iLink™ from ADIC Security Specifics

FOR MORE INFORMATION
To learn more about ADIC's Support plans or to purchase or renew an existing support contract, please visit **www.adic.com/support** or contact:

AMERICAS AND ASIA PACIFIC
Phone: **1.800.827.3822**
E-mail: **servicesales@adic.com**

EUROPE, MIDDLE EAST, AND AFRICA
Phone: **00800.9999.3822**
Phone: **+33.130.87.5353**
E-mail: **europeservicesales@adic.com**

Table of Contents

1.0 Introduction

This paper describes security features of the ADIC iLink™ technology designed to support IT departments' security administration and security planning. Topics covered include:

- Deployment and network topologies and security barriers (i.e. firewalls)
- Network ports and protocols
- Data transmission security: confidentiality, integrity, non-repudiation
- Vendor/user trust relationships
- User authentication and authorization

2.0 Overview

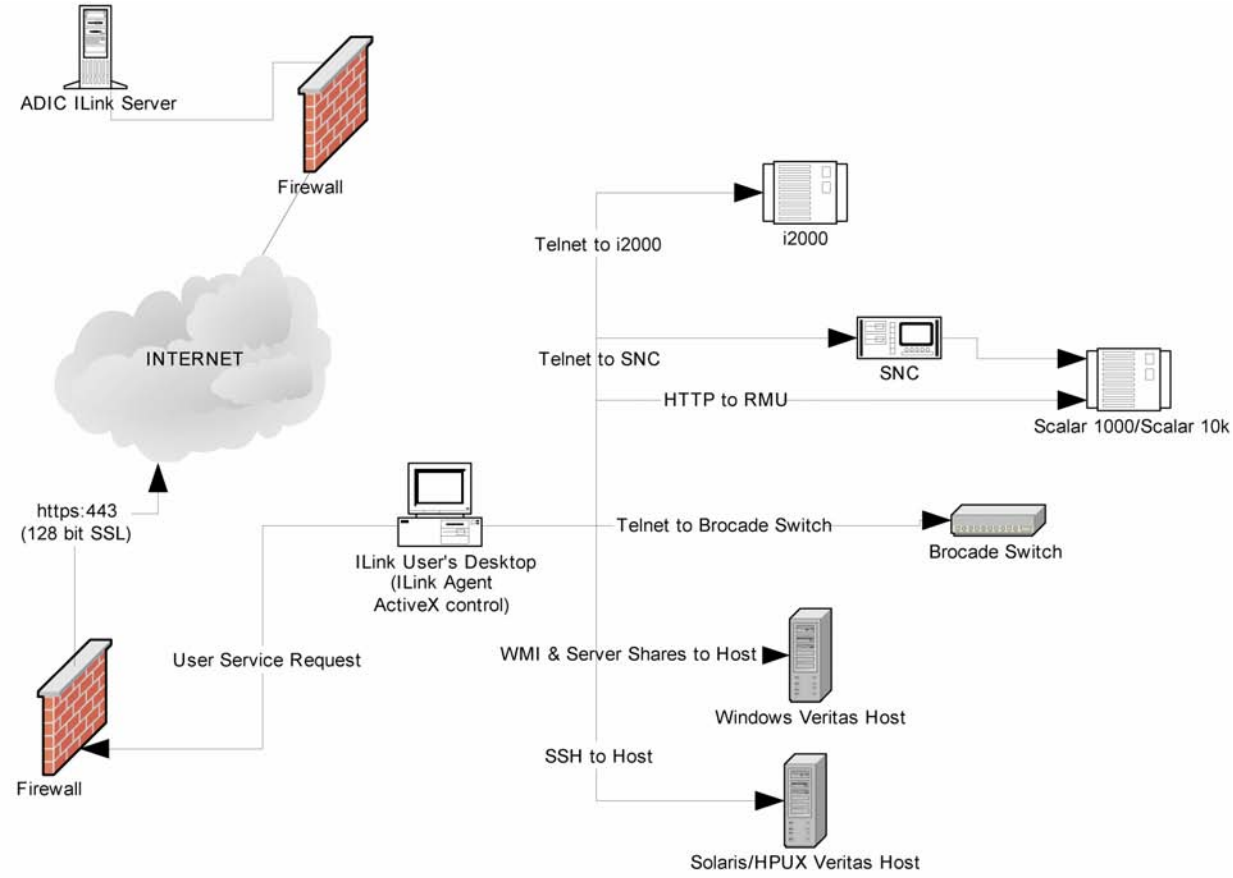
iLink is a key component of ADIC's iSurety™ service approach. The iSurety approach leverages advanced technology to save end users time and money and provide faster, more certain resolution for complex, system-wide backup issues when compared with traditional service alone. iSurety links ADIC's service teams and resources with its customers, their ADIC libraries and disk-backup systems, and the diagnostic information from their storage environment. iSurety leverages technologies such as remote access to ADIC technical service resources via iLink™ and e-mail home, online service request processing, web-based event status tracking, and the ADIC Customer Service Center (CSC) web site, which provides on-line configuration, service, and product information.

ADIC's iLink service technology enables advanced troubleshooting of customer issues by analyzing information from the ADIC libraries and devices as well as the broader attached storage ecosystem. Unlike similar service methods which look only at a single proprietary device's logs, iLink enables the gathering of logs and connectivity information from multiple components in the environment and transmits the service data to ADIC for analysis. The end result is improved fault isolation and root cause analysis because analysts can look at the entire data path in their diagnostic process.

To gather information iLink uses scripts, called "diagnostics," which query specified devices. Diagnostics are obtained from ADIC over a secure, user initiated connection and then executed from a local workstation by the administrator. Service data gathered from devices is then transmitted back to ADIC over the secure link for analysis. For the most robust fault analysis, ADIC recommends that all diagnostics be executed, but the end user has total control over what scripts are run and what information is sent back to ADIC service personnel.

3.0 Network Architecture

The figure below illustrates the basic iLink ecosystem consisting of the end user's data center and iLink server in ADIC's Secure Service Center (SSC).



4.0 Ports and Firewalls

In order to obtain the diagnostics used for iLink analysis and send service data back to ADIC, a connection must be established between ADIC and a Windows workstation in the end user's data center. To do this, the local administrator makes an https connection to ADIC using their web browser by logging in to the appropriate area of the ADIC Customer Service Center and clicking on the active iLink button within the relevant service request (see the iLink Deployment Guide for greater detail on the usage process). This methodology guarantees that the end user has total control over the execution of iLink processes, and it eliminates the need to install a bulky client-side application. Using https guarantees a secure, SSL-enabled connection. For this connection to work through a customer firewall, the following is required:

- All connections are initiated via outbound request
- SSL connections are initiated through HTTPS over port 443

5.0 Browser Support and HTTP Proxies

Diagnostic and service data transmission occurs using an ActiveX® control. For this reason, iLink requires the use an ActiveX enabled web browser. HTTP proxies can be implemented by the end user via built-in browser support. Currently, ADIC supports the following browsers for use with iLink:

- Microsoft® Internet Explorer, version 5.5 and up

6.0 Authentication

SSL provides authentication and encryption for iLink communications. Authentication guarantees that the end user is connecting to an ADIC iLink server. Encryption encodes data so that it cannot be read as it is transmitted between the end user's data center and ADIC. SSL accomplishes authentication and encryption through the use of electronic documents called "certificates." These certificates contain an encryption key as well as authentication information about the company that owns the iLink server, ADIC.

Certificates are sent by the iLink server to the local workstation during the initial connection to the iLink server. Once a certificate is obtained, the end user's web browser uses embedded code logic to read the certificate and independently verify the identity of iLink server to which they are connecting. Once the server has been authenticated, encryption key information in the certificate is used to encode iLink transmissions.

7.0 Certificates to Verify Trusted Source

iLink uses X.509v3 format certificates to provide authentication and encryption data to the end user work station. For authentication, the x.509 certificate includes information about the owner of the certificate, ADIC, and the organizations, called certificate authorities, responsible for issuing the certificate to ADIC and guaranteeing it is valid. By independently contacting the certificate authority(s), the end user system verifies the identity of the iLink server so a trust relationship can be established for running diagnostic code. iLink certificates are issued and signed by a Verisign (a known certificate authority (CA)).

In addition to authentication, the X.509 certificate includes public key encryption information. SSL uses public key encryption to encode information and guarantee that any information sent to ADIC can only be read by ADIC. Once the end user system has received and verified the iLink certificate, it will generate a symmetric encryption key that can be used to securely pass information to and from the iLink server.

8.0 Diagnostic Signature Certificate Chain

Running the iLink diagnostics does require the download of an Agent in the form of an ActiveX® control. This module is downloaded the first time a diagnostic needs to be run and may be updated during future iLink sessions if functionality is upgraded. To ensure security, the ActiveX control is downloaded in a signed CAB file from the iLink server. The signed CAB is signed by a certificate issued by VeriSign®, so the browser will trust it. In addition, the Agent uses SiteLock coding to ensure that it can only be instantiated from servers in the iLink domain.

For increased security, every diagnostic obtained from ADIC must also be verified. When any diagnostic is downloaded, the ActiveX Agent Controller validates that the diagnostic was signed by the trusted code-signing certificate from VeriSign.

9.0 Gathering data from devices

Every iLink diagnostic indicates the device (switch, host, library, etc) from which it will collect service data. When the user executes a diagnostic, a login to the device is required – just as with any normal access. These logins will be performed by the end user via the local iLink diagnostic - ADIC will retain no end user login data. This login process allows the diagnostic to gather necessary service log information and collect it at the user's workstation. Where possible, iLink leverages native remote management protocols to gather information. This currently includes SSH on UNIX® and WMI on Windows® 2000 and up. If SSH or WMI is not running on both the workstation and target device, Telnet or HTTP will be used. To minimize the possibility of this issue, the iLink Agent download includes SSH and Telnet clients that will be run from the end user's workstation.

After service data has been gathered from all necessary devices, it is collected at the workstation. The user can then review the information that has been collected and confirm that it should be sent to ADIC. Once this final check is performed by the end user (and they click send), the data is parsed and sent to ADIC over the secure SSL connection.

NOTE: At no time is any user login information cached, collected, or stored by iLink. Service logs collected from hosts, switches, and libraries will be stored on the workstation so that it can be re-sent if a break occurs during transmission to ADIC. After logs have been transmitted to ADIC, the user can delete this information from their workstation.

10.0 SSH

SSH, secure shell, is a secure communication protocol for remote access that runs over port 22. To leverage SSH, SSH must be enabled on both the workstation where the script is installed and the UNIX host where iLink is collecting service data. iLink does provide an SSH daemon, as part of the Agent download. SSH uses native OS authentication, and runs the shell commands in the environment of the user who is authenticated. To collect certain log information, this may require a root login.

11.0 WMI

Windows Management Instrumentation (WMI) is a remote management / data gathering function provided by Windows NT4 (SP 4) and up. Remote WMI invocations connect to the DCOM port 135 on the host where service data is being collected. For WMI connections to work properly, DCOM must be enabled, and port 135 must be accessible. WMI uses the native Windows security to validate the invoking user's logon access. To collect certain log information, this may require administrative login.

12.0 Telnet and HTTP

Telnet and HTTP communications will be run over their standard ports. Telnet uses port 23 and HTTP uses port 80.

13.0 Secure Service Center (SSC)

The Secure Service Center is a secure facility where the ADIC Technical Support agents that are working on iLink incidents reside. There are SSCs located in Denver, Colorado, Bohmenkirch, Germany, and Northampton, United Kingdom to support iLink remote service capabilities for our world wide customers. Only authorized Technical Support team members are allowed access to the SSCs. These analysts are well versed in both the ADIC technology, and the broader storage environment. By leveraging this centralized methodology, ADIC is better able to respond promptly to customer events with appropriate levels of service expertise, retain a high level of physical security, ensure global consistency, and provide a higher level of training and skill set for service personnel.

14.0 Glossary of Terms

Component - A component is a logical or physical piece of hardware or software within an environment. Each component has a name, type, and a collection of properties associated with it. A component can also include the scripts that are used to discover its property values. Components are associated with one another using relationships, which define how the components depend on one another. Examples of components include: a database, the Microsoft Windows XP operating system, or a web server.

SSL (Secure Sockets Layer) - A protocol used for establishing a secure communications channel over the Internet. SSL ensures that information is sent only to the server you intended to send it to and arrives unaltered. A secure communications channel is established between the server and the client over which all data is encrypted. Digital signatures ensure message integrity, and digital certificates ensure trust in an individual or website. SSL uses 40-bit and 128 bit encryption. The level of encryption is determined by the configuration of the end user's browser. ADIC will always attempt to use the highest level of security possible.
SSL is commonly used on web sites for secure credit card transactions. If you are viewing a web page that is protected by SSL, you will see the padlock symbol in the Internet Explorer status bar.

HTTP (Hypertext Transfer Protocol) - The client/server protocol used to access information on the World Wide Web. HTTP defines how messages are formatted and transmitted, and what action web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, the browser sends an HTTP command to the web server directing it to fetch and transmit the requested page.

HTTPS (Hypertext Transfer Protocol Secure) - The client/server protocol used to access secure web servers. If the URL contains HTTPS rather than HTTP, the browser sends the messages to a secure port number rather than to the default port (80).

ActiveX - Active X is a set of technologies that enables software components to interact with one another in a networked environment, regardless of the language in which the components were created.
Before downloading an ActiveX control, Internet Explorer displays a warning box. This warning communicates the following:

- The ActiveX control was signed using a digital certificate by ADIC.
- ADIC asserts that the software is safe.
- ADIC purchased the certificate from VeriSign, a public certificate authority (CA).
- Verisign has confirmed the identity of ADIC as the iLink vendor based in Redmond, Washington.
- ActiveX is used primarily to develop interactive content for the World Wide Web, although it can be used in desktop applications and other programs. ActiveX controls can be embedded in web pages to produce multimedia effects, interactive objects, and sophisticated applications. The core technology elements of ActiveX are COM and DCOM.

Certificate Authority - Certificate authority refers to an issuer of security certificates that are used in SSL connections. The certificate authority issues a certificate (also called a digital certificate or an authentication certificate) to an applicant company, which can then put the certificate on its site. Certificate Authorities can be verified by parent authorities using root chain (certificate chain) information stored in the certificate.

Certificate - A certificate is a data record used for authenticating network entities such as a server or a client. iLink certificates use the X.509v3 format to provide pieces of information about its owner (called the subject) and the signing Certificate Authority (called the issuer), plus encryption information in the form of the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates.

Certificates provide a way to securely deliver software components over the Internet. When the certificate is provided by a certificate authority, you can be certain that the software came from the manufacturer identified at the time of download and that the code was unaltered or corrupted since it was created and signed.

15.0 Conclusion

ADIC's iLink technology represents an innovative, flexible and highly secure method of jump starting the troubleshooting and diagnostic experience for ADIC customers. When combined with other iSurety technologies, and ADIC onsite service programs, customers will experience an enhanced level of service when compared to other standard service methodologies.

For further information or assistance in leveraging iLink for use in your storage ecosystem, please contact your ADIC sales person.

FOR MORE INFORMATION
To learn more about ADIC's Support plans or to purchase or renew an existing support contract, please visit **www.adic.com/support** or contact:

AMERICAS AND ASIA PACIFIC
Phone: **1.800.827.3822**
E-mail: **servicesales@adic.com**

EUROPE, MIDDLE EAST, AND AFRICA
Phone: **00800.9999.3822**
Phone: **+33.130.87.5353**
E-mail: **europeservicesales@adic.com**