在14.X中配置UTF-8(IDN)域名

目录

简介

本文档介绍如何配置和使用在14.x代码中添加到安全邮件网关(ESA)和安全邮件云网关(CES)的新UTF-8国际域名(IDN)功能

作者：Anvitha Prabhu和Libin Varghese，思科TAC工程师。

要求

Cisco 建议您了解以下主题：

ESA概念和配置

使用的组件

本文档中的信息基于AsyncOS for ESA 14.0及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

14.x中支持的语言，用于IDN支持

印度地区语言

印地语、泰米尔语、泰卢固语、卡纳达语、 马拉蒂、旁遮普语、马拉雅拉姆语、孟加拉语、 古吉拉特语、乌尔都语、阿萨姆语、尼泊尔语、 孟加拉，波多，多格里、克什米尔、康卡尼、 迈蒂利、曼尼普里、奥里亚、梵语、桑塔利、信德、图鲁。

欧洲/亚洲语言

法语、俄语、日语、德语、乌克兰语、韩语、西班牙语、意大利语、中文、荷兰语、泰语、阿拉伯语、哈萨克语

IDN支持的格式

- 完整IDN域：अनअन्वतिा@जीमेल.कोम,ಅನ್ವಿತಾ@ಯಾಹೂ.ಜಕೊತ್
- 部分IDN域：.कोम,ಯಾಹೂ.ಜಕೊತ್
- ASCII、IDN组合：测试@जीमेल.कोम

IDN在哪里受支持？

SMTP路由

导航至"网络" — >"SMTP路由"->"添加路由"-> "添加IDN域" — > "提交"->

DNS域

我们可以在DNS服务器中添加或编辑IDN域。

导航至"Network -> DNS -> Edit settings -> "下的"Alternate DNS server overrides"下的"Add the IDN domain。
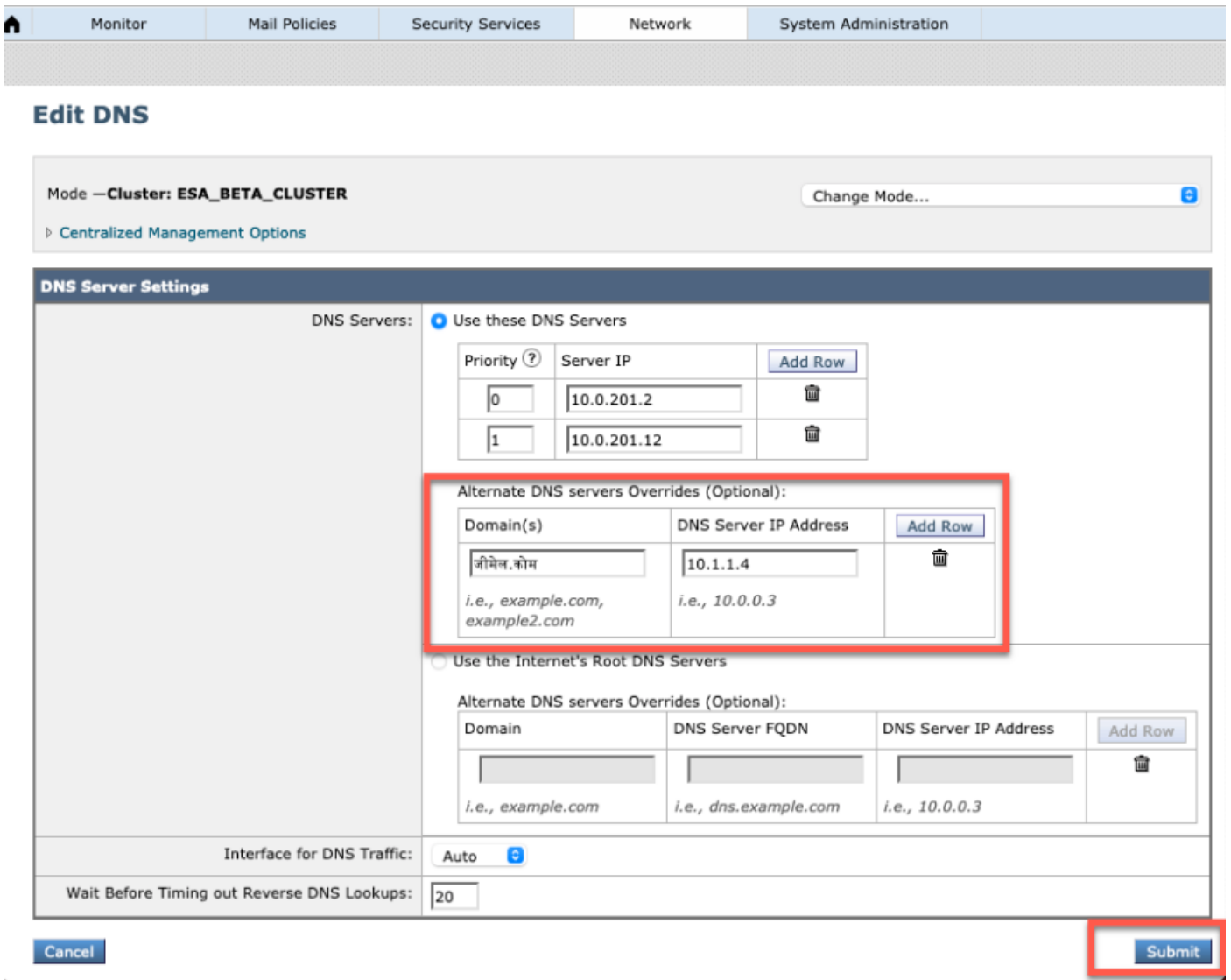
NOTE:

·公共IDN域由公共/Internet根DNS服务器解析。

·本地IDN域名：在本地DNS服务器中，创建区域文件，其中记录采用相当于IDN域的二进制代码格式[例如：xn‑2scrj9c.xn‑2scrj9c.]，以处理本地IDN域名的解析。

侦听器 — RAT/HAT

我们可以在以下方面使用IDN支持：

- 入站/出站侦听程序 — >在默认域中添加/编辑IDN域
- HAT/RAT ->在HAT/RAT中添加/编辑IDN域
- 使用IDN导入/导出HAT/RAT表

要使用IDN配置收件人访问表(RAT)，请导航到**邮件策略-> 收件人访问表(RAT)**，然后单击**添加收件人 — >添加IDN域 — >提交 — >提交**

Recipient Access Table Overview

Success — Recipient Access Table entry for "जीमेल.कोम" was added.

Mode —Cluster: **ESA_BETA_CLUSTER**   Change Mode...

▷ Centralized Management Options

Overview for Listener: Incoming   **Items per page** 20

Add Recipient...   Clear All Entries   Import RAT...

Order	Recipient Address	Default Action	All Delete
1	humaaralab.com	Accept	☐
2	doosralab.com	Accept	☐
3	जीमेल.कोम	Accept	☐
	All Other Recipients	Reject	

Edit Order...   Export RAT...   Delete

要配置主机访问表(HAT)发件人组（包含IDN域），请导航至邮件策略-> HAT概述 ->添加新发件人组 — > **提交并添加具有IDN主机名的发件人 — > 提交-> 提交-> 提交**

Sender Group: IDN_Support - Incoming

Success — Sender "जीमेल.कोम" was added.

Mode —Cluster: **ESA_BETA_CLUSTER**   Change Mode...

▷ Centralized Management Options

Sender Group Settings

Name:	IDN_Support
Order:	9
Comment:	IDN Support
Policy:	ACCEPTED
SBRS (Optional):	Not in use
External Threat Feed (Optional): *For IP lookups only*	None
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview   Edit Settings...

Find Senders

Find Senders that Contain this Text: ⑦		Find

Sender List: Display All Items in List   **Items per page** 20

Add Sender...

Sender	Comment	All Delete
जीमेल.कोम	idn sender	☐

<< Back to HAT Overview   Delete

NOTE:您可以按照相同的流程编辑任何发件人组并添加IDN域。

传入/传出邮件策略 — 发件人/收件人

要配置传入邮件策略以处理IDN，请导航至"邮件策略" -> "添加策略" -> "提供策略名称" — > "添加用户"

您可以选择在发件人/收件人中使用IDN域，或尝试任意组合 — >提交 — >提交

要配置传入邮件策略以处理IDN，请导航至"邮件策略" -> "添加策略" -> "提供策略名称" — > "添加用户"

您可以选择在发件人/收件人中使用IDN域，或尝试任意组合 — >提交 — >提交

Incoming Mail Policies

Add User

○ Any Sender
● Following Senders
○ Following Senders are Not

Email Address:

@ibixr.xbx

(e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group:

Query: LDAP.group

Group: [   ] [Add Group] [Remove]

○ Any Recipient
● Following Recipients

e-jre@ozxaza.zbaf

(e.g. user@example.com, user@, @example.com, @.example.com)

☐ Cisco Security Awareness not configured.

LDAP Group:

Query: LDAP.group

Group: [   ] [Add Group] [Remove]

☐ Following Recipients are Not

Email Address:

(e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group:

Query: LDAP.group

Group: [   ] [Add Group] [Remove]

[Cancel]   [OK]

NOTE:您可以按照相同的流程处理传出邮件策略。

异常表

要将IDN域名添加到例外表，请导航至

邮件策略 — >异常表->添加发件人验证异常-> 添加IDN域 — > 提交-> 提交

Sender Verification Exception Table

Success — Entry was added

Mode —Cluster: ESA_BETA_CLUSTER   Change Mode...

▷ Centralized Management Options

Find Sender Verification Exception

Search for Email Address: ⑦ [   ] [Find]

Sender Verification Exception Table

[Add Sender Verification Exception...]   [Clear All Sender Verification Exceptions]

Order	Exception	Behavior	SMTP Response	Delete
1	@जीमेल.कोम	Allow	N/A	🗑

地址列表

要将IDN域名添加到地址列表，请导航至

邮件策略 — >地址列表 — > 添加地址列表-> 在框中输入IDN域-> 提交-> 提交

Add Address List

Mode —Cluster: ESA_BETA_CLUSTER   Change Mode...

▷ Centralized Management Options

New Address List Details

Address List Name: [IDN-Support]

Description: [IDN-Support-test]

List Type:
- ○ Full Email Addresses only
- ○ Domains only
- ○ IP Addresses only
- ● All of the above

Addresses: [जीमेल.कोम, ఆస్త్రా@యాహూ.ఫోతె, @ @ಮಾಡುತ್ತೀರ] e.g.: user@example.com, user@, @example.com, @[1.2.3.4], @.example.com

[Cancel]   [Submit]

Address Lists

Mode —**Cluster: ESA_BETA_CLUSTER**   Change Mode...

▷ Centralized Management Options

Address Lists

Add Address List...

Address List Name	Description	Used for	Addresses	All Delete
IDN-Support	IDN-Support-test		(3) ಅನ್ವಿತಾ@ಯಾಹೂ.ಮೊತ, @जीमेल.कोम,...	☐

Delete

目标控制

要将IDN域名添加到目标控制，请导航至

邮件策略 — >目标控制 — >添加目标->您可以添加IDN域名 — > 提交-> 提交

| A | Monitor | Mail Policies | Security Services | Network | System Administration |

Add Destination Controls

Mode —**Cluster: ESA_BETA_CLUSTER**   Change Mode...

▷ Centralized Management Options

Destination Controls

Destination:	जीमेल.कोम
IP Address Preference:	Default (IPv6 Preferred)
Limits:	Concurrent Connections: ○ Use Default (500) ● Maximum of 500 (between 1 and 1,000) Maximum Messages Per Connection: ○ Use Default (50) ● Maximum of 50 (between 1 and 1,000) Recipients: ● Use Default (No Limit) ○ Maximum of 0 per 60 minutes Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60 Apply limits: Per Secure Email hostname: ● System Wide ○ Each Virtual Gateway (recommended if Virtual Gateways are in use)
TLS Support:	Default (None) DANE Support: ⑦ Default (None)
Bounce Verification:	Perform address tagging: ● Default (No) ○ No ○ Yes Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.
Bounce Profile:	Default Bounce Profile can be configured at Network > Bounce Profiles.

Note: DANE will not be enforced for domains that have SMTP Routes configured.

Cancel   Submit

Destination Controls

Success — Your changes have been committed.

Mode —**Cluster: ESA_BETA_CLUSTER**

Change Mode...

▷ Centralized Management Options

Destination Control Table

Items per page 20

Add Destination...

Import Table

Domain ▲	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
doosralab.com	Default	Default connection limit, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	☐
humaaralab.com	Default	Default connection limit, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	☐
जीमेल.कोम	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Default	Default	Default	Default	☐
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	None	Off	Default	

Export Table

Delete

* Bounce Verification settings apply only if bounce verification address tagging is in use. See *Mail Policies > Bounce Verification.*
^ DANE will not be enforced for domains that have SMTP Routes configured.

Global Settings

Certificate:	Client-Cert
Send an alert when a required TLS connection fails:	Enabled

Edit Global Settings...

退回配置文件

退回邮件和警告邮件的收件人可以在退回配置文件下配置IDN域名。

导航至**网络** -> **退回配置文件** -> **添加退回配置文件** ->输入名称 — >配置退回配置文件的值 — >为退回邮件和警告邮件的收件人 — >选择**替代地址**，然后您可以选择使用IDN域地址。

LDAP

您现在可以使用IDN域名进行LDAP接受/组查询，如图所示。

本地垃圾邮件隔离区

您可以看到本地SPM隔离区在用户电子邮件地址/域/主题中显示IDN域名

Search

Note: For best performance your search should contain an envelope recipient.

Messages Received: ○ Today ● Last 7 days ○ Date Range: [   ] and [   ]

Where [From ▾] [Contains ▾] : [   ]

Envelope Recipient ⑦ [Is ▾] : [   ]

[Clear Search]   14 items found   [Search]

Search Results   Items per page [25 ▾]

Displaying 1 — 14 of 14 items.

[Release] [Delete]

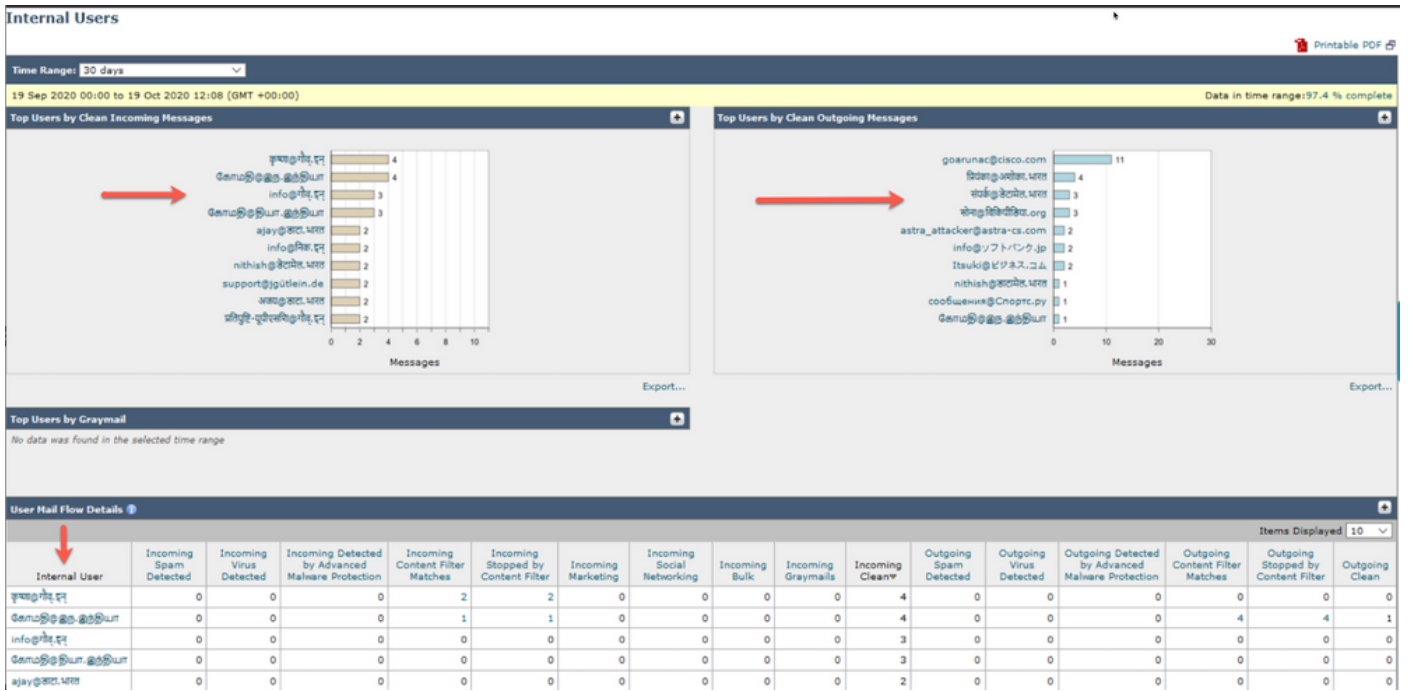| ☐	From	Envelope Recipient	To	Subject	Date ▾	Size
☐		anvitha@doosralab.com		[SUSPICIOUS MESSAGE] this is to test policy	10 Feb 2021 16:30 (GMT -06:00)	3.6K
☐	➡	अनअन्विता2@जीमेल.कोम		Please read as this is very என்று நம்புகிறேன் for both the countries. ⬅	09 Feb 2021 21:49 (GMT -06:00)	7.3K
☐	➡	あなたは誰ですか2@ヤフー.com		this is japanese test 今は17時38分です	09 Feb 2021 21:37 (GMT -06:00)	3.5K
☐		你是誰2@明天.在		Please read as this is very என்று நம்புகிறேன் for both the countries.	09 Feb 2021 21:18 (GMT -06:00)	3.4K
☐	➡	你是誰2@明天.在		Please read as this is very என்று நம்புகிறேன் for both the countries.	09 Feb 2021 17:13 (GMT -06:00)	7.6K
☐		anvitha@humaaralab.com		Please read as this is very என்று நம்புகிறேன் for both the countries.	09 Feb 2021 17:11 (GMT -06:00)	8.8K
☐		anvitha@humaaralab.com		Please read as this is very என்று நம்புகிறேன் for both the countries کو .	09 Feb 2021 17:02 (GMT -06:00)	4.7K
☐		anvitha@humaaralab.com		Please read as this is very என்று நம்புகிறேன் for both the countries.	09 Feb 2021 17:00 (GMT -06:00)	5.1K
☐		anvitha@humaaralab.com		Please read as this is very ಮೂಡುತ್ತಿದ್ದೀರಿ ಎಂದು ಭಾವಿಸುತ್ತೇನೆ for both the countries.	09 Feb 2021 16:54 (GMT -06:00)	5.2K
☐		anvitha@doosralab.com		this is a test	09 Feb 2021 16:01 (GMT -06:00)	3.3K
☐		anvitha@humaaralab.com		Please read as this is very என்று நம்புகிறேன் for both the countries کو .	09 Feb 2021 15:49 (GMT -06:00)	8.1K
☐		anvitha@humaaralab.com		Please read as this is very என்று நம்புகிறேன் for both the countries.	09 Feb 2021 15:41 (GMT -06:00)	8.8K
☐		anvitha@humaaralab.com		Please read as this is very आशा for both the countries.	08 Feb 2021 21:53 (GMT -06:00)	5.0K
☐		anvitha@humaaralab.com		Please read as this is very आशा for both the countries.	08 Feb 2021 21:47 (GMT -06:00)	3.9K

[Release] [Delete]

NOTE:本地PVO隔离区显示与垃圾邮件隔离区类似的行为。

验证和故障排除

1)有关ESA和SMA（安全邮件和Web管理器）的报告现在支持IDN。我们可以在报告中看到IDN格式的用户名/域/电子邮件地址

导航至**监控**->内**部用户**

2)在邮**件跟踪**中，我们可以看到IDN域名，也可以使用IDN域名/用户名/电子邮件地址进行过滤

3)使用CLI命令grep或tail查看"mail_logs"，并在日志中看到IDN域

```
Mon Feb  8 21:47:11 2021 Info: Start MID 23569633 ICID 148853
Mon Feb  8 21:47:11 2021 Info: MID 23569633 ICID 148853 From:
```

```
        <@.>



Mon Feb  8 21:47:19 2021 Info: MID 23569633 ICID 148853 RID 0 To: <test@lab.com>
Mon Feb  8 21:47:52 2021 Info: MID 23569633 Subject 'Please read as this is very  for both the
countries.'
Mon Feb  8 21:47:52 2021 Info: MID 23569633 SDR: Domains for which SDR is requested: reverse DNS
host: sample.host.com, helo: lab.com, env-from: ., header-from: Not Present, reply-to: Not
Present
Mon Feb  8 21:47:53 2021 Info: MID 23569633 SDR: Consolidated Sender Reputation: Tainted, Threat
Category: N/A, Suspected Domain(s) : lab.com. Youngest Domain Age: 3 months 29 days for domain:
lab.com
Mon Feb  8 21:47:53 2021 Info: MID 23569633 SDR: Tracker Header :
87dSxFfNYdSiOahrxSUZFOrdpenKiF6J2uKiPf+SFKCtj52hNCpe6LDQ8UFAliGnUDA7FsuXLvHTcaATt6AKG4PWLpwEeo/d
cIPBUOdxB48=
Mon Feb  8 21:47:53 2021 Info: MID 23569633 ready 605 bytes from

        <@.>



Mon Feb  8 21:47:53 2021 Info: MID 23569633 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Mon Feb  8 21:47:53 2021 Info: MID 23569633 interim verdict using engine: CASE spam positive
Mon Feb  8 21:47:53 2021 Info: MID 23569633 using engine: CASE spam positive
Mon Feb  8 21:47:53 2021 Info: ISQ: Tagging MID 23569633 for quarantine
Mon Feb  8 21:47:53 2021 Info: MID 23569633 interim AV verdict using McAfee CLEAN
Mon Feb  8 21:47:53 2021 Info: MID 23569633 interim AV verdict using Sophos CLEAN
Mon Feb  8 21:47:53 2021 Info: MID 23569633 antivirus negative
Mon Feb  8 21:47:53 2021 Info: MID 23569633 AMP file reputation verdict : SKIPPED (no attachment
in message)
Mon Feb  8 21:47:53 2021 Info: MID 23569633 using engine: GRAYMAIL negative
Mon Feb  8 21:47:53 2021 Info: MID 23569633 Custom Log Entry: SDR Age is less than 1 Year
Mon Feb  8 21:47:53 2021 Info: MID 23569633 Outbreak Filters: verdict negative
Mon Feb  8 21:47:53 2021 Info: MID 23569633 Message-ID '<d35764$mf971@esa1.lab.com>'
Mon Feb  8 21:47:53 2021 Info: MID 23569633 queued for delivery
Mon Feb  8 21:47:53 2021 Info: New SMTP DCID 250225 interface 10.0.202.17 address 10.0.201.5
port 6025
Mon Feb  8 21:47:53 2021 Info: DCID 250225 STARTTLS command not supported
Mon Feb  8 21:47:53 2021 Info: Delivery start DCID 250225 MID 23569633 to RID [0] to offbox
IronPort Spam Quarantine
Mon Feb  8 21:47:53 2021 Info: Message done DCID 250225 MID 23569633 to RID [0] (external
quarantine)
Mon Feb  8 21:47:53 2021 Info: MID 23569633 RID [0] Response 'ok:  Message 27293054 accepted'
Mon Feb  8 21:47:53 2021 Info: Message finished MID 23569633 done
Mon Feb  8 21:47:58 2021 Info: DCID 250225 close
```

相关信息

- [思科邮件安全设备 — 最终用户指南](#)
- [技术支持和文档 - Cisco Systems](#)