



Connectivity Security White Paper

Electronic Service Agent for Linux & Windows

July 2015

Table of Contents

I.....Introduction	2
Useful Documentation.....	2
Terms and Definitions	2
II.....Reasons for Activating ESA	3
Reasons for activating ESA for Linux and Windows	3
III.....Activating ESA for Linux and Windows	4
IV.....ESA for Linux Connectivity	5
Outbound Connectivity without Proxy Server	5
Outbound Connectivity with your Proxy Server	5
Configuring ESA to use a Proxy Server.....	6
Outbound Connectivity with ESA supplied Service and Support Proxy Server	7
Configuring the ESA supplied Service and Support Proxy Server	7
Verify Electronic Service Agent Connectivity.....	8
V.....Security Protocols and Encryption	9
Communication between ESA and IBM	9
IPv6 support	9
Communication between your browser and the ESA daemon.....	9
ESA Web User Interface Authentication	9
Communication between ESA and Integrated Management Module.....	9
VI.....Service information sent to IBM	10
Data Sent to IBM.....	10
Data retrieved from IBM by ESA.....	11
VII.....Appendix	12
IBM Server Address List	12

Introduction

This document describes the connectivity, security and service information, sent by Electronic Service Agent (ESA) for Linux & Windows when ESA communicates with the IBM Service Delivery Center (SDC). The functionality that is described in this document refers to ESA version 7.1.5 and later.

ESA 7.1.5 for Linux and Windows is available for download at - <http://www.ibm.com/support/esa>

ESA supports the following types of systems:

- Linux and Windows on Pure Systems
- Linux and Windows on a System x blades
- Linux and Windows installed on a stand-alone System x system

Useful Documentation

A complete set of ESA documentation can be found at: <http://www-01.ibm.com/support/esa/documentation.htm>.

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 may not be familiar to the reader.

Term	Definition
ESA	Electronic Service Agent
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
SDC	Service Delivery Center
SNAT	Source Network Address Translation
TLS	Transport Layer Security
PAM	Pluggable Authentication Module

Reasons for Activating ESA

Reasons for activating ESA for Linux and Windows

- 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 and status information to IBM
- Automatically report performance information to IBM
- View reports generated using your data on the IBM Electronic Support website

Activating ESA for Linux and Windows

After you install ESA, you must activate and configure it. You can activate the ESA by using the activation wizard or command activation on your Linux or Windows system.

For information on how to activate Electronic Service Agent, see [Electronic Service Agent for Windows User's Guide](#).

While activating ESA, you must specify a port number that is used to connect to ESA through the web browsers. For example, <https://hostname:5024/esa>, where *hostname* is the fully qualified name or the IP address of the system running ESA. Port 5024 is the default port. If you have activated ESA on a different port, use that port number in the web address.

IBM Electronic Service Agent can connect to the IBM Electronic Support SDC through direct Internet (HTTPS) connection, service and support proxy, or HTTP proxy connection paths. IBM Electronic Service Agent uses these connection paths to report problems and send service information to the IBM Electronic Support SDC. IBM Electronic Service Agent uses IPv4 to connect to the IBM Electronic Support SDC.

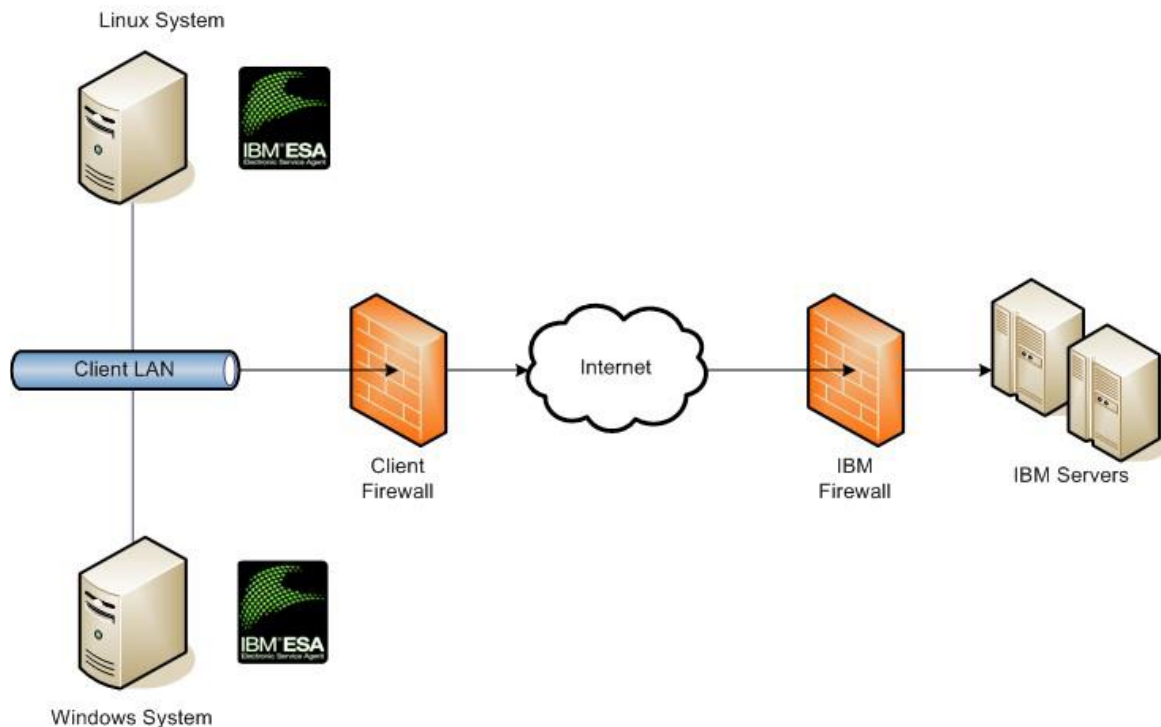
If you use only a default direct Internet connection, no additional configuration is needed. However, if a direct connection is not always available, you can configure IBM Electronic Service Agent to communicate with IBM using a proxy server. You can specify up to three proxy servers. IBM Electronic 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 Linux Connectivity

ESA for Linux and Windows supports outbound Internet connectivity. Outbound modem connectivity is not supported in ESA for Linux and Windows.

Outbound Connectivity without Proxy Server

The following diagram shows the default setup of ESA on Linux and Windows 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 80 and port 443. You can use Source Network Address Translation (SNAT) and masquerading rules to hide the ESA system's source IP address.

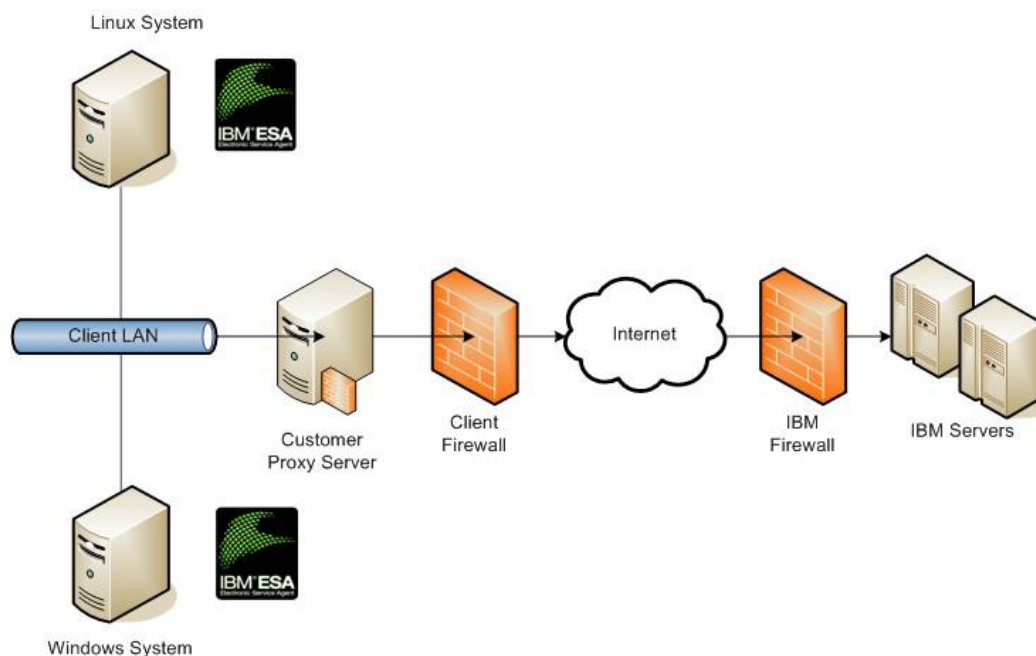
On your firewall, you may choose to limit the specific IP addresses to which the ESA system can connect. Section [IBM Server Address List](#) contains the list of IP addresses and ports of the IBM servers.

Outbound Connectivity with your Proxy Server

The following diagram shows the ESA for Linux and Windows 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 HTTP/1.1. Optionally, basic proxy authentication may be configured so that the ESA authenticates before attempting to forward packets through your proxy server.



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) may be configured so that the ESA authenticates before attempting to forward packets through your proxy server.

Configuring ESA to use a Proxy Server

Connecting IBM Electronic Service Agent through the IBM Service and Support proxy or your HTTP proxy can be fast and easy from your business network, and minimizes the number of systems that are directly connected to the Internet.

You can use the ESA web user interface to configure your service connection. You can also use the **esacli connectionSettings** command to configure your service connection. For information on how to configure service connection, see [Electronic Service Agent for Linux and Windows 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,

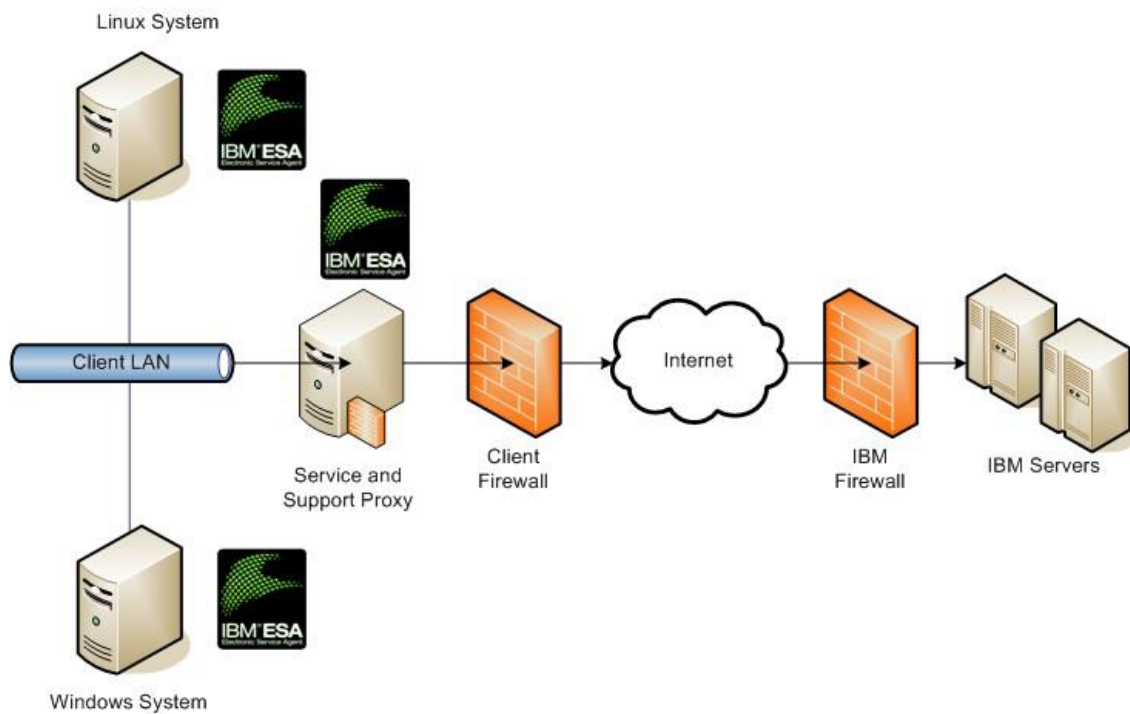
IBM Electronic Service Agent establishes a TLS Internet connection between the proxy and the IBM Electronic Support SDC. This connection is authenticated using the system ID and password that is previously created.

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 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 Linux & Windows system that is connected to IBM using the Service and Support proxy server supplied by ESA.



Configuring the ESA supplied Service and Support Proxy Server

You can use the ESA web user interface to create the IBM Service and Support proxy server. You can also use the `esacli supportProxySettings` command to create the IBM service and support proxy. For information on how to configure ESA supplied service and support proxy server, see [Electronic Service Agent for Linux and Windows User's Guide](#).

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 to a backup server.

When you have completed configuration of your connectivity settings, test for connectivity to IBM. For information on how to test connectivity to IBM, see [Electronic Service Agent for Linux and Windows 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 a new configuration information when an appropriate HTTPS path cannot be established. Your data is never uploaded using the HTTP protocol.

HTTPS is achieved by encapsulating the HTTP application protocol with the Transport Layer Security (TLSv1) cryptographic protocol.

IPv6 support

Call home does not fully support the IPv6 protocol at this time.

Communication between your browser and the ESA daemon

The ESA web user interface (default port is 5024) uses the HTTPS protocol for securing administrative requests between your browser and the ESA subsystem (daemon) running within Linux or Windows.

HTTPS is achieved by encapsulating the HTTP application protocol with the Transport Layer Security (TLSv1) cryptographic protocol.

ESA Web User Interface Authentication

The ESA Web User interface uses the Pluggable Authentication Module (PAM) to authenticate users. ESA uses the PAM login service definition found in the `/etc/pam.conf` file.

Communication between ESA and Integrated Management Module

Electronic Service Agent (ESA) uses an Integrated Management Module (IMM) to monitor the ESA installed system. ESA will register with the IMM to receive notification of hardware failure events. ESA first attempts to establish a secure HTTPS on port 5989 to the IMM and uses HTTP on port 5988 when HTTPS is not available. HTTPS is achieved by encapsulating the HTTP application protocol within either the Transport Layer Security (TLSv1) cryptographic protocol.

Service information sent to IBM

This section outlines what Service information is sent to IBM.

Data Sent to IBM

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

Table 1: Data sent to IBM from ESA

Reason	Description
Serviceable hardware problem	When a serviceable hardware problem occurs on a monitored endpoint system, Electronic Service agent automatically transmits this data to IBM support.
Dynamic System Analysis	<p>When a serviceable hardware problem occurs on a monitored endpoint system, Electronic Service Agent automatically detects the problem and collects Dynamic System Analysis data from the monitored endpoint system.</p> <p>Electronic Service Agent automatically transmits DSA data to IBM support for diagnostic purposes. Dynamic System Analysis collects information about the following aspects of a system, if applicable:</p> <ul style="list-style-type: none">• System configuration• Installed packages• Kernel Modules• Network interfaces and settings• Performance data and details for running processes• Hardware inventory, including PCI and USB information• IBM LightPath status• Service Processor status and configuration• Vital product data, firmware, and basic input/output system (BIOS) information• Drive Health Information• ServeRAID configuration• LSI RAID and controller configuration• Event logs for the operating system, ServeRAID controllers, and service processors

	For more information on IBM Dynamic System Analysis (DSA) see http://www.ibm.com/support/entry/portal/docdisplay?lnodocid=SERV-DSA
Inventory	Electronic Service Agent collects and transfers inventory data. ESA collects data about the hardware and software that is currently installed such as physical, logical, and virtual hardware, software applications, and operating systems. ESA automatically transmits inventory to IBM support in regularly scheduled intervals. ESA collects networking configuration information including IP addresses.
System Status Updates	Electronic Service Agent collects and transmits regularly scheduled status updates to IBM support. These reports provide IBM support with high-level information on the health and status of monitored endpoint systems.

Data retrieved from IBM by ESA

ESA downloads program updates from IBM using secure connections. The list of program updates includes:

- ESA updates
- Dynamic System Analysis updates

Appendix

IBM Server Address List

The IP addresses listed in the table below can change over time. Using DNS names is recommended to avoid IP address change issues. The following IP addresses and ports are used by ESA:

Table 2: Default ports used by ESA

IP address	Port	Host name	Purpose
207.25.252.197	443	eccgw01.boulder.ibm.com	Service information reporting
129.42.160.51	443	eccgw02.rochester.ibm.com	Service information reporting
129.42.26.224	443	www-945.ibm.com	Problem reporting
129.42.50.224	443	www-945.ibm.com	Problem reporting
129.42.42.224	443	www-945.ibm.com	Problem reporting
170.225.15.41	443	www6.software.ibm.com	Extended error data and system configuration reporting
192.109.81.20	443	www.ecurep.ibm.com	Extended error data and system configuration reporting
204.146.30.17	80,443	www-03.ibm.com	Configuration updates
129.42.54.216	80, 443	www.ibm.com	Configuration updates
129.42.56.216	80, 443	www.ibm.com	Configuration updates
129.42.60.216	80, 443	www.ibm.com	Configuration updates

© IBM Corporation 2015

IBM Corporation

Marketing Communications

Systems Group

Route 100

Somers, New York 10589

Produced in the United States of America

July 2015.

All Rights Reserved

This document was developed for products and/ or services offered in the United States. IBM may not offer the products, features, or services discussed in this document in other countries.

The information may be subject to change without notice. Consult your local IBM business contact for information on the products, features and services available in your area.

All statements regarding IBM future directions and intent are subject to change or withdrawal without notice and represent goals and objectives only.

IBM, the IBM logo, System x are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both. A full list of U.S. trademarks owned by IBM may be found at <http://www.ibm.com/legal/copytrade.shtml>.

Other company, product, and service names may be trademarks or service marks of others.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

This equipment is subject to FCC rules. It will comply with the appropriate FCC rules before final delivery to the buyer.

Information concerning non-IBM products was obtained from the suppliers of these products.

Questions on the capabilities of the non-IBM products should be addressed with the suppliers.

The IBM home page on the Internet can be found at <http://www.ibm.com>.

The IBM System x home page on the Internet may be found at <http://www.ibm.com/systems/x>.

PSW03007-USEN-00