Configuring Inbound and Outbound Email

SL1 version 12.3.0

Table of Contents

Chapter

1

Introduction to Inbound and Outbound Email

Overview

This manual is intended for system administrators responsible for configuring SL1. SL1 can receive email messages from external sources and process those messages to trigger events, create tickets, and monitor the speed of email servers. It can also send email messages, either automatically for a number of different scenarios or manually at a user's discretion in some other scenarios.

This manual describes how to configure SL1 to process inbound and outbound email. You must configure the inbound and outbound email settings before configuring events from email, tickets from email, or email round-trip monitoring policies.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Infrastructure Requirements

To use the inbound email functions of SL1, you must configure your IT infrastructure so that at least one DNS MX record maps to the IP address of the Database Server or All-In-One Appliance. If a DNS MX record does not exist for the IP address of your Database Server or All-In-One Appliance, no email will be delivered to SL1. If you are not responsible for DNS records, ask your system administrator for help with this step.

Typically, the DNS MX record that maps to the IP address of the system will be a sub-domain of your primary domain. If you want email to be sent from outside your corporate network to your SL1 system, you might need to configure an externally accessible email address that forwards to the appropriate email address for the SL1 system. The general steps to do this in your email system are:

1. Configure a new mailbox for an address that uses your primary domain. For example, "support@company.com".
2. Create a mail contact for the address used by your SL1 system. For example, "ticket@monitoring.company.com".
3. Configure the mailbox you created in step 1 to automatically forward all mail to the contact you created in step 2.

Chapter

2

General Inbound and Outbound Email Settings

Overview

This chapter describes the global settings in SL1 that allow SL1 to receive and send email messages. You must configure SL1 as described in this chapter before defining policies for events from email, tickets from email, or email round-trip policies.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Configuring System Email Settings

To configure the system settings for email:

1. Go to the **Email Settings** page (System > Settings > Email).
2. To define settings for inbound email, provide values in the following field:
    - ***Authorized Email Domains***. Type the SMTP domains that SL1 will use to receive incoming mail. The list of domains should include:
        - All domains used for loopback addresses in email round-trip monitoring policies.
        - All domains used to generate tickets from emails.
        - All domains used to receive event messages from third-party monitoring systems.
        - Each entry in this field must be a fully-qualified email domain and cannot exceed 64 characters. If you include a list of domains, separate the list with commas.
        - Each domain in this field must be managed by the Database Server or All-In-One Appliance. This means that a DNS MX record must already exist or be created that maps each domain specified in this field to the Database Server or All-In-One Appliance. When creating the DNS MX record, use the fully qualified name of the Database Server or All-In-One Appliance as the name of the email server.
3. The other fields on this page pertain to outbound email and are not required to configure inbound email. However, if you want to define settings for outbound email, provide values in the following fields:
    - ***System From Email Address***. Type the default email address that SL1 should use to send outbound emails.

NOTE: Some outbound email servers, such as Gmail, might overwrite the ***System From Email Address*** value and instead use the email address of the authenticated user.

- ***Email Formal Name***. Type the name that will appear in the ***from*** field in email messages sent from SL1.
- ***Email Gateway***. Type the IP address or fully qualified name of the SMTP relay server used by SL1. Examples of when SL1 sends outgoing email messages are:
    - Automatically in response to Tickets from Email policies.
    - Automatically in response to changes in a ticket (ticket is assigned, edited, or resolved).
    - Automatically based on Ticket Escalation policies.
    - Automatically when executing Email Round-Trip Monitoring policies.

- Automatically when executing Run Book policies that include email actions.
- Automatically based on Report Jobs policies.
- Manually, when a user selects the **Send Message** page from the ticket panel pages.

NOTE: To use the email server that is built in to SL1, type the IP address or fully qualified name of the Database Server or All-In-One Appliance in the ***Email Gateway*** field. If SL1 cannot use its built-in SMTP relay server to route email messages directly to their destination server (for example, due to firewall rules or DNS limitations), SL1 can use another relay server. If you do so, make sure you have configured your network to allow the Database Server or All-In-One Appliance to access this SMTP Relay server.

NOTE: The ***Email Gateway*** field must be configured to use the appropriate port number to use, which is designated by a preceding colon. When no port number is specified, SL1 uses the default SMTP port (25).

- ***Email Gateway Alt***. Type the IP address or fully qualified name of the SMTP relay server SL1 should use if the primary email gateway is unavailable.
- ***Escalation Notify Subject***. Type the subject line that SL1 will use when sending ticket escalation notification emails.

NOTE: The ***Escalation Notify Subject*** field can include one or more variables. For a list of the variables you can include, see the section on "Global Settings for Inbound Email and Outbound Email" in the ***System Administration*** manual.

4. Click **[Save]**. If the settings were saved successfully, the message "Email Settings Saved" is displayed at the top of the page.

System Settings that Affect Inbound Email

To define global settings that affect all inbound email, perform the following steps:

1. Go to the **Behavior Settings** page (System > Settings > Behavior):
2. To define settings for inbound email, provide the following values in the following field:

   - ***Strip FQDN From Inbound Email Device Name***. In Events from Email policies, specifies how SL1 will match the regular expression for device name. Choices are:

     - *Enabled*. SL1 will search the text string in the incoming email and match all characters up to the first period that appears in the text string. If multiple devices in SL1 match the characters up to the first period (for example, my_device.1 and my_device.2), SL1 will align the event with the matching device with the highest Device ID.

  - *Disabled*. SL1 will search the text string in the incoming email for a match for the device name. The text string must include an exact match to the regular expression (defined in the Events from Email policy), including any text following a period in the device name. If SL1 does not find an exact match in the incoming email, SL1 creates an entry in the system log.

- ***Inbound Email Alert Message.*** In each event policy, the ***First Match String*** and ***Second Match String*** fields specify the string or regular expression used to correlate the event with a log message. To trigger an event, the text of a log message must match the value in the ***First Match String*** and ***Second Match String*** fields in that event's policy. For Events from Email policies, this field specifies whether only the email message body will be written to the device log or whether both the email message subject and email message body will be written to the device log. Choices are:

  - *Email Message Body Only*. Only the email message body is written to the device log. The ***First Match String*** and ***Second Match String*** fields can examine and match only the email message body.

  - *Email Message Subject and Body*. Both the email message body and the email message subject are written to the device log. The ***First Match String*** and ***Second Match String*** fields can examine and match against both the email message body.

NOTE: The global setting ***Inbound Email Alert Message*** affects how events are triggered. This field does not affect the ***Regex Pattern*** field in the Event from Email policy. The ***Regex Pattern*** field in an Event from Email policy specifies the device log to which the alert should be written.

3. Click the **[Save]** button.

Enabling TLS for Inbound Email

By default, Transport Layer Security (TLS) is not enabled for incoming email. To enable TLS, you will need a valid TLS certificate and key file.

To enable TLS for inbound email:

1. Obtain the content of the TLS certificate file, like the following example:

```
-----BEGIN CERTIFICATE-----
MIIEGzCCAwOgAwIBAgIUAsngd+MwWuAV16vfpkljjLxtl+4wDQYJKoZIhvcNAQEL
BQAwgZwxCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhWaXJnaW5pYTEPMA0GA1UEBwwG
UmVzdG9uMRUwEwYDVQQKDAxTY2llbmNlbG9naWMxDTALBgNVBAsMBE1PU1MxFjAU
BgNVBAMMDU1PU1MtQUlPLTMtNDAxKzApBgkqhkiG9w0BCQEWHHlhbWluZy5zaGFv
QHNjaWVuY2Vsb2dpYy5jb20wHhcNMjQwNzE2MTcxMzI2WhcNMzQwNzE0MTcxMzI2
WjCBnDELMAkGA1UEBhMCVVMxETAPBgNVBAgMCFZpcmdpbmlhMQ8wDQYDVQQHDAZS
ZXN0b24xFTATBgNVBAoMDFNjaWVuY2Vsb2dpYzENMAsGA1UECwwETU9TUzEWMBQG
A1UEAwwNTU9TUy1BSU8tMy00MDErMCkGCSqGSIb3DQEJARYceWFtaW5nLnNoYW9A
c2NpZW5jZWxvZ2ljLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMCs98Y/CubDuuMlrbnQswdTvji9NoI87yory+LrIdO0eL8P/3SRWyIppccSdc+/
g4TNm6466+BK+bmtUkwizsTWBOUrORXf2xmXVdgMEIwccVnn5RxXfqPY+QbcI31v
uqfXSEvrVwBH03+amwiU/EgKkPQdmgYPWSOPa0nEZKsXcVvtp7I26CYluSYKlL/0
2OMcBS0YIa/RYG8S7+8fG3NKqytiTfDOEx9W1p0lm/nusXGtntOvwLE8gzE+Nz3U
IQ4ta8FLgj8w9sODOZCovYZisuQu+KiXNXqN42CcT6/PE35XmGrw3U2YXEx1NPIS
zEOP7jyIRjo1hoKY2NbywnMCAwEAAaNTMFEwHQYDVR0OBBYEFEhdXy/hDkvwyXDT
mcc7+TjN8wcaMB8GA1UdIwQYMBaAFEhdXy/hDkvwyXDTmcc7+TjN8wcaMA8GA1Ud
EwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAJP2BIJwIaVeYksgjPlpEBC9
qQFA+QNsjs/wReiPTRjiw8IfEvL05/ezBrdRf41pO9ETaCXrpZN5L7vtT6kn8Foc
69GL8uGUU6kKxqwsdHF8CEBj8rvHJLVnuGSJvgPP4BBOLrMjBE4uzAh5Vd7z6Bsh
NZFHmtw5QeqOafWVwBJL4KiRbTlU1RBOrP3gE2WybpEOBeQDtIqovR+noYDUMyVc
Z20jjk3LkWjIUS8knfK8Wf73wF9s4wTTnYfaoLweymFT0/geXzhkm8lHYatVG7e/
xgZdw5/cSsHToNvO5jriAoR/GDtZUlhw1q2qv+JRY5Hs+jrCxq/ZpIMA1mDUATU=
-----END CERTIFICATE-----
```

2. Obtain the content of TLS key file, like the following example:

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQDArPfGPwrmw7rj
Ja250LMHU744vTaCPO8qK8vi6yHTtHi/D/90kVsiKaXHEnXPv4OEzZuuOuvgSvm5
rVJMIs7E1gTlKzkV39sZl1XYDBCMHHFZ5+UcV36j2PkG3CN9b7qn10hL61cAR9N/
mpsIlPxICpD0HZoGD1kjj2tJxGSrF3Fb7aeyNugmJbkmCpS/9NjjHAUtGCGv0WBv
Eu/vHxtzSqsrYk3wzhMfVtadJZv57rFxrZ7Tr8CxPIMxPjc91CEOLWvBS4I/MPbD
gzmQqL2GYrLkLviolzV6jeNgnE+vzxN+V5hq8N1NmFxMdTTyEsxDj+48iEY6NYaC
mNjW8sJzAgMBAAECggEAPhX+aXVbD+02RYeYqW2kotHLVAE0lVcJQi+GrYJTDiLz
Xa3MBUXpdeKxtqouKFlwCdUvOz9lTosaWUiOYlY9BpRoU2hQJspRkbeAQ/PvSRbJ
N81PuIhBGI8L/7fj/8GHBhqLA1u8VyzN7CpnlqZbfONavi7juNwtPxYx3j1YqwB9
JzS4wGdr4y+1XazJc3tXI3qHAAGgUAvhvcuwuLsIQluwOGvhYl+5QdXBvJ+zqOZ0
ylckh/OaJ8obfuEbHnTxAdvaCyihPBNPOj65HZvJnU8yNaO8apeezmALWfBGaB+o
WapGkiaXpQIt3AnE7FD3VX8MxWLLvTA+8AIFSPP/wQKBgQDyqKeJWGhThULt31CO
IMS+Qe3bBuNtxambyJAZ/NvBnT2tgB5f09lFMlByx7S+luU3Ty06j0gCVztaBjCp
LTRnQWnGQ0CibArfL1z0Gh/HkZIodKsocNUdydCDryL8iCYJSZg+Sbawj2dlcqLi
9YcQOJSpYbvO2CQ8VjT/YPxIQwKBgQDLRNEEXv5EM4wQYZaEmBlOdHPvZdc2FqqS
LUUmoK6+N3d3eSBEvIWGjgWYV9wrIePaYGxhE/A9cySjtpkn85P5PRRh7y82XrHf
EdWwjEWFeMTP6Szxn4A6F/zZjCQ+9EjzybMOoGakXwhqpBmKIuDKDP06w3sDwpw1
4KNOdDnSEQKBgDGblRSZBEr+1V3352oG/PHAXLYIRHpujGwSppMJhIuib7eGl68T
ijmBPb0ZYrQL+TRDdYWhQSFpX/LZjR0o5qutTciAezg5SkeyURh+Nrz/35dxsoQD
/S2n0n75UPe7hbskVoF1ZGnYB1VQCEjJ1SDV0F6IYnK48T98iD0lQK4tAoGADgtD
JboqdyvYkYksjRy1IuaI3BF9PQ9z2YWnMXQInrvWVTrZL+aWkyVc3Zm0bIZ656uh
0VM/Vf+OmIEVM91wa9f8gIe2C1ufjnn8+aW3Z/FgJ71Eja0nftwJbD5ygqb+I1nc
NTZ/4Ptv6W5NFW4zecJL/LNk3G2lvVM39UOyewECgYBmI04hXERWEAZRiDKDSpPd
3eKhLUQG5SX1LLYc3vos9d4U9ydrBWlJbKlXSpxtofGuGt1nCPOeT8KyrKInNhhp
3MwSc7PnqsQPzkSl224pfPusaaT4rfbcU5PmAmpdWAk4XfVj3z6qwQlonasi1cTt
EtpHMlXJJDPbeK8hVaQfog==
-----END PRIVATE KEY-----
```

3. Prepare the following query, using the above content as an example:

```
update master.system_settings_com set enable_tls=1, tls_certificate="
-----BEGIN CERTIFICATE-----
MIIEGzCCAwOgAwIBAgIUAsngd+MwWuAV16vfpkljjLxtl+4wDQYJKoZIhvcNAQEL
BQAwgZwxCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhWaXJnaW5pYTEPMA0GA1UEBwwG
UmVzdG9uMRUwEwYDVQQKDAxTY2llbmNlbG9naWMxDTALBgNVBAsMBE1PU1MxFjAU
BgNVBAMMDU1PU1MtQUlPLTMtNDAxKzApBgkqhkiG9w0BCQEWHHlhbWluZy5zaGFv
QHNjaWVuY2Vsb2dpYy5jb20wHhcNMjQwNzE2MTcxMzI2WhcNMzQwNzE0MTcxMzI2
WjCBnDELMAkGA1UEBhMCVVMxETAPBgNVBAgMCFZpcmdpbmlhMQ8wDQYDVQQHDAZS
ZXN0b24xFTATBgNVBAoMDFNjaWVuY2Vsb2dpYzENMAsGA1UECwwETU9TUzEWMBQG
A1UEAwwNTU9TUy1BSU8tMy00MDErMCkGCSqGSIb3DQEJARYceWFtaW5nLnNoYW9A
c2NpZW5jZWxvZ2ljLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMCs98Y/CubDuuMlrbnQswdTvji9NoI87yory+LrIdO0eL8P/3SRWyIppccSdc+/
g4TNm6466+BK+bmtUkwizsTWBOUrORXf2xmXVdgMEIwccVnn5RxXfqPY+QbcI31v
uqfXSEvrVwBH03+amwiU/EgKkPQdmgYPWSOPa0nEZKsXcVvtp7I26CYluSYKlL/0
2OMcBS0YIa/RYG8S7+8fG3NKqytiTfDOEx9W1p0lm/nusXGtntOvwLE8gzE+Nz3U
IQ4ta8FLgj8w9sODOZCovYZisuQu+KiXNXqN42CcT6/PE35XmGrw3U2YXEx1NPIS
zEOP7jyIRjo1hoKY2NbywnMCAwEAAaNTMFEwHQYDVR0OBBYEFEhdXy/hDkvwyXDT
mcc7+TjN8wcaMB8GA1UdIwQYMBaAFEhdXy/hDkvwyXDTmcc7+TjN8wcaMA8GA1Ud
EwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAJP2BIJwIaVeYksgjPlpEBC9
qQFA+QNsjs/wReiPTRjiw8IfEvL05/ezBrdRf41pO9ETaCXrpZN5L7vtT6kn8Foc
69GL8uGUU6kKxqwsdHF8CEBj8rvHJLVnuGSJvgPP4BBOLrMjBE4uzAh5Vd7z6Bsh
NZFHmtw5QeqOafWVwBJL4KiRbTlU1RBOrP3gE2WybpEOBeQDtIqovR+noYDUMyVc
Z20jjk3LkWjIUS8knfK8Wf73wF9s4wTTnYfaoLweymFT0/geXzhkm8lHYatVG7e/
xgZdw5/cSsHToNvO5jriAoR/GDtZUlhw1q2qv+JRY5Hs+jrCxq/ZpIMA1mDUATU=
-----END CERTIFICATE-----", tls_key="
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQDArPfGPwrmw7rj
Ja250LMHU744vTaCPO8qK8vi6yHTtHi/D/90kVsiKaXHEnXPv4OEzZuuOuvgSvm5
rVJMIs7E1gTlKzkV39sZl1XYDBCMHHFZ5+UcV36j2PkG3CN9b7qn10hL61cAR9N/
mpsIlPxICpD0HZoGD1kjj2tJxGSrF3Fb7aeyNugmJbkmCpS/9NjjHAUtGCGv0WBv
Eu/vHxtzSqsrYk3wzhMfVtadJZv57rFxrZ7Tr8CxPIMxPjc91CEOLWvBS4I/MPbD
gzmQqL2GYrLkLviolzV6jeNgnE+vzxN+V5hq8N1NmFxMdTTyEsxDj+48iEY6NYaC
mNjW8sJzAgMBAAECggEAPhX+aXVbD+02RYeYqW2kotHLVAE0lVcJQi+GrYJTDiLz
Xa3MBUXpdeKxtqouKFlwCdUvOz9lTosaWUiOYlY9BpRoU2hQJspRkbeAQ/PvSRbJ
N81PuIhBGI8L/7fj/8GHBhqLA1u8VyzN7CpnlqZbfONavi7juNwtPxYx3j1YqwB9
JzS4wGdr4y+1XazJc3tXI3qHAAGgUAvhvcuwuLsIQluwOGvhYl+5QdXBvJ+zqOZ0
ylckh/OaJ8obfuEbHnTxAdvaCyihPBNPOj65HZvJnU8yNaO8apeezmALWfBGaB+o
WapGkiaXpQIt3AnE7FD3VX8MxWLLvTA+8AIFSPP/wQKBgQDyqKeJWGhThULt31CO
```

```
IMS+Qe3bBuNtxambyJAZ/NvBnT2tgB5f09lFMlByx7S+luU3Ty06j0gCVztaBjCp
LTRnQWnGQ0CibArfL1z0Gh/HkZIodKsocNUdydCDryL8iCYJSZg+Sbawj2dlcqLi
9YcQOJSpYbvO2CQ8VjT/YPxIQwKBgQDLRNEEXv5EM4wQYZaEmBlOdHPvZdc2FqqS
LUUmoK6+N3d3eSBEvIWGjgWYV9wrIePaYGxhE/A9cySjtpkn85P5PRRh7y82XrHf
EdWwjEWFeMTP6Szxn4A6F/zZjCQ+9EjzybMOoGakXwhqpBmKIuDKDP06w3sDwpw1
4KNOdDnSEQKBgDGblRSZBEr+1V3352oG/PHAXLYIRHpujGwSppMJhIuib7eGl68T
ijmBPb0ZYrQL+TRDdYWhQSFpX/LZjR0o5qutTciAezg5SkeyURh+Nrz/35dxsoQD
/S2n0n75UPe7hbskVoF1ZGnYB1VQCEjJ1SDV0F6IYnK48T98iD0lQK4tAoGADgtD
JboqdyvYkYksjRy1IuaI3BF9PQ9z2YWnMXQInrvWVTrZL+aWkyVc3Zm0bIZ656uh
0VM/Vf+OmIEVM91wa9f8gIe2C1ufjnn8+aW3Z/FgJ71Eja0nftwJbD5ygqb+I1nc
NTZ/4Ptv6W5NFW4zecJL/LNk3G2lvVM39UOyewECgYBmI04hXERWEAZRiDKDSpPd
3eKhLUQG5SX1LLYc3vos9d4U9ydrBWlJbKlXSpxtofGuGt1nCPOeT8KyrKInNhhp
3MwSc7PnqsQPzkSl224pfPusaaT4rfbcU5PmAmpdWAk4XfVj3z6qwQlonasi1cTt
EtpHMlXJJDPbeK8hVaQfog==
-----END PRIVATE KEY-----
";
```

4. SSH to the SL1 server and run the query in step 3.
5. Log in to the SL1 user interface, go to the **Email** page (System > Settings > Email), and Click **[Save]**. By saving your existing email settings again, the certificate data provided in the previous steps will be updated within the configuration.

To verify that TLS is enable for inbound email:

1. SSH to the SL1 server and go to **/etc/postfix/main.cf**.
2. Verify that the following content exists in **main.cf**:

```
smtpd_tls_security_level = may
smtpd_tls_mandatory_protocols = !SSLv2,!SSLv3,!TLSv1
smtpd_tls_cert_file = /opt/em7/lib/python3/sl_
messaging/certificate/postfix.pem
smtpd_tls_key_file = /opt/em7/lib/python3/sl_
messaging/certificate/postfix.key
```

Chapter

3

Events from Email

Overview

SL1 can generate events based on emails that the system receives from external devices. Before configuring SL1 to generate events from email, you must follow the steps listed in the *General Inbound and Outbound Email Settings* section.

This chapter describes how to perform the following configuration tasks that are required before SL1 can generate events from email:

- *An email originator*. An email originator is a policy that defines how an inbound email should be processed to generate a log message for a device in the system.
- *An email event policy*. An email event policy defines how log messages generated from emails should generate events.
- *Correctly formatted inbound emails*.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

System Settings that Affect Events from Email

The **Behavior Settings** page (System > Settings > Behavior) allows you to define global parameters. The following parameter affects Event from Email policies:

- ***Strip FQDN From Inbound Email Device Name***. This field in the **Behavior Settings** page specifies how SL1 will match the regular expression for the device name in an Event from Email policy. Choices are:
  - *Enabled*. SL1 will search the text string in the incoming email and match all characters up to the first period that appears in the text string. If multiple devices in SL1 match the characters up to the first period (for example, my_device.1 and my_device.2), SL1 will align the event with the matching device with the highest Device ID.
  - *Disabled*. SL1 will search the text string in the incoming email for a match for the device name. The text string must include an exact match to the regular expression (defined in the Events from Email policy), including any text following a period in the device name. If SL1 does not find an exact match in the incoming email, SL1 creates an entry in the system log.
- ***Inbound Email Alert Message.*** In each event policy, the ***First Match String*** and ***Second Match String*** fields specify the string or regular expression used to correlate the event with a log message. To trigger an event, the text of a log message must match the value in the ***First Match String*** and ***Second Match String*** fields in that event's policy. For Events from Email policies, this field specifies whether only the email message body will be written to the device log or whether both the email message subject and email message body will be written to the device log. Choices are:
  - *Email Message Body Only*. Only the email message body is written to the device log. The ***First Match String*** and ***Second Match String*** fields can examine and match only the email message body.
  - *Email Message Subject and Body*. Both the email message body and the email message subject are written to the device log. The ***First Match String*** and ***Second Match String*** fields can examine and match against both the email message body.

NOTE: The global setting ***Inbound Email Alert Message*** affects how events are triggered. This field does not affect the ***Regex Pattern*** field in the Event from Email policy. The ***Regex Pattern*** field in an Event from Email policy specifies the device log to which the alert should be written.

Viewing the List of Event From Email Policies

TIP: To sort the list of policies, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Edit Date*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

The **Emailer Redirection** page (Events > Inbound Email) displays the following information about each Event from Email policy:

- ***Originator Address***. Fully-qualified email address from which SL1 will accept event messages. If an incoming email message comes from the same email address as specified in this field, SL1 will process that email message as an event. The originator address is usually the address of another monitoring system that is escalating events through SL1. When used in this way, SL1 becomes a "manager of managers."
- ***Alignment Type***. Specifies how SL1 should handle inbound email messages that do not include a match with the ***Regex Pattern***. The ***Regex Pattern*** tells SL1 which element to align with the resulting event. Choices are:
  - *If device not found, discard unmatched email*. If the inbound email does not include text that matches the ***Regex Pattern***, discard the email. No event will be created from this instance of the inbound email.
  - *If device not found, align unmatched email with default element*. If the inbound email does not include text that matches the ***Regex Pattern***, align the email with the element specified in the ***Default Element*** field. The resulting event will be aligned with the ***Default Element***.
  - *Override device search, align email with default element.* Do not try to match the email with the ***Regex Pattern***. Instead, automatically align the email with the element specified in the ***Default Element*** field. The resulting event will be aligned with the ***Default Element***.
- ***Regex Type***. Part of the email message where the ***Regex Pattern*** will appear. Choices are:
  - Subject
  - Body
- ***Regex Pattern***. For classic regex pattern types, this is a specific, plain-text string that appears in the email directly before the name or IP address of the device to associate with the event message. For advanced regex pattern types, this is a regex pattern that SL1 uses to extract the value to use as hostname or IP address of the device to associate with the event message.

NOTE: This pattern does not trigger the event; it only informs SL1 which device to associate with the event message. SL1 will search all event definitions with a source of ***Email*** and then compare the entire email message to the ***Match String*** field in each event definition to determine if an event should be triggered.

NOTE: If the ***Regex Type*** is *Body*, and the email body is in HTML format, SL1 will strip out the HTML constructs before searching for the string or regex pattern.

  - For classic regex pattern types, SL1 will look for the specified text string in the email subject or body, find the device name or IP address that immediately follows it, and associate the message with the appropriate device. For example, if the ***Regex Pattern*** was "Alert for", and the ***Regex Type*** was *Subject*, and the email subject was "Alert for sc-xyz-33-12 - Settings changed", the string evaluation would return "sc-xyz-33-12 - Settings changed".

    - For advanced regex pattern types, SL1 will look for the specified pattern in the email subject or body and then extract the hostname or IP address of the device to associate with the event message. For example, if the ***Regex Pattern*** was "Alert for (.*)-", and the ***Regex Type*** was *Subject*, and the email subject was "Alert for sc-xyz-33-12 - Settings changed", the pattern evaluation would return "sc-xyz-33-12".

- ***Default Element***. If in the ***Alignment Type*** field, one of the following options is selected, followed by the default element to use:

    - *If device not found, align unmatched email with default element*.
    - *Override device search, align email with default element*.

  The default element can be an Organization, Device, Asset, Interface, Vendor, User Account, or Virtual interface.

NOTE: If the ***Default Element*** is not associated with the current user's organization, this field will display the value *Restricted*.

- ***ID***. Unique, numeric ID associated with the Event from Email policy. SL1 automatically assigns this ID to the policy.
- ***Edit User***. The user who created or last edited the Event from Email policy.
- ***Edit Date***. Date the Event from Email policy was created or last edited.

Filtering the List of Event From Email Policies

The **Emailer Redirection** page includes six filters, in the top row in the list of policies. You can specify one or more parameters to filter the display of Event from Email policies. Only Event from Email policies that meet all the filter criteria will be displayed in the **Emailer Redirection** page.

You can filter by one or more of the following parameters. The list of Event from Email policies is dynamically updated as you select each filter.

- For each filter except ***Edit Date***, you must enter text to match against. SL1 will search for Event from Email policies that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:
  - , (comma). Specifies an "or" operation. For example:

    "dell, micro" would match all values that contain the string "dell" OR the string "micro".
  - & (ampersand). Specifies an "and" operation. For example:

    "dell & micro" would match all values that contain the string "dell" AND the string "micro".
  - ! (exclamation mark). Specifies a "not" operation. For example:

    "!dell" would match all values that do not contain the string "dell".
- ***Originator Address***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Emailer Redirection** page will display only Event from Email policies that have a matching originator email address.
- ***Alignment Type***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Emailer Redirection** page will display only Event from Email policies that have a matching alignment type.
- ***Regex Type***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Emailer Redirection** page will display only Event from Email policies that are associated with a matching regex type (either Body or Subject).
- ***Regex Pattern***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Emailer Redirection** page will display only Event from Email policies that include a matching regex pattern.
- ***Default Element***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Emailer Redirection** page will display only Event from Email policies that include a matching default element.
- ***ID***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Emailer Redirection** page will display only Event from Email policies that include a matching ID.
- ***Edit User***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Emailer Redirection** page will display only Event from Email policies that have a matching "created by" or "edited by" value.
- ***Edit Date***. You can select from a list of time periods. The **Emailer Redirection** page will display only Event from Email policies that have been created or edited within that time period. Choices are:
  - *All*. Display all policies that match the other filters.

- *Last Minute*. Display only policies that have been created within the last minute.
- *Last Hour*. Display only policies that have been created within the last hour.
- *Last Day*. Display only policies that have been created within the last day.
- *Last Week*. Display only policies that have been created within the last week.
- *Last Month*. Display only policies that have been created within the last month.
- *Last Year*. Display only policies that have been created within the last year.

Configuring an Event from Email Policy

SL1 uses each Event from Email policy to determine whether an incoming email comes from a source that is authorized to trigger events. Perform the following steps to configure an email originator:

1. Go to the **Emailer Redirection** page (Registry > Events > Inbound Email):
2. In the **Emailer Redirection** page, click the **[Create]** button. The **Add Policy** modal page appears.
3. To define the Event from Email policy, supply values in the following fields:

    - ***Originator Address.*** Enter the fully-qualified email address from which SL1 will accept event messages. If an incoming email message comes from the same email address as specified in this field, SL1 will process that email message as an event. The originator address is usually the address of another monitoring system that is escalating events through SL1. When used in this way, SL1 becomes a "manager of managers."
    - ***Alignment Type***. Specifies how SL1 should handle inbound email messages that do not include a match with the ***Regex Pattern***. The ***Regex Pattern*** tells SL1 which element to align with the resulting event. Choices are:

        - *If device not found, discard unmatched email*. If the inbound email does not include text that matches the ***Regex Pattern***, discard the email. No event will be created from this instance of the inbound email.
        - *If device not found, align unmatched email with default element*. If the inbound email does not include text that matches the ***Regex Pattern***, align the email with the element specified in the ***Default Element*** field. The resulting event will be aligned with the ***Default Element***.
        - *Override device search, align email with default element*. Do not try to match the email with the ***Regex Pattern***. Instead, automatically align the email with the element specified in the ***Default Element*** field. The resulting event will be aligned with the ***Default Element***.

    - ***Regex Pattern.*** Enter a specific string that appears directly before the name or IP address of the device to associate with the event message. SL1 will then find the device name or IP address in the email message and associate the message with the appropriate device. See the ***Formatting Inbound Emails*** section for more information.
    - ***Regex Pattern Type*** Specify if you want advanced control over the regex behavior. Choices are:

    - *Classic*. Select this option if you want the SL1 to use simple text matching to search for the ***Regex Pattern***.
    - *Advanced*. Select this option if you want the SL1 to search for the ***Regex Pattern*** using advanced regex. Advanced regex patterns can be up to 255 character in length and support all of the special characters supported by Python regex.

> NOTE: The ***Regex Pattern*** string does not trigger the event; this string only informs SL1 which device to associate with the event message. To trigger an event, SL1 will search all event definitions with a source of ***Email*** and then compare the entire email message to the ***Match String*** field in each event definition.

- ***Regex Type.*** Select either *Body* or *Subject* from the drop-down list. This is the part of the email message where the ***Regex Pattern*** will appear.
- ***Default Element***. If you selected *If device not found, align unmatched email with default element* or *Override device search, align email with default element* in the ***Alignment Type*** field, then the ***Default Element*** field specifies the default element to use. Clicking on the binoculars icon (🔍) opens the **Element Alignment** modal page, where you can search for and select a default element. The default element can be an Organization, Device, Asset, Interface, Vendor, User Account, or Virtual Interface.

> NOTE: If the ***Default Element*** is not associated with the current user's organization, this field will display the value *Restricted*.

4. Click the **[Save]** button.
5. An email originator must be created for each address/regex combination that you will use to create events from email.

Creating an Event Policy of Type "Email"

When SL1 receives an inbound email message that is authorized to trigger events and successfully matches the email to a device, SL1 compares the email message against all event policies with a source of ***Email***. If the email message does not match one or more event policies, SL1 will not generate an event but will add the email message to the device logs of the matched device.

This section will describe how to create an event policy of type "email" and how to define matching criteria based on the contents of the email. For information on additional event options, such as occurrence count/time, detection weight, identifier patterns/formatting, auto-clearing, and expiry delays, see the ***Events*** manual.

To create an event policy of type "email", perform the following steps:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Click the **[Create]** button. The **Event Policy Editor** page appears.
3. To define an event policy based on an incoming email message, supply values in the following fields:

- ***Event Source.*** Select *Email* from the drop-down list.
- ***Policy Name.*** Enter a name for the policy.
- ***Event Message.*** Enter the message associated with this event. To use the body of the email as the event message, leave the default value of "%M" in this field. For more information on Event Message formatting, see the ***Events*** manual.
- ***Event Severity.*** Select a severity for this event from the drop-down list.
- ***Policy Description.*** Enter a description of the event. This field is optional.

4. Click the **[Save]** button.
5. The event policy will now match every valid email message received from authorized external devices. To configure the event policy to match only against emails containing specific text, perform the following steps.
6. Click the **[Advanced]** tab.
7. Provide values in each of the following fields:

    - ***Match Logic.*** Select either *Text Search* or *Regex Match* from the drop-down list. If you select *Text Search*, the SL1 system will use simple text matching to compare strings. If you select *Regex Match*, the SL1 system will use regular expressions to compare strings.
    - ***First Match String.*** Enter the text string or regular expression that SL1 will compare to the text in the email subject or body.
    - ***Second Match String.*** Optionally, enter a second text string or regular expression. If you enter a value in this field, the email must match both the contents of the ***First Match String*** field and the ***Second Match String*** field for the event to trigger.

NOTE: Match Strings are compared to the subject and body of received emails.

8. Click the **[Save]** button.

Formatting Inbound Email

For SL1 to process events from inbound emails, you must configure your external devices to send email using certain formatting rules. Inbound emails must meet the following requirements to be processed as events by SL1:

- The email must be sent to the following address:

  ```
  notify@domain-name-of-SL1
  ```

  Where "domain-name-of-SL1" is one of the fully qualified domain names of the Database Server or All-In-One Appliance, i.e., one of the domain names you entered in the ***Authorized Email Domains*** field in the **Email Settings** page.

- The "from" address used by the external device must match an address defined in the ***Originator Address*** field in an email originator policy.

- The email message must contain a string that matches the regular expression defined in the ***Regex Pattern*** field in the email originator policy. If the email originator has the ***Regex Type*** set to *Body*, the string must be included in the email body. If the email originator has the ***Regex Type*** set to *Subject*, the string must be included in the email subject.
- The ***Regex Pattern*** string must be followed by the IP address, hostname, or device ID of a device monitored by the SL1 system. If an event is created, it will be associated with the specified device. For example, if the email originator has the ***Regex Pattern*** field set as "Event," the ***Regex Type*** set to *Subject*, and a device with an IP address of 192.168.1.1 is monitored in the system, a valid email subject would be:

```
Event 192.168.1.1
```

NOTE: There must be a space between the regex pattern and the IP address, hostname, or device ID.

- If you are using the "%M" substitution in your email event policies, ensure the message you wish to substitute is contained within the body of the email.
- If you are using Match Strings in your email event policies, ensure that matching text is contained within the body of the email.

NOTE: You can specify how an Event from Email policy will match a regular expression to a device name in the **Behavior Settings** page (System > Settings > Behavior).

How SL1 Processes Events from Email Policies

When SL1 receives an email from an Events from Email policy, SL1 examines all the Events from Email policies and executes the first policy that matches the incoming email.

SL1 will log debug messages for each policy that did not match the incoming email message. After SL1 finds the first matching policy, SL1 does not examine any other policies and does not generate any more debug messages.

If SL1 does not find any Events from Email policies that match the incoming email, SL1 generates the error message "E701 Could not match device to email...".

Chapter

4

Tickets from Email

Overview

SL1 can create tickets based upon email messages sent to SL1. Before configuring SL1 to create tickets from email, you must follow the steps listed in the *General Inbound and Outbound Email Settings* section.

This chapter will describe how to configure a Tickets From Email policy, which allows SL1 to generate tickets from email, and how to send an email message to trigger an automatic ticket.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (···).

This chapter covers the following topics:

Viewing the List of Ticket from Email Policies

TIP: To sort the list of policies, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again.

The **Tickets From Emails** page (Registry > Ticketing > Email Tickets) displays the following about each Ticket from Email policy:

- ***Policy Name***. Name of the Ticket from Email policy.
- ***Destination Email***. Fully qualified email address associated with the policy. SL1 will process all email messages received in this mailbox as tickets.
- ***Template***. Name of the ticket template the SL1 will use to create the ticket.
- ***Template ID***. Numeric ID for the ticket template SL1 will use to create the ticket.
- ***Edit User***. SL1 user who created or last edited the Ticket from Email policy.
- ***Edit Date***. Date the Ticket from Email policy was created or last edited.

Filtering the List of Ticket from Email Policies

The **Tickets From Emails** page (Registry > Ticketing > Email Tickets) includes filters in the top row in the list of policies. You can specify one or more parameters to filter the display of Ticket from Email policies. Only Ticket from Email policies that meet all the filter criteria will be displayed in the **Tickets From Emails** page.

You can filter by one or more of the following parameters. The list of Ticket from Email policies is dynamically updated as you select each filter.

- For each filter except ***Edit Date***, you must enter text to match against. SL1 will search for Ticket from Email policies that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:
  - , (comma). Specifies an "or" operation. For example:

    "dell, micro" would match all values that contain the string "dell" OR the string "micro".
  - & (ampersand). Specifies an "and" operation. For example:

    "dell & micro" would match all values that contain the string "dell" AND the string "micro".
  - ! (exclamation mark). Specifies a "not" operation. For example:

    "!dell" would match all values that do not contain the string "dell".
- ***Policy Name***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that have

a matching name.

- ***Destination Email***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that are associated with a matching destination email.
- ***Template***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that include a matching template name.
- ***Template ID***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that include a matching template ID.
- ***Edit User***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that have a matching "created by" or "edited by" value.
- ***Edit Date***. You can select from a list of time periods. The **Tickets From Emails** page will display only Ticket from Email policies that have been created or edited within that time period.

    - *All*. Display all policies that match the other filters.
    - *Last Minute*. Display only policies that have been created within the last minute.
    - *Last Hour*. Display only policies that have been created within the last hour.
    - *Last Day*. Display only policies that have been created within the last day.
    - *Last Week*. Display only policies that have been created within the last week.
    - *Last Month*. Display only policies that have been created within the last month.
    - *Last Year*. Display only policies that have been created within the last year.

Creating a Ticket from Email Policy

Perform the following steps to create a Ticket From Email policy:

1. Go to the **Tickets From Emails** page (Registry > Ticketing > Email Tickets).
2. In the **Tickets From Emails** page, click the **[Create]** button. The **Add Policy** page appears.
3. In the **Add Policy** page, provide a value in each of the following fields:

    - ***Policy Name.*** Enter a name for the policy.
    - ***Destination Email.*** Enter the email address to which ticket emails will be sent. The email address you enter in this field must use one of the fully qualified domain names of the Database Server or All-In-One Appliance, i.e., one of the domain names you entered in the ***Authorized Email Domains*** field in the **Email Settings** page. Each Ticket from Email policy should have a unique email address.
    - ***Reply Email.*** Enter the email address from which SL1 will send notification emails. Users will reply to this email address to add notes to tickets created from email.

- ***Ticket Template***. Select a ticket template from the drop-down list. For more information on creating a ticket template, see the ***Ticketing*** manual. The ticket template used will define the ticket queue and other attributes of tickets created by this Ticket from Email policy.
- ***Ticket Access***. Select a security level from the drop-down list. The following options are available:
    - ***Open Access***. Any email sent to the ***Destination Email*** address will create a ticket.
    - ***Any Registered Users***. Email sent to the ***Destination Email*** address from an email address associated with a user account in the SL1 system will create a ticket.
    - ***Registered Users in Queue***. Email sent to the ***Destination Email*** address will create a ticket if:
        - The "from" email address is associated with a user account in the SL1 system.
        - The user account also has access to the ticket queue defined in the ticket template.
- ***Ticket Creation Successful***. Message that indicates that a ticket has been created successfully from the email.
    - If included in this field, the characters "%t" (without quotation marks) will be replaced with the ticket ID of the newly created ticket.
    - If included in this field, the characters "%W" (without quotation marks) will be replaced with a link to the newly created ticket.
- ***Error: Sender not in Queue***. Message that indicates that the ticket could not be created because the ***Registered Users in Queue*** option has been set, and the sender's email address does not match a user account that has access to the ticket queue defined in the selected ticket template.
- ***Ticket Creation Failed***. Message that indicates that the ticket could not be created.
- ***Ticket Change Status/Update***. Message that indicates that a note added by email successfully updated a ticket.
    - If included in this field, the characters "%t" (without quotation marks) will be replaced with the ticket ID of the newly created ticket.
    - If included in this field, the characters "%W" (without quotation marks) will be replaced with a link to the newly created ticket.
- ***Error: Sender not Registered***. Message that indicates that the ticket could not be created because the ***Any Registered Users*** option has been set, and the sender's email address does not match a user account.

4. Click the **[Save]** button.

Sending an Email to Create a Ticket

To create a ticket, an inbound email must meet the following requirements:

- The email is sent to an address defined in the ***Destination Email*** field in a Tickets from Email Policy.
- The email is sent from an address that meets the criteria for the ***Ticket Access*** setting in the Tickets from Email Policy

If an inbound email meets both these criteria, a ticket will be created. The body of the email will be inserted as the first note in the ticket.

If the "%7" character is included in the ***Ticket Description*** field in the ticket template, the subject of the email will be substituted in for the "%7" character.

All other attributes of the ticket, such as queue and severity, are defined by the ticket template associated with the Tickets From Email policy.

Using Email to Add a Note to a Ticket

SL1 automatically sends a notice email (to the original sender of the email) if a ticket is created successfully from an email or if the ticket is updated with an email.

The user who receives the automatic notice email can add a note to the ticket by replying back to SL1. To add a note to the ticket, the user who receives the automatic notice from SL1 should:

- reply to the automatic notice
- not change the subject of the email
- in the body of the email, include the text to attach to the ticket

Chapter 5

Email Round-Trip Monitoring Policies

Overview

Email Round-Trip Monitoring Policies monitor round-trip email delivery. Each policy generates performance data for the time between SL1 sending an email to a device and SL1 receiving a reply email from the device.

To configure an Email Round-Trip Monitoring Policy, you must create the policy in SL1 and then configure the external device to reply to the emails from SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Viewing the List of Email Round-Trip Monitoring Policies

The **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip) displays the following about each email policy:

- ***Policy Name***. Name of the policy.
- ***Send Address***. Address to which the policy sends test messages.
- ***Policy ID***. Unique, numeric ID assigned to the policy automatically by SL1.
- ***Device Name***. Name of the device associated with the policy.
- ***IP Address***. IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- ***Device Category***. Device category of the device associated with the policy.
- ***Organization***. Organization for the device associated with the policy.

Filtering the List of Email Round-Trip Monitoring Policies

The **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip) includes seven filters. You can filter the list of policies by one or multiple of the following parameters: policy name, send address, policy ID, device name, IP address, device category, and organization. You can specify one or more parameters to filter the display of policies. Only policies that meet all the filter criteria will be displayed in the **Email Round-Trip Monitoring** page.

You can filter by one or more of the following parameters. The list of policies is dynamically updated as you select each filter.

- For each filter, you must enter text to match against. SL1 will search for policies that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:
    - , (comma). Specifies an "or" operation. For example:

      dell, micro

      would match all values that contain the string "dell" OR the string "micro".

    - ! (exclamation point). Specifies a "not" operation. For example:

      !dell

      would match all values that do not contain the string "dell".

- ***Policy Name***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching name.

- ***Send Address***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching send address.
- ***Policy ID***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching policy ID.
- ***Device Name***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching device name.
- ***IP Address***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching IP address.
- ***Device Class***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching device class.
- ***Organization***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching organization.

Creating an Email Round-Trip Monitoring Policy

Perform the following steps to configure an Email Round-Trip Monitoring policy:

1. Go to the **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip).
2. Click the **[Create]** button. The **Create Email Round-Trip Policy** modal window is displayed.
3. To create an Email Round-Trip policy, supply a value in the following fields:

    - ***Select Device.*** From the drop-down list, select the device to monitor. By default, the current device is selected in this field.

NOTE: Before you can define an Email Round-Trip policy, you must decide which managed device you want to associate with the policy. You might want to associate the policy with the device to which SL1 will send test messages, but you aren't required to do so. Alternately, you might want to create a virtual device to associate with an Email Round-Trip policy (for details on defining a virtual device, see the manual ***Managing Devices***). Although SL1 will use only the ***Send To Address*** to execute the policy, the reports that result from the Email Round-Trip policy will be aligned with the device you specify in the ***Select Device*** field.

- ***Policy Name.*** Enter a name for the policy.
- ***Validation Type***. Can select only *Email Round Trip*.
- ***Send To Address.*** Email address for external email server. Must be a valid email address. This mailbox must be configured to auto-respond to messages from the Email Round-Trip policy.
- ***Address Masquerade.*** Email address to use as *From* address. Must be a valid email address. You should choose an address that allows the external email client to easily identify the incoming email as one from the Email Round-Trip policy.
- ***Timeout.*** Number of seconds SL1 should wait for a response email message. If SL1 does not receive a response message after the specified number of seconds, SL1 generates an event.

- ***State***. Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:
  - *Enabled*. SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Processes) for the ***Data Collection: E-Mail round-Trip*** process.
  - *Disabled*. SL1 will not collect the data specified in this policy, from the device, until the ***State*** field is set to *Enabled*.
- ***Message Body*** Body of the email message to be sent. In some cases, the auto-responder on the external email server may search this message body. Therefore, you should choose a message body that allows the external email client to easily identify the incoming email as one from the Email Round-Trip policy.

4. Click **[Save]**.

CAUTION: SL1 will begin sending email to the specified address when the policy is created. You may wish to configure the monitored device before saving the policy.

Configuring the Monitored Device

For an Email Round-Trip Monitoring policy to work correctly, the monitored device must forward the received email back to the SL1 system. You must configure the monitored device to automatically forward the email when policy emails are received. Most email systems allow you to define rules that will automatically forward a received email when the received email meets certain criteria; refer to the documentation for the specific email system on your device for instructions on how to set up a rule for the Email Round-Trip policy. Follow these guidelines when defining your rule:

- Email received from SL1 for Email Round-Trip policies can be identified by the "from" address you defined in the ***Address Masquerade*** field and the body text you entered in the ***Message Body*** text area.
- The email generated by the monitored device must be sent from the same address the policy email was delivered to.
- The email generated by the monitored device must be sent to the following address:

  ```
  notify@domain-name-of-SL1
  ```

  Where "domain-name-of-SL1" is one of the fully qualified domain names of the Database Server or All-In-One Appliance, i.e., one of the domain names you entered in the ***Authorized Email Domains*** field in the **Email Settings** page.
- The subject of the email sent by SL1 must be included in the email generated by the monitored device.
- The body of the email sent by SL1 must be included in the email generated by the monitored device.

Chapter

6

Configuring Outbound Email

Overview

SL1 uses outbound email in a number of scenarios. Some examples of when SL1 sends outgoing email messages include:

- Automatically, in response to Tickets from Email policies
- Automatically, in response to changes in a ticket (such as when the ticket is assigned, edited, or resolved)
- Automatically, based on Ticket Escalation policies
- Automatically, when executing Email Round-Trip Monitoring policies
- Automatically, when executing Run Book policies that include email actions
- Automatically, based on Report Jobs policies
- Manually, when a user selects the **Send Message** page from the ticket panel pages

This chapter describes how to configure the following encryption and authentication options for outbound email in SL1:

- Encryption using SMTP with TLS or SMTPS
- SMTP authentication using PLAIN/LOGIN/CRAM MD5
- SMTP authentication using OAuth2 (for Office 365)

NOTE: While it is possible to configure SMTP encryption settings without implementing SMTP authentication for outbound email and vice versa, ScienceLogic recommends that you configure SMTP encryption if you are going to implement SMTP email authentication.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Configuring SMTP Encryption for Outbound Email

To ensure the security of outbound emails, ScienceLogic recommends implementing Simple Mail Transfer Protocol (SMTP) encryption. To configure SMTP encryption for outbound email in SL1, you must first know which encryption method your mail transfer agent (MTA) supports:

- SMTP with Transport Layer Security (TLS), which is widely accepted as the preferred method for SMTP encryption
- Secure SMTP (SMTPS), which is supported for MTAs that require it but otherwise is not considered a preferred option

Using SMTP with TLS Encryption for Outbound Email

To configure SL1 to use SMTP with TLS encryption:

1. Either use SSH to access the primary Database Server or All-In-One Appliance and log in as an administrator, or log in to the classic SL1 user interface as an administrator and go to the Database Tool page (System > Tools > DB Tool.

   > **NOTE:** The **Database Tool** page is available only in versions of SL1 prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

2. Run the following SQL query:

```
UPDATE master.system_settings_com SET secure = 2 WHERE comm_method = 0;
```

Using SMTPS Encryption for Outbound Email

To configure SL1 to use SMTPS encryption:

1. Either use SSH to access the primary Database Server or All-In-One Appliance and log in as an administrator, or log in to the classic SL1 user interface as an administrator and go to the Database Tool page (System > Tools > DB Tool.

   > **NOTE:** The **Database Tool** page is available only in versions of SL1 prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

2. Run the following SQL query:

```
UPDATE master.system_settings_com SET secure = 1 WHERE comm_method = 0;
```

Configuring SMTP Authentication for Outbound Email

To configure SMTP outbound email authentication in SL1, you must do the following:

1. Create a credential for SMTP authentication.
2. Link the credential to the outbound email settings.

The type of authentication you use is determined by your mail server:

- If you are using Office 365 for outbound email, then you should use OAuth2 SMTP authentication.
- Otherwise, you should use PLAIN, LOGIN, or CRAM-MD5 SMTP authentication.

Configuring SMTP Authentication Using PLAIN, LOGIN, or CRAM-MD5 for Outbound Email

To configure SMTP authentication for mail servers that support PLAIN, LOGIN, or CRAM-MD5 authentication methods:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and then select *Create Basic/Snippet Credential*. The **Create Credential** modal appears.
3. Supply values in the following fields:
    - ***Name***. Type a unique name for the credential.
    - ***Username***. Type the username to be used for SMTP authentication.
    - ***Password***. Type the password to be used for SMTP authentication.
    - ***Hostname/IP***. Type "%D".
    - ***Port***. Type "25".

> **NOTE:** You must have values in the ***Hostname/IP*** and ***Port*** fields in order to save and use the credential, but these field values are not actually used for authentication.

4. Click **[Save & Close]**.
5. On the **Credentials** page, make a note the ***ID*** number of the credential you just created.
6. Either use SSH to access the primary Database Server or All-In-One Appliance and log in as an administrator, or log in to the classic SL1 user interface as an administrator and go to the Database Tool page (System > Tools > DB Tool.

NOTE: The **Database Tool** page is available only in versions of SL1 prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

7. Run the following SQL query, replacing `<id>` with the credential ID that you noted in the step 5:

```
UPDATE master.system_settings_com SET auth_cred = <id> WHERE comm_method
= 0;
```

Configuring SMTP Authentication Using OAuth2 for Outbound Email

OAuth2—the Open Authorization 2.0 standard—uses a request/challenge exchange mechanism to retrieve authorization and refresh tokens.

- The authorization token is typically short-lived and is used for the SMTP authentication.
- The refresh token is used when the authorization token has expired and a new one is required.

ScienceLogic has created a helper script (smtp_auth_helper) that can help you perform the initial request/challenge exchange. After that exchange completes, the refresh token is cached and used to get authorization tokens as needed.

NOTE: Refresh tokens might expire after a set period of time or might be manually expired. The OAuth2 provider controls this expiry; SL1 does not.

Configuring OAuth 2 SMTP Authentication for Office 365

To configure OAuth2 SMTP authentication for Office 365:

1. Ensure that your Office 365 account is properly configured for OAuth2, and that the correct SMTP relay permissions are set.

NOTE: For information about configuring OAuth2 and setting the correct SMTP relay permissions for Office 365, refer to Microsoft's documentation.

2. In SL1, go to the **Credentials** page (Manage > Credentials).
3. Click the **[Create New]** button and then select *Create SOAP/XML Credential*. The **Create Credential** modal appears.
4. Supply values in the following fields:
    - ***Name***. Type a unique name for the credential.
    - ***URL***. Type "https://login.microsoftonline.com/".
    - ***HTTP Auth User***. Type the email address or username of the account used to send email.
    - ***Embedded Password***. Type the Client ID from your OAuth2 provider.

- ***Embed Value [%1***]. Type "oauth2/v2.0/devicecode".
- ***Embed Value [%2]***. Type "oauth2/v2.0/token".
- ***Embed Value [%3]***. Type your Tenant ID.
- ***Embed Value [%4]***. Type "offline_access https://outlook.office.com/SMTP.Send".

5. Click **[Save & Close]**.
6. On the **Credentials** page, make a note the ***ID*** number of the credential you just created.
7. Now, you must authorize the system to use OAuth2 tokens. To do so, use SSH to access the primary Database Server or All-In-One Appliance as an administrator, and then run the following command:

```
sudo smtp_auth_helper
```

```

```

8. Select option 2.
9. Follow the prompts by first entering the credential ID you noted in step 6 and then press Enter.
10. When the question, "Are you using o365?" appears, type "y" and then press Enter.
11. Verify the credential ID is correct, and then type "y" and press Enter.

NOTE: This will run the SQL query to enable SMTP encryption with TLS, and it will set the ***Email Gateway*** to outlook.office365.com:587 automatically.

12. The script will run a basic check of the credential to see if it contains the required information.
    - If information is missing, it will print an error and the script will exit. In this scenario, you should correct the errors and then rerun the script. Continue doing this until all errors are fixed.
    - If no information is missing, you can proceed to the next step.
13. A verification URL and verification code will appear. Open a web browser, copy and paste the full verification URL into the address bar, and then press Enter.
14. When prompted, copy and paste the verification code. You will then have 15 minutes to complete the remainder of the setup.
15. If your OAuth2 provider is configured correctly, you will prompted to log in to your Microsoft account and authorize your OAuth2 provider application for email permissions.
16. A message confirms whether the Oauth2 token retrieval was successful.

Testing SMTP Authentication

To verify that SMTP authentication is working as expected:

1. Use SSH to access the primary Database Server or All-In-One Appliance as an administrator, and then run the following command:

```
sudo smtp_auth_helper
```

2. Choose option 3. The system will perform a test of your mail server connection and authentication. No mail is sent during this test.
3. In the test output, confirm that the connection and authentication were successful.

TIP: The test output might be quite long. To determine if the test was successful, look in the last few lines for a message similar to "Authentication successful" to confirm that the authentication worked.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010