The bridge to possible

Know more about the ESA and functionalities

Armando Sanchez

December 2021

What's coming up?

Community Helping Community

Save the Children

- ☆ Helpful Votes
- ✓ Accepted Solutions
- Subscribe to categories
- Fill out your profile
- Post documents
- #HelpingTheCommunity

Cisco donates $ 1 to the fund Save the Children for your every action!

Check here

Spotlight Awards

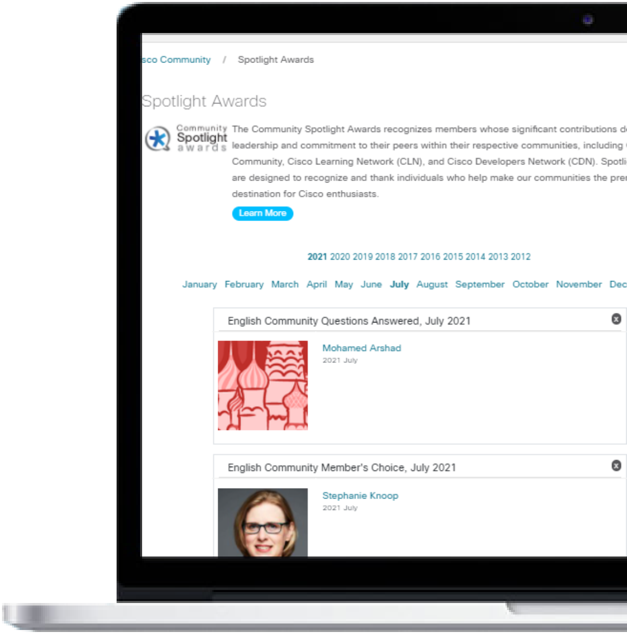
Get recognized by the Cisco Community

New Awardees every month!

Stand out for your effort and commitment helping other members. Spotlight Awards highlight outstanding members. Be the next recipient!

Now you can also nominate a candidate!

Click here



sco Community / Spotlight Awards

Spotlight Awards

The Community Spotlight Awards recognizes members whose significant contributions d
leadership and commitment to their peers within their respective communities, including
Community, Cisco Learning Network (CLN), and Cisco Developers Network (CDN). Spotli
are designed to recognize and thank individuals who help make our communities the pre
destination for Cisco enthusiasts.

Community Spotlight awards
Learn More
2021 2020 2019 2018 2017 2016 2015 2014 2013 2012
January February March April May June July August September October November Dec

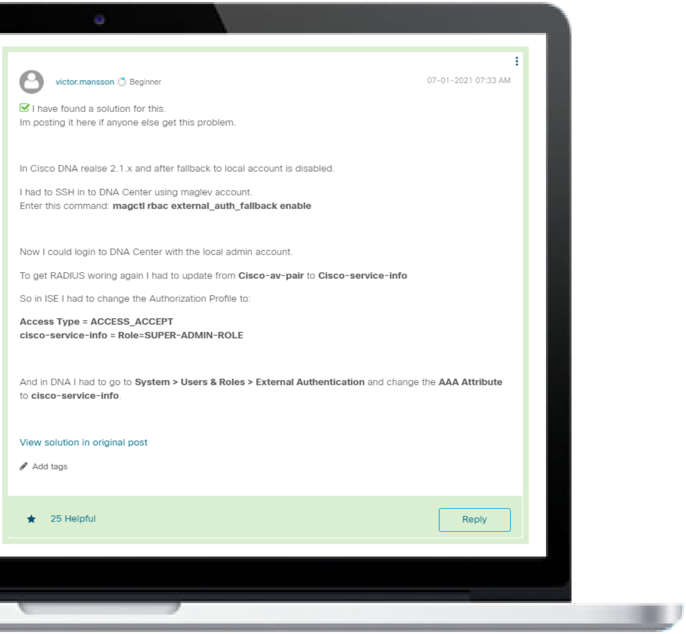
English Community Questions Answered, July 2021

Mohamed Arshad
2021 July

English Community Member's Choice, July 2021

Stephanie Knoop
2021 July

Connect, Engage, Collaborate!



victor.mansson Beginner 07-01-2021 07:33 AM

☑ I have found a solution for this.
Im posting it here if anyone else get this problem.

In Cisco DNA realse 2.1.x and after fallback to local account is disabled.

I had to SSH in to DNA Center using maglev account.
Enter this command: **magctl rbac external_auth_fallback enable**

Now I could login to DNA Center with the local admin account.

To get RADIUS woring again I had to update from **Cisco-av-pair** to **Cisco-service-info**

So in ISE I had to change the Authorization Profile to:

Access Type = ACCESS_ACCEPT
cisco-service-info = Role=SUPER-ADMIN-ROLE

And in DNA I had to go to **System > Users & Roles > External Authentication** and change the **AAA Attribute** to **cisco-service-info**.

When you ask a Question and receive a correct Answer, **accept it as a solution!**

That helps other users find correct answers.

Accept as Solution

We all are sensitive to be highlighted.

Helpful votes motivate enthusiastic members by giving them a **token of recognition!**

★ 25 Helpful

Our Expert

Armando Sanchez

Presenter

[Download the Presentation]!

Cisco Secure Email Gateway
by
Armando Sánchez

Dec 14th , 2021

Agenda

- Email Authentication
- Security Engines
- API’s
- Email Remediation

Email Authentication

SPF DKIM DMARC

Email Authentication

SPF, DKIM, DMARC.

Sender Policy Framework (SPF) is **an email authentication protocol that domain owners use to specify the email servers they send email from**, making it harder for fraudsters to spoof sender information.

DKIM (DomainKeys Identified Mail) is a protocol that allows an organization to take responsibility for transmitting a message by **signing** it in a way that mailbox providers can verify.

DMARC

DMARC (Domain-based Message Authentication, Reporting, and Conformance), is **a DNS TXT Record that can be published for a domain to control what happens if a message fails authentication**

Reference:

https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-spf-dkim-dmarc.pdf

MXC CENTERS

Email Authentication

SPF, DKIM, DMARC.

- SPF and DMARC **are DNS based** configurations
- Under the ESA we just need to activate the verifications under the policies.
- For DKIM if we are signing with the ESA we need to create a profile in order to sign the domain.

Security Engines

Security Engines

We know the importance of Security under our emails.

- Anti-Spam
- Anti-Virus
- Advanced Malware Protection (AMP)
- Graymail
- URL Reputation
- Outbreak Filters

API’s

API’s

- The AsyncOS API for Cisco Secure Email Gateway (or AsyncOS API) is a representational state transfer (REST) based set of operations that provide secure and authenticated access to the email gateway reports, report counters, and tracking

- Requirements:
  - Enable APIs
  - User Account
  - Testing App or script

- Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/api/b_ESA_API_Guide_14-0/b_ESA_API_Guide_chapter_01.html

API’s

- Requests:

https://{appliance}:{port}/esa/api/v2.0/{resource}/{resource_attributes}

where:

{appliance}:{port} is the FQDN or the IP address of the email gateway and the TCP port number on which the email gateway is listening.

{resource} is the resource you are attempting to access, for example, reports, tracking, quarantine, configuration, or other counters.

{resource_attributes} are the supported attributes for a resource, for example, duration, and so on.

Each request must contain user credentials, or a valid authorization header.

Each request must be set to accept: application/json

API’s

- Examples:

- GET /api/v2.0/login/privileges
- GET /api/v2.0/health/
- GET /esa/api/v2.0/config/system_time?
- GET /esa/api/v2.0/config/appliances?

- https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-programming-reference-guides-list.html

Email Remediation

Email Remediation

- What is Remediation? Email Remediation is a secure layer when an email when it is not desired or changed their reputation within AMP engine, will be deleted or forwarded from the user's mailbox.

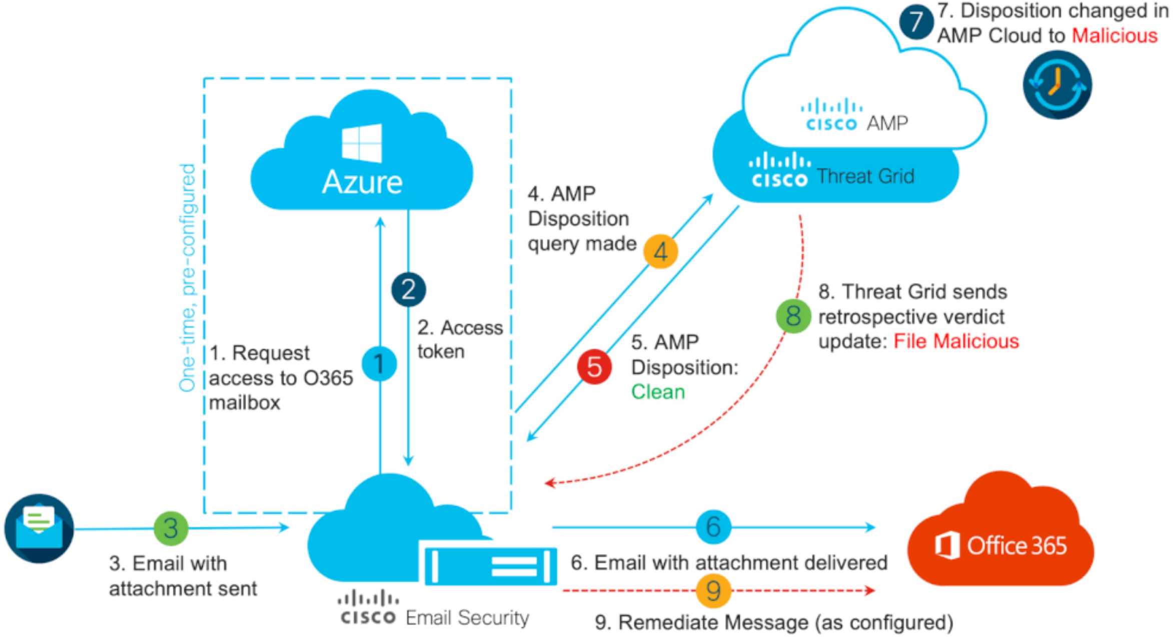
- Exchange On Premise / Office365 or Hybrid (Graph API)

Email Remediation

- Mailbox Auto Remediation (MAR) vs Search and Remediate : The main difference is when it is triggered

  MAR = AMP retrospective verdict received

  Search and Remediate = manual trigger the remediation via Tracking.


7. Disposition changed in AMP Cloud to Malicious
7
cisco AMP
cisco Threat Grid
Azure
One-time, pre-configured
4. AMP Disposition query made
4
2
2. Access token
1
1. Request access to O365 mailbox
8
8. Threat Grid sends retrospective verdict update: File Malicious
5
5. AMP Disposition: Clean
3
3. Email with attachment sent
cisco Email Security
6
6. Email with attachment delivered
9
9. Remediate Message (as configured)
Office 365

MXC CENTERS

Email Remediation

Base Link: https://docs.ces.cisco.com/docs/office-365-configuration-guide

Troubleshooting:

- Validate FW rules between ESA and Exchange server.
- Check traiblaizer config under ESA/SMA and access to port 4431.
- Check certificate configuration if you are using a custom certificate, verify it is added into the ESA Custom List.

The bridge to possible

Do you still have questions?

Use the "Q&A" panel

Forum Ask Me Anything

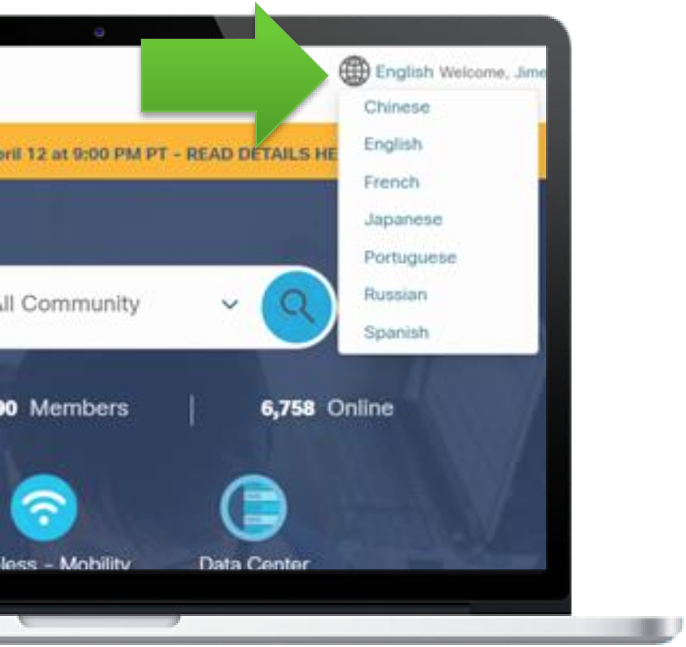
Find our expert on the Discussion Forum

Any new questions on the topic of this webinar will be answered thereafter until this Friday: December 17, 2021

Submit a new Question

Are you a New Member? Ask all your questions before the end of the month and maybe you will become the next Spotlight Awardee!

Wherever you are, stay connected …



- Facebook CiscoSupportCommunity
- Twitter @cisco_support
- YouTube CiscoSupportChannel
- LinkedIn Cisco Community
- Instagram CiscoSupportCommunity

Do you have any Comments?

Take our Survey!

CISCO

The bridge to possible