

all IP1000[™]

User Guide





Information in this document is subject to change without notice.
© 2005 Arxceo Corporation, Huntsville, AL 35806. All rights Reserved.

Reproduction of this document in any manner whatsoever without written permission from Arxceo is strictly prohibited.

Trademarks used in this text: Arxceo, Ally IP1000, Tag-UR-IT, PnPro, NetFailOpen and the Arxceo logo are trademarks or registered trademarks of Arxceo Corporation. Microsoft and Windows Embedded XP are registered trademarks of Microsoft Corporation. Other brands, trademarks or trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Arxceo disclaims any proprietary interest in brands, trademarks and trade names other than its own.

Arxceo believes the information in this publication to be accurate as of its publication and is not responsible for inadvertent errors.

Table of Contents

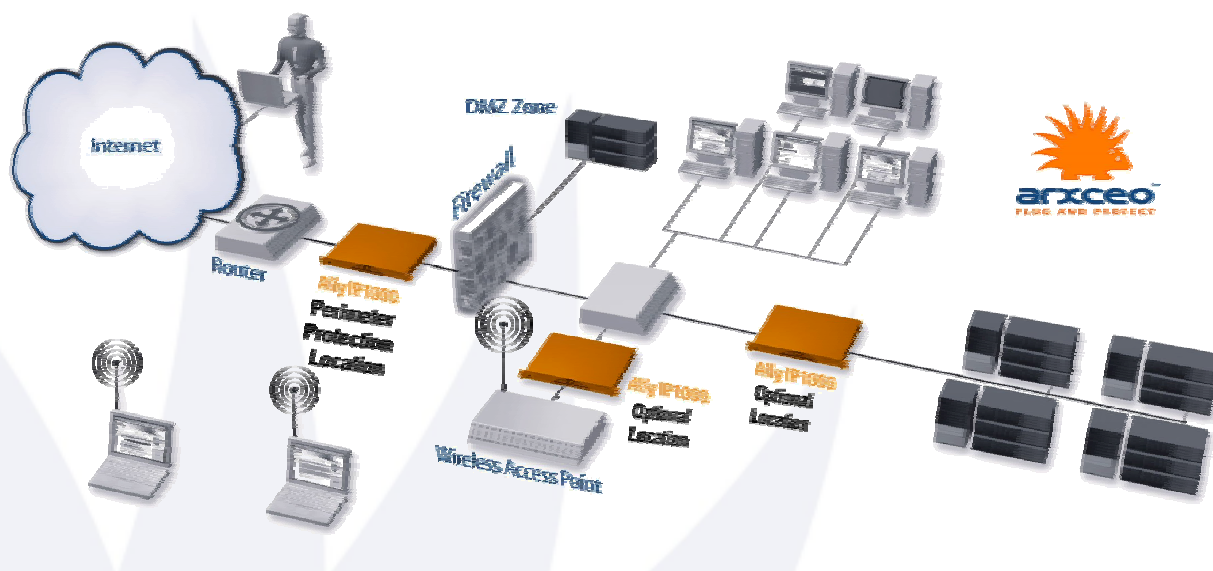
Ally IP1000 Placement	4
Connection	5
Ally IP1000 Back Panel	6
Management	7
Command Line Management	8
Confirmation	8
Intrusion Protection Information	10
Reviewing Intrusion Messages in the Event Log.....	12
Appendix A.....	13
Appendix B.....	18
Appendix C.....	25
Customer Support	29
Product Specifications.....	30
License Agreement.....	31

Congratulations on purchasing the Arxceo Ally IP1000™. The following steps will be your guide to Plug and Protect™ your valuable systems and data, simply and securely.

An Ally IP1000 is easy to install and typically requires very little configuration. However, the appliance can be extensively configured to allow for use in a wide variety of networks.

Ally IP1000 Placement

The following diagram illustrates the most common Ally IP1000 installation, appropriately called the **Perimeter Protection** position. As shown, the Ally IP1000 is on the perimeter of the network, in a position to evaluate incoming traffic prior to being passed to internal systems. This placement, between your router and existing firewall, allows the Ally IP1000 to provide anomaly detection and prevention to your organization's network. Additional security, such as thwarting worm propagation from infected internal systems, can be provided by deploying Ally products at common gateways or network traffic intersections.



In the Perimeter Protection position, there are only a few steps to perform to finalize the Ally IP1000 configuration for your specific environment. *If you are installing in a configuration different from the Perimeter Protection position, please contact your Arxceo authorized reseller or Arxceo Technical Support if you have any questions about the installation.*

NOTE: As you begin the Ally IP1000 installation, there will be a brief Internet service outage while the Ally IP1000 is being inserted into the network. However, the NetFailOpen™ technology within the appliance will allow Internet communication to resume as soon as the Ally IP1000 network cables are properly connected, even though the appliance has not been powered on. Depending on your particular network policies and/or Service Level Agreements (SLA's), Arxceo recommends that the network outage be communicated to all users prior to beginning the installation procedure.

Connection

The first step in protecting your environment is to connect the Ally IP1000 to the network. Each connector is detailed in the diagram and table below.

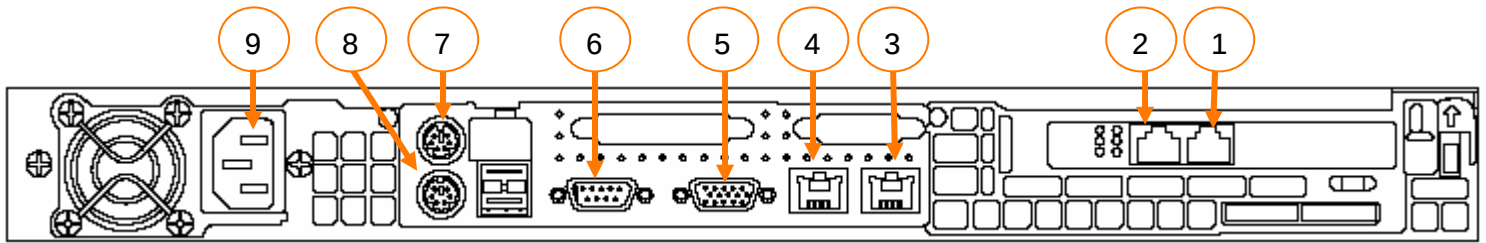
BEFORE YOU BEGIN – NetFailOpen Cabling Requirements: The Ally IP1000 NetFailOpen feature ensures network traffic will continue flowing in the case of a system component failure or power loss. If such a failure occurs, Network Adapters 1 and 2 (as shown in the diagram below) automatically bridge the two networks together and continue passing traffic, ***without providing protection***, while the problem is being resolved.

NetFailOpen only becomes activated when the Ally IP1000 is not operable; therefore, you will not receive a notification alerting you that network traffic is continuing without active protection being applied by the appliance. If you prefer to have all network traffic stop during a failure, use Adapters 3 and 4 as the Outside and Inside Adapters. In this case you will need to change the software Network Adapter Configuration to match this physical setup by using either the Ally Management Console or the command line interface.

To make certain this feature will function correctly it is important to ensure that network traffic passes through the Ally IP1000 while it is powered off. This requires selecting the proper cables to connect the appliance to the network. Typically, you should use a straight-through cable when connecting an Ally IP1000 network adapter to a switch and a crossover cable when connecting directly to another appliance such as a firewall or router.

When the Ally IP1000 is powered on, Network Adapters 1 and 2 automatically sense the type of cable used and modify their internal configuration as needed to provide network communication. However, this auto-sensing capability is lost when the appliance is powered off. Therefore, you must not assume that the NetFailOpen feature will keep your network operational in the event of an Ally IP1000 system failure unless you have verified that network communication continues when the appliance is powered off.

Using the following diagram and table, insert the Ally IP1000 into your network.



Ally IP1000 Back Panel

Ally IP1000 Back Panel Connectors		
Connector		Description
1	Network Adapter 1 "Outside" Adapter	Connect this network interface to your "outside" Internet access point.
2	Network Adapter 2 "Inside" Adapter	Connect this network interface to your "inside" LAN.
3	Network Adapter 3 "Management" Adapter	Connect this network interface, preferably to an out-of-band management network, to allow remote Ally IP1000 configuration and to send SNMP alerts and/or Syslog messages to a centralized network management facility. NOTE: Many of our customers want to be able to re-configure, monitor and manage the Ally IP1000 from a remote location, such as their office. However, like any product on the market, allowing remote access from a public network to the management interface of a network security device such as the Ally IP1000 introduces a potential point of attack. The Ally IP1000 Inside and Outside Adapters do not use an IP or MAC address. This unique approach helps protect the Ally IP1000 and your network from attacks. However, the Ally IP1000 management interface utilizes a limited IP protocol stack to provide secure remote administration and reporting. Although this interface is protected by a number of Ally IP1000 security features, we recommend that you connect this port and the management ports of all your network security devices to an out-of-band (private) network. Many facilities have created an out-of-band network by installing an inexpensive switch and network cables between the server room and a few administrators' offices. This ensures better security while providing easier remote access for administrators.
4	Network Adapter 4	This network interface is not used in the default Perimeter Protection configuration.
5	Monitor Connector	Optionally, connect a monitor here to manage the Ally IP1000 from a local console.
6	Not in Use	
7	Mouse Connector	Optionally, connect a mouse/pointing device here.

Ally IP1000 Back Panel Connectors		
	Connector	Description
8	Keyboard Connector	Optionally, connect a keyboard here.
9	Power Cord Connector	Plug the enclosed power cord here.

Once the desired connections have been made, determine that network traffic is flowing through the Ally IP1000 while it is powered off. Adjust the cabling configuration, if necessary, until network communication is restored. Then apply power to the Ally IP1000.

Management

The Ally IP1000 is managed through a graphical user interface (GUI), called the Ally Management Console. The GUI provides a convenient, secure portal for remotely managing the configuration settings or for viewing the Ally IP1000's event log, blacklists, and statistics counters. The Ally Management Console can be accessed through the Management Adapter from a remote web browser or from a locally attached monitor, keyboard, and mouse. (A command line interface is also available. This interface provides access to most, but not all, of the features provided by the Ally Management Console.)

Connecting to the Ally Management Console from Another System on the Administrative (or out-of-band) Network:

- 1) Temporarily change the IP address and subnet mask of another system on your out-of-band management network to 10.x.x.x, 255.0.0.0 (Do not use 10.1.2.3)
- 2) Key in <https://10.1.2.3> into the URL address field of the web browser on the system used in step 1. This address references the Ally IP1000 Management Adapter's default IP address preset by Arxceo, prior to shipment.
- 3) Login as Username: administrator
Password: arxceo
- 4) The first time the Ally Management Console is accessed, you will be required to accept the End User License Agreement (EULA). If you do not accept the terms of the EULA, the product will pass network traffic without providing protection.
- 5) Select the "Login Account Management" page on the Ally Management Console. Use the "Change Password" command to change the administrator account password.
- 6) Select the Ally Management Console "Network Adapter Configuration" page. Set the Management Adapter IP address, subnet mask, and other IP configuration information as appropriate for your out-of-band administrative network, or enable automatic configuration through DHCP if desired. Select "Apply". This will cause the web browser system to lose access to the Ally IP1000 if you have changed the IP address to match your out-of-band address scheme.
- 7) Reset the IP address and subnet mask of the system used in Step 1 back to the original address. All systems, including the Ally IP1000, should now be assigned appropriate IP addresses used by your organization.
- 8) Now you can use the system from Step 1 to reconnect to <https://xxx.xxx.xxx.xxx>, where xxx.xxx.xxx.xxx is the new address of the Ally IP1000.

Accessing the Ally Management Console from a Local Console:

- 1) Attach a monitor, keyboard, and mouse to the Ally IP1000
- 2) Login as Username: administrator
Password: arxceo
- 3) At the command prompt, enter "AllyMC" to run the Ally Management Console.
- 4) Login as Username: administrator
Password: arxceo
- 5) The first time the Ally Management Console is accessed, you will be required to accept the End User License Agreement (EULA). If you do not accept the terms of the EULA, the product will pass network traffic without providing protection.

- 6) Select the “Login Account Management” page on the Ally Management Console. Use the “Change Password” command to change the administrator account password.

Command Line Management

Most of the functions provided by the Ally Management Console are available through these command line programs: AllyRTCfg, AllyAgentCfg, AllyEvent, AllyClearLog, AllySetIP, AllyTime, AllyReboot, and AllyShutdown. As mentioned above, the Ally Management Console can be started with the AllyMC command.

Enter these commands at the command prompt with the argument -? to view the available options.

NOTE: *The first time you execute one of the Ally command line programs you will be required to accept the End User License Agreement (EULA), unless it has been previously accepted from the Ally Management Console. If you do not accept the terms of the EULA, the product will pass network traffic without providing protection.*

For best security practice, be sure to run the Ally Management Console and add a password to the administrator account.

Before leaving the local console unattended, logout of the system by entering the “logout” command in the command window. This will password protect the console.

Confirmation

The next step to Plug and Protect™ is to ensure no known, or trusted, IP Address has been “blacklisted” based on the default Ally IP1000 configuration. Once the Ally IP1000 has been online for approximately two minutes, perform the following from the Ally Management Console or from the command line window:

Ally IP1000 Command	What Happens?
View the Ally Management Console “Blacklist” page. Or enter the following command at the local console: AllyRTCfg –blacklist	Display Current Blacklist: This command displays the currently “blacklisted” IP Addresses and identifies whether the address was detected on the “inside” or “outside” network. Blacklisted IP Addresses should be reviewed to verify if they are “trusted”. If a Trusted IP Address appears in this list, the next command in this table should be used to place it on the “whitelist”. This will allow the node to continue to function properly while analysis to determine why it was “blacklisted” occurs. If the IP Address is not a Trusted IP Address, then the “blacklisted” entry should remain on the blacklist, with no further actions to be taken.

Ally IP1000 Command

What Happens?

Use the Ally Management Console “Blacklist” page to add a Trusted IP Address to the Inside or Outside “Whitelist” according to the location of the Trusted IP Address. Or enter the following command at the local console: AllyRTCfg –apwhitelist xx.xxx.xx.xxx INOUT <i>where xx.xxx.xx.xxx is replaced with the Trusted IP Address from the “blacklist” and INOUT is replaced with 1 for the Inside Adapter or 0 for the Outside Adapter to indicate the location of the Trusted IP address. In the normal installation, the INOUT value is almost always “1”.</i>	Add Trusted IP Address to Permanent Whitelist: This command automatically removes the IP Address from the “blacklist” and adds the IP Address to the permanent “whitelist” for the Inside or Outside Adapter. <i>It is important to remember there are separate blacklists and whitelists for both the Outside and Inside adapters.</i>
---	---

Arxceo recommends performing the following three steps as a component of your scheduled systems security maintenance:

1. **Review Blacklist:** Perform the steps listed above in order to see IP Addresses that have been blacklisted.
2. **Review Ally IP1000 Statistics:** The current Ally IP1000 statistics counters can be viewed from the Ally Management Console “Statistics” page or by entering the “AllyRTCfg – stats” command at the local console.
3. **Review Ally IP1000 Event Log:** The Ally IP1000 records security events and configuration information in the system event log. The event log can be viewed from the Ally Management Console “Event Log” page or by entering the “AllyEvent” command at the local console.

Additionally, whenever a trusted IP address, or system, seems to have lost network access, review the blacklist as described above. Ally IP1000 Intrusion Protection Messages indicating when and why an IP address was blacklisted will be found in the event log.

Intrusion Protection Information

The Ally IP1000 is now protecting your network and will provide protection message information on a variety of intrusions. The following table lists and describes each type of intrusion and details the protections provided through the default Ally IP1000 configuration.

Intrusions Prevented Automatically by Default	
Area	Description and Protection
SYN or ACK Denial of Service (DoS) Attacks	By default, the Ally IP1000 is configured to stop ACK floods and prevent SYN floods from getting to any computer protected by the Ally appliance. SYN requests arrive first, and the Ally IP1000 responds in place of the destination server with a Tag-UR-IT marked SYN/ACK and then waits for the responding ACK. Only ACK responses that contain the matching Tag-UR-IT mark are permitted beyond the appliance. Therefore, false ACK traffic is dropped. In this fashion, SYN floods are reflected by the Ally appliance, which merely marks the packets, rather than keeping track of state (session) information. State information is recovered from the ACK packet, which contains the Tag-UR-IT mark. The Ally device can be configured to detect SYN floods, rather than ACK floods. However, it is possible for an attacker to create false blacklists of 'good' IP addresses if they can determine that you are blacklisting on SYN requests, rather than ACK responses.
IP Fragments	Due to physical differences between various networking hardware, IP packets may be broken into various fragments when routed on the Internet. Endpoint devices rarely have the requirement to support fragmented packet reassembly. Originally, fragments were defined within the standard to be held by the destination device and put together once the rest of the transmission arrived. This method of reassembling fragments at the destination device has been exploited by numerous network attacks. With today's robust networking gear, the only fragmented traffic that is typically seen is intentional fragmentation by attackers trying to sneak exploits past signature-based detection devices.
Unknown Packet Types	By default, 'unknown' packet types are not discarded by the Ally IP1000. Enabling the dropping of these packets prevents unknown packet types from entering your network. However, these types include legacy protocols and services such as IPX/SPX (Novell network) and native Microsoft NetBios (unless it's encapsulated within TCP/IP).
DNS Cache Poisoning	DNS cache poisoning is prevented by default by the Ally appliance. This feature prevents false DNS resolution replies from entering your network.
DNS Tunneling	The use of the DNS protocol for anything other than DNS resolutions is prevented by default. As an example, a user could set up a system to use DNS for web surfing unless this feature is enabled.

Intrusions Prevented Automatically by Default	
Area	Description and Protection
Information Leakage	Previously transmitted data is often used by network cards to fill in non-required fields or to increase packet sizes to meet the required minimum frame size of various protocols. For instance, Ethernet packets must be at least 64 bytes in length. Packets that are shorter than this required minimum are padded with a previous transmission's data to create a 64 byte packet length. Therefore, confidential information on the inside of your LAN that has been accessed correctly, and without encryption, can be sent out to the Internet on the next DNS resolution request, as one example. ALLY IP1000 changes the content of all bytes beyond the exact size required, or within non-required fields, in order to prevent data leakage.
Network Reconnaissance: IP Address Discovery; TCP Port Discovery; UDP Port Discovery; OS Fingerprinting	A critical part of an attacker's network reconnaissance is to determine what addresses, ports, operating systems and firewall devices are used in your network. The Ally IP1000 prevents address discovery, port discovery, bounce-scanning and other types of network recons by default.
IP Spoofing	Attackers frequently change their packets to show a different IP address than the one they are actually using. For connection-oriented sessions, such as HTTP and TCP/IP, the Ally appliance prevents any connection into the network unless the original source IP address remains unchanged throughout the session. For example, only ACK responses that match the originator's IP address from the initial SYN request are allowed into the network.
Resource Flooding & Denial of Service (DoS)	The Ally IP1000 protects against DoS and its variants along with illegitimate large amounts of traffic intended to overload a system to an extent it is unable to respond to legitimate traffic. Examples of DoS and other resource floods that are thwarted by the Ally IP1000 are: SYN; SYN/ACK; ACK; RESET; 3-way connection 'hogs' (handshake takes place, but no data sent); Invalid TCP packets; and Open Idle Connections.
Session Hijacking: Initial Sequence Number (ISN) Guessing; IPID Guessing	Session hijacking involves brute force methods to attempt to match an existing ISN, IPID, and other fields within the IP and TCP header. By default, the Ally IP1000 hardens, encrypts and randomizes many of the IP and TCP fields to prevent session hijacking. Windows XP nodes sitting behind a typical firewall have a 12% likelihood of being hijacked. With an Ally IP1000 in place, this likelihood drops to a 0.00001% chance of success.
Worm Mitigation	Worms typically propagate by scanning for the next target victim. The Ally IP1000 detects these scans and blacklists the offending node and drops any further traffic from that node. Therefore, worm propagation is stopped from coming into your network by default.

Reviewing Intrusion Messages in the Event Log

Based on the Ally IP1000 default configuration (described in Appendix B), certain Ally IP1000 Intrusion Protection Messages will be written to the system event log. This log can be viewed as described below. Appendix A contains a complete listing of the Ally IP1000 intrusion protection messages.

Use the Ally Management Console “Event Log” page to view the most recent 100 event log messages. You may also use the “Save to File” command on that page to save the **entire** event log to a file on the local system that is running the web browser.

The command line program, AllyEvent, can be run from the local console to view the most recent 100 event log messages. Additionally, the Ally IP1000 event log messages can be viewed on the local console using the Windows Event Viewer.

To access the Windows Event Viewer,

1. At the Ally IP1000 console, enter “eventvwr”
2. The Windows Event Viewer will be displayed.
3. Click on the “System” log.

Ally IP1000 messages can be identified by the word “Ally” in the SOURCE column. The Ally IP1000 Message Number will be in the EVENT column. Message details can be viewed by clicking on the message.

NOTE: For security reasons, this Event Log cannot be interpreted on a machine other than an Ally IP1000.

The Ally IP1000 can also be configured to transmit SNMP alerts and/or Syslog messages to a centralized network management facility through the Ally IP1000 management adapter. More details are available in the help messages displayed in the Ally Management Console.

Appendix A

Ally IP1000 Notification Message Types

The Ally IP1000 records configuration information and intrusion protection notifications in the system event log. The table below lists each message that may be generated by the Ally IP1000. The number and the associated Message Content text will appear in the event log entry.

The *italicized text* found below in each Message Content table entry indicates variable information that will appear in the event log message. For example, in Message Number 6 – Incomplete Connection Timeout, either ‘are’ or ‘are not’ will be displayed, depending on the “Log Connection Resets” configuration parameter setting.

The Type column assigns a brief name to each message. This name is used to reference the message in the Ally IP1000 documentation, but does not appear in the actual event log entry. The Type column also assigns the message to one of four general message categories: Configuration, Configuration Event, Detection and Information. Configuration and Configuration Event messages are always written to the event log while Detection and Information messages can be optionally disabled.

Ally IP1000 Notification Message Types		
Message Number - Type		Message Content
1	Configuration Inside and Outside Adapters	(Device ALLY) has been started. Network adapter (Network Adapter Number) is assigned to handle inside network traffic. Network adapter (Network Adapter Number) is assigned to handle outside network traffic.
2	Configuration Management Adapter	Network adapter (Network Adapter Number) is assigned to handle management traffic. Outbound connection requests (<i>‘are’</i> or <i>‘are not’</i>) blocked. Discarded outbound connection requests (<i>‘are’</i> or <i>‘are not’</i>) logged.
3	Configuration Mode	(Device ALLY) is currently in (<i>‘Pass Through (Inactive)’</i> or <i>‘Filter (Active)’</i>) mode.
4	Configuration Inside Authentication	Authentication of the source IP address for an inside-to-outside session request (<i>‘is’</i> or <i>‘is not’</i>) performed (<i>‘for the first connection only’</i> or <i>‘for all connections’</i> or <i>‘’</i>).
5	Configuration Outside Authentication	Authentication of the source IP address for an outside-to-inside session request (<i>‘is’</i> or <i>‘is not’</i>) performed (<i>‘for the first connection only’</i> or <i>‘for all connections’</i> or <i>‘’</i>).
6	Configuration Incomplete Connection Timeout	Incomplete TCP connections will timeout in (Connection Timeout Number) seconds. Connection resets (<i>‘are’</i> or <i>‘are not’</i>) logged.
7	Configuration Maximum Concurrent Connections	Up to (Maximum Number of Connections) concurrent (<i>‘inside-to-outside’</i> or <i>‘outside-to-inside’</i>) connections from the same source IP address to one destination IP address and port are allowed.
8	Configuration Idle Connection Timeout	Idle connections will timeout in (Idle Connection Timeout Number) seconds.

Ally IP1000 Notification Message Types		
Message Number - Type		Message Content
9	Configuration IP Fragment Policy	Fragmented packets are ('passed through without analysis' or 'discarded'). If discarded, fragmented packets ('are' or 'are not') logged.
10	Configuration Log Invalid TCP Flags	Packets with invalid TCP flags ('are' or 'are not') logged.
11	Configuration Log Invalid TCP Option	Packets with invalid TCP options ('are' or 'are not') logged.
12	Configuration Prevent Data Leaks	Packet pad bytes ('are' or 'are not') scrubbed to prevent data leaks.
13	Configuration Port Scan Detection	TCP port scan detection is based on the ('SYN' or 'ACK') packet received during the three-way handshake of the connection request. IP address blacklisting due to port scan detection ('is' or 'is not') enabled on the inside adapter and ('is' or 'is not') enabled on the outside adapter.
14	Configuration Inside Port Scans	On the inside adapter, (<i>Inside Scan Number</i>) connection requests received from the same IP address in (<i>Inside Scan Timeout Number</i>) seconds will cause that IP address to be placed on the inside adapter's blacklist.
15	Configuration Outside Port Scans	On the outside adapter, (<i>Outside Scan Number</i>) connection requests received from the same IP address in (<i>Outside Scan Timeout Number</i>) seconds will cause that IP address to be placed on the outside adapter's blacklist.
16	Configuration Blacklist Time Period	An IP address will remain on the blacklist for (<i>Blacklist Time Period Number</i>) seconds. Blacklisting events ('are' or 'are not') logged.
17	Configuration TCP Policy	TCP packets are ('passed through without' or 'handled according to policy' or 'discarded without') analysis.
18	Configuration ARP Policy	ARP packets are ('passed through without' or 'handled according to policy' or 'discarded without') analysis. If discarded, ARP packets ('are' or 'are not') logged.
19	Configuration ICMP Policy	ICMP packets are ('passed through without' or 'handled according to policy' or 'discarded without') analysis. If discarded, ICMP packets ('are' or 'are not') logged.
20	Configuration UDP Policy	UDP packets are ('passed through without' or 'handled according to policy' or 'discarded without') analysis. If discarded, UDP packets ('are' or 'are not') logged.
21	Configuration Other IP Policy	Other IP packets are ('passed through without' or 'handled according to policy' or 'discarded without') analysis.
22	Configuration Non-IP Non-ARP Policy	Packets that are not IP and are not ARP are ('passed through without' or 'handled according to policy' or 'discarded without') analysis.
23	Configuration ICMP Echo Request Policy	ICMP Echo packets are ('passed through without analysis' or 'discarded').

Ally IP1000 Notification Message Types		
Message Number - Type		Message Content
24	Configuration ICMP Echo Reply Policy	ICMP Echo Reply packets are ('passed through without analysis' or 'discarded').
25	Configuration ICMP Destination Unreachable Policy	ICMP Destination Unreachable packets are ('passed through without analysis' or 'discarded').
26	Configuration ICMP Port Unreachable Policy	ICMP Port Unreachable packets are ('passed through without analysis' or 'discarded').
27	Configuration ICMP Source Quench Policy	ICMP Source Quench packets are ('passed through without analysis' or 'discarded').
28	Configuration ICMP Redirect Policy	ICMP Redirect packets are ('passed through without analysis' or 'discarded').
29	Configuration ICMP Time Exceeded Policy	ICMP Time Exceeded packets are ('passed through without analysis' or 'discarded').
30	Configuration ICMP Parameter Problem Policy	ICMP Parameter Problem packets are ('passed through without analysis' or 'discarded').
31	Configuration ICMP Timestamp Request Policy	ICMP Timestamp packets are ('passed through without analysis' or 'discarded').
32	Configuration ICMP Timestamp Reply Policy	ICMP Timestamp Reply packets are ('passed through without analysis' or 'discarded').
33	Configuration ICMP Information Request Policy	ICMP Information Request packets are ('passed through without analysis' or 'discarded').
34	Configuration ICMP Information Reply Policy	ICMP Information Reply packets are ('passed through without analysis' or 'discarded').
35	Configuration ICMP Address Mask Policy	ICMP Address Mask Request packets are ('passed through without analysis' or 'discarded').
36	Configuration ICMP Address Mask Reply Policy	ICMP Address Mask Reply packets are ('passed through without analysis' or 'discarded').
37	Configuration ICMP Traceroute Policy	ICMP Traceroute packets are ('passed through without analysis' or 'discarded').
38	Configuration ICMP Conversion Error Policy	ICMP Conversion Error packets are ('passed through without analysis' or 'discarded').
39	Configuration ICMP Domain Name Policy	ICMP Domain Name Request packets are ('passed through without analysis' or 'discarded').
40	Configuration ICMP Domain Name Reply Policy	ICMP Domain Name Reply packets are ('passed through without analysis' or 'discarded').
41	Configuration DNS Policy	DNS packets are ('handled according to policy' or 'discarded without') analysis. If discarded, DNS packets ('are' or 'are not') logged.
42	Configuration DNS Tunneling Detection	DNS tunneling detection is ('enabled' or 'disabled'). If enabled, (Number of DNS Tunnel Packets) tunnel packets in (DNS Tunnel Timeout Number) seconds will cause the originating IP address to be blacklisted.
43	Configuration DNS Cache Poisoning Detection	DNS cache poisoning packets ('are' or 'are not') discarded.
44	Configuration Maximum Segment Size Range	The TCP Maximum Segment Size range has been set to (Numeric Value) - (Numeric Value).
45	Configuration Remote System Statistics Timeout	Remote system information is retained for (Numeric Value) seconds after verification.

Ally IP1000 Notification Message Types		
Message Number - Type		Message Content
46	Configuration Permanent Blacklist/Whitelist	The permanent blacklist and/or whitelist has been ('updated' or 'initialized').
47	Configuration Normal Start	Normal startup for the (Device ALLY) driver has completed.
48	Detection Dynamic Blacklist Add	The IP address (IP Address) was added to the ('inside' or 'outside') adapter's blacklist because ('port scanning' or 'DNS tunneling') was detected.
49	Detection Dynamic Blacklist Remove	The IP address (IP Address) has been removed from the ('inside' or 'outside') adapter's blacklist.
50	Information Connection Reset	The Connection from IP address (Source IP Address) port (Source Port) to (Destination IP Address) port (Destination Port) has been reset.
51	Detection Discard TCP Packet, Flags	A TCP Packet with flags (Hexadecimal Representation of TCP Flags) from IP address (Source IP Address) to (Destination IP Address) was discarded.
52	Detection Discard TCP Packet, Option	A TCP Packet with option (Hexadecimal Representation of TCP Option) from IP address (Source IP Address) to (Destination IP Address) was discarded.
53	Detection Discard Fragmented Packet	A fragmented packet from IP address (Source IP Address) to (Destination IP Address) with IP id (IP ID) was discarded.
54	Detection Discard Outbound Management	An outbound connection request packet on the management adapter was discarded.
55	Detection Discard ARP Packet	An ARP packet from IP address (Source IP Address) was discarded.
56	Detection Discard ICMP Packet	An ICMP ('echo (ping) reply' or 'destination unreachable' or 'port unreachable' or 'source quench' or 'redirect' or 'echo (ping)' or 'time exceeded' or 'parameter problem' or 'timestamp' or 'timestamp reply' or 'information request' or 'information reply' or 'address mask request' or 'address mask reply' or 'traceroute' or 'conversion errors' or 'domain name request' or 'domain name reply') packet from IP address (Source IP Address) to (Destination IP Address) was discarded.
57	Detection Discard UDP Packet	A UDP packet from IP address (Source IP Address) port (Source Port) to (Destination IP Address) port (Destination Port) was discarded.
58	Detection Discard DNS Packet	A DNS ('query' or 'response') packet from IP address (Source IP Address) to (Destination IP Address) was discarded because a possible DNS ('tunneling' or 'cache poisoning') attempt was detected.
59	Configuration Event Configuration Reload	('Console User' or User Name) reloaded the configuration from ('the factory default settings').

Ally IP1000 Notification Message Types		
Message Number - Type		Message Content
60	Configuration Event Set Adapter Number	(<i>'Console User'</i> or <i>User Name</i>) set the (<i>'inside'</i> or <i>'outside'</i> or <i>'management'</i>) adapter to network interface number <i>'Network Interface Number'</i> .
61	Configuration Event Set Management IP	(<i>'Console User'</i> or <i>User Name</i>) changed the management adapter to IP address (<i>IP Address</i>), netmask (<i>Mask</i>), gateway (<i>Gateway</i>), DNS1 (<i>DNS1</i>), DNS2 (<i>DNS2</i>).
62	Configuration Event Clear Statistics	(<i>'Console User'</i> or <i>User Name</i>) cleared the packet statistics.
63	Configuration Event Set SNMP/Syslog Agent Variable	(<i>'Console User'</i> or <i>User Name</i>) set the ALLY SNMP/Syslog agent's configuration variable (<i>Variable Name</i>) to (<i>New Variable Value</i>).
64	Configuration Event SNMP/Syslog Agent Reload	The ALLY SNMP/Syslog agent was directed to (<i>'reload its configuration'</i> or <i>'restart'</i>) by (<i>'Console User'</i> or <i>User Name</i>).
65	Configuration Event User Change	(<i>'Console User'</i> or <i>User Name</i>) (<i>'added'</i> or <i>'removed'</i> or <i>'changed'</i>) account (<i>User Name</i>).
66	Configuration Event Password Change	(<i>'Console User'</i> or <i>User Name</i>) changed his/her password.
67	Configuration Event Time Change	(<i>'Console User'</i> or <i>User Name</i>) changed the system time to (<i>Time</i>).
68	Configuration Event Reboot	(<i>'Console User'</i> or <i>User Name</i>) (<i>'rebooted'</i> or <i>'shutdown'</i>) the ALLY system.
69	Configuration Event Set Management DHCP	(<i>'Console User'</i> or <i>User Name</i>) changed the management adapter to a DHCP IP address.

Appendix B

Ally IP1000 Default Configuration Matrix

The matrix below identifies the Ally IP1000 configurable parameters, the default setting for each parameter, and the implication of each parameter setting to the overall intrusion protection system.

The Ally IP1000 can be configured through the Ally Management Console from a web browser or additionally through the AllyRTCfg command line program from the local console. The following table identifies the Ally Management Console page and the AllyRTCfg command line option associated with each configuration parameter.

Ally IP1000 Factory Default Configuration					
Configuration Parameter	Possible Settings	Default	Intrusion Implication	Mgmt. Console Page	AllyRTCfg Option
Pass Through Mode	▪ Enabled ▪ Disabled	Disabled	Enable Pass Through Mode to turn off the Ally IP1000 filter. All network traffic will simply be passed through without inspection or intervention. When Pass Through Mode is enabled the other Ally IP1000 configuration parameters are ignored and NO PROTECTION is provided.	General Filtering Options	-pt
IP Fragment Policy	▪ Discard All ▪ Allow All	Discard All	It is uncommon to find fragmented IP traffic on an internal network. These packets are sometimes used in malicious attacks. The Ally IP1000 can be configured to allow the propagation of IP fragments; however, the Ally never reassembles fragmented packets.	General Filtering Options	-df
Prevent Data Leaks	▪ Enabled ▪ Disabled	Enabled	Transmitted Ethernet packets must be at least 64 bytes in length; however, many packets contain less than that amount of actual header and data information. These short packets must be "padded" with additional bytes to fill the minimum packet size. Most systems do not specifically "zero out" these pad bytes. This practice produces data leaks. By default, the Ally IP1000 reinitializes all pad bytes before retransmitting a packet, erasing any leaked values.	General Filtering Options	-zp

Ally IP1000 Factory Default Configuration

Configuration Parameter	Possible Settings	Default	Intrusion Implication	Mgmt. Console Page	AllyRTCfg Option
Remote System Timeout	Any unsigned 32-bit integer	3600 seconds (1 hour)	The Ally IP1000 discovers information about systems on the both the outside and the inside networks through its analysis of network traffic. The "Retain Remote System Information" time value controls the length of time this information is retained for each system.	General Filtering Options	-sit
TCP Policy	▪ Discard All ▪ Analyze ▪ Allow All	Analyze	Selecting "Analyze" activates the TCP policy parameters, i.e. the next 12 entries in this table.	General Filtering Options	-at
Inside-to-Outside Address Authentication	▪ Disabled ▪ First Connection per Session ▪ All Connections	First Connect per Session	The Ally IP1000 Address Authentication feature guarantees that the source IP address contained in a TCP connection request is not spoofed. The Ally IP1000 verifies the requestor's address before forwarding the connection request to the intended recipient. There are three Address Authentication modes: All Connections, First Connection per Session, and Disabled. The Address Authentication mode is configured independently for connection requests received on the Inside Adapter (inside-to-	TCP Policy	-id
Maximum Number of Inside-to-Outside Concurrent Connections	Any unsigned 32-bit integer	150		TCP Policy	-mci
Outside-to-Inside Address Authentication	▪ Disabled ▪ First Connection per Session ▪ All Connections	All Connections		TCP Policy	-od

Ally IP1000 Factory Default Configuration

Configuration Parameter	Possible Settings	Default	Intrusion Implication	Mgmt. Console Page	AllyRTCfg Option
Maximum Number of Outside-to-Inside Concurrent Connections	Any unsigned 32-bit integer	150	outside) and for requests received on the Outside Adapter (outside-to-inside). Select the Address Authentication mode "All Connections" for maximum protection. This setting authenticates the source IP address in every connection request received on the associated interface. The Address Authentication mode may be set to "First Connection per Session" to increase the speed at which multi-connection sessions are established. This setting is especially useful when the applications communicating through the Ally create multiple connections from a specific source IP address to a single destination IP address and port number, e.g. web browsers. The "Maximum Number of Concurrent Connections" value is only referenced in the "First Connection per Session" mode. This value places a limit on the number of concurrent connections that can exist between a specific source IP address and a single destination IP address and port number.	TCP Policy	-mco
Incomplete Connection Timeout	5 – 25 seconds	5 seconds	An "incomplete" connection is one in which the TCP connection establishment three-way handshake process has not been completed. The Incomplete Connection Timeout value indicates the amount of time the Ally IP1000 will retain pending connection information.	TCP Policy	-ct

Ally IP1000 Factory Default Configuration

Configuration Parameter	Possible Settings	Default	Intrusion Implication	Mgmt. Console Page	AllyRTCfg Option
Idle Connection Timeout	0 = Never Timeout - Any other unsigned 32-bit integer	600 seconds (10 min)	An "idle" connection is an established TCP connection over which no traffic has been transmitted for some period of time. The "Idle Connection Timeout" value determines the amount of time a connection may be idle before the Ally resets that connection. Specify "0" to indicate that idle connections are to remain open indefinitely.	TCP Policy	-it
Inside Adapter Port Scan Prevention	- Enabled - Disabled	Disabled	Port Scan Prevention is one of the Ally IP1000 features designed to provide anti-reconnaissance protection. This feature limits the number of TCP connection requests from a specific source IP address that will be allowed to pass through the Ally over a specified time period. Systems that exceed the port scan threshold are added to the dynamic blacklist associated with the adapter on which the port scans were received. No further traffic from a dynamically blacklisted system is passed through the Ally until the "Blacklist Timeout" occurs. The Port Scan Prevention threshold is configured independently for the Inside and Outside Adapters. This threshold consists of a maximum number of connection requests received in a specified number of seconds.	TCP Policy	-si
Blacklist Due to Port Scanning on the Inside Adapter after Scans/Seconds	Any unsigned 32-bit integers	25/5		TCP Policy	-ssi -sti
Outside Adapter Port Scan Prevention	- Enabled - Disabled	Enabled		TCP Policy	-so
Blacklist Due to Port Scanning on the Outside Adapter after Scans/Seconds	Any unsigned 32-bit integers	25/5		TCP Policy	-sso -sto
Port Scan Method	- SYN - ACK	ACK	This option determines whether the Ally IP1000 will detect port scans by counting the number of initial TCP connection request packets (SYN) received from a system or the number of three-way handshake completion packets (ACK) received from that system. By default, the Ally uses the ACK packet for port scan detection.	TCP Policy	-psb

Ally IP1000 Factory Default Configuration

Configuration Parameter	Possible Settings	Default	Intrusion Implication	Mgmt. Console Page	AllyRTCfg Option
Maximum Segment Size Range	Any unsigned 32-bit integers	450 - 1460	During the establishment of a TCP connection the two communicating systems negotiate a Maximum Segment Size (MSS). This value determines the maximum packet size that will be transmitted during the conversation ($MSS + 40 =$ maximum packet size). The Ally IP1000 limits the MSS values to a specified range. This feature helps prevent an attacker from consuming excessive network resources by establishing connections that generate many very small packets.		-minmss -maxmss
UDP Policy	▪ Discard All ▪ Analyze ▪ Allow All	Analyze	Selecting "Analyze" activates the UDP policy parameters, i.e. the next 4 entries in this table.	General Filtering Options	-av
DNS Policy	▪ Discard All ▪ Analyze	Analyze	Domain Name Service (DNS) is a UDP based protocol. This is the protocol that converts domain names to IP addresses. Typically, DNS traffic should be allowed to pass through the Ally IP1000. Selecting "Analyze" activates the DNS sub-policy parameters, i.e. the next 3 entries in this table.	UDP Policy	-ad
DNS Cache Poisoning Detection	▪ Enabled ▪ Disabled	Enabled	Some systems accept DNS information that was not specifically requested. This allows an attacker to replace a legitimate name resolution with another address. This is referred to as DNS Cache Poisoning. It causes an unsuspecting system to connect to an imposter system instead of the intended destination.	UDP Policy	-dv

Ally IP1000 Factory Default Configuration

Configuration Parameter	Possible Settings	Default	Intrusion Implication	Mgmt. Console Page	AllyRTCfg Option
DNS Tunneling Detection	▪ Enabled ▪ Disabled	Enabled	There are applications that allow network conversations to be clandestinely established using DNS traffic. The Ally detects this DNS Tunneling by counting the number of DNS messages sent from a particular source IP address during a specified time period. Systems that exceed this threshold are added to the dynamic blacklist associated with the adapter on which these messages were received. No further traffic from a dynamically blacklisted system is passed through the Ally IP1000 until the "Blacklist Time Period" has elapsed.	UDP Policy	-dt
Blacklist Due to DNS Tunneling after DNS Packets/ Seconds	Any unsigned 32-bit integers	10/5	The DNS Tunneling threshold consists of a maximum number of DNS packets received in a specified number of seconds.	UDP Policy	-tc -tt
ICMP Policy	▪ Discard All ▪ Analyze ▪ Allow All	Analyze	Selecting "Analyze" activates the ICMP policy parameters, i.e. the next 12 entries in this table.	General Filtering Options	-ai
ICMP Echo Request Policy	▪ Discard All ▪ Allow All	Allow All	Select the types of ICMP packets that will be allowed to pass through the Ally IP1000. By default, all ICMP packet types are allowed except "Destination Unreachable" and "Port Unreachable". These packets are discarded to prevent UDP port scanning and certain Denial of Service (DoS) attacks.	ICMP Policy	-ec
ICMP Echo Reply Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-er
ICMP Source Quench Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-sq
ICMP Redirect Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-re
ICMP Time Exceeded Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-te
ICMP Parameter Problem Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-pp
ICMP Timestamp Request Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-ts
ICMP Timestamp Reply Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-tr
ICMP Information Request Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-ir
ICMP Information Reply Policy	▪ Discard All ▪ Allow All	Allow All		ICMP Policy	-ip

Ally IP1000 Factory Default Configuration

Configuration Parameter	Possible Settings	Default	Intrusion Implication	Mgmt. Console Page	AllyRTCfg Option
ICMP Destination Unreachable Policy	▪ Discard All ▪ Allow All	Discard All	Discard ICMP Destination Unreachable packets to prevent certain Denial of Service (DoS) attacks.	ICMP Policy	-du
ICMP Port Unreachable Policy	▪ Discard All ▪ Allow All	Discard All	Discard ICMP Port Unreachable packets to prevent UDP Port Scanning.	ICMP Policy	-pu
Other IP Policy	▪ Discard All ▪ Allow All	Allow All	Select "Discard All" to discard all "unknown" packet types, i.e. packets that are not TCP, UDP, or ICMP.	General Filtering Options	-au -aa
ARP Policy	▪ Discard All ▪ Allow All	Allow All	Address Resolution Protocol (ARP) is the protocol that converts IP addresses to MAC addresses. Typically, ARP traffic should be allowed to pass through the Ally IP1000.		
Non-IP Non-ARP Policy	▪ Discard All ▪ Allow All	Allow All	Select "Discard All" to discard traffic that is not IP or ARP based.	General Filtering Options	-ut
Blacklist Time Period	Any unsigned 32-bit integers	3600 seconds (1 hour)	This parameter specifies the amount of time an IP address suspected of TCP Port Scanning or DNS Tunneling will remain on the dynamic blacklist.	Blacklist	-bt
Management Adapter Outbound Connections	▪ Block ▪ Allow	Block	For additional security the Management Adapter is, by default, not allowed to establish outbound TCP connections. There are no applications installed on the Ally IP1000 that attempt to establish outbound connections.	Network Adapter Config.	-bm

Appendix C

Command Line Options for Notification Messaging

The Ally IP1000 records configuration information and intrusion protection notifications in the system event log. Additionally, the Ally IP1000 can be configured to transmit each event log message to one or two SNMP servers and one or two Syslog servers. To enable this feature, you must specify the IP address and SNMP Version or Syslog Level for each server using the Ally Management Console “Notification Options” page or the AllyAgentCfg command line program.

The table below lists each message that may be generated by the Ally IP1000. Each message type is identified by a Message Number that appears in the event log entry. The Type column assigns a brief name to each message. This name is used to reference the message in the Ally IP1000 documentation, but does not appear in the actual event log entry.

The Type column also assigns the message to one of four general message categories: Configuration, Configuration Event, Detection and Information. Configuration and Configuration Event messages are always written to the event log while Detection and Information messages can be optionally disabled. Use the Ally Management Console “Notification Messages” page or the AllyRTCfg command line program to enable or disable the generation of Detection and Information messages in the event log.

Any Ally IP1000 message that is written to the event log can be optionally sent to the configured SNMP and/or Syslog servers. The disposition of each message type can be individually specified. Use the Ally Management Console “Notification Messages” page or the AllyAgentCfg command line program to enable or disable the generation of SNMP alerts and/or Syslog messages.

NOTE: SNMP alerts and Syslog messages will not be generated for message types that have been disabled and are not included in the Ally IP1000 event log.

Message disposition is more easily configured from the Ally Management Console GUI. However, if you are managing the Ally IP1000 from the command line interface, the following table shows the AllyRTCfg and AllyAgentCfg command line options associated with each message type.

Command Line Options for Notification Messaging				
Message Number - Type		Enable / Disable in Event Log	Generate SNMP Alert	Generate Syslog Message
		AllyRTCfg option	AllyAgentCfg option	AllyAgentCfg option
1	Configuration Inside and Outside Adapters	N/A	-man	-may
2	Configuration Management Adapter	N/A		
3	Configuration Mode	N/A	-mmon	-mmoy
4	Configuration Inside Authentication	N/A	-mdn	-mdy
5	Configuration Outside Authentication	N/A		
6	Configuration Incomplete Connection Timeout	N/A	-mcn	-mcy
8	Configuration Idle Connection Timeout	N/A		
7	Configuration Maximum Concurrent Connections	N/A	-mmun	-mmuy
9	Configuration IP Fragment Policy	N/A	-mfrn	-mfry
10	Configuration Log Invalid TCP Flags	N/A	-mlfn	-mlfy
11	Configuration Log Invalid TCP Option	N/A	-mlon	-mloy
12	Configuration Prevent Data Leaks	N/A	-mzpn	-mzpy
13	Configuration Port Scan Detection	N/A	-mpsn	-mpsy
14	Configuration Inside Port Scans	N/A		
15	Configuration Outside Port Scans	N/A		
17	Configuration TCP Policy	N/A	-mgn	-mgy
18	Configuration ARP Policy	N/A	-mapn	-mapy
20	Configuration UDP Policy	N/A	-mupn	-mupy
21	Configuration Other IP Policy	N/A	-mopn	-mopy
22	Configuration Non-IP Non-ARP Policy	N/A	-mnpn	-mnpy
19	Configuration ICMP Policy	N/A	-min	-miy
23	Configuration ICMP Echo Request Policy	N/A		
24	Configuration ICMP Echo Reply Policy	N/A		

Command Line Options for Notification Messaging				
Message Number - Type		Enable / Disable in Event Log	Generate SNMP Alert	Generate Syslog Message
		AllyRTCfg option	AllyAgentCfg option	AllyAgentCfg option
25	Configuration ICMP Destination Unreachable Policy	N/A		
26	Configuration ICMP Port Unreachable Policy	N/A		
27	Configuration ICMP Source Quench Policy	N/A		
28	Configuration ICMP Redirect Policy	N/A		
29	Configuration ICMP Time Exceeded Policy	N/A		
30	Configuration ICMP Parameter Problem Policy	N/A		
31	Configuration ICMP Timestamp Request Policy	N/A		
32	Configuration ICMP Timestamp Reply Policy	N/A		
33	Configuration ICMP Information Request Policy	N/A		
34	Configuration ICMP Information Reply Policy	N/A		
35	Configuration ICMP Address Mask Policy	N/A		
36	Configuration ICMP Address Mask Reply Policy	N/A		
37	Configuration ICMP Traceroute Policy	N/A		
38	Configuration ICMP Conversion Error Policy	N/A		
39	Configuration ICMP Domain Name Policy	N/A		
40	Configuration ICMP Domain Name Reply Policy	N/A		
41	Configuration DNS Policy	N/A	-mdnsn	-mdnsy
42	Configuration DNS Tunneling Detection	N/A		
43	Configuration DNS Cache Poisoning Detection	N/A		
44	Configuration Maximum Segment Size Range	N/A	-mmssn	-mmssy
45	Configuration Remote System Statistics Timeout	N/A	-msysn	-msysy
46	Configuration Permanent Blacklist/Whitelist	N/A	-mbwn	-mbwy
47	Configuration Normal Start	N/A	-mnsn	-mnsy

Command Line Options for Notification Messaging				
Message Number - Type		Enable / Disable in Event Log	Generate SNMP Alert	Generate Syslog Message
		AllyRTCfg option	AllyAgentCfg option	AllyAgentCfg option
16	Configuration Blacklist Time Period	N/A	-mbln	-mbly
48	Detection Dynamic Blacklist Add	-lb		
49	Detection Dynamic Blacklist Remove			
50	Information Connection Reset	-lr	-mrn	-mry
51	Detection Discard TCP Packet, Flags	-lf	-mfln	-mfly
52	Detection Discard TCP Packet, Option	-lo	-mon	-moy
53	Detection Discard Fragmented Packet	-ldf	-mdfn	-mdfy
54	Detection Discard Outbound Management	-lbm	-mmsn	-mmsy
55	Detection Discard ARP Packet	-la	-mdan	-mday
56	Detection Discard ICMP Packet	-ldi	-mdin	-mdiy
57	Detection Discard UDP Packet	-ldu	-mdun	-mduy
58	Detection Discard DNS Packet	-ldns	-mddn	-mddy
59	Configuration Event Configuration Reload	N/A	-mcln	-mcly
60	Configuration Event Set Adapter Number	N/A	-msan	-msay
61	Configuration Event Set Management IP	N/A	-mipn	-mipy
69	Configuration Event Set Management DHCP	N/A		
62	Configuration Event Clear Statistics	N/A	-mscn	-mscy
63	Configuration Event Set SNMP/Syslog Agent Variable	N/A	-mavn	-mavy
64	Configuration Event SNMP/Syslog Agent Reload	N/A	-marn	-mary
65	Configuration Event User Change	N/A	-mucn	-mucy
66	Configuration Event Password Change	N/A	-mpcn	-mpcy
67	Configuration Event Time Change	N/A	-mtn	-mty
68	Configuration Event Reboot	N/A	-mbn	-mby

Customer Support

Please contact your Authorized Arxceo Reseller for hardware and software support for your Ally IP1000.

Additional information is available on our website at www.arxceo.com;

Further support or additional questions may be directed to support@arxceo.com or by calling 866-4ARXCEO.



Product Specifications

- System
 - AMD Opteron 64Bit CPU
 - Memory: PC2100 ECC DDR SDRAM; 2 x 184-pin DIMM; 4GB Max
 - Chipset: AMD 8111
 - Network: Dual 1000BaseT controller with NetFailOpen™; dual 100BaseT (one used for remote management access)
 - Video: Integrated ATI Rage XL (does not include a monitor)
- Chassis
 - Form Factor: Mini 1U; 14" deep rack-mountable IDE/SATA Chassis
 - Dimensions: 16.7"W x 1.7"H x 14"D, 14.3 lbs
- Storage:
 - 2 x 3.5" Hard Drive Bays; includes one drive greater than 40GB
 - CD ROM drive
- Multiple I/O:
 - USB: 2 x Front 2 x Rear USB ports
 - Serial Ports: 1 x Rear Serial Port
 - Keyboard/Mouse: 1 x PS/2 KB connector; 1 x PS/2 Mouse connector (does not include keyboard or mouse)
- Front Panel:
 - Power On/Off Button
 - System Reset Button
 - LEDs: Power, Hard drive activity, 2 network activity, System overheat
- Power Supply:
 - 200 Watt AC Power Supply
 - Thermal Control with PFC
- Cooling:
 - 1 x 100mm blower fan in chassis
- Operating System:
 - Microsoft Embedded Windows XP
- Environmental:
 - Operating Temperature: 10°– 35°C (50° to 90°F)
 - Operating Relative Humidity: 8% to 90% (non-condensing)
- Regulatory Compliance:
 - FCC Class B, EN 55022 Class B, EN61000-3-2/3-3, CISPR 22 Class B
 - UL listed (USA); CLU listed (Canada); TUV Certified (Germany); CE Marking (Europe)

866.427.9236

Arxceo, Ally IP1000, Tag-UR-IT, PnPro, NetFailOpen and the Arxceo logo are trademarks or registered trademarks of Arxceo Corporation. Other product names are trademarks of their respective owners. Arxceo believes the information in this publication to be accurate as of its publication date. Arxceo is not responsible for inadvertent errors. © 2005 Arxceo Corporation, Huntsville, AL 35806.

**License Agreement for Embedded Software
And Notice of Third Party Software**

THIS AGREEMENT (the "Agreement") CONSTITUTES A LEGAL AGREEMENT BETWEEN THE PURCHASER OF THIS HARDWARE ("You"), AND ARXCEO CORPORATION ("ARXCEO") REGARDING THE SOFTWARE EMBEDDED IN THE HARDWARE OR OTHERWISE INSTALLED ON THE HARDWARE AS DELIVERED. YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE OPENING THIS PACKAGE. OPENING THIS PACKAGE WILL BE CONSTRUED AS YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THEM, PROMPTLY RETURN THE UNOPENED PACKAGE FOR A REFUND. USE OF THE EMBEDDED SOFTWARE OUTSIDE OF THIS AGREEMENT CONSTITUTES A VIOLATION OF U.S. AND INTERNATIONAL COPYRIGHT LAW.

1. **Grant of License:** ARXCEO grants to you a limited, revocable license of the ARXCEO software and/or firmware (the "Software") that is embedded in or otherwise installed as delivered on the enclosed hardware (the "Equipment"), solely as the Software is installed at the date of purchase, and solely on the Equipment at one site; such license is strictly limited to use of the Software, in an unmodified state, on the unmodified Equipment. From time to time, ARXCEO may, in its sole discretion, provide upgraded software for replacement of the Software and/or Third Party Products (as defined in Section 5) in connection with the Equipment (an "Upgrade"). Each Upgrade is governed by the terms set forth in ARXCEO's distribution materials (e.g., the terms presented on ARXCEO's web page linking to the upgrade, if provided by Internet download, or the terms of any documentation accompanying physical media distribution, if any) associated with that specific Upgrade (the "Upgrade Materials"), which may list specific models of equipment or specific purchase plans to which the Upgrade is made available or licensed. You understand and agree that use of an Upgrade shall be governed by the license in the Upgrade Materials associated with such Upgrade (the Upgrade License); that this agreement does not grant any rights in, create any expectation of, and does not otherwise cover any Upgrade; and that because this license gives you no rights in any Upgrade, use of an Upgrade with equipment not specified in the Upgrade License or otherwise outside the scope of the Upgrade License is a violation of copyright in that Upgrade.

2. **Copy Restrictions/Ownership of Software.** The Software is licensed, not sold. Your rights in the Equipment are subject to the terms of your purchase or leasing arrangement therefore, and do not in any way enlarge or imply rights in the Software; in all cases, ARXCEO retains title to the Software including any and all copies (whether authorized or not), regardless of form or media, and to all copyrights therein. The Software and accompanying written materials are copyrighted. You may make one copy of the Software (the "Backup Copy") solely for backup and archival purposes, which copy must be held in strict confidentiality, and may not be transferred except together with the Equipment. You agree not to make any copy other than the single first-generation Backup Copy. You agree not to extract the Software or any portion thereof to other media (other than the making of the Backup Copy), upload the Software or any portion thereof to any equipment (other than the restoration of the Backup Copy to the Equipment in an unmodified state), or modify the Software in any manner.

3. **Transfer and Other Restrictions.** You may transfer the Software only both (a) with a copy of this Agreement, and (b) as installed on the Equipment, which transfer may be made to another party only on a permanent basis and only if the other party accepts the terms and conditions of this Agreement. Upon such transfer, you must transfer all accompanying written materials, and either transfer or destroy all copies of the Software. Any transfer or attempted transfer in violation of this provision is void. You may not lease, rent, merge, time share, or use the Software in the operation of any service bureau. You agree not to reverse engineer, decompile or disassemble the Software, except to the extent you are permitted to do so by applicable law that cannot be waived by this Section 3. You may not use the Software for or in connection with any purpose or activity that (i) violates or infringes upon the rights of any others (including without limitation the right of privacy or the right of publicity, copyright, and trade secret), (ii) may be illegal, abusive, profane, obscene, immoral, indecent, threatening, slanderous, libelous, scandalous, or offensive to an average person, (iii) violates any law, regulation, or regulatory advisory, opinion, including particularly without limitation, those in the areas of antitrust, fair trade and securities law, or medical information (by way of non-limiting example, HIPAA requirements), or (iv) involves or relates to operation of nuclear facilities, aircraft navigation, aircraft communication, aircraft flight control, devices or systems in which serious injury or death to the operator of the device or system, or to others due to a malfunction (including, without limitation, software related delay or failure) could reasonably be foreseen. You shall be responsible to ensure compliance with the foregoing.

4. **Termination.** The licenses and rights granted in connection with this Agreement are effective for the operational life of the unmodified Equipment or until earlier terminated. The Agreement will terminate if you fail to comply with any provision of this Agreement, such termination to be automatically effective without notice except to the extent that notice is required by non-waivable provision of law, in which case the termination shall be effective immediately upon such notice as the law shall require. You may voluntarily terminate at any time. Upon termination, you agree to destroy or purge all copies of the Software and accompanying written materials. You acknowledge and agree that upon termination of this Agreement, any attempt to access or use the Software is prohibited and unauthorized, and you agree that you will not make any such attempts. The provisions of Sections 3, 4, 5, 8, 9, 10, and 11 shall survive any termination of this Agreement.

5. **ARXCEO's Licensors and Third Party Software:** In addition to the Software, the Equipment includes the following software programs and code that are owned by ARXCEO's licensors, respectively ("Third Party Products"): the Microsoft XP Embedded program ("MSXPE"), licensed from Microsoft Corporation ("MS") and subject to the MS EULA Attached as Schedule A; Apache Tomcat ("Tomcat"), licensed by Apache ("Apache") under the ASF Apache License version 2.0, Attached as Schedule B; and possibly other code received by ARXCEO as "free software" without restrictions. The Third Party Products are provided as a convenience to You, and are not considered part of the Software. Your license to MSXPE is your sole source of license, rights, remedies, warranties, and benefits related to MSXPE. You agree to all of the terms of the MS EULA, and agree with ARXCEO that you will comply with all such terms. Your license to the remaining Third Party Products is directly with and from Apache or the other licensors thereof, and you agree to comply with the terms of such licenses. In addition to the terms set forth in the relevant third party licenses (including without limitation the MS EULA and the Apache license), you agree that **all Third Party Products are subject to all restrictions and obligations on You (but not the rights, remedies, or warranties in Your favor, or the obligations of ARXCEO) that are set forth in this Agreement for the Software**, to the same extent as if the Third Party Products were considered Software, provided that in the event of a conflict between the terms of this Agreement and the terms of a Third Party EULA, the Third Party EULA controls, but only with respect to the specific Third Party Product covered under that

EULA. In no event shall the immediately foregoing sentence be construed to imply, create, or require any requirement, restriction, or obligation of ARXCEO with respect to the Third Party Products or their licensing. You agree with ARXCEO that you shall not use the Third Party Products with any equipment other than the unmodified Equipment. No fees charged are allocated to the Third Party Products, which are provided free of charge. ARXCEO is not the licensor of the Third Party Products (except for MSXPE, for which ARXCEO is the sublicensor), and is not the agent of the licensors thereof. Such licensors alone remain responsible for the licensing, performance, accessibility, operation, and warranties (if any) of such Third Party Products. Without limiting the foregoing in any manner, You shall be deemed on notice of and in agreement with at least those limitations and obligations regarding Third Party Products that are listed in any license text included in physical form (e.g., on paper) with the Equipment or displayed in connection with or linked to any configuration screen. You agree to bear full and sole responsibility for any failure to comply with the license agreements provided herewith for the Third Party Products, and You agree to defend, indemnify, and hold harmless ARXCEO and its officers, agents, employees, directors, subcontractors, shareholders and representatives from and against any and all claims, losses, liabilities (including without limitation claims of induced or contributory infringement), expenses (including without limitation reasonable attorneys fees), and damages arising out of or related to any and all breaches of such license agreements and any infringement of the intellectual property rights of MS or Apache.

6. Support and Remediation: ARXCEO's standard obligations regarding the performance of the Software are set forth in Section 7 of this Agreement. In the event that You desire to obtain extend support services, You may purchase support services on a yearly basis calculated from the date of purchase (each year of coverage being a "Support Term") by (1) notifying ARXCEO of your intent to purchase support services for the upcoming Support Term no later than: (A) for the first Support Term, the expiration of the Warranty Period, and (B) for all subsequent Support Terms, thirty (30) days prior to the end of the immediately preceding

Support Term (the "Support Renewal Notice"); and (2) paying the then-current support fee as published on ARXCEO's website. In the event You fail to provide a timely Support Renewal Notice or otherwise allow a period of time after the Warranty Period to occur without a Support Term being in effect, then You shall not be eligible for a later Support Term until the parties mutually agree on the terms of a separate Maintenance and Support Agreement, which may include a requirement of an initial fee and separate yearly fees. Provided that You have maintained payments and made timely Support Renewal Term notices at all times, during any Support Term for which You have paid all fees in advance, ARXCEO shall provide to You all updates to the Software (within the same version number as provided on the Equipment as originally purchased) that are incorporated generally into new installations of that version of the Software as provided to new customers; and ARXCEO shall use reasonable commercial efforts to respond to calls of a technical nature for support and assistance regarding the proper operation of the unmodified Software, by providing telephonic instruction or advice regarding possible user error leading to problems, or regarding proposed work-arounds, fixes, or alternatives. The foregoing notwithstanding, at any time following the expiration of five (5) years from the date of purchase of the Equipment, ARXCEO may notify You of the "retirement" of the Software, following which all subsequent Support Renewal Notices shall be of no force or effect, no new Support Terms shall begin, and ARXCEO shall have no obligation to provide the support services after the expiration of the then-current Support Term. At any time, regardless of whether a Support Term is then in effect, in the event that any part or all of the Software, or any of the Third Party Products, in ARXCEO's sole judgment become or are likely to become the subject of any claim of infringement of third party rights, then (i) the license granted with respect to any affected part of the Software may be automatically terminated upon notice of such judgment to You, (ii) You shall immediately cease use of the affected part of the Software and of any affected Third Party Products, and (iii) if the You remain in a Support Term for which the Support Fee has been paid, ARXCEO at its own election and expense will either (a) provide substitute software; or (b) modify the Software so that it no longer infringes (or if the issue is with a Third Party Product, so that the Software uses different, non-infringing software or otherwise ceases to rely upon the infringing aspects of the Third Party Software) and operates to ARXCEO's standards, or if none of the foregoing is feasible in ARXCEO's sole discretion, then You shall be entitled to a refund of the applicable licensing fee from ARXCEO for the portion of the Software affected, prorated according to the number of months remaining in a five year period from the date of purchase of the Equipment; except that no refund will be provided where the infringement, likelihood of infringement, or failure to comply with standards is related to any modification of the Software or use of any software with the Software other than the Third Party Products provided with the Equipment.

7. LIMITED WARRANTY. ARXCEO warrants that the Software as installed on the date of purchase will, for a period of ninety (90) days from that date, provide operation of or access to the material functions of the Equipment, when used as directed in the documentation for the Equipment. As the exclusive remedy for any breach of warranty, ARXCEO will at its sole discretion and election either (1) provide substitute or replacement software for loading onto the Equipment, (2) repair the Software or instruct operational work-arounds to minimize the impact of any error while retaining major functionality of the Software; (3) instruct return of the Equipment and Software and refund the purchase price upon receipt of the same; or (4) treat the failure as a failure of hardware and respond under any maintenance and support contractual terms related to the Equipment, or under any warranty applicable to the Equipment. Without limiting such other remedies as may be available to ARXCEO (including without limitation remedies in the nature of breach of contract, infringement, or other legal theory), the warranty is void in the event of any modification of the Equipment or Software or the use of the Software on any hardware other than the Equipment. EXCEPT AS EXPRESSLY STATED IN THIS SECTION, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. EXCEPT AS EXPRESSLY STATED IN THIS SECTION, ARXCEO HEREBY EXPRESSLY DISCLAIMS, TO THE MAXIMUM EXTENT PERMISSIBLE BY LAW, ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITING THE DISCLAIMER ABOVE, ARXCEO DOES NOT WARRANT THAT THE SOFTWARE OR FUNCTIONS OF THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAM WILL BE UNINTERRUPTED OR ERROR FREE, THAT DATA OUTPUT WILL BE WITHOUT ERROR, OR THAT PROGRAMS DEFECTS WILL BE CORRECTED.

8. LIMITATION OF LIABILITY. ARXCEO's entire liability in connection with the Software is strictly limited to, and in no event shall exceed, the amount of payment made by you to ARXCEO for the specific Equipment on which any Software in issue is installed, as evidenced by a copy of your purchase receipt. IN NO EVENT WILL ARXCEO OR ITS VENDORS BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, PUNITIVE OR INCIDENTAL DAMAGES, OR ANY DAMAGES, HOWEVER CATEGORIZED, FOR LOSS OF

BUSINESS PROFITS, LOSS OF DATA OR INFORMATION, DATA OR EQUIPMENT FAILURE, OR LOSS OF USE, EVEN IF ARXCEO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9. Indemnity: You agree to defend, indemnify, and hold harmless ARXCEO and its officers, agents, employees, directors, subcontractors, shareholders and representatives from and against any and all claims, losses, liabilities, expenses (including reasonable attorneys fees), and damages arising out of or related to (1) any violation of the provisions of Sections 2 or 3 of this Agreement; (2) any exceeding of the scope of the license granted in Section 1; (3) any modification of the Software or Equipment by You or persons under Your control or direction; or (4) any combination, operation or use of the Software with other software or with hardware other than the Equipment, unless such combination, operation or use was expressly and specifically approved in writing by ARXCEO.

10. General Provisions. All notices and other communications hereunder directed to ARXCEO shall be in writing and shall be sent by certified or registered mail (return receipt requested) addressed to Arxceo Corporation, 1525 Perimeter Parkway, Suite 225, Huntsville, AL 35806. Compliant notices shall be deemed effective three (3) business days after being deposited in the mail. This Agreement shall be binding upon and shall inure to the benefit of the parties and their respective successors and permitted assigns. This Agreement and all questions of its interpretation, performance, enforcement and the rights and remedies of the parties hereunder shall be determined in accordance with the laws of the State of Alabama, without regard to principles governing conflicts of laws. The parties hereby consent to the exclusive jurisdiction of the courts residing in the State of Alabama. The headings in this Agreement are inserted for convenience only and shall not be used in the interpretation hereof. This Agreement may only be amended by a written document signed by both parties. No waiver of any provision of this Agreement, or of a breach hereof, shall be effective unless it is in writing and signed by both parties. No waiver of a breach of this Agreement shall constitute a waiver of a subsequent breach. All provisions of this Agreement are severable, and the unenforceability or invalidity of any of them shall not affect the validity or enforceability of the remaining provisions of this Agreement. This Agreement constitutes the entire understanding between the parties and supersedes all previous understandings, agreements, communications and representations, whether written or oral, concerning the subject matter hereof. With the sole exception that Upgrade Licenses shall be fully effected by their terms when delivered with any Upgrade (see Section 1), no amendment to (including without limitation any enlargement of) the terms of this Agreement shall be of any force or effect unless in a writing signed by both parties. In the event You issue or issued a purchase order or other instrument related to the subject matter of this Agreement, you agree that such purchase order or instrument is for Your internal administrative use only and shall not be effective to add to, subtract from, override, supersede, supplement, or otherwise affect the rights and obligations of the parties, this Agreement or any of the terms of this Agreement.

11. Commercial Computer Software. The Software is commercial computer software, and all documentation is commercial computer software documentation, each of which was developed solely at private expense.



Arxceo Corporation
1525 Perimeter Parkway,
Suite 225
Huntsville, AL 35895

☎ 256.637.8336
✉ 256.637.2888

www.arxceo.com