Connectivity Security White Paper

Electronic Service Agent for AIX

July 2025

Table of Contents

Introduction

This document describes the connectivity, security, and service information, sent by Electronic Service Agent (ESA) for AIX when ESA communicates with the IBM Service Delivery Center (SDC). The functions that are described in this document refer to ESA version 7.0 and later.

ESA version 7 and later is available in the following products:

- All installations of AIX 7.3 or later.

ESA runs in the following environments when the system or solution vendor is IBM:

- AIX installed on a stand-alone Power system.
- AIX installed on a logical partition (no hardware problem reporting)

> **Note**: ESA does not activate under the following conditions:
>
> 1. The system vendor is not IBM (for example, Bull or Hitachi).

Useful Documentation

A complete set of ESA documentation can be found at:
https://www.ibm.com/docs/en/aix/7.3?topic=management-electronic-service-agent

Terms and Definitions

It is assumed that the reader has a basic understanding of Internet Protocol (IP) networks and protocols. The following is a list of terms and acronyms that might not be familiar to the reader.

Term	Definition
ESA	Electronic Service Agent
FRU	Field Replaceable Unit
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LPAR	Logical Partition
PAM	Pluggable Authentication Module
SDC	Service Delivery Center
SNAT	Source Network Address Translation
SRC	System Reference Code

SRN	System Reference Number
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
EED	Extended Error Data
ESS	Elastic Storage Server
IPMI	Intelligent Platform Management Interface

Reasons for Activating ESA for AIX

Reasons for activating ESA for AIX

- Automatically report a hardware problem to IBM
- Automatically send extended error data for problem analysis by IBM
- Automatically report inventory and system configuration information to IBM
- Automatically report heartbeat to IBM
- ESA routinely checks for access key expiry and updates.
- View reports generated that uses your data on the IBM Electronic Support website

Activating ESA for AIX

After you install ESA, you must activate and configure it. You can activate the ESA by using the respective commands for AIX. There is no need to activate ESA on a Logical Partition (LPAR) managed by the HMC, the HMC invokes ESA on LPAR commands to collect the software inventory, without requiring activation. For information on how to activate Electronic Service Agent, see Electronic Service Agent for AIX User's Guide.

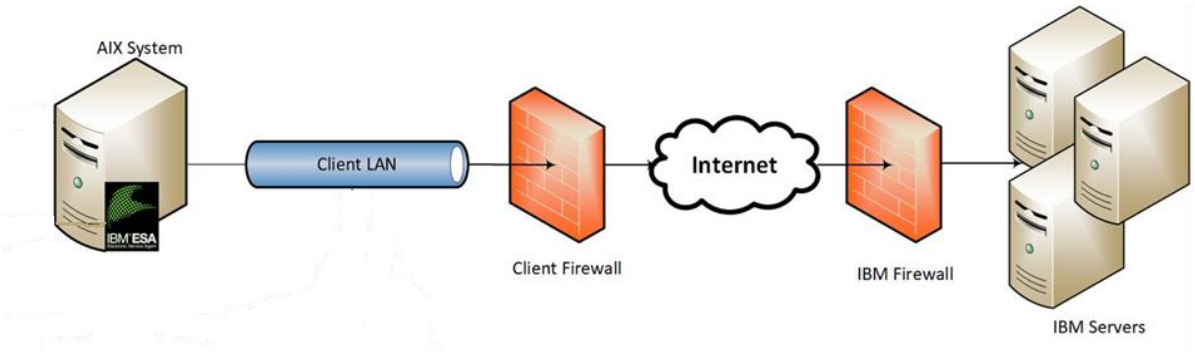
If you use a default direct Internet connection, no additional configuration is needed. However, if a direct connection is not available, you can configure IBM Electronic Service Agent to communicate with IBM using a proxy server. You can specify up to three proxy servers. IBM Electronic Service Agent uses the connections in the order they appear, so if one service connection is not configured, busy, or unavailable, the next service connection is used.

ESA for AIX Connectivity

ESA for AIX only supports outbound Internet connectivity. Modem connectivity is not available with ESA for any versions of AIX. VPN and inbound connectivity are not supported.

Outbound Connectivity without Proxy Server

The following diagram shows the default setup of ESA on AIX that is connected to IBM without a proxy server.



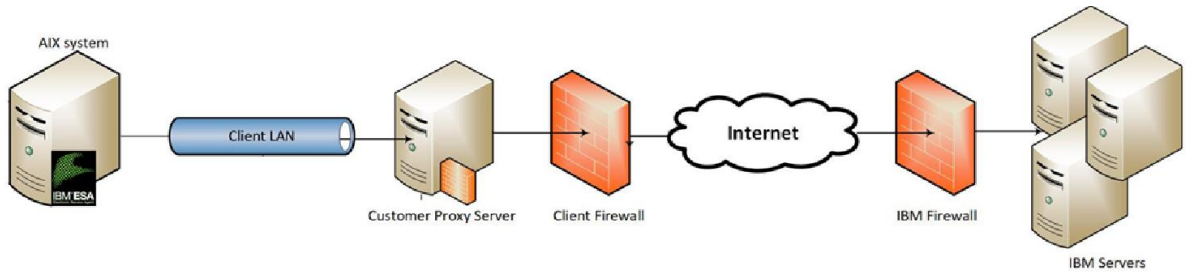
In this setup, ESA connects through your internet connection by the default route. For this type of configuration, you can optionally use a second network card to physically separate the local system network from the internet enabled network.

For ESA to communicate successfully, your external firewall must allow outbound packets to flow freely on port 443. You can use Source Network Address Translation (SNAT) and masquerading rules to hide the ESA system's source IP address.

On your firewall, you can choose to limit the specific IP addresses to which the ESA system can connect. Section IBM Server Address List contains the list of IP addresses and ports of the IBM servers.

Outbound Connectivity with your Proxy Server

The following diagram shows the ESA for AIX that is connected to IBM using a proxy server supplied by you. This is not the default setup, and you must configure ESA to use your proxy.



To forward ESA packets, the proxy server must support the basic proxy header functions (as described in RFC #2616) and the CONNECT method. Optionally, basic proxy authentication (RFC #2617) can be configured so that the ESA authenticates before attempting to forward packets through your proxy server.

Configuring ESA to use a Proxy Server

Connecting the IBM Electronic Service Agent through the HTTP proxy can be fast and easy for your business network and minimizes the number of systems that are directly connected to the internet.

You can also log in to your AIX system to configure your service connection. For more information, see Electronic Service Agent for AIX User's Guide.

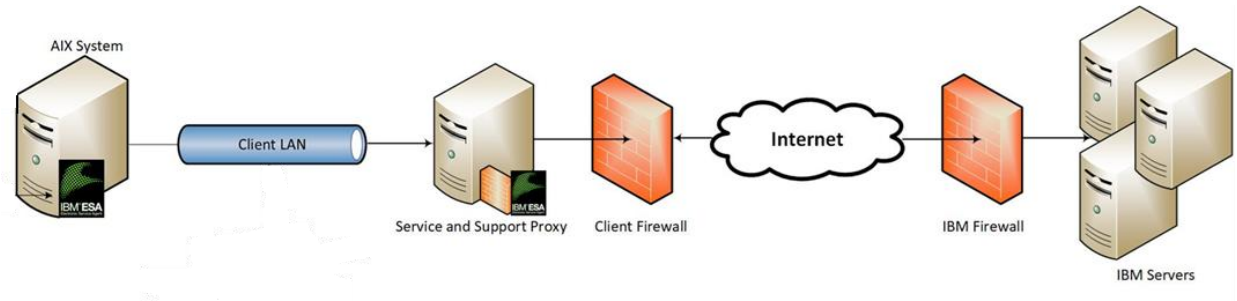
If you select the proxy path to send your information, then the following process applies:

1. At the scheduled time, IBM Electronic Service Agent collects the information to be transmitted and queues it for transmission.
2. Using the TLS connection between the system and the IBM Electronic Support SDC, IBM Electronic Service Agent establishes a TLS internet connection between the proxy and the IBM Electronic Support SDC. This connection is authenticated by using the system ID and password that is previously created.
3. IBM Electronic Service Agent sends the collected information through the proxy to the IBM Electronic Support SDC.
4. After the information arrives at the IBM Electronic Support SDC, the information is transferred to the appropriate IBM database.

Outbound Connectivity with ESA supplied Service and Support Proxy Server

ESA supplies a Service and Support Proxy Server. This proxy server can be deployed in your environment to aggregate connectivity to IBM through a single Internet-enabled system. This proxy only supports the destinations that are listed in section IBM Server Address List and as such cannot be used in your environment to serve as a general-purpose proxy server.

The following diagram shows the ESA for AIX that is connected to IBM by using the Service and Support proxy server that is supplied by ESA.



Verify Electronic Service Agent Connectivity

IBM Electronic Service Agent communicates with several IBM servers, and all connections with IBM are backed up by redundant sites. So, if a primary connect point is unavailable, a connection is attempted at a backup server.

After configuring your connectivity settings, test for connectivity to IBM. For more information, see Electronic Service Agent for AIX User's Guide.

Security Protocols and Encryption

Communication between ESA and IBM

ESA uses the HTTPS protocol for transmission of data between your site and the IBM Service Delivery Center. The HTTP protocol serves as a backup path for initiating the download of new configuration information when an appropriate HTTPS path cannot be established. Your data is never uploaded by using the HTTP protocol.

HTTPS is achieved by encapsulating the HTTP application protocol with the Transport Layer Security (TLS) cryptographic protocol.

IPv6 support

The IPv6 protocol is supported fully by Call home.

IPv4 support

The IPv4 protocol is also supported fully by Call home.

Service information sent to and from IBM

This section outlines what Service information is sent to IBM.

Data Sent to IBM

This is a list of data that might be sent to IBM, the command, or component that is used to collect the information and brief descriptions of the contents.

Table 1: Data sent to IBM from AIX

Reason	Command/Component	Description
Problem reporting	AIX diagnostics (Diag)	The SRC/SRN and FRU information are collected by using the AIX diagnostics package.
Extended error data	snap	The "snap -g" data is collected and sent as the result of a hardware problem that is reported to IBM.
System configuration	snap	Automated system configuration is collected and sent weekly by default and uses the "/usr/sbin/snap -g -c -d /var/esa/data/temp/snap" command.
Contact information	ESA	Contact information is reported to IBM, securely stored at IBM, and used only by designated IBM service personnel for contacting you about problems with your system.
ESA supplemental service information	uname, lsmcode, hostname, lsattr Commands: • prtconf | grep "System Model" • lslpp -l | grep bos.esagent • lsattr -EH -l sys0 | grep systemid	Includes ESA AIX version, firmware level, machine type, machine manufacturer, machine serial and machine model.

	• # prtconf | grep -i "firmware level"	
Operational Test	Internally generated by ESA	While ESA is active on your system, it performs a daily operational test (also known as. heartbeat) with IBM.

Data received from IBM

Reason	Command/Component	Description
UAK (Update Access Key)	/usr/esa/bin/uak_aix_expiry /usr/esa/bin/uak_expiry /usr/esa/bin/uak_update All above commands internally uses AIX ioctl command.	POWER10 and later servers include a UAK that is checked when system firmware and OS updates are applied to the system. The access keys include an expiration date. If the calendar date is beyond the expiration date of update access key, the system firmware updates are not processed. IBM Electronic Service Agent updates these automatically.
UAK (Update Access Key)	/usr/esa/bin/uak_expiry /usr/esa/bin/uak_update All above commands internally uses AIX ioctl command.	POWER8 (and later) servers include an UAK that is checked when system firmware updates are applied to the system. The access keys include an expiration date. If the calendar date is beyond the expiration date of update access key, the system firmware updates are not processed. IBM Electronic Service Agent updates these automatically.

Appendix: IP address and port for IBM Connectivity

Overview

This appendix identifies the IP addresses and ports that are used by AIX when it is configured to use internet connectivity.

If your AIX ESA supports the simplified connectivity path, view the section Simplified Connectivity Options.

Simplified Connectivity Options

From ESA version 6 / 7 for AIX, a new Call Home server environment is deployed that provides a front-end proxy to the current Call Home infrastructure. This environment simplifies the IT for Call Home customers by reducing the number of customers facing IBM servers, enabling IPv6 connectivity, and providing enhanced security by supporting NIST 800-131A. Customers have fewer IBM addresses to open on their firewall. All Call Home internet traffic flows through the Call Home proxy and then fans out to various internal IBM service providers.

This list applies to all pre-defined ports and addresses that are used by ESA, but not to those ESA functions, which allows the entry of a target address / port.

Table 2: Address and port used by ESA

Host name	IP Address	Port	Protocol	Additional detail
esupport.ibm.com	192.148.6.11	443	HTTPS (to IBM), HTTP (from IBM)	• esupport.ibm.com IPv4 address 129.42.56.189 is disabled. Corresponding IPv6 is disabled as well. • esupport.ibm.com IPv4 address 129.42.60.189 is disabled. Corresponding IPv6 is disabled as well.

A new IP address (192.148.6.11) is enabled and returned from DNS. The old IP addresses 129.42.18.70, 129.42.19.70 and (129.42.21.70) are disabled and no longer returned from DNS. For more information, see https://www.ibm.com/support/pages/node/6853429.

IBM Corporation

Marketing Communications

Systems and Technology Group

Route 100

Somers, New York 10589

Produced in the United States of America

July 2025.

PSW03007-USEN-00