



AlgoSec AutoDiscovery

Software Version: A30.10

User Guide

View our most recent updates in our online [ASMS Tech Docs](#).

Document Release Date: 5 April, 2020 | **Software Release Date:** April 2020

Legal Notices

Copyright © 2003-2020 AlgoSec Systems Ltd. All rights reserved.

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

AutoDiscovery	5
AutoDiscovery business service types	5
Get started with AutoDiscovery	5
Log in to AutoDiscovery	7
Define sensors and subnets	10
Define an AutoDiscovery sensor	10
Configure an AutoDiscovery subnet	11
Install AutoDiscovery	13
AutoDiscovery server architecture	13
Deploy the AutoDiscovery server	14
AutoDiscovery system requirements	15
AutoDiscovery required ports	17
Traffic collection options	17
Install AutoDiscovery sensors	20
Sensor installation options	20
AutoDiscovery sensor system requirements	21
Install additional AutoDiscovery sensors	21
AutoDiscovery sensor system requirements	25
Discover map-based services	28
Discover from detected business services	28
Discover services by server and port	31
Discover services from a query	32
Discover query-based services	34
Perform a query	34
Manage business services	37
View business services	37
View the network topology map	37
Filter business services	39
Add connections manually	44
Resolve DNS names	47

Edit business service properties	48
AutoDiscovery baseline map	49
Save the current map as the baseline	50
Compare the current map to the baseline	51
Remove servers from the baseline	51
Resolve DNS names in the baseline	52
Export AutoDiscovery data	53
Defining the AutoDiscovery Server	53
Exporting a CSV File	53
Configure AutoDiscovery	54
Manage AutoDiscovery users	54
Manage AutoDiscovery user roles	55
Configure AutoDiscovery parameters	57
AutoDiscovery parameter reference	57
Troubleshoot AutoDiscovery	62
Send us feedback	63

AutoDiscovery

AlgoSecAutoDiscovery enables you to detect business service traffic from across your network and import them as business service flows into AppViz. AppViz organizes the business needs associated with specific traffic flows as business applications.

AutoDiscovery business service types

AutoDiscovery both collects user traffic logs from across your network, and maps the collected traffic to business services.

AutoDiscovery business services are organized into the following types:

Map-based business services	Map-based business services start with a server and port. Traffic data from AutoDiscovery sensors provides data for all URLs and clients communicating with the server.
Query-based business services	Query-based business services start with the query on a server, or a server and port. Queries discover the server's connection at a specific instance. These services are a snapshot of the service at the time it is created, and are not updated.

Note: Web-based business services (which start with a URL as the entry point) have been deprecated. Previously defined web-based business services continue to function, but new ones cannot be discovered.

Get started with AutoDiscovery

This procedure provides steps for setting up an AutoDiscovery system for the first time after installing the AutoDiscovery server and sensors.

Note: AutoDiscovery is installed separately from ASMS. For details, see [Install AutoDiscovery](#).

Do the following:

1. Log in to AutoDiscovery. For details, see [Log in to AutoDiscovery](#).
2. Define the AutoDiscovery sensors and subnets to manage the traffic detected by AutoDiscovery.

For details, see [Define sensors and subnets](#).

Tip: Depending on your system configuration, you may want to install additional sensors instead of only using the default sensor installed with the AutoDiscovery server. If you install additional sensors, make sure to define them in AutoDiscovery before you continue.

For more details, see [Install AutoDiscovery sensors](#).

3. Verify that NetFlow traffic flows successfully to the AutoDiscovery server via the sensor you defined.

Configure NetFlow traffic flow to your sensor

Configure your NetFlow export device, such as VmWare or Cisco Nexux, to send NetFlow packets to the AutoDiscovery sensor IP address, on port 2055.

The following table lists the data that must be, or is recommended to be, included by the exporter in the NetFlow packets:

Required	<ul style="list-style-type: none">• Source VLAN• NetFlow Version• IPv4 Protocol• IPv4 Source address• IPv4 Destination address• Source port• Destination port
-----------------	---

Recommended	<ul style="list-style-type: none">• Counter bytes• Counter packets• TCP flags
--------------------	---

4. Create an AutoDiscovery business service to collect your traffic.

For details, see:

- [Discover map-based services](#)
- [Discover query-based services](#)

5. Switch to AppViz. Connect your AutoDiscovery server to AppViz and start importing your application flows into AppViz.

For more details, see:

- [Manage business services](#)
- [Export AutoDiscovery data](#)
- [Configure AutoDiscovery](#)
- [Troubleshoot AutoDiscovery](#)

Log in to AutoDiscovery

This procedure describes how to log in to AutoDiscovery.

Note: Before connecting to an AFA machine, ensure that you have the most recent version of AutoDiscovery installed, and your AFA machine is loaded with a license that also supports AutoDiscovery.

For more details, see [Install AutoDiscovery](#).

Do the following:

1. Navigate to **https://[AutoDiscoveryServerIP]:9443**.

A login page appears, similar to the ASMS login page.

2. Log in with your AutoDiscovery username and password.

Note: AutoDiscovery credentials may be different than your ASMS credentials.
The default credentials are **administrator / admin**.

The **Welcome to AlgoSecAutoDiscovery** page appears.

3. Click the **AlgoSecAutoDiscovery Web Console** link.

First time logging in to AutoDiscovery

The first time that you log in to AutoDiscovery, you are prompted to connect to an AFA server, with the **afa** user pre-defined. For example:

Connect to AlgoSec Firewall Analyzer

Enter the following details to connect to Firewall Analyzer

AlgoSec Firewall Analyzer host

Linux user used to install AFA

This password is used once to connect AutoDiscovery to Firewall Analyzer

Linux user

Linux password

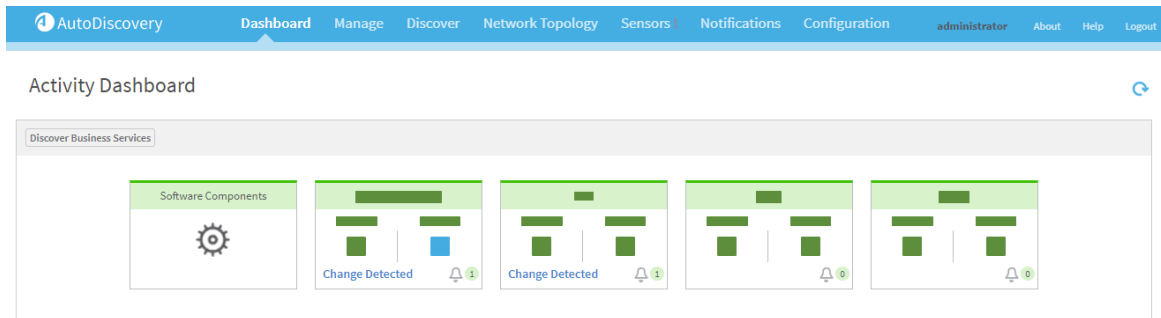
Linux user password

Cancel Login

Enter the following details, and click **Login**.

AlgoSec Firewall Analyzer host	The hostname or IP address of your AFA server.
Linux password	Enter afa , which is the Linux password used to connect AutoDiscovery to AFA.

You are logged in and the **Activity Dashboard** appears. For example:



Note: To log out, click **Logout** at the top-right of the AutoDiscovery screen.

Define sensors and subnets

This topic describes how to configure AutoDiscovery sensors and subnets, which define which traffic is collected from your network.

Define an AutoDiscovery sensor

This procedure describes how to define an AutoDiscovery sensor to discover your traffic.

Note: We recommend using the default sensor installed together with the AutoDiscovery server. Depending on your system configuration, you may need additional sensors. For more details, see [Install AutoDiscovery](#).

Do the following:

1. In AutoDiscovery, click the **Sensors** tab, and click **New**.
2. In the **Define new sensor** dialog, define your sensor as follows:

Host Name	Enter the sensor host name or IP address.
Sensor Name	Enter a display name for your sensor.
Network Sensor Port	If you are using a port other than the default port configured, enter the port number. The default port is 9545 .
Use SSL	Select to enable SSL-encrypted communication between the AutoDiscovery server and sensor. Note: This is relevant only if you have additional sensors installed separately. If selected, you must additionally configure SSL-encrypted communication on the sensor.

3. (Optional): Enable **Sampling Mode** for your sensor.

This configures your sensor to capture only a sample of the traffic detected and can reduce pressure on the sensor.

Note: Enabling Sampling Mode also disables SSL Certificate collection, IP flow collection, and may affect the detection of HTTP titles.

Do the following:

- a. Open the `/opt/autodiscovery/networksensor/NetworkSensor.cfg` sensor configuration file.
- b. In the `NetworkSensor.cfg` file, locate the `capture_sampling_rate` parameter.
Define the value as `<x>`, where the sensor analyzes 1 out of every `<x>` packets.

Configure an AutoDiscovery subnet

Configure an AutoDiscovery subnet to ignore irrelevant endpoints/traffic and enable your system to focus on relevant data only.

By default, sensors only discover traffic that resides in the common internal networks, such as `192.168.x.x`.

Note: Each time a new local network sensor is defined, the subnet that it belongs to is added to the list of subnets.

In this case, the subnet name will include the location (IP address) of the network sensor.

Do the following:

1. In AutoDiscovery, select the **Configuration > Subnet Management > Subnets**.
2. On the **Subnets** page, do one of the following:

Add a new subnet	Click New . In the Create or Edit Subnet dialog, enter the subnet values as needed.
Edit or delete an existing subnet	Click Edit or Delete in the row of the relevant subnet.
Delete multiple subnets	Select the subnets you want to delete and click Delete .

Subnet fields include the following:

Name	Enter the subnet name.
Subnet (CIDR)	Enter the subnet mask in CIDR format.
Inspect Traffic	<p>Select to enable traffic inspection. This includes HTTP transaction (URL) discovery and DNS resolution for servers in the subnet. Clear this option to disable traffic inspection.</p> <p>Note: This option is only relevant when editing a subnet, not adding a new one.</p>
Group	(Optional) Select a group for the subnet in the drop-down menu.

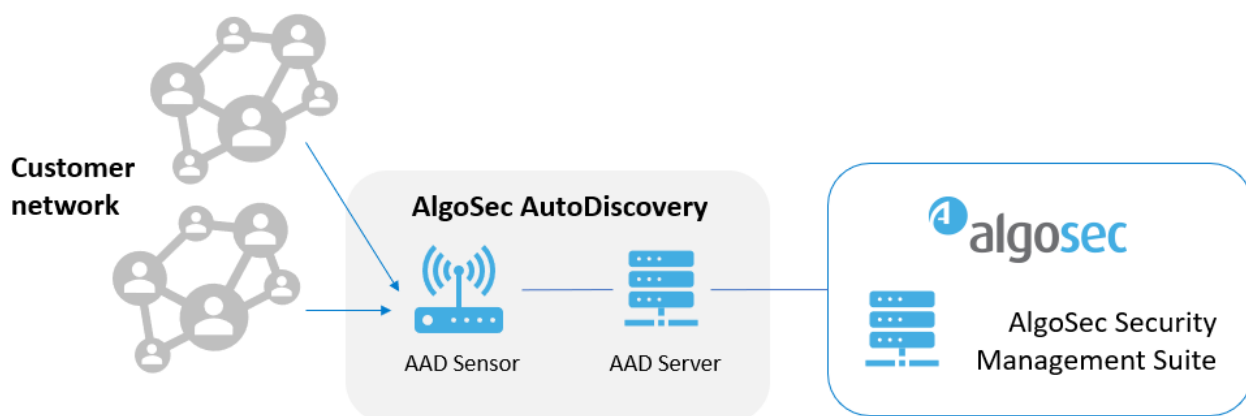
Install AutoDiscovery

AutoDiscovery is an additional ASMS component, layered over AppViz, which enables you to discover business service flows directly from your network and import them into AppViz.

AutoDiscovery is managed, licensed, and installed separately from ASMS. To use AutoDiscovery, ensure that your ASMS license includes support for AutoDiscovery.

AutoDiscovery server architecture

The following image shows how the AutoDiscovery sensor captures network traffic between computers across the network and sends traffic data to the AutoDiscovery server.



- **The AutoDiscovery sensor** collects traffic from your network, including statistical data using NetFlow/SFlow methods, simulated/mirrored packets, or direct traffic. For more details, see [Traffic collection options](#).
- **The AutoDiscovery server** creates business service maps, hosts the AutoDiscovery web client, and communicates with ASMS.

Note: Each AutoDiscovery installation provides a server and a single sensor, which usually supports statistical data collection or simulated/mirrored packet collection.

To collect traffic directly, you may need to deploy additional sensors throughout your network. For more details, see [Install AutoDiscovery sensors](#).

Deploy the AutoDiscovery server

The AutoDiscovery server is available as a CentOS-based virtual appliance in OVF format. This procedure describes how a system administrator can deploy a AutoDiscovery server.

The server installation provides an Apache Tomcat server, a PostgreSQL database, and a single sensor.

Do the following:

1. Verify that your AutoDiscovery machine complies with the system requirements. For details, see [AutoDiscovery system requirements](#).

Note: Your AutoDiscovery machine is a separate machine from your main ASMS or AFA machine, and has different specifications and requirements.

2. On the AlgoSec portal, navigate to **Downloads > Software > AlgoSec AutoDiscovery**.

3. Do one of the following:

New installation

- a. Select **New Installation - Select Deployment Type > VMWare**.
- b. Select **A30.10** to install the AutoDiscovery version relevant for ASMS A30.10.
- c. Click **Next**, and then click the **Download** button next to the **AutoDiscovery Server - OVF (VMWare)** option.

Save the **AAD-ServerOvf.zip** on the AutoDiscovery server.

- d. Extract the downloaded file, and deploy the virtual appliance to a virtual Linux machine.

Upgrade

- a. Select **Upgrade (All Deployments)**.
- b. Select **A30.10** to upgrade to AutoDiscovery A30.10.
- c. Click **Next**, and then click the **Download** button next to the **AutoDiscovery Upgrade - RPM (VMWare)** option.

Save the downloaded **.rpm** file on your virtual Linux machine.

- d. Use the downloaded **.rpm** file to upgrade the server installation. For example:

```
rpm -U AutoDiscoveryServer-A30.10.x86_64.rpm
```

Each server installation or upgrade comes with a local sensor.

4. After completing the installation, configure traffic collection from your network. For example, do the following:
 - a. Configure NetFlow collection in VMware VSphere.
 - b. Direct the NetFlow output to the AutoDiscovery server, which has a local sensor installed.

Tip: You may have other traffic collection methods planned, using additionally installed sensors. For more details, see [Traffic collection options](#) and [Install AutoDiscovery sensors](#).

AutoDiscovery system requirements

The AutoDiscovery default and recommended installation provides both an AutoDiscovery server and sensor.

The AutoDiscovery server must be deployed to a Linux VMWare server with the following specifications:

VMWare version	AutoDiscovery can be deployed on virtual machines that use VMWare ESX versions 5.5 and higher.
-----------------------	--

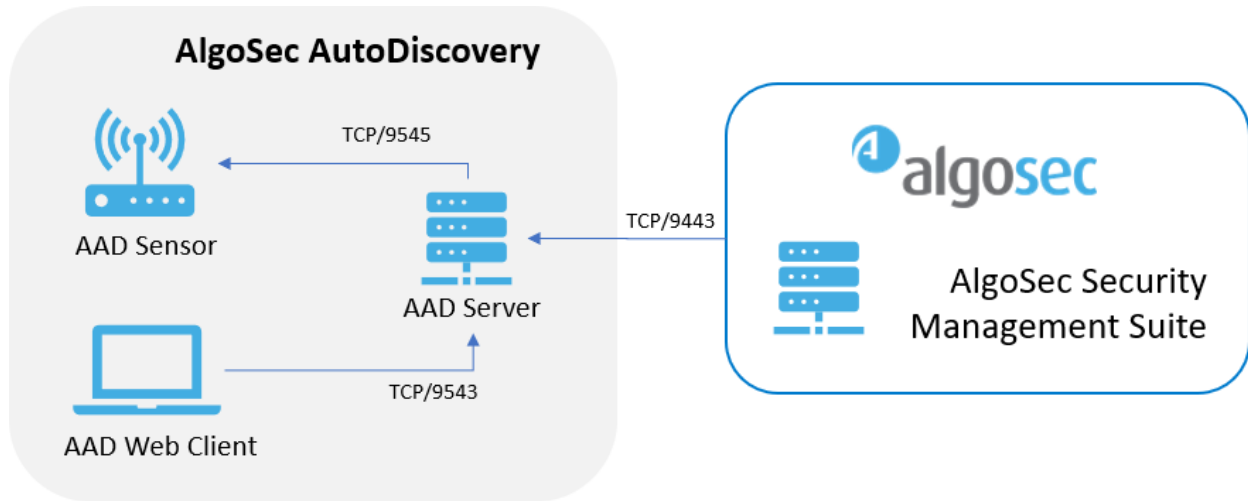
Minimum hardware requirements	<p>Minimum hardware requirements for the AutoDiscovery server include:</p> <ul style="list-style-type: none"> • Dual CPU / Dual core CPU • 4GB RAM for the server • 1GB RAM for the sensor • 10GB free disk space for the server • 16MB free disk space for the sensor, when using thick provisioning during the VM deployment <p>Note: These specifications are appropriate for PoC installations and environments with low traffic levels only.</p>
Recommended hardware requirements	<p>Recommended hardware requirements for the AutoDiscovery server include:</p> <ul style="list-style-type: none"> • 4-8 CPUs or cores • 8GB RAM • 30GB free disk space <p>Note: These specifications are appropriate for production environments with a rate of up to 2000 transactions per minute.</p>
Networking requirements	<p>Connect the virtual appliance to a port group configured with Promiscuous mode.</p> <p>For more details about required ports, see AutoDiscovery required ports.</p>

If you are deploying additional sensors, system requirements for the sensor installations may depend on the traffic collection method. For more details, see [Traffic collection options](#) and [Install AutoDiscovery sensors](#).

Tip: If you have issues decoding HTTP(s) because the certificate is unavailable, we also recommend using the sensor installed together with the AutoDiscovery server instead of installation additional sensors.

AutoDiscovery required ports

The following image shows the traffic between the AutoDiscovery components.



Traffic between AutoDiscovery components uses the following ports:

- **TCP/9545.** From the AutoDiscovery to each sensor configured.
- **TCP/9543.** From AppViz on the ASMS machine to the AutoDiscovery server.
- **TCP/9443.** From the AutoDiscovery web client component to the AutoDiscovery server.

Traffic collection options

AutoDiscovery can collect traffic using statistical capture with NetFlow/SFlow methods or full capture.

Tip: You can also configure AutoDiscovery to use multiple methods, with or without direct collection, to create the collection methods that work best for each part of your network.

We recommend using statistical capture with NetFlow/SFlow methods for high traffic systems. System requirements for the AutoDiscovery sensor may differ depending on the traffic collection options you configure.

Statistical capture	<p>Statistical capture is quicker as it passes a summary of the traffic instead of the full content.</p> <p>Additionally, statistical capture usually does not need additional sensor installations other than the default sensor installed with your AutoDiscovery server.</p> <p>Note: AutoDiscovery supports NetFlow/SFlow using the VSphere Enterprise Plus edition.</p> <p>For more details, see NetFlow system configuration requirements.</p>
Full capture	<p>Full capture collects more details about your traffic, and may require additional sensor installations.</p> <p>For more details, see Install AutoDiscovery sensors.</p>

For more details, see [Statistical vs. Full Capture](#).

Note: Regardless of your configuration, configure a physical router or switch, or a Virtual Distributed Switch, to direct traffic to your sensor. For more details, see the documentation for your router or ESX or NetFlow/SFlow packet broker.

Statistical vs. Full Capture

The following table compares the traffic collection features available for statistical capture using NetFlow/SFlow or full capture:

Feature	NetFlow/SFlow	Full Capture
Discovery of business service maps based on a server/port entry point	Yes	Yes
Change detection and change alerts	Yes	Yes
Business service dependencies	Yes	Yes
Subnet dependencies	Yes	Yes
Activity monitoring	Yes	Yes
Topology view	Yes	Yes

Feature	NetFlow/SFlow	Full Capture
Identification of SSL certificate expiration dates	No	Yes
Identification of database (schema) names	No	Yes
Identification of URLs	SFlow only	Yes
Monitoring of failed connections in business services	No	Yes
Identification of web server type	No	Yes
DNS name resolution using captured traffic, without the need to access a DNS Server from AutoDiscovery Server.	No	Yes
Large scale deployments	Yes	More complicated
Support for ESX inner traffic	Only for enterprise plus edition	Promiscuous mode

NetFlow system configuration requirements

When using NetFlow:

NetFlow version support	AutoDiscovery supports NetFlow versions 5, 6, 7, 9, and IpFix.
Traffic ports	Direct the NetFlow output to the IP address of the AutoDiscovery machine. Any port can be used, and all incoming traffic is captured.
Separate server and sensor	We recommend using a single-server setup, where the AutoDiscovery server and sensor are deployed together. However, you can also separate the sensor and AutoDiscovery server, or configure multiple NetFlow statistics outputs from separate networks using multiple network cards.

Install AutoDiscovery sensors

By default, each AutoDiscovery server installation comes pre-installed with a single sensor, used to capture data from across your network.

You may need additional sensors if you want to use direct traffic collection, full traffic capture, or if you want to separate your AutoDiscovery server and sensor machines. For more details, see [Traffic collection options](#).

This topic describes how to install additional sensors as needed, either directly on a Windows or Linux machine, or as a VMWare OVF.

Sensor installation options

The following table describes the supported configurations for installing additional sensors, and the high-level steps required for each configuration:

ESX with port mirroring	<p>Do the following:</p> <ol style="list-style-type: none"> 1. Deploy an AutoDiscovery sensor to each ESX server. 2. Configure each sensor to view traffic in promiscuous mode.
Physical server with port mirroring	<p>Do the following:</p> <ol style="list-style-type: none"> 1. Prepare a separate server for the AutoDiscovery sensor. The server can be physical or virtual, and Windows or Linux. 2. Direct mirrored traffic to the sensor.
Local mode with direct capture	<p>Install a sensor on any server from which you want to capture traffic.</p>

For more details, see [Install additional AutoDiscovery sensors](#).

Note: To configure statistical traffic collection with NetFlow/SFlow, we recommend using the sensor installed together with the AutoDiscovery server.

For more details, see [Install AutoDiscovery](#).

AutoDiscovery sensor system requirements

Additional AutoDiscovery sensors must be installed on a Linux or Windows server with the following minimum specifications:

CPU	4-core CPU, if expected traffic load has a maximum of 2 Gbps 8-core CPU if expected traffic load is more than 2 Gbps
Memory	8 GB
Disk space	1 GB free disk space
Network adapters	At least 2 network adapters: <ul style="list-style-type: none"> • 1 adapter connected to each source mirror port or LAN • 1 adapter connected to the LAN, for communication with the AutoDiscovery server
Software (Windows only)	When installing a Windows sensor, make sure you have the following software installed on the AutoDiscovery sensor machine: <ul style="list-style-type: none"> • OpenSSL, version 1.0.2. Download and install this from slproweb.com. • Visual C++ Redistributable Packages for Visual Studio 2013. Download and install these from https://www.microsoft.com/.

When deploying on a virtual machine, network cards must be physically connected to the switch / router.

Install additional AutoDiscovery sensors

This procedure describes how to install additional AutoDiscovery sensors.

Do the following:

1. Verify that your AutoDiscovery sensor machine complies with the system requirements. For details, see [AutoDiscovery sensor system requirements](#).

Note: If you are installing additional sensors, you must do so using different

machines than the ones you are using for the AutoDiscovery server and the ASMS installation. Each additional sensor must be installed on its own machine.

2. On the AlgoSec portal, navigate to **Downloads > Software > AlgoSec AutoDiscovery**.
3. Do one of the following:

New installation

- a. Select **New Installation - Select Deployment Type**.
- b. Select your installation type, either a **VMWare OVF**, or a **Windows** or **Linux** installation file.
- c. Select **A30.10** to install the AutoDiscovery sensor version relevant for AutoDiscovery Server **A30.10**.
- d. Click **Next**, and then click the **Download** button next to the **AutoDiscovery Sensor** option for the selected installation type.

A **.zip** file is downloaded for your installation.

Upgrade

- a. Select **Upgrade (All Deployments)**.
- b. Select **A30.10** to upgrade to AutoDiscovery A30.10.
- c. Click **Next**, and then click the **Download** button next to one of the following options:

AutoDiscovery Upgrade for Sensor for Windows x64	Upgrades your separate Windows sensor installation
---	--

AutoDiscovery Upgrade for Linux Sensor	<p>Upgrades your separate Linux sensor installation.</p> <p>Note: This option does not upgrade the local sensor installed on your AutoDiscovery server.</p>
---	--

A **.zip** file is downloaded for your upgrade.

4. Deploy the downloaded file on your sensor machine, depending on your OS type.
For example:

Run an AutoDiscovery sensor installation on VMWare

Deploy your downloaded OVF file to a virtual machine with the required specifications.

Run an AutoDiscovery sensor installation on Linux

This procedure describes how to run an AutoDiscovery sensor installation on Linux.

Do the following:

- a. Extract the contents of the **AutoDiscoverySensor-3000.10.0-40-Linux.zip** file.
- b. Run in installation:

```
./AutoDiscovery-Linux-x64.run
```

- c. Create a directory for the AAD sensor service files. Run:

```
mkdir /opt/autodiscovery
```

Note: If the **/opt/autodiscovery** directory already exists, delete the

```
networksensor
```

 sub-directory. Run:

```
rm -rf /opt/autodiscovery/networksensor
```

- d. If the **networksensor** directory does not yet exist, create it for the network sensor logs. Run:

```
mkdir /var/log/autodiscovery
```

- e. Place the AAD sensor files in the correct directory. Run:

```
mv AutoDiscovery-Linux-x64/networksensor /opt/autodiscovery
```

- f. Enable the AAD sensor service. Run:

```
systemctl enable /opt/autodiscovery/networksensor/networksensor.service
```

If an error occurs, run:

```
systemctl link /opt/autodiscovery/networksensor/networksensor.service
```

- g. Stop the **firewalld** service to open the sensor up to Netflow, SFlow and AAD server communication. Run:

```
systemctl stop firewalld
```

- h. Start the **networksensor** service. Run:

```
systemctl start networksensor
```

- i. Verify that the **networksensor** is alive by tailing its log and seeing that new lines are added. Run:

```
tail -f /var/log/autodiscovery/networksensor.log
```


- j. Exit by pressing **CTRL+C**.

Your sensor is installed and ready to use with AutoDiscovery.

Run an AutoDiscovery sensor installation on Windows

Do the following:

- a. Extract the contents of the downloaded **AutoDiscoverySensor-3000.10.0-40-Windows-x64.zip** file.
- b. Run the extracted **AutoDiscoverySensor-Windows-x64.msi** file.
- c. Click **Next** to start the wizard.

Accept the EULA, and continue through the wizard as instructed.

- d. The installation notifies you that a reboot will be required after the installation is complete.

Verify that all other files are saved and that your system can be rebooted safely when ready, and click **OK**.

The wizard confirms when the installation is complete.

Your sensor is installed and ready to use with AutoDiscovery.

AutoDiscovery sensor system requirements

This section describes system requirements for AutoDiscovery sensors installed in addition to the one provided by the AutoDiscovery installation. Additional sensors are most often configured for full traffic capture.

Note: The number of sensors to install and where to install them depends on your network's load and topology.

For example, if you have packet brokers or standalone sniffers already collecting traffic on your network, you can send the traffic they collect to a single sensor. This avoids the need to thoroughly cover your network with sensors.

Configure one of the following:

Full capture with port mirroring or TAP specifications

Configure full capture by connecting an AutoDiscovery sensor to a mirrored switch port or a TAP device.

In both cases, the output rate must match the AlgoSec appliance collector rate and interface.

System requirements for full capture include the following:

Collection rates	<p>Supported collection rates are 250,000 packets(s) for an AlgoSec 2062 appliance-based collector and 1,000,000 packet(s) for an AlgoSec 2322 appliance.</p> <p>These are recommended collection rates, since AlgoSec AutoDiscovery is statistical in nature and a loss of a few packets has no adverse effect.</p>
ESX infrastructure	<p>In order to enable port mirroring for a Sensor is installed on an ESX server, the server must be configured in promiscuous mode and the traffic must be mirrored to a port group.</p> <p>Adding a Sensor to that port group will enable the Sensor to capture all of the traffic.</p>
Log formats	<p>From version 2.4.3, the Sensor can optionally receive traffic in the following log formats:</p> <ul style="list-style-type: none"> • ERSPAN (type 2 and 3) • GRE (IP 800 and Transparent Ethernet Bridging 6558) • Encapsulated Remote Mirroring in VMware environments (on VDS from VSphere 3.5.1 and up)
Port mirroring hardware requirements	<p>When installed in port mirroring mode, memory and CPU requirements depend on the amount of traffic monitored.</p> <p>Estimated minimum requirements include:</p> <ul style="list-style-type: none"> • Dual CPU/dual core • 2GB RAM • 10MB free disk space • 2 Network Adapters - one connected to the mirror port, the other connected to the LAN.

Note: For information on how to configure mirroring for a port, see your Switch/Router/Firewall documentation.

Full capture with TCPReplay

TCPReplay enables full traffic capture by simulating the traffic in collected PCAP files and sending that traffic to the AutoDiscovery sensor.

For example, use TCPReplay to collect PCAP files as follows:

- By Packet Brokers, such as VSS or Fluke
- By open source tools, such as Ethereal or TCPdump

Tip: Multiple PCAP files can be merged and played back simultaneously. This requires timing synchronization of better than 1 ms when collecting data.

Discover map-based services

You can discover map-based business services from a list of potential business services detected by AutoDiscovery. Alternatively, you can search for map-based services directly by server and port, with or without performing a query to find the desired server.

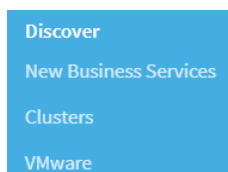
Note: AutoDiscovery can identify the following protocols regardless of whether the default port is being used: HTTP/S, Oracle database access, MS-SQL database access, DNS, and NetFlow/SFlow.

Discover from detected business services

To discover and define detected map-based business services:

1. Hover over the **Discover** tab.

A drop-down menu appears.



2. Select **New Business Services**.

The **New business services** page appears.

Name	URL	Server	Port	Virtual	Clients	Last Seen	Freq.	Match
localhost:9546		localhost (127.0.0.1)	9546 (illumint)	false	1	57 minutes ago	Low	152
localhost:5432		localhost (127.0.0.1)	5432 (postgresql)	false	1	just now	Medium	139

Each entry in the table represents a detected business service that has not yet been defined as a business service in AutoDiscovery. For details on the information provided in each column, see [Detected Business Service Fields](#).

Note: All the detected business services are map-based business services (which start with a server and port as the entry point). Web-based business services (which start with a URL as the entry point) have been deprecated. URL information is still provided when the traffic collection method supports URL identification, but only for the sake of identifying the business service.

3. To filter the detected business services, do the following:
 - a. Type what you want to search for into the search field.
You can search by:
 - Name
 - URL (when supported by the traffic collection option)
 - Server name
 - Server IP address
 - b. Click **Search**.
4. Select the check box for each detected business service you want to define.
5. Click **Discover Selected**.

The **Define Business Service** dialog box appears, displaying your selections with their default name from the name column.



6. If desired, modify the name of the business service(s).
7. Click **Define**.

A notification at the bottom of the page indicates that the business services were created successfully.

The business services are removed from the table, and appear as business services in the **Manage** tab.

Detected Business Service Fields

Column	Description
Name	<p>The default name for the potential business service.</p> <p>For HTTP applications, when full capture is enabled, the default name is extracted from the browser title. If this is not possible, the URL itself is used as the name.</p> <p>For virtual servers defined in a load balancer, the default name is the virtual server name.</p> <p>In other cases, the server name or IP address, with the listening port, is the default name.</p>
URL	<p>The URL for the potential business service. This is only provided when both of the following are true:</p> <ul style="list-style-type: none"> • The traffic collection method supports URL identification • The site is not SSL encrypted (http, not https) or the sensor is configured to support SSL communication.
Server	<p>The name and IP address of the server.</p> <p>Note: Sometimes, the DNS name can take a few moments to resolve. If it does not appear, refresh your screen.</p>
Port	The port number into which traffic is detected.
Virtual	Indicates if the server is a virtual server defined in the load balancer. If true, this indicates that this URL is likely to be a web application.
Clients	<p>The number of active clients using the application.</p> <p>By default, an active client is a client that used the application in the last 10 minutes. For more details, see Configure AutoDiscovery parameters.</p>
Last Seen	The time in which traffic to this server/port was last detected.
Frequency	High, Medium, or Low. Indicates how frequent the traffic to the potential business service is detected.

Column	Description
Match	A high match level indicates a good chance that this is really a business service and not a database access or some website access. It is calculated based on the information in the other columns.

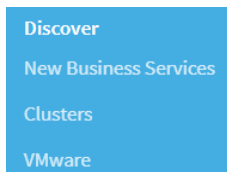
Discover services by server and port

If you know the server information of the business service you are looking for, you can find it directly by searching for the server and port.

To discover by server/port:

1. Hover over the **Discover** tab.

A drop-down menu appears.



2. Select **New Business Services**.

The **New business services** page appears.

3. Click **Discover by Server/Port**.

The **Discover by server/port** window opens.

4. Complete all the fields.
5. Click **OK**.

The map-based business service is created and will appear in the **Manage** tab.

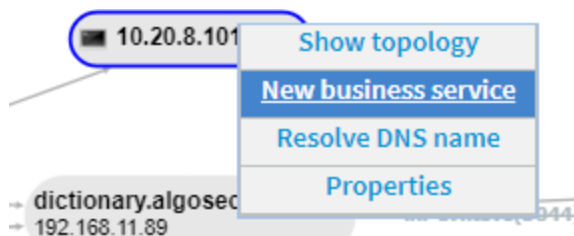
Discover services from a query

Find the server you want to base a new business service on by starting from a query. Do this to create a fully-functional, map-based business service, who's data is updated automatically.

Note: This is different than a query-based business service, where the data is not updated automatically.

Do the following:

1. Perform a simple or advanced query. For details, see [Perform a query](#).
2. On the topology map that appears, locate and click the server you want to base your business service on, and then select **New Business Service**. For example:



3. In the Discover by server/port dialog that appears, do one or both of the following:
 - In the Server (Name or IP Address) field, rename the server as needed.
 - Ensure that **New Business Service** is selected, and enter a name for your new service

For example:

Discover by server/port

Server (Name or IP Address) 10.20.8.101

Port Number 22

New Business Service MyService

Existing Business Service Please select

OK Cancel

4. Click **OK**.

The map-based business service is created and will appear in the **Manage** tab.

Discover query-based services

You can discover business services based on network topology queries. The query is a snapshot of connections at one point in time.

Note: AutoDiscovery can identify the following protocols regardless of whether the default port is being used: HTTP/S, Oracle database access, MS-SQL database access, DNS, and NetFlow/SFlow.

Perform a query

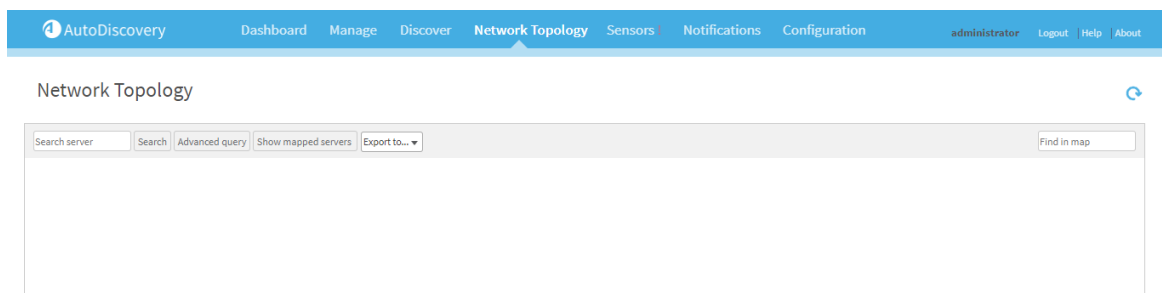
You can perform a query to view a snapshot of connections (the connections at the time the query is performed). When you save a query, you create a query-based business service that appears in the **Manage** tab.

Note: Unlike map-based business services, query-based business services are not updated. They are a snapshot of the connections at the time the query is performed.

To perform a query:

1. Click the **Network Topology** tab.

The **Network Topology** page appears, empty.

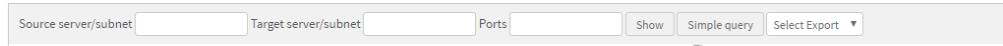


2. Do one of the following:
 - To perform a simple search, in the **Search server** field, enter a name or IP address of a particular server.

- To perform an advanced search, do the following:

1. Click **Advanced Query**.

Additional fields appear.



The screenshot shows a search bar with three input fields: 'Source server/subnet', 'Target server/subnet', and 'Ports'. To the right of these fields are three buttons: 'Show', 'Simple query', and 'Select Export' (with a dropdown arrow).

2. Enter one or more of the following, in the appropriate field.

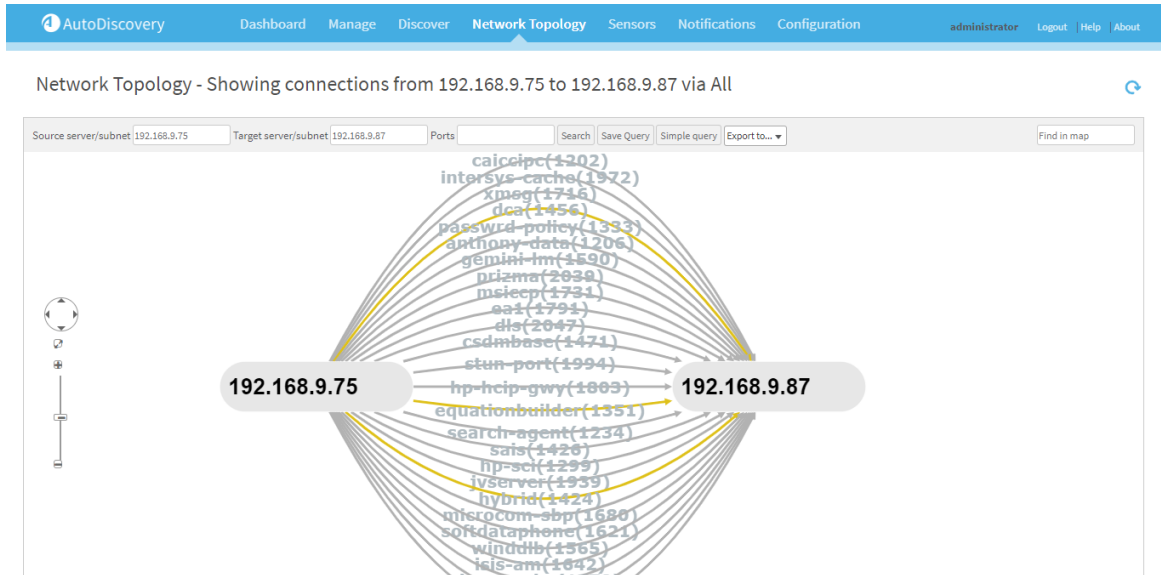
- Source server or subnet (in CIDR notation).
- Target server or subnet (in CIDR notation).
- Ports

3. Click **Show**.

The network topology data appears. For more details, see [Manage business services](#).

Note: When searching for a subnet with a large number of servers, the topology screen will take time to display.

Note: By default, the maximum number of server results for a query is 500. If the query returns a higher number of servers, then only 500 will appear. For more details, see [Configure AutoDiscovery parameters](#).



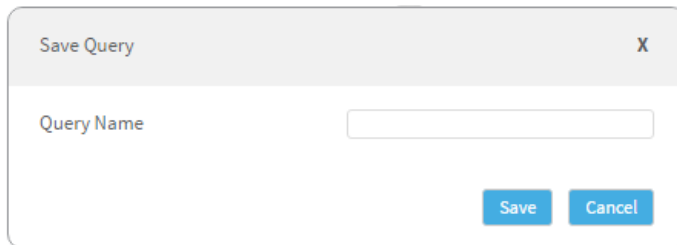
Note: To view the topology for one of the servers in the current map, click the server.

In the menu that appears, click **Show Topology**.

4. To save the query as a business service, do the following:

a. Click **Save Query**.

The **Save Query** dialog box appears.



b. Type a name for the query-based business service.

c. Click **Save**.

The query-based business service is created and the query will appear in the **Manage** tab.

Manage business services

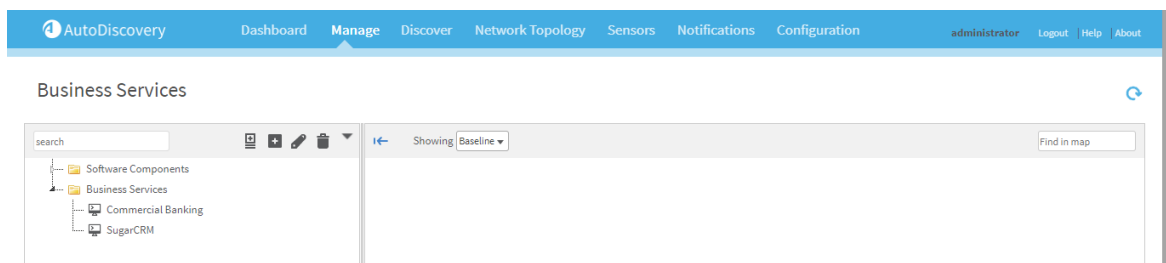
This section describes how to manage business services in AutoDiscovery.

View business services



To view a business service:

1. Click the **Manage** tab.

The **Business Services** page appears.



The icon next to each business service signifies its type.

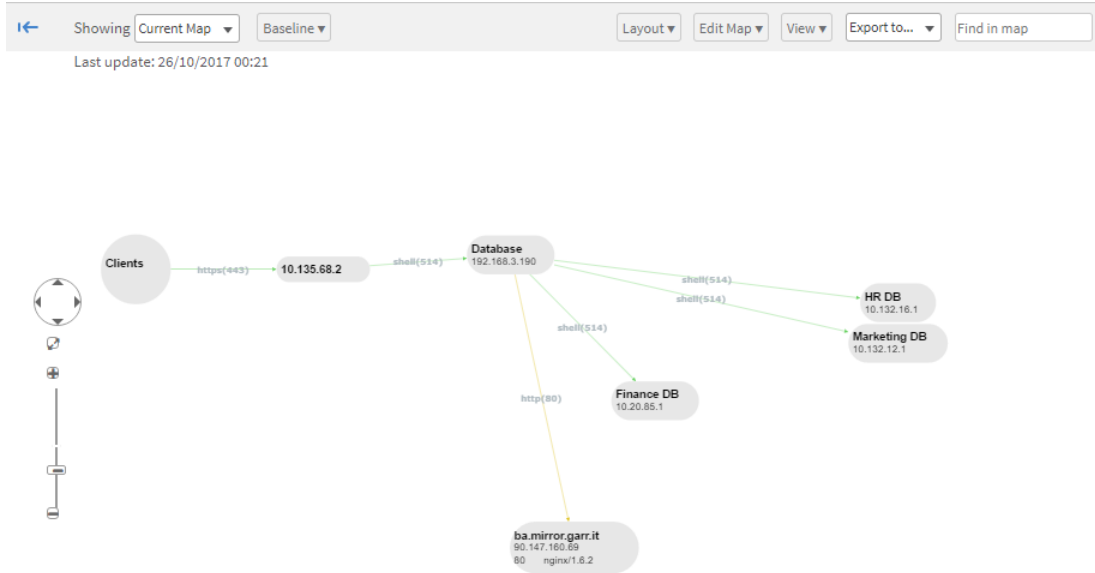
-  signifies a map-based business service
-  signifies a query-based business service

2. Select the desired business service.

The business service's network topology map appears. For more details, see [View the network topology map](#).

View the network topology map

When you view a business service or perform a query, the network topology map appears. The map includes the relevant servers and connections.



Note: The network topology data is collected every 4 minutes and stored for 24 hours. Data for servers and connections that have not been active for more than 24 hours is discarded and will not appear in the topology window.

For more details, see [Configure AutoDiscovery parameters](#).

Servers

Each server appears with its DNS name and IP address. To view more properties, click a server and select **Properties** from the dropdown menu.

For example:

Server Properties X

Display name	<input type="text" value="cs9.wac.phicdn.net"/>
Host name	<input type="text" value="cs9.wac.phicdn.net"/>
IP Address	<input type="text" value="93.184.220.29"/>
Operating system type	<input type="text"/>
Software components	<input type="text" value="80 - ECS (frf/879B)"/>
MAC Address	<input type="text" value="08:5b:0e:0c:14:da"/>
Vendor	<input type="text" value="Fortinet, Inc."/>
Impacted business services	<input type="text"/>
Events	<input type="text"/>

Connections

For each connection, the following details appear:

Connection direction	The arrow shows which server is the source and which server is the target of the connection.
Port number	The port number used for this connection.
Connection activity level	<p>The color of the connection arrow shows the activity level of the connection.</p> <ul style="list-style-type: none"> • Green. The latest activity over the connection took place less than 5 minutes ago. • Yellow. The latest activity over the connection took place more than 5 minutes ago but less than 25 minutes ago. • Gray. There was no activity over the connection for more than 25 minutes.

Additionally, the width of the connection arrow reflects the number of detected packets. The line will be thicker for connections on which a large number of packets have been detected.

Clicking on a connection displays additional details.

<p>192.168.253.127 => e9706.dscg.akamaiedge.net Port: https(443) Protocol: TCP Last seen: 1 hours ago Frequency: Every 30 minute(s) Client reset count: 0 Server reset count: 0</p>

Filter business services

You can filter out irrelevant elements in business services with **Discovery Filters**. Each filter specifies elements that should not be included in one business service (local) or all business services (global). You can manage filters in the following contexts:

All filters	<p>In the discovery filter configuration area, you can manage every filter in AutoDiscovery.</p> <p>Filters can be global or local, and they can filter by servers, clusters, business services or connections.</p>
All filters that affect a specific business service	<p>From a business service's map, you can view all the filters that affect it.</p> <p>This includes all global filters and the local filters specific to the business service. You can remove local filters or create new filters (local or global).</p> <p>See Manage a business service's filters.</p>
Individual servers	<p>From a business service's map, you can select a specific server to filter out, automatically creating a local filter to remove the specific server from the business service.</p> <p>See Remove servers.</p>

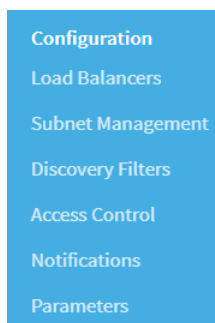
Note: Discovery filters are not supported for query-based business services.

Add filters

To add a new filter:

1. Hover over the **Configuration** tab.

A drop-down menu appears.



2. Select **Discovery Filters**.

The **Discovery Filters** page appears.

Scope	Filter	Description	Creation Date	Created By	Operations
vcenter-qa.algosec.com:443	Anything from any source to any target on port 137		14/2/2016 15:33	illuminitserver	Delete
vcenter-qa.algosec.com:443	Anything from any source to any target on port 139		14/2/2016 15:33	illuminitserver	Delete
vcenter-prd.algosec.com:443	the server 10.20.1.110		24/5/2016 15:11	administrator	Delete
vcenter-prd.algosec.com:443	Anything from any source to any target on port 139		6/3/2016 08:38	illuminitserver	Delete
vcenter-prd.algosec.com:443	Anything from any source to any target on port 137		6/3/2016 08:38	illuminitserver	Delete
v.6.11 [Jenkins]	the server 192.168.3.131		16/11/2017 16:46	administrator	Delete
storage.algosec.com:80 (http://192.168.2.29)	Anything from any source to any target on port 139		2/2/2016 14:32	Roy,Tal	Delete
storage.algosec.com:80 (http://192.168.2.29)	Anything from any source to any target on port 137		2/2/2016 14:32	Roy,Tal	Delete
JPetStore	Anything from any source to any target on port 139		1/3/2016 15:41	illuminitserver	Delete
JPetStore	Anything from any source to any target on port 137		1/3/2016 15:41	illuminitserver	Delete
JOEP-LT.algosec.com:1657	the server 10.20.3.189		24/5/2016 15:05	administrator	Delete
jira.algosec.com Map	Anything from any source to any target on port 137		2/2/2016 14:11	Roy,Tal	Delete
jira.algosec.com Map	Anything from any source to any target on port 139		2/2/2016 14:11	Roy,Tal	Delete
JIRA	Anything from any source to any target on port 137		10/4/2016 11:53	illuminitserver	Delete
JIRA	Anything from any source to any target on port 139		10/4/2016 11:53	illuminitserver	Delete
Jenkins Dashboard	Anything from any source to any target on port 139		10/4/2016 14:02	illuminitserver	Delete

3. Click **New**.

The **New Discovery Filter** window appears.

New Discovery Filter

Filter out Server Host Name or Ip Address

Filter out connection

From Server Host Name or Ip Address

To Server Host Name or Ip Address

On port Port number

Description

Scope

Set as global filter (applicable for all business services)

Specific business service 10.20.1.49:443

OK Cancel

4. Complete the fields using the information in [Discovery filter fields](#).

5. Click **OK**.

The filter is created and appears in the list.

Discovery filter fields

Field	Description
Filter out	Select this option to filter out a server, cluster, or business service. Specify the desired element in the drop-down menus.
Filter out connection	Select this option to filter out a connection. Specify the connection in the drop-down menus.
Description	Type a description for the filter.
Scope	Select one of the following: <ul style="list-style-type: none"> • Set as global filter (applicable for all business services). The filter will affect all business services. • Specific business service. The filter will only apply to the business service you select in the drop-down menu.

Delete filters

To delete a filter:

1. Hover over the **Configuration** tab.
A drop-down menu appears.
2. Select **Discovery Filters**.
The **Discovery Filters** page appears.
3. In the **Operations** column of the filter's row, click the **delete** link.
A confirmation message appears.
4. Click **Yes**.

Manage a business service's filters

Note: Global filters can only be removed from the discovery filters configuration area.

To manage a business service's filters:

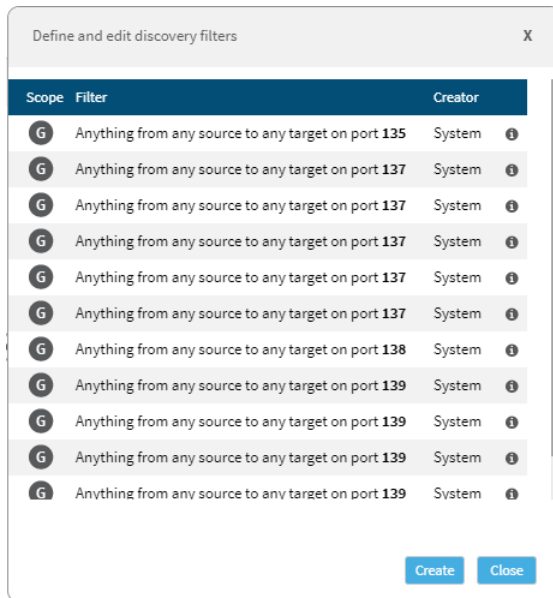
1. View the desired Business Service. For details, see [View business services](#).


2. Hover over .

A menu appears.

3. Select **Filter Out**.

The **Define and edit discovery filters** window appears.



4. To remove a local scope filter (a filter specific to the business service), click .

5. To create a new filter, do the following:

a. Click **Create**.

The **New Discovery Filter** window appears.

New Discovery Filter

Filter out Server Host Name or Ip Address

Filter out connection

From Server Host Name or Ip Address

To Server Host Name or Ip Address

On port Port number

Description

Scope

Set as global filter (applicable for all business services)

Specific business service 10.20.1.49:443

OK Cancel

b. Complete the fields using the information in [Discovery filter fields](#).

c. Click **OK**.

The filter is created and appears in the Discovery Filter configuration area.

Remove servers

To remove servers:

1. View the desired Business Service. For details, see [View business services](#).

2. Click on the server you want to remove.

A menu appears.

3. Select **Filter out**.

A confirmation message appears.

4. Click **Yes**.

The filter appears in the Discovery Filter configuration area.

Add connections manually

You can add relevant connections to a business service manually.

The arrows for manually added connections appear dotted (not solid) in the map. Manually added connections will always remain in the map until they are manually removed.

To servers to a business service manually:

1. Click the **Manage** tab.

The **Business Services** page appears.

2. Select the business service which contains the desired server.

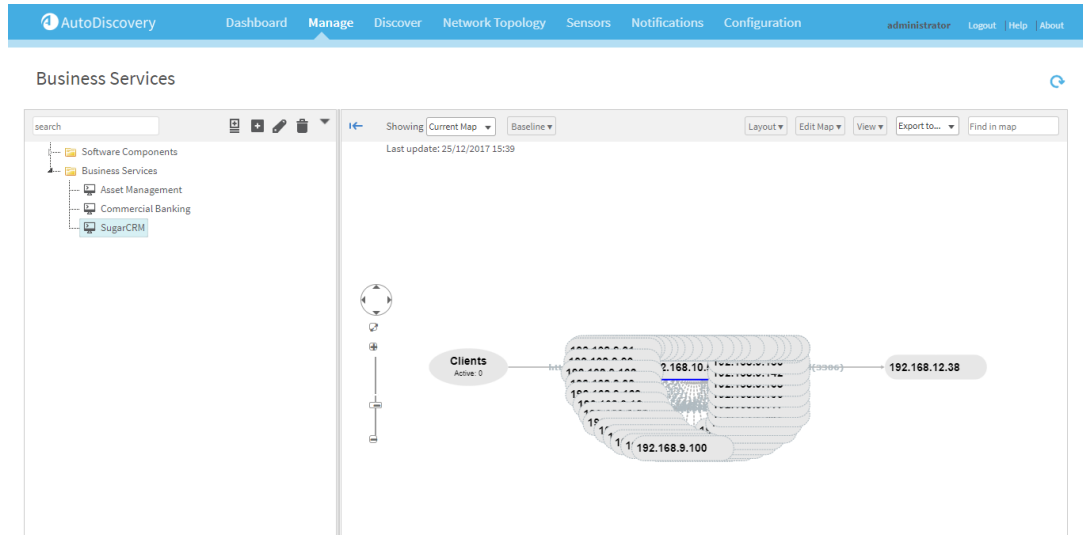
The business service's map appears.



3. Do one of the following to add a connection to/from a server in the business service:
 - a. Click the desired server.

View connections in the map and individually add them to the business service

- a. Click the desired server.
A menu appears.
- b. Click **Show Outgoing** or **Show Incoming**.
The connections appear in the map.



c. Click on the server you want to add.

The **Add Link** dialog box appears.



d. Select the connection you want to add to the business service in the **Relation** drop-down menu.

e. Click **Add**.

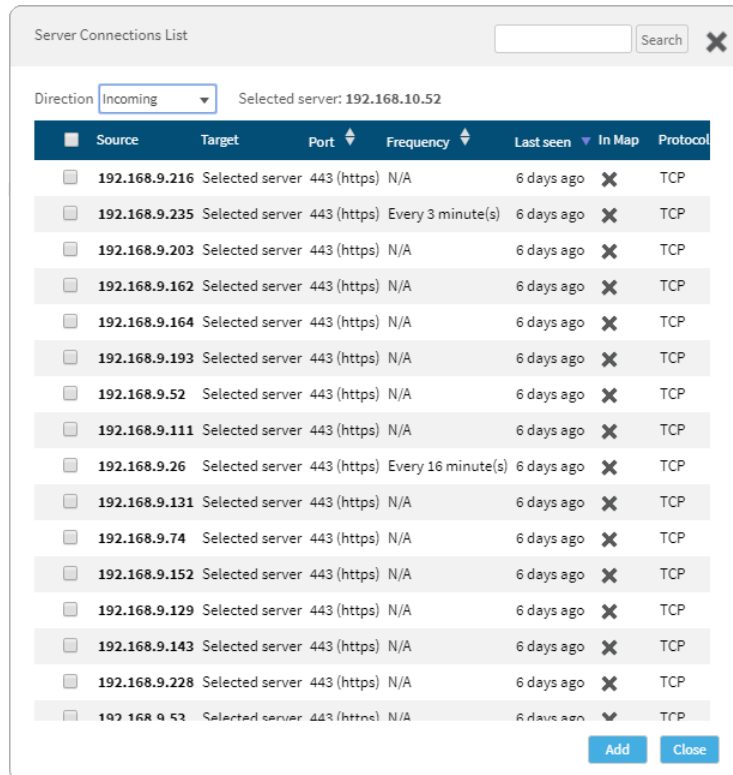
View the connections in a search-able list and easily add multiple connections to the business service

a. Click the desired server.

A menu appears.

b. Click **Show connections list**.

The **Server Connections List** window appears.



Switch between incoming and outgoing connections using the **Direction** drop-down menu.

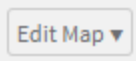

- c. Select the connections you want to add.
- d. Click **Add**.

The server is added to the business service.

Resolve DNS names

You can resolve the DNS name for a specific server, for every server in the map, or for every server in every Business Service.


To resolve DNS names:

1. View the desired Business Service. For details, see [View business services](#).
2. To resolve the DNS name for a single server:
 - a. Click on the server.
A menu appears.
 - b. Select **Resolve DNS name**.
3. To resolve the DNS name for every server in the map:
 - a. Hover over .
A menu appears.
 - b. Select **Resolve DNS names**.
4. To resolve every DNS name for every server in every Business Service:
 - a. Hover over .
A menu appears.
 - b. Select **Resolve All**.

Edit business service properties

Use the following procedure to edit the properties of a defined business service.

To edit a business service:

1. Click the **Manage** tab.
The **Business Services** page appears.
2. Select the desired business service.
3. Click .
The **Business service properties** dialog box appears.

- For a map-based business services:
- For query-based business services:

The screenshot shows a dialog box titled "Business service properties" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name: jira
- Priority: Normal
- Description: (empty)
- Owner Name: (empty)
- Owner Email: (empty)
- Owner Phone: (empty)
- Basic Query: (selected)
- Advanced Query: (unselected)
- Server List: jira (with a Remove button)
- Server: (empty) (with an Add button)
- OK button
- Cancel button

4. Edit the desired field(s).
5. Click OK.

AutoDiscovery baseline map

When viewing business services, the current business service map appears in the right pane. If desired, you can set the current map as the baseline.

Note: When importing AutoDiscovery data into AppViz, AppViz imports a map for each business service. If the business service has a baseline map defined, AppViz will import the baseline. Otherwise, AppViz will import the business service's current map.

- To save the current map as the baseline, see [Save the current map as the baseline](#).
- To compare the current map with the baseline, see [Compare the current map to the baseline](#).

- To edit the baseline map by removing servers, see [Remove servers from the baseline](#) .
- To edit the baseline map by resolving DNS names, see [Resolve DNS names in the baseline](#).

Save the current map as the baseline

To save a business service's current map as the baseline:

1. Click the **Manage** tab.

The **Business Services** page appears.

2. Select the desired business service.

The business service's map appears.



3. Hover over **Baseline** .

A menu appears.

4. Select **Save as baseline**.

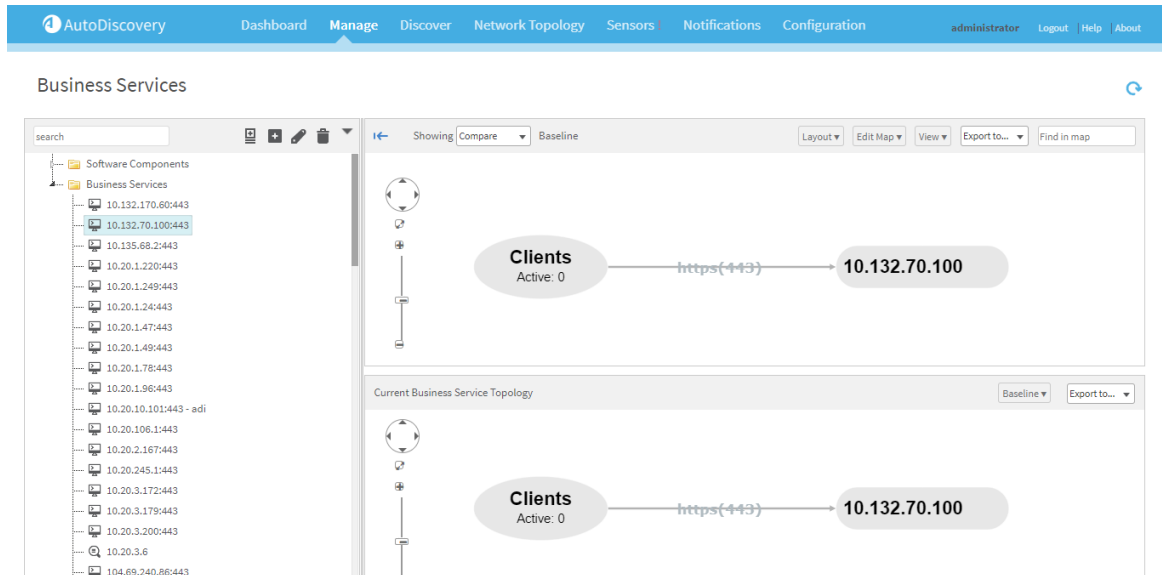
The current map is saved as the baseline.

Compare the current map to the baseline

To compare the baseline map with the current map:

1. View the desired Business Service. For details, see [Manage business services](#).
2. In the **Showing** drop-down menu, select **Compare**.

The right pane displays both the current and baseline maps.



Remove servers from the baseline

To remove a server from the baseline:

1. View the desired Business Service. For details, see [Manage business services](#).
2. In the **Showing** drop-down menu, select **Baseline**.

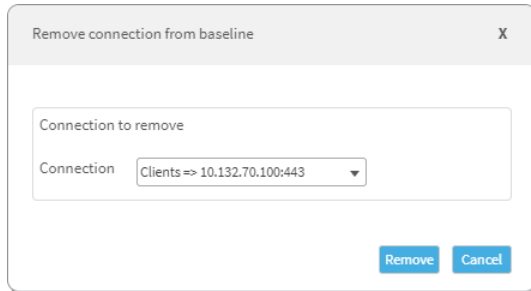
The baseline map appears in the right pane.

3. Hover over .

A menu appears.

4. Select **Remove from Baseline**.

The **Remove connection from baseline** window appears.



5. Select the connection to remove in the drop-down menu.
6. Click **Remove**.

Resolve DNS names in the baseline

To resolve the DNS names for servers in the baseline map:

1. View the desired Business Service. For details, see [Manage business services](#).
2. In the **Showing** drop-down menu, select **Baseline**.

The baseline map appears in the right pane.

3. Hover over .

A menu appears.

4. Select **Resolve DNS names**.

Export AutoDiscovery data

You can export the traffic logs, including the business service/application mapping information, from AutoDiscovery as a CSV file.

Defining the AutoDiscovery Server

To define the AutoDiscovery server in AppViz:

1. Open a terminal and log in as "root" and the related password.
2. Run `/usr/share/bflow/auto_discovery_setup_config.sh`

The following prompts appear:

```
Enter auto discovery URL :Enter auto discovery API user name :Enter auto
discovery API password:
```

3. Complete the prompts.

Exporting a CSV File

To export the CSV file:

1. Open a terminal and log in as "root" and the related password.
2. Run `/usr/share/bflow/./BusinessFlow-CLI.sh -t export_auto_discovery -o <file_name>.csv`

Where `<file_name>` is either the relative or absolute file name.

The file is created and saved under `/home/bflow/config/discovery_from_logs.`

Configure AutoDiscovery

This topic describes how to define AutoDiscovery users, user roles, and configuration parameters.

Manage AutoDiscovery users

This procedure describes how to add or edit AutoDiscovery users.

Do the following:

1. In AutoDiscovery, select the **Configuration** tab > **Access Control** > **Users**.
2. Do one of the following:

Add new users

- a. Click **New User**.
- b. In the **New User** dialog, define the following details:
 - A username
 - A user password
 - At least one user role.

Edit an existing user

In the row for the user you want to edit, do one of the following:

Change a user's name or role	Click the Edit link. In the Edit User dialog, enter a new User name and select a new role as needed.
Change a user's password	Click the Change password link. In the Change password dialog, enter the new password.

Delete existing users

Select the checkbox next to one or more users listed, and click **Delete Selected**.

In the confirmation message that appears, click **Yes**.

Note: Each user must have at least one role assigned. For more details, see [Manage AutoDiscovery user roles](#).

Manage AutoDiscovery user roles

Each user role defines a group of permissions that can be assigned together to any user.

By default, AutoDiscovery is installed with the **Administrators** and **Viewers** roles. You can clone these roles and edit them, or create new roles from scratch.

Do the following:

1. In AutoDiscovery, select the **Configuration** tab > **Access Control** > **Roles**.
2. Do one of the following:

Add a new role

- a. Click **New Role**.
- b. In the **New Role** dialog, do the following:
 - Enter a name for your new role
 - Select the permissions you want this role to have.

To select all permissions, select the **Permissions** checkbox above the list. Expand or collapse each item to view and select permissions at a greater granularity.
 - Select whether you want these permissions to apply to all business services, or selected business services only.
- c. Click **Save** to add the new role to the list.

Edit an existing role

a. In the row for the user you want to edit, click the **Edit** link.

b. In the **Edit Role** dialog, do the following:

- Edit your role name.
- Update the permissions you want this role to have.

To select all permissions, select the **Permissions** checkbox above the list. Expand or collapse each item to view and select permissions at a greater granularity.

- Select whether you want these permissions to apply to all business services, or selected business services only.

Note: Administrators must have permissions applied to all business services.

c. Click **Save** to save your changes.

Clone an existing role for editing

a. In the row for the user you want to clone, click the **Clone** link.

A new role is created, called **Copy of ...**

b. Edit the new role as any other existing role. For details, see [Edit an existing role](#).

c. Click **Save** to save your changes.

Delete AutoDiscovery roles

Select the checkbox next to one or more roles listed, and click **Delete Selected**.

In the confirmation message that appears, click **Yes**.

Note: You cannot delete the **Administrator** role.

Configure AutoDiscovery parameters

This procedure describes how to define AutoDiscovery behavior using the available configuration parameters.

Do the following:

1. In AutoDiscovery, select the **Configuration** tab > **Parameters**.
2. Find the parameter you want to change, and modify the value in the **Value** column.
For more details, see [AutoDiscovery parameter reference](#).
3. To save your change, click the **Update** link in the row for the parameter you modified.

Tip: To restore a parameter's default value, click the **Restore to default** link for the parameter you want to restore.

AutoDiscovery parameter reference

AutoDiscovery parameters include the following:

- [Global parameters](#)
- [Business service creation parameters](#)

Global parameters

The following parameters determine global AutoDiscovery behavior:

- [Active Clients Timeout](#)
- [Cluster sensitivity](#)
- [Default Business Service Depth](#)
- [Default Business Service frequency](#)

- [Extract URL Details](#)
- [Save baseline automatically](#)
- [Topology results limit](#)
- [Topology storage hours](#)

Active Clients Timeout

The time of inactivity, in minutes, after which a business service's client is considered inactive.

A number between **1** and **1440** (24 hours)

Default = **10**

Cluster sensitivity

Determines the percentage by which the cluster severity is reduced compared to the average severity of its members. The average is rounded to the closes severity level.

A number between **0** and **100**

- Default = **30**
- **0** = The cluster severity is exactly the average of its members
- **100** = The average severity is divided by 2.

Default Business Service Depth

The maximum number of nodes from the entry point to include in newly defined business services.

Default = **2**

Default Business Service frequency

The default frequency threshold (in minutes) for business service connections. Connections with a lower frequency are not included in newly defined business services.

A number between 1 and 100.

Default = 10

Extract URL Details

Determines whether to attempt to access web servers in order to extract additional details from them.

Default = **false**

Save baseline automatically

Determines whether to automatically save the initial baseline for topology business services.

Default = **false**

Topology results limit

The maximum number of results returned for a Network Topology query.

Default = 500

Topology storage hours

The number of hours that topology relations are stored.

A number between 24 and 1440 (between 1 and 60 days).

Default = 24

Business service creation parameters

AutoDiscovery provides the following additional parameters to determine business service creation behavior:

- [Entry point must have DNS name](#)
- [Default Business Service Depth](#)
- [Min number of clients for entry point](#)

- [Min percentage of clients for entry point](#)
- [Min match score for entry point](#)
- [Min frequency score for entry point](#)
- [Max last seen hours for entry point](#)
- [Max number of candidates to processes](#)
- [Business service auto-creation interval](#)

Entry point must have DNS name

Determines whether entry points used to create a business service must have DNS names.

Default = **true**

Min number of clients for entry point

Defines the minimum number of clients required to define a server as an entry point.

Default = **30**

Min percentage of clients for entry point

Defines the minimum percentage of clients required to define a server as an entry point.

Default = **50**

Min match score for entry point

Defines the minimum matching score to define a server as an entry point.

Default = **120**

Min frequency score for entry point

Defines the minimum frequency score to define a server as an entry point.

Values: **HIGH, MEDIUM, LOW**

Default = **HIGH**

Max last seen hours for entry point

Defines the largest number of hours since a server was last seen to define that server as an entry point.

Default = **24**

Max number of candidates to processes

Defines the maximum number of business service recommendations to handle in a single process.

Default = **15**

Business service auto-creation interval

Defines how often AutoDiscovery runs the auto-creation process to create business services.

0 = job is disabled.

Default = **24**

Troubleshoot AutoDiscovery

If you need to send a support archive to AlgoSec for troubleshooting, do the following:

At the top right of the AutoDiscovery page, click **Help > Support files**.

A zip file is saved locally, named **AAD_support_<date><ID>.zip**

Send us feedback

Let us know how we can improve your experience with the User Guide.

Email us at: techdocs@algosec.com

Note: For more details not included in this guide, see the online [ASMS Tech Docs](#).