit**.

   Your license is sent to the email address you used to log in to the AlgoSec portal.

   Save it to a location accessible by the AFA server.

Online license requirements

AlgoSec provides online licenses, which are inactivated to start.

To activate your license, ensure that the AFA server can access the AlgoSec licensing server, including the following:

Internet connection	The AFA server must be connected to the internet. If your AFA server cannot connect to the internet for the duration of the license activation, request a pre-activated, offline license from AlgoSec. For details, see Obtain a license. **Note:** Offline licenses may take several days to issue.
Proxies	If your browser settings use a proxy, you must also configure AFA to use the proxy.
HTTPS traffic	Your connection must allow **HTTPS** traffic (**TCP/443**) from your AlgoSec server to www.algosec.com. Outbound web proxies must not manipulate or sanitize traffic.

No data about the configuration of analyzed devices is passed back to AlgoSec over the internet or to any third party.

Install a license

This procedure describes how to install a license. For details about obtaining your license, see Obtain a license.

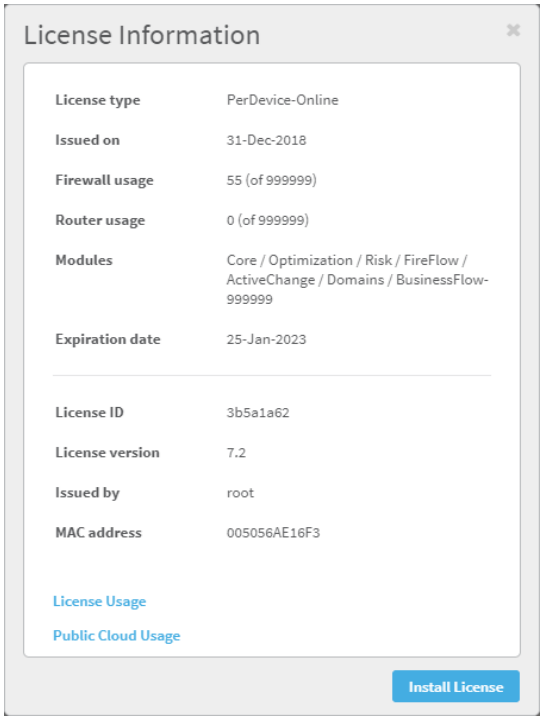
If you have just defined your first administrator user directly in AFA, click **Install License** in the **Firewall Analyzer** window.

In all other cases, do the following:

1. In AlgoSec Firewall Analyzer or AppViz, click your username at the top right, and select **License**.

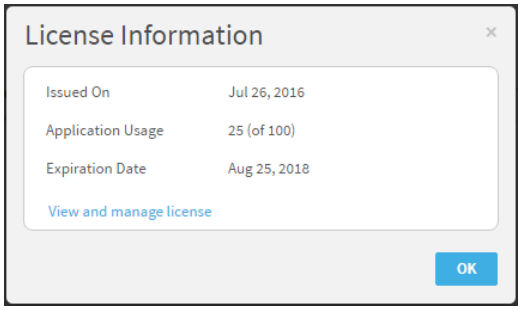
   From AlgoSec Firewall Analyzer

   If you are in AlgoSec Firewall Analyzer, the **License Information** dialog appears. For example:



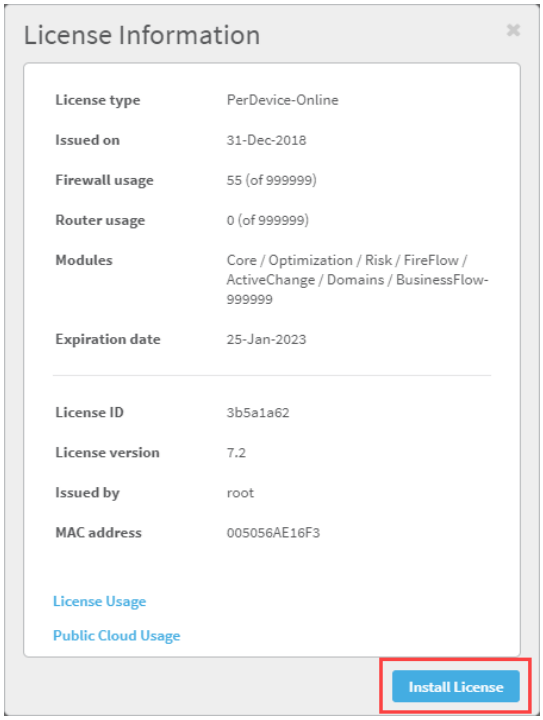
From AppViz

If you are in AppViz, the **License Information** dialog is displayed as follows:

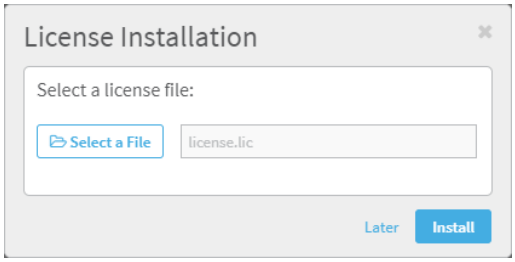


From there, click **View and manage license** to jump to the **License Information** dialog in AlgoSec Firewall Analyzer.

2. In the AlgoSec Firewall Analyzer**License Information** dialog, click **Install License**.



3. Accept the **End-User License Agreement** that appears.
4. In the **License Installation** dialog, click **Select a File**. Then, browse to and select the license file (**license.lic**) you received by email. For example:



5. Click **Install**.
6. Log out of AFA, and then log in again.

HA/DR clusters

If you are running AFA on an HA/DR cluster, you must first break the cluster, and then apply a license file to each node. Rebuild the cluster when you're done. For details, see Break a cluster and Build a cluster.

Do the following:

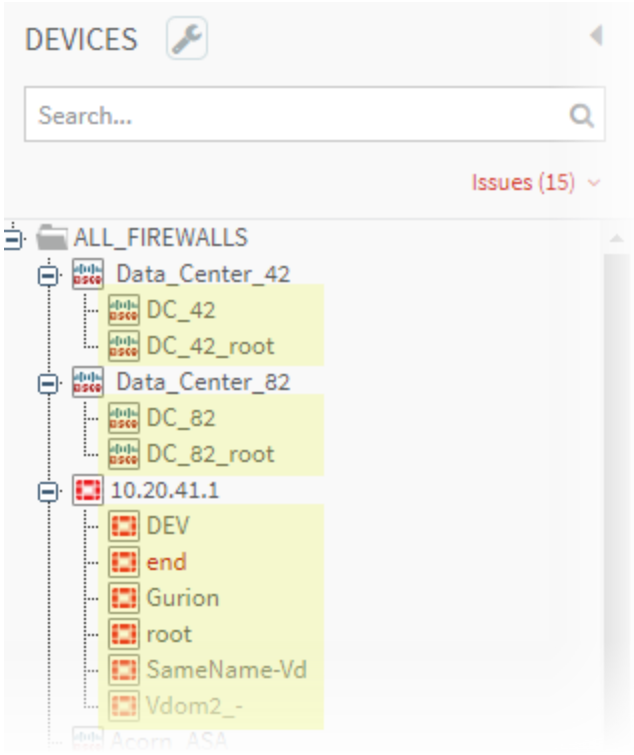
1. On the secondary appliance, open a terminal and login as user: **root**
2. Connect to the ASMS Administration interface. For details, see Connect to the Administration Interface.
3. Enter **12**.
4. When prompted, enter the path to the license file (**license.lic**) you received by email.

   The license is installed.

License usage

An ASMS license is used for every on-premises or private cloud device shown at the lowest level of the device tree.

For example, the highlighted devices in the following image each consume a single license.



Note: Some exceptions exist. For details, see AlgoPedia.

Virtual router licensing

- In LSYS/VSYS systems, licenses are consumed at the LSYS/VSYS level instead of the virtual router (VR level). This means that using multiple VRs in a single VSYS consumes only one license.
- During upgrades, any licenses consumed by VRs are not calculated towards total consumption.

Public cloud licensing

While public cloud assets (AWS and Azure) do not consume licenses, ASMS does track your public cloud asset usage.

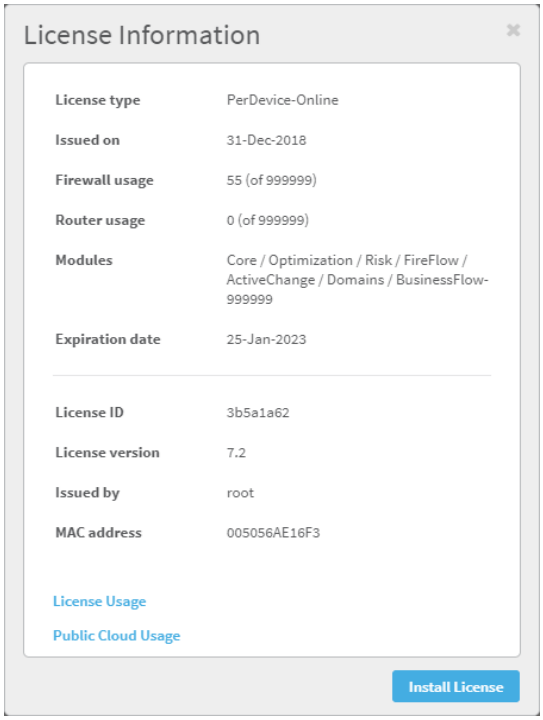
When you renew licenses, AlgoSec sales personnel will check your cloud usage and sell you enough licenses for the number of assets actually in use.

View license usage statistics

Do the following:

1. In AlgoSec Firewall Analyzer, click your username at the top right, and select **License**.

   The **License Information** window appears. For example:



2. Click the links at the bottom of the dialog to download license usage spreadsheets:

License Usage	Licenses consumed by all on-premises devices. **Tip:** Scroll to the bottom of the report to view a list of deleted devices. Sample on-premises and private cloud license usage report
Public Cloud Usage	Cloud asset details, including the following: • Number of cloud assets managed by ASMS, sampled hourly • Top monthly average count, per year. Sample public cloud license usage report

Note: License usage spreadsheets are protected against modifications.

Tip: If you are having issues where different locations in your system are showing

different numbers of devices and licenses used, reload your license and check again. This updates the data for any devices that had been deleted or modified and clarifies the statistics.

Sample on-premises and private cloud license usage report

The following table shows a shortened sample license usage report. While we've removed some rows, we've left the full total counts complete.

License Type	**Total**						
Topology Infrastructure Devices	1						
Virtual Firewall	33						
Stand-Alone Firewall	16						
Total	**50**						
Active Devices							
License Type	**Brand**	**Display Name**	**Tree Name**	**Device IP**	**Parent Name**	**Last Completed Report**	**Device License ID**
Stand-Alone Firewall	Check Point	Clover	Clover	172.31.10.125	N/A	afa-10451	Clover
Stand-Alone Firewall	Check Point	Rose_ checkpoint	Rose_ checkpoint	10.82.18.20	m_10_ 20_12_1	afa-193	192.168.6.254
…							
Topology Infrastructure Devices	Cisco router	10.20.15.1	10_20_15_1	10.90.15.5	N/A	afa-159	10_20_15_1
Virtual Firewall	Cisco ASA	10.20.245.1_ admin	admin	10.20.245.1	10_20_ 245_1	afa-557	admin
Virtual Firewall	Fortinet FortiManager	Violet_Fortinet	Violet_Fortinet	10.82.18.20	N/A	afa-531	192.168.6.254
…							
Deleted Devices							
License Type	Brand	Display Name	Tree Name	Device Ip	Parent Name	Last Completed Report	Device License ID
Virtual Firewall	Juniper - Junos Space Security Director	Event-Horizon_ APEX	Event_Horizon_ APEX	198.1.1.1	N/A	afa-154	Event_Horizon_ APEX
Virtual Firewall	Juniper - Junos Space Security Director	Event-Horizon_ ARO_SMT	Event_Horizon_ ARO_SMT	192.168.101.254	N/A	afa-155	Event_Horizon_ ARO_SMT
…							

Sample public cloud license usage report

Summary - Top monthly average				
Year	**Top Month**	**Month avg. AWS_ Assets**	**Month avg. Azure_ Assets**	**Month avg. total**
2019	May	635	42	677
Report produced on:	**30-May-2019**			
Breakdown				
Date	**Hour**	**AWS_Assets**	**Azure_Assets**	**Total**
27-May-19	11	570	0	570
27-May-19	12	570	0	570
27-May-19	13	570	0	570
27-May-19	14	570	0	570

Update licenses

Contact AlgoSec to update your licenses in the following scenarios:

Expired licenses	When there are less than 45 days remaining on your license, the **License** link in the Administration menu turns red. To ensure continuous use, make sure to update your license before it expires.
Exceeded licenses	Your license is valid for a specific number of devices or reports. Update your license if you require additional devices or reports. **See also**: Public cloud licensing
ASMS product upgrades	To upgrade your AlgoSec solution with additional modules or components, you must also update your license.

Logins and other basics

This topic describes the very basics of working with ASMS, such as logging in and out and supported browsers.

Supported browsers

View ASMS in one the following web browsers, at screen resolution of **1920x1080** or above.

- **Mozilla Firefox**
- **Google Chrome**
- **Microsoft Edge**
- **Internet Explorer 11** and higher. Internet Explorer 8.0 is supported for FireFlow requestors only.

Log in to ASMS

Log in to ASMS from any desktop computer using the credentials provided by an AFA administrator.

Do the following:

1. In your browser, navigate to **https://<algosec_server>** where **<algosec_server>** is the ASMS server IP address or DNS name.

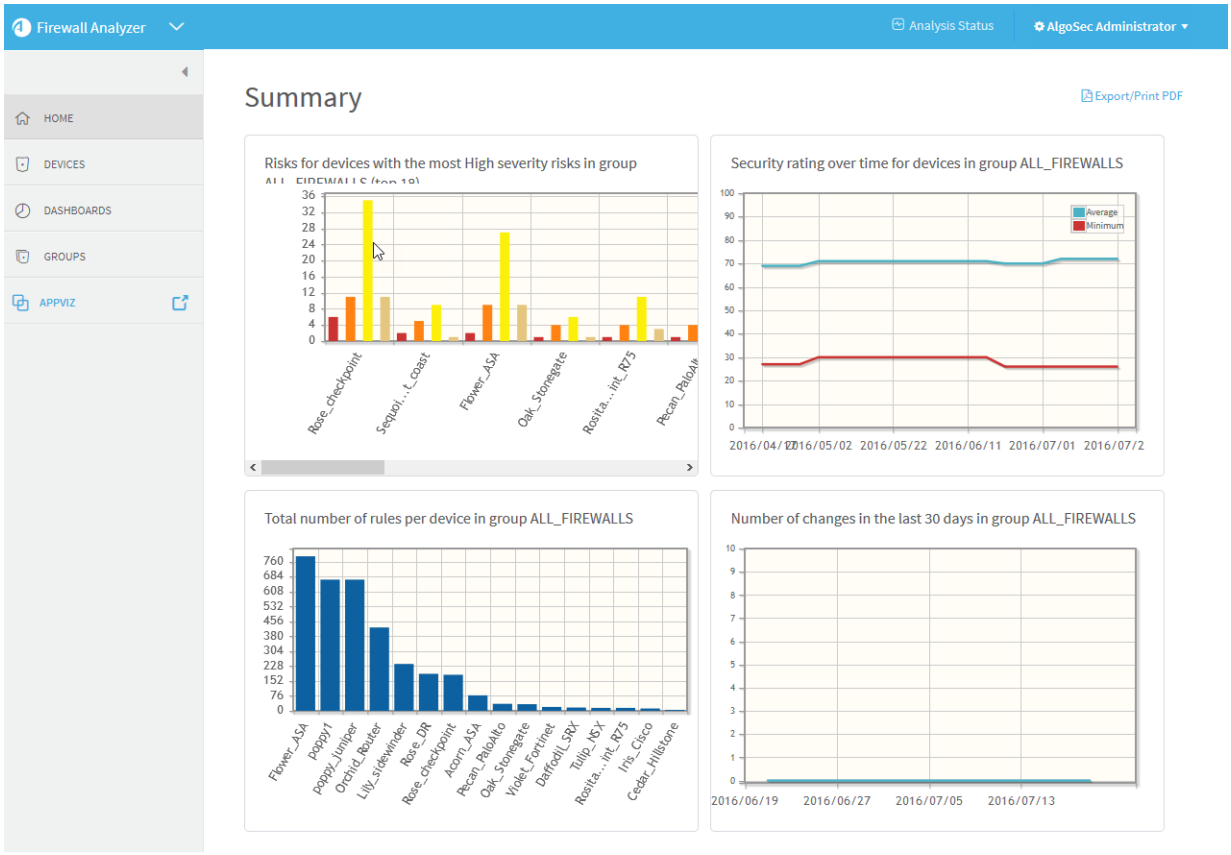
   If a warning message about the web server's certificate appears, click **Accept** or **OK**. For more details, contact your network administrator.

   The **Security Management Suite** login page appears.

2. In the **Username** and **Password** fields, enter your username and password, and click **Login**.

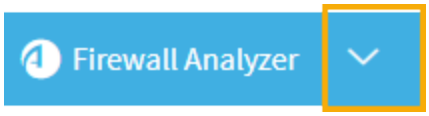
You are logged in, and ASMS displays AFA by default.

For example:

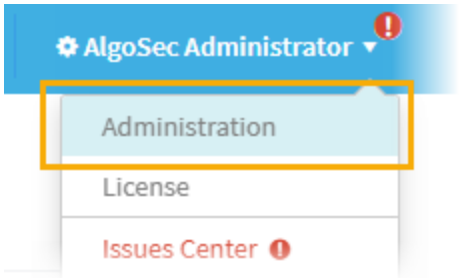


Switch ASMS products

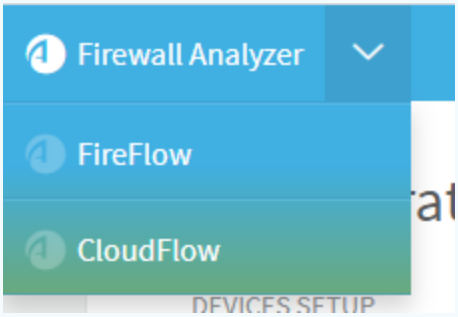
If you are a user in multiple ASMS products, such as AFA, FireFlow, and AppViz, switch between products using the dropdown at the top-left, above the main menu.



If you are an administrator for any of these products, the relevant administration menu is available from your user dropdown at the top-right:



Note: CloudFlow is now accessible from inside ASMS. Click the dropdown at the top-left and select **CloudFlow**.



For more details, see our CloudFlow Help Center.

Adjust your screen space

To adjust the screen space available for your main workspace, hide, display, or change the size of the main menu on the left.

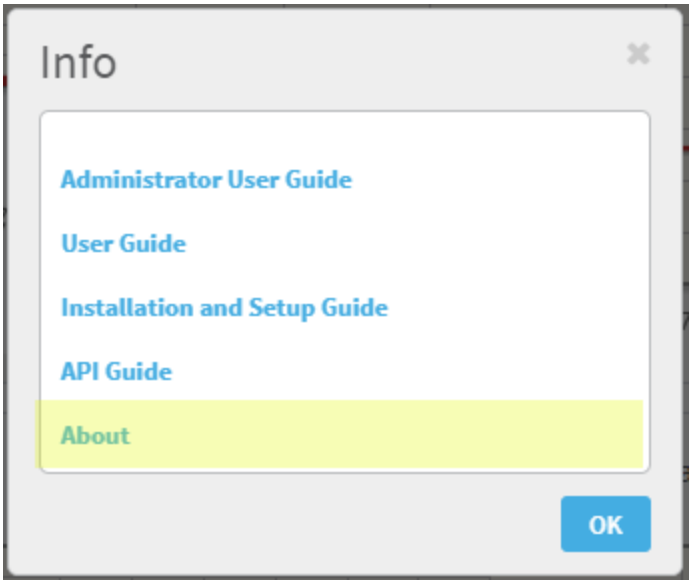
- **To adjust the size of the main menu**, hover between the menu and the workspace and drag the border left or right.
- **To collapse the menu entirely**, click at the top. When collapsed, click to expand it again.

View ASMS product details

This procedure describes how you can identify your AFA, FireFlow, or AppViz installation version and build number.

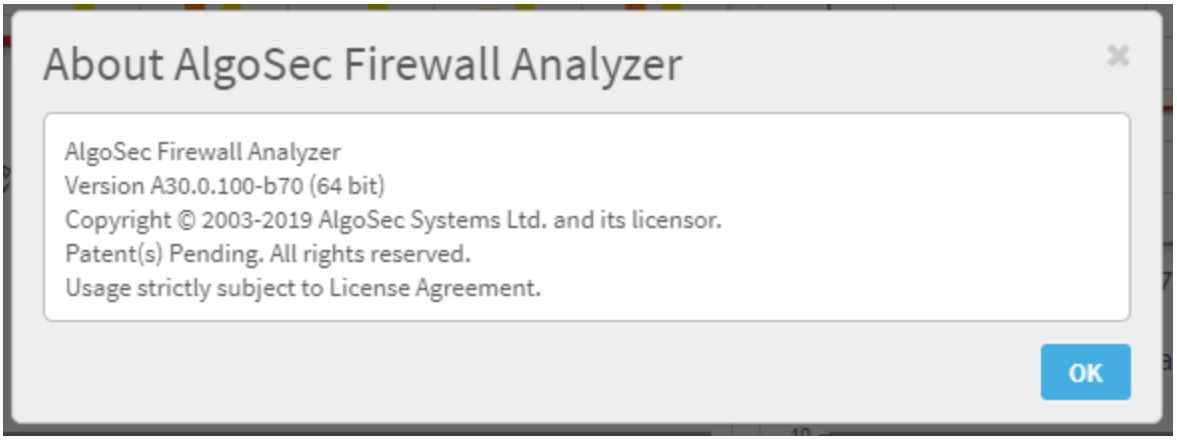
Do the following:

1. In the toolbar, click your username and then select **About** or **Info**.
2. For example, if you're in AFA, in the **Info** dialog, click **About**.



The **About** dialog appears, showing details about the product you have installed.

For example:



Note: If you are running the FIPS 140-2 compliant version of AFA, this information is indicated in the window.

Log out of ASMS

Log out of ASMS by clicking your username at the top right, and selecting **Logout**.

You are logged out of all ASMS products available to you.

Note: If Single Sign On is configured, you must browse to the **Logout** page hosted on your IdP to log out.

For more details, see the *AlgoSec Firewall Analyzer Administrator Guide*.

Send us feedback

Let us know how we can improve your experience with the Installation and Setup Guide.

Email us at: techdocs@algosec.com

Note: For more details not included in this guide, see the online ASMS Tech Docs.