



Getting Started with ArcSight Logger™

The Logger appliance package includes rack installation instructions, which you can use to rack mount your appliance. Refer to this guide to configure your Logger appliance and connect to it for the first time.

The *ArcSight Logger Administrator's Guide* explains in detail how to deploy, configure and use ArcSight Logger. The Administrator's Guide (in Adobe Acrobat form) is available from ArcSight Logger online help and as a download from the ArcSight Customer Support site <https://support.arcsight.com>.

Installation Instructions

1. Unpack the appliance and its accompanying accessories.
2. Follow the rack installations instructions to securely mount it.
3. Make the rear panel connections.
4. Power-on the appliance.
5. Once you have verified the unit is operational, power-off the unit and continue to the Initialization section.

CAUTION

Read through the instructions, cautions, and warnings in the *Product Information Guide* carefully. Failing to do so can result in bodily injury or appliance malfunction.

Initialization

Before logging in to ArcSight Logger for the first time, the unit must be initialized with at least one valid IP address. There are three ways to accomplish this:

- A. Attach a terminal to the serial port on ArcSight Logger and use the Command Line Interface to change the default IP addresses (see section A: Initialize ArcSight Logger using the CLI and a Terminal); or
- B. Attach a monitor and keyboard to the rear panel connectors and use the Command Line Interface to change the default IP addresses (see section B: Initialize ArcSight Logger using the CLI and a Monitor); or
- C. Configure a host to be a subnet that matches the predefined ArcSight Logger IP (192.168.35.35), such as 192.168.35.10 and use a browser from that host to log in and change the default IP (see section C: Using a Browser to initialize ArcSight Logger).

A. Initialize ArcSight Logger using the CLI and a Terminal

1. Connect a terminal to the serial port on ArcSight Logger using a null modem cable with DB-9 connector. The serial port expects a standard VT100-compatible terminal: 9600 bps, 8-bits, no parity, 1 stop bit (8N1), no flow control.
2. Turn it on and wait for it to boot up.
3. Enter user name and password (initially, admin/password), then 'set password' to set the default administrator user's password. You will be prompted to enter the current and new password.
4. Enter 'set ip eth0 <ip>/<prefix>', replacing <ip> with the IP address desired and <prefix> with the number of bits in the subnet mask (for example, /24 = 255.255.255.0).
5. Enter 'set hostname mydomain.mycompany.com', replacing mydomain.mycompany.com with the fully-qualified domain name (FQDN) of the desired host.
6. Enter 'set dns <search_domain_name1>,<search_domain_name2>,... <nameserver1> <nameserver2>', where each <search_domain_nameN> is a search domain, and each <nameserverN> is the IP address of a name server. Example: set dns mydomain1.mycompany.com,mydomain2.mycompany.com 192.0.2.1 192.0.2.2.
7. Enter 'set defaultgw <ip>', replacing <ip> with your default gateway IP address.
8. The preceding changes take effect immediately. To confirm that the settings are correct for your environment, enter 'show config'.

B. Initialize ArcSight Logger using the CLI and a Monitor

1. Connect a keyboard and monitor to the rear panel connectors on ArcSight Logger. Turn on ArcSight Logger and wait for it to boot up.
2. Enter user name and password (initially, admin/password), then 'set password' to set the default administrator user's password. You will be prompted to enter the current and new password.
3. Enter 'set ip eth0 <ip>/<prefix>', replacing <ip> with the IP address desired and <prefix> with the number of bits in the subnet mask (for example, /24 = 255.255.255.0).
4. Enter 'set hostname mydomain.mycompany.com', replacing mydomain.mycompany.com with the fully-qualified domain name (FQDN) of the desired host.
5. Enter 'set dns <search_domain_name1>, <search_domain_name2>, ... <nameserver1> <nameserver2>', where each <search_domain_nameN> is a search domain, and each <nameserverN> is the IP address of a name server. Example: 'set dns mydomain1.mycompany.com, mydomain2.mycompany.com 192.0.2.1 192.0.2.2'.
6. Enter 'set defaultgw <ip>', replacing <ip> with your default gateway IP address.
7. The preceding changes take effect immediately. To confirm that the settings are correct for your environment, enter 'show config'.

C. Using a browser to initialize ArcSight Logger

1. Attach ArcSight Logger to a network. Turn it on. Attach a network addressable computer to the same network and configure it to be on the same subnet as the default IP address of ArcSight Logger (192.168.35.35).
2. Open Flash-enabled browser (Microsoft Internet Explorer 6.0/7.0, or Firefox 1.5 or later).
3. Type the default IP address of the ArcSight Logger into the browser URL:
https://192.168.35.35/
4. At the login screen, use the following credentials to login as the administrator:
 - a. Username = admin
 - b. Password = password
5. Click the **System Admin** tab, and then click **System Configuration**.
6. On the sub-menu, click **Settings** to expand the sub-menu. Then click **Platform**.
7. Click the **Network** tab and change the IP address, hostname, DNS address and default gateway.
 - a. Other network information can also be entered or changed at this time.
 - b. Click **Update Settings** to apply the changes.
8. On the sub-menu (under System Configuration), click **System Reboot**.
9. After Logger reboots, login again to verify that the network settings have been changed:
 - a. Use the new IP address to access the ArcSight Logger.
 - b. Confirm that the settings are correct for your environment.

After Initialization

ArcSight Logger is ready for use. Go to the *ArcSight Logger Administrator's Guide* to find out how to use the appliance to suit your needs. Also, please read the release notes (if available) for any late-breaking information. The release notes are available on the ArcSight Customer Support site at <https://support.arcsight.com>.

Customer Support

Phone: 1-866-535-3285 (North America)
+44 (0)870 141 7487 (EMEA)
E-mail: support@arcsight.com
Web: <https://support.arcsight.com>