

SIA

Valutazione prodotto di AntiSPAM

E' supportato il routing delle e-mail verso domini differenti?

- ▶ Si, le mail possono essere ruotate verso domini differenti
- ▶ DNS MX lookup and smart relay host for Outbound traffic
- ▶ DNS MX lookup, static domain based and user based LDAP routing for Inbound traffic

Come viene configurato?

IronMail provides several capabilities for routing email. Email addressed to a specific domain may be mapped to a specific internal mail server. An LDAP directory's information may also be used to specify how mail is routed—IronMail will look up the LDAP mail server information and route the message accordingly. Plus, administrators must explicitly specify which of their internal servers may send messages through IronMail to the outside world. (Unless internal servers are identified in the Internal Routing list, IronMail will not deliver their mail.)

Domains and machine names in IronMail's routing table (*Mail-Firewall > Mail Routing > Domain-based*) take precedence over the route that is specified here in the SMTP properties window. Any messages addressed to a domain listed in the Domain-based routing table will be delivered directly to that domain's mail server, rather than to the Static Host identified here.

If enabled, IronMail will try to resolve sub-domains to a top-level domain identified in the Domain-based routing table (*Mail-Firewall > Mail Routing > Domain-based*). That is, if messages are addressed to "subdomain.domain.com" and "domain.com" is in the routing table, IronMail will deliver it to the internal mail server mapped to that domain. If this option is not enabled, IronMail will only deliver messages to sub-domains if the sub domains have been specifically added to the routing table.

Domain-based Routing

Specific domains or sub-domains may be mapped to specific internal mail servers. All messages to that domain or sub-domain will be processed by the specified mail server. IronMail uses the following logic to deliver the message:

1. Use LDAP routing information if LDAP routing is enabled.
2. If LDAP is not enabled, or if LDAP does not provide a route, use the sub-domain route existing in this table.

]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

3. If a sub-domain route does not exist in this table, deliver it to the mail server hosting the next-level of the destination domain.
4. Step three repeats until the top-level domain is reached.
5. If the IP address sending the message is not on the Allow Relay list (*Mail-Firewall > Allow Relay*), IronMail responds with a “571 Cannot relay” message, and the connection is dropped.
6. 6. If a message is addressed to a domain not mapped here and Skip Internal Server for Outbound Messages is enabled, (*Mail Firewall > SMTP & SMTPS Services “Skip Internal Server for Outbound Messages”*) IronMail checks the message’s

LDAP-based Routing

There are three IronMail configurations for LDAP use:

1. **Do not use LDAP:** IronMail will not use the information in an LDAP server for any purpose. (This is IronMail’s default setting.)
2. **Use LDAP for mail routing only:** IronMail will look up the routing information stored on an LDAP server for individual users when mail is delivered to them, and route the message to specified mail servers accordingly.
3. **Use LDAP for Policy Manager Groups only:** IronMail will use an LDAP server’s group information for email policies created in IronMail’s Policy Manager.

These configurations are based on how the LDAP server is set up. If the LDAP server is set up for individuals, then IronMail can use its information for *routing* purposes only. If it is set up for groups, then IronMail can use its information for IronMail’s Policy Manager *groups*. Using LDAP for *email routing purposes* is set in this LDAP-based Routing window. LDAP configuration for *group management* is set in IronMail’s *Policy Manager > Group Manager > LDAP* window.

Internal Routing

Administrators must provide the IP addresses of any internal server allowed to deliver, through IronMail, messages to external domains. The IP address of the default mail server (entered during the Initial Configuration Wizard when IronMail was installed) is listed by default. Whenever a server’s IP address is added here, it is automatically added to IronMail’s Allow Relay List (*Mail-Firewall > Allow Relay*). Note, however, that if an IP address in this table is deleted or edited, the Allow Relay List must be manually updated to reflect the change.

E’ supportato il masquerading?

- ▶ Si, è supportato tramite controllo dell’header di posta e della sua relativa modifica
- ▶ IronMail supporta la funzionalità di domain address masquerading in maniera daerente e conforme agli standard RFC 821 e RFC 822

Come viene configurato?

IronMail’s Address Masquerade function allows administrators to “map” one domain name to another for either inbound or outbound messaging. This option is intended to ease the transition when a domain name changes for any reason. Mapping domains on the IronMail appliance protects an enterprise’s end users from having to manually change the domain information in

]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

their email clients. For example, if "mycompany.com" acquires "yourcompany.com," and wants all mail addressed to "yourcompany.com" to now be routed to "mycompany.com," these two domains would be mapped for *inbound* mail.

(Mapping domains for *inbound* messages affects the *routing* of incoming email.)

Alternately, mapping domains for *outbound* messages affects *replies* to outgoing email. That is, when "yourcompany.com" is mapped to "mycompany.com," the recipients of outbound messages will see "mycompany.com" as the REPLY TO address.

Quali sono gli antivirus supportati?

- ▶ McAfee
- ▶ Sophos
- ▶ Authentium (Command Software: used by Verisign)

If one or more anti-virus *licenses* (see *System > Updates > License Manager*) have been purchased and installed on the IronMail appliance, it is capable of scanning all messages, whether incoming or outgoing, for viruses.

Administrators may purchase licenses for McAfee and/or Sophos products. These antivirus engines are seamlessly embedded within IronMail's queue architecture, providing robust protection against even the very newest viruses and worms. Virus definition or "identity" files can be automatically downloaded once an hour to ensure that IronMail is able to stop the most recent threats.

Come avviene la gestione degli alias del tipo seguente:

nickname : name.surname@domain.com

▶ Nella corrente versione di IronMail, gli aliases che si possono configurare sono relative alla parte dominio: user@domain1.it sarà trasformato in user@otherdomain.com

▶ Nella prossima versione, si potranno configurare anche aliases del tipo
nickname : name.surname@domain.com

Come si viene informati della presenza di una nuova versione di Ironmail?

▶ Attraverso il sito web di CipherTrust, attraverso la CipherTrust Newletters ed attraverso il supporto degli ingegneri di CipherTrust e di Hacking Team

]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

Qual'è la procedura di upgrade del firmware dell'appliance?

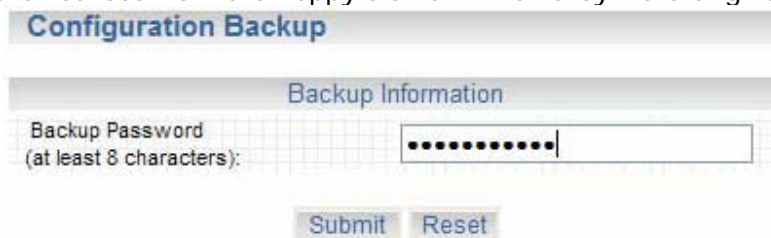
► L'aggiornamento del firmware è eseguito tramite CD. Tutti gli altri update sono configurati ed eseguiti tramite la web GUI.

Qual'è la procedura per esportare ed importare la configurazione e le regole?

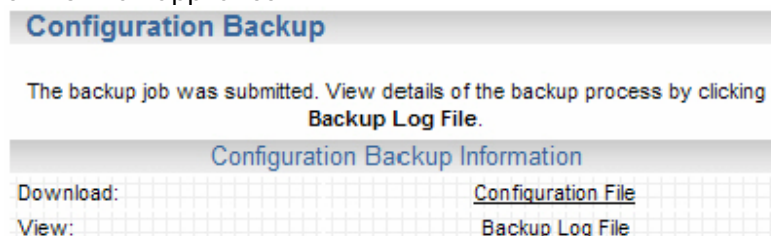
► IronMail possiede, nell'interfaccia di amministrazione, tutti i tools necessari per eseguire operazioni di backup e restore (granular) della configurazione e delle politiche definite.

Backup

IronMail allows administrators to backup the configuration settings for the appliance (e.g., email policies, Mail and Queue Service settings, etc.) in case of disk failure, or so those settings may be easily duplicated on other IronMail appliances. (Note that IronMail does not include licensing information for program features in its backup. If a backup of configuration settings needs to be restored, reinstall the licenses from the floppy disk on which they were originally delivered.)



Enter a password to be associated with the backup file and click **Submit**. (This password will be required when the backup is restored.) A "Configuration Backup Information" table is displayed which contains hyperlinks to download the backup file and view a log of the backup process. Do not rename or edit this file name after downloading the backup file to disk. Changing the file's name will cause the Restore function to fail, and may produce other unintended consequences. Regardless of the IronMail name with which the backup file is associated, it may be safely restored to any other IronMail appliance.



]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

When IronMail saves a backup configuration to disk, it uses an automatic naming scheme, identifying the appliance's name, version number, latest release number, and date (e.g., "myironmail.3-0.1-5.200201011352.zip"). The backup information is encrypted, stored in a proprietary file format that only IronMail can read, and cannot be viewed in Plain Text. The encryption method is "one way"—even CipherTrust Technical Support cannot decrypt this file. The "zip" file extension has been supplied to the backup file name solely for the purpose of "tricking" a browser into downloading the file, rather than trying to open it. Do not forget the password!

Restore

If more than one IronMail appliance is installed in the enterprise, the configuration settings and policies of one may be easily and quickly "pushed" to the others using this Restore function. (Software feature licenses—e.g., for IronWebMail, Secure WebDelivery, Anti-Virus, etc.—cannot be pushed to other appliances via this "restore" method.)

The screenshot shows a web interface for restoring configuration. At the top, there is a header "Configuration Restore". Below it, a text box instructs the user: "Browse to a saved Configuration file, enter the password associated with it, and click Submit. After clicking Submit, IronMail must restart the web server." Below this is a section titled "Restore Information" containing two input fields: "File Location:" with a "Browse..." button, and "Password:". At the bottom of the form are three buttons: "Submit", "Reset", and "View Log File".

Browse to the backup file previously created, and enter the password associated with that file. IronMail reads all the configuration data and enters it into the appliance.

When IronMail saves a backup configuration to disk, it uses an automatic naming scheme, identifying the appliance's name, version number, latest release number, and date (e.g., "myironmail.3-0.1-5.200201011352.zip"). The name of the IronMail is stored within the backup file that is created. Therefore, under no circumstances rename or edit this file!

Changing the file's name will cause the Restore function to fail, and may produce other unintended consequences. Regardless of the IronMail name with which the backup file is associated, it may be safely restored to any other IronMail appliance.

Note: When an IronMail configuration is backed up, that appliance's host name, IP address and subnet are saved. Restoring that backup configuration to another IronMail appliance, however, will not over-write the second box's host name, IP address, and subnet.

E' possibile installare il server di quarantena sullo stesso appliance della management console?

- ▶ No, la CMC (Centralized Management Console) è un appliance dedicato.

]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

E' possibile bloccare attacchi di tipo Denial of Service e bloccare automaticamente il sorgente dell'attacco?

► Si, sia attraverso il blocco dell'indirizzo di posta mittente, sia attraverso il blocco dell'indirizzo IP sorgente

The Mail-IDS (Intrusion Detection System) program area provides a variety of tools designed to detect network attacks against the email gateway, as well as a tool to test for weaknesses or vulnerabilities in specific internal mail servers. IronMail will automatically generate alerts for certain types of network attacks, notifying administrators immediately by email, pager, or SNMP that an event has occurred. For all attack events, IronMail will log their occurrence so they may be viewed in IronMail's log files and daily reports, and in IronMail's Dashboard. Administrators, therefore, should configure IronMail's Alert Manager (*Monitoring > Alert Manager*) to send to them alerts that the Mail-IDS services generate. And administrators should routinely monitor IronMail's Dashboard and Mail-IDS Report throughout each day.

Application Level Protection

- Denial of Service Protection
- Password Strength
- Password Cracking
- Configure

Network Level Protection

- Analysis Console
- Configure
- Signature Manager
- Footnotes

Protection at the System Level

- Program Integrity
- Filesystem Integrity

Anomaly Detection

- Configure
- Anomaly Rules

Vulnerability Assessment

Ironmail è in grado di spedire trap SNMP al sistema CA Unicenter?

► Si, IronMail supporta completamente il protocollo SNMP V2 ed è in grado di spedire traps ad una SNMP console.

► Qualsiasi prodotto che supporta lo standard SNMP V2 potrà ricevere traps dall'appliance Ironmail.

► Ciphertrust fornisce il proprio MIBs

]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

Come viene erogato il servizio di reportistica?

- ▶ Ci sono parecchi builtin reports già predefiniti (html e graphs) e disponibili attraverso l'utilizzo dell'interfaccia grafica di amministrazione.
- ▶ Per esigenze specifiche, IronMail genera files CSVs per la costruzione dei propri customs reports.

IronMail can generate daily reports in HTML format showing detailed information about the messages it processed each day. Additionally, the reports may be archived as "CSV" (comma separated values) files, for analysis in third-party applications.

While Reports provide a "high level" overview of IronMail's message-processing activity, Logs show "low level"—or detailed—information about message processing at the level of the individual message. Depending on the logging level configured for each IronMail subsystem, the logs will report on the specific steps it took when processing individual messages. While logs are used primarily by CipherTrust Support engineers for troubleshooting purposes, administrators are well advised to become familiar with them as well. (Summary logs can also be exported in "real time" as SysLogs.)

All messages that IronMail processes (with the exception of messages IronMail drops because of an email policy's action) may be saved to disk and archived.

IronMail generates its Reports and Logs, and archives messages, at approximately 12:30 AM each morning. Note that because IronMail generates these files the next day, the files' date will be offset from the date of the actual data by one day. For example, a report dated January 27th, 2003 contains data about messages IronMail processed on January 26th, 2003.

E' possibile schedulare la generazione di un report e spedire il risultato ad un indirizzo e-mail?

- ▶ Si. Basta configurare opportunamente l'appliance attraverso l'utilizzo dell'interfaccia grafica di amministrazione.

Come viene erogato il servizio di monitoring e logging?

- ▶ IronMail gestisce 30 differenti tipi di logs (uno per ogni processo + summary logs).
- ▶ Si può configurare il livello di ciascun log.
- ▶ IronMail supporta anche il formato syslog.

IronMail's reporting and monitoring tools are what make IronMail such a robust and usable appliance. Through its logs, administrators can determine exactly which IronMail processes

]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

examined a message—indeed, whether or not IronMail even received the message. When an IronMail policy acts upon a message, the reports and logs will describe exactly what condition of the policy caused IronMail to act.

In addition to reporting on IronMail's internal message-processing, this program area also contains "Health Monitor"—a subsystem that examines all other core application subsystems, as well as hardware, to ensure that the appliance is operating as designed. And on the belief that IronMail cannot truly protect an enterprise's email system if the appliance, itself, is vulnerable, an Alert Manager generates email, pager, or SNMP trap alerts to the administrator whenever Health Monitor detects that IronMail is not performing as designed.

Health Monitor

Health Monitor is an IronMail subsystem that examines the appliance's overall performance, running a series of tests to ensure that all services and processes are performing as designed. Health Monitor "wakes up" at a user-defined interval and runs automatically in the background to test its many subsystems. IronMail will also monitor the status of any internal servers that are "in-line" with IronMail. (Health Monitor will send the mail server a connection request to ensure that it is responsive. Note that if an intermediary device is between IronMail and the mail server, Health Monitor will incorrectly infer from the intermediary device's response that the internal server is functioning normally.)

IronMail offers 6 levels of logging, primarily to assist CipherTrust Support engineers when technical support is required. Logging at "level 1" records minimal information; logging at "level 6" records the most information.

Ordinarily, IronMail's logs should be set to "6" during the first several weeks after the appliance is installed. This provides the detailed information required when troubleshooting any problems during the initial integration of IronMail into the network. Because IronMail's logs can easily grow in size—especially in high mail-volume environments (50,000+ message per day)—administrators are encouraged to lower the log level to "3" afterward, which is adequate for most purposes. Anytime more detail is required, administrators can return to this "properties page" and temporarily raise the level.

View Health Monitor's log by navigating to *Monitoring > Reports/Log Files > Detailed Logs > "Int - Health Monitor."*

DNS Hijack Protection

IronMail's daily, as well as "on demand," Program Integrity and Filesystem Integrity tests (*Mail-IDS > System Level*) ensure that administrators know in a timely fashion if hackers have added, deleted, or tampered with any files on the IronMail appliance. DNS Hijack Protection extends that protection to the enterprise DNS server by comparing the "known, good" MX and A record information on the DNS servers with the MX and A record information IronMail has cached locally on disk. If the MX or A records on the DNS server ever change from what IronMail expects them to be, the administrator is immediately notified. IronMail can perform this DNS query and comparison every time Health Monitor performs its tests.

Alert Manager

IronMail continuously monitors its core subsystems, as well as its ability to communicate with internal mail servers. If any part of IronMail's functionality fails to perform as designed, IronMail will generate an "alert." The alerts, by themselves, don't do anything. Rather, the Alert Manager—which processes all IronMail-generated alerts—must be configured to send them to an administrator.

IronMail's alert management is configured on the basis of two groups:

]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

- **IronMail subsystems:** The IronMail application is comprised of seventeen core subsystems. Each one is designed to generate alerts when anomalous conditions are experienced. Administrators will create logical groupings of these seventeen subsystems.
- **Alert Levels:** IronMail is designed to look for specific types of problems—such as a subsystem stopping unexpectedly, or restarting after it was stopped. There are a finite number of anomalies that IronMail can report on (see the table of alerts). Each anomaly has been “hard coded” with one of seven “alert levels” indicating the degree of criticality of the problem. IronMail administrators will create an alert mechanism (email, pager, SNMP trap) for any or all of the “alert levels,” for each grouping of subsystem they have created.

SysLog Configuration

IronMail can generate and transmit the same data it generates for its *Summary Log*—*the Summary Log reports for each message it processes the date and timestamp, process ID, message ID, Action number and Action code, and other details*— (Monitoring > Reports/Log Files > Summary Logs) in SysLog format for integration with a network’s SysLog logging system.

In addition to configuring IronMail to communicate with the SysLog server—as provided below—the SysLog server must be configured to recognize IronMail’s data. IronMail uses the SysLog **User** facility and **Info** level for the data it sends. Therefore, a “user.info” variable must be created for `/var/log/ironmailname_syslog`.

Detailed Logs

IronMail records in its Detailed Logs all the actions it takes as it processes messages. The amount of detail recorded in these logs is controlled by the Logging Level configured for each of IronMail’s Queue Services and Mail Services. (For example navigate to *Mail-Firewall > Configure Mail Services > SMTP Service > “Log Level”* in the secondary properties window for the SMTP Service.)

Ordinarily, a log level of “3” is adequate for day-to-day monitoring—a value of “3” will provide enough information to indicate that a Service is running properly, and at that level, will not bloat in size to an unmanageable level. It is recommended, however, that the logging level for Mail services (e.g., SMTP/SMTPS, POP3, POP3S, etc.) be set to “6”—*the highest (Note that in high email-volume environments (50,000+ messages per day), with the logging level set to “6”—the highest—Detailed Logs can easily grow to 100 MB or more each day.)*—for the first several weeks after IronMail is placed in the “mail flow” of the network. This will ensure that adequate information is available if troubleshooting mail-flow problems is required. Once IronMail is processing messages without incident, the logging level should be lowered to “3.”

Similarly, the logging level for the Queue services (e.g., Content Filtering Queue, Anti-Spam Queue, etc.) should be raised to “6” during the period that “policy testing” is underway. A log level of “6” will be required to see the specific reasons a message was detected and acted upon by one of IronMail’s spam or email policies. Once the policy testing is complete, these log levels may be returned to “3.”

Note that in high mail-volume environments, some logs may grow very large, up to 100-200 MB in size. Log files larger than just 1 MB will typically take longer to open in IronMail’s web interface than administrators will care to wait. Administrators are encouraged, then, to use an SSH client (such as the freely available “Putty” client) to open these logs. Within the command line interface, logs open instantly, and queries within them, are as fast.

Summary Logs

Whereas the Detailed Log files record the specific actions IronMail takes when processing messages, the information is spread across multiple files. This Summary Log consolidates all message processing data into one file, and displays the information in a slightly different way.

]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

The Summary Log displays seven pipe-separated (“|”) fields of data. Each line in the Summary Log displays information about each IronMail process that examined or processed a message. Note that the descriptions of IronMail processes are not grouped together by message. The processes of multiple messages are commingled. As with the Detailed Logs, administrators must follow the “trail of bread crumbs” using the “Message Identifier” to trace a single message in this log. The Summary Log may be viewed in “real time” for troubleshooting and policy-tuning purposes, or it may be exported so that a third party application can perform advanced grouping, sorting, and querying within it.

The **first field** is the date and timestamp when the message was received by the SMTP Service. The **second field** is the “[process ID](#)”—a number used internally by IronMail to identify which IronMail processes are processing a message. For example, the JoinQ has one process number, while the SMTP Service has another process number.

The **third field** is the “message identifier”—a number IronMail uses to uniquely identify a message. If the message is accepted by the SMTP Service, the “message identifier” becomes the Message ID. If the message is not accepted by IronMail, this value will be the source IP address and port number.

The **fourth field** is the “Action” number—a “0” or “1”—indicating whether IronMail took an action on the message because of the rules of an email policy. A “0” means no action was taken—the message passed straight through IronMail untouched. A “1” means that IronMail performed some action on the message.

The **fifth field** is an internal numeric code representing the action IronMail took—a number representing, for example, whether IronMail stamped an outgoing message with a footer, or deleted a file attachment, etc. (See Action Codes for a list of all IronMail actions.)

The **sixth field** displays textual information returned by the process. For example, process “21” (the SMTP Service) will return the Mail From, Mail To, and Message ID number of a message, and the “200” process (the Virus Scan Queue) will report “No virus found in this message.”

The **seventh field** displays any details about the action as applicable. For example, a Mail Monitoring rule based on a particular Subject will have the text of the rule’s Subject displayed here.

IronMail can transfer Summary Log files to an archive server, either manually or automatically. If archive server information is provided in the six Archive Information input fields at the top of the page and the **Transfer** check box is selected in the table below, IronMail will automatically transfer the files at the specified hour. When the Archive Information input fields are left blank, or if the **Transfer** check box is deselected in the table below, Summary Logs may be manually transferred by entering archive server information in the secondary browser window that opens when clicking the **Show all files** hyperlink.