# **Configure Secure Malware Analytics Appliance RADIUS over DTLS Authentication for Console and OPadmin Portal**

## Contents

| <b>Introduction</b>  |  |  |
|----------------------|--|--|
| <u>Prerequisites</u> |  |  |
| Requirements         |  |  |
| Components Used      |  |  |
| <u>Configure</u>     |  |  |
| <b>Configuration</b> |  |  |
| <u>Verify</u>        |  |  |
| <u>Troubleshoot</u>  |  |  |

## Introduction

This document describes Remote Authentication Dial In User Service (RADIUS) authentication feature which was introduced in the Secure Malware Analytics Appliance (formerly Threat Grid) version 2.10. It allows users to log in to the Admin portal as well as Console portal with credentials stored in the Authentication, Authorization and Accounting (AAA) server that supports RADIUS over DTLS authentication (draft-ietf-radext-dtls-04). In this case, Cisco Identity Services Engine was used.

In this document you find necessary steps to configure the feature.

## Prerequisites

#### Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Malware Analytics Appliance (formerly Threat Grid)
- Identity Services Engine (ISE)

#### **Components Used**

The information in this document is based on these software and hardware versions:

- Secure Malware Analytics Appliance 2.10
- Identity Services Engine 2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configure

This section provides detailed instructions on how to configureSecure Malware Analytics Appliance and ISE for RADIUS Authentication feature.

Note: In order to configure the authentication, ensure that communication on port UDP 2083 is allowed between Secure Malware Analytics Appliance Clean interface and ISE Policy Service Node (PSN).

#### Configuration

Step 1. Prepare Secure Malware Analytics Appliance certificate for authentication.

RADIUS over DTLS uses mutual certificate authentication which means that the Certificate Authority (CA) certificate from ISE is needed. First check what CA signed RADIUS DTLS certificate:



Step 2. Export the CA certificate from ISE.

Navigate to Administration > System > Certificates > Certificate Management > Trusted Certificates, locate the CA, select Export as shown in the image, and save the certificate to the disk for later:

| Identity Services Engine           | Norm + Contest Velicity + Operations          | - Marcalan                     | a Math Cartan   |   |                          |                         |                   |  |
|------------------------------------|---|--------------------------------|---|---|--------------------------|-------------------------|-------------------|--|
| * System + Mently Management       | Salacel Resources 1 Device Portal Recognition | policit functions = 1.         | and Service - Thready                                 | Careful AMIC                                |                          |                         |                   |  |
| Department Literating +Dertificati | a Linging Elimination Toyota 18               | etes L'Asses - Adre            | Access 1 Settings                                     |   |                          |                         |                   |  |
| 0                                  |   |                                |   |   |                          |                         |                   |  |
| a facilitate Research              |   |                                |   |   |                          |                         |                   |  |
| - Constant and appropriate         | Trusted Certificates                          |                                |   |   |                          |                         |                   |  |
| Bysten Certificates                | /in drawn drawn Xiers                         | - March                        |   |   |                          | liter .                 | ayi               | - 14                                     |
| Trusted Certificates               | Printly Rame                                  | <ul> <li>Bate</li> </ul>       | Trusted Par   | Serial Rundler                              | Interf To                | Insued By               | Yorke Property    | Appendix Ser                             |
| 0087 Own Pulle                     | Balances Cyber Trust Root                     | Ended                          | Ours Services   | 0.000                                       | Balances Cyler Trust Ro. | Ballmore Cyber Nutl Is  | PA, 12 Pay 2000   | 26,0296.2                                |
| Cardhoate Righting Respects        | Coss-Sk Naveladuring                          | © Deated                       | Endpointing<br>Infrastructure<br>Automation           | 0.001210.00                                 | One Handscheitig Dr.     | Oct 101 (3.314)         | 54, 11 Jan 2015   | 1946, 14 Play (                          |
| Certificate Periods Oneck Settings | Circle 400 Next Ok.                           | S finalized                    | Own Services  |   | Own-HOC Rest: GA         | Case Hill Red Ch.       | Tes, 6.4pt 2003   | Ac, 4.8pt 205                            |
| + Certificate Authority            | <ul> <li>Class-United Root CA.</li> </ul>     | E Studied                      | Class Services  |   | Our Consignation         | Ones Literating Post DL | The, 10 May 2013  | 5.0, 10 Key 3                            |
|                                    | Casa Manufacturing CI (2002)                  | C Evaluation                   | Endpoints<br>Infrastructure<br>Administration         | -   | Out Mendletiving Du.     | Gaus Rev. (3, 19)       | Mars, 53 Nov 2012 | $T_{\rm N_2} \gtrsim N_{\rm P} \lesssim$ |
|                                    | Casa-Rost CX.2048                             | © Institut                     | Endpaires<br>Infrastructure<br>Automation             | P1022201                                    | Over Real Or 2018        | Core Role 28, 2948      | 14, 14 May 2004   | 1999, 14 PM                              |
|                                    | Cara-Rost CA 2009                             | Enabled                        | Once Services   | <ul> <li>(a) (b) (b) (b) (b) (c)</li> </ul> | Chen Rose CA 2018        | Case Rest CA 2010       | 74, FA9, 2010     | - Mar. 10 Aug. 2                         |
|                                    | Cara-Real CAPE                                | Ended                          | Our Several   | 30.00 00 19-0 10                            | Own-Road Ox RD           | Com Rest CARD           | 766, 18769 (1988) | A. 10 Key (1)                            |
|                                    | Casa-Nam GAME                                 | Contract (                     | Endpoints<br>Infrastructure<br>Automation             |   | Own-Roam (3x 74)         | Onco Asso: (3,74)       | 1964, 13 Nov 2012 | $Tra_{1} \lesssim Tray ($                |
|                                    | Casa-000-42                                   | C Evaluation                   | Case Services   |   | One-40049                | One 80049               | 10a), 9 Jan 2014  | Sec. 9 bel 200                           |
|                                    | Induit set signal server certificate          | C Stated                       | Endpointin<br>Infrastructure<br>Automatication        | 50.40 06 14 00 00                           | worst table Liener.c.    | want with Limon.        | 754,21748-2019    | NG 20 Meb 20                             |
|                                    | DyCercBalanteet Ct.                           | C Ended                        | One Services  | 0.000000000                                 | Diplort Oxfort Rule DX   | Diplore Data Nucl Di-   | Ph, 18 Nov 2006   | No. 10 No. 1                             |
|                                    | Diplanisaria                                  | Evaluation                     | Endpoints<br>Infrastructure<br>Automatice             | 01.0C NC 20.00.00                           | DipCert High Insurance.  | OpCert High Assurance.  | PH, 10 Nov 2006   | No. 11 No. 7                             |
|                                    | Diplicat Brief High Associate Server CA       | <ul> <li>Evaluation</li> </ul> | Endpoints<br>Infrastructure<br>Admontatio             | OF BEET AND CR.                             | Depted Sent Hep-Am.      | Option replanations.    | 36,00000          | 54,1234.3                                |
|                                    | DeferringelA, most                            | Contract (2)                   | Infrastructure<br>Endersette                          | 01  | Informação.              | Outwreep/Ox.            | 100,00 Per 2006   | Ac. 10 Per 10                            |
|                                    | DIT fast (A.O. GetMate Autority)              | C Statist                      | Own Services  | 44.47 30 80 04.40.                          | 007 Aug (3.10            | 007 Aut (0.10           | Set, 10 Sep 2000  | 7m, 30 km 2                              |
|                                    | Instanto 55, 104-02                           | C Strating                     | Case Services   | 75.07.06.77.00.00                           | Pp8 arrit 10, 104 62     | (particle from (A.)     | No. 17 Dec 2010   | Sec. Print 2                             |
|                                    | 2 umanta                                      | D finded                       | Cara Service<br>Cara Service<br>Englishis<br>Addition | 12 34 34 78                                 | uters or                 | UPON OL                 | PH, 25 Jan 2017   | West, 22-3472                            |

Step 3. Add Secure Malware Analytics Appliance as Network Access Device.

Navigate to Administration > Network Resources > Network Devices > Add to create a new entry for TG and enter the Name, IP address of the Clean interface and select DTLS Required as shown in the image. Click Save at the bottom:

| thereby Services Engine              | None + Context thicking + Operations + Policy * Administration + Work Centers   |
|--------------------------------------|---|
| + System + Hently Management +       | - Network Resources + Denite Partial Management pedinit Services + Faed Service + Thread Centric NAC  |
| *Anteron Devices - Network Device Gr | tops Network Denter Profess Enternal RADIUS Servers RADIUS Server Seguences AVIC Managers Enternal MDM + Location Services  |
| •                                    |   |
| Network Devices                      | Network Devices (ull > keet develophilit) deen<br>Network Devices   |
| Owtaut Device                        | Norte Inscription (Inscription)   |
| Device Security Settings             | Description   |
|                                      |   |
|                                      | (PA0000 -) *P: (0.02.00.02  |
|                                      |   |
|                                      |   |
|                                      | * Device Profile 🔛 Casco x 😟  |
|                                      | Model Name T  |
|                                      | Software Version  |
|                                      |   |
|                                      | * Network Denter Droug  |
|                                      | Location (at Locations 👌 for In Sector)   |
|                                      | PHIC No. Of Sector Delast   |
|                                      | Device Types (at posts types 📀 )  |
|                                      |   |
|                                      | Interface and the second se |
|                                      |   |
|                                      | AADIUS UOP Settings   |
|                                      | Potest MOUS   |
|                                      | - Shared Securit  |
|                                      | Use Second Shared Secret 🛄 2  |
|                                      | (2000)  |
|                                      | CAVAL T20 [NE PORM]   |
|                                      | Monde DTLA Bettings ()  |
|                                      | DTLA Report (2012)  |
|                                      | Gut Part (200 See In Judget )   |
|                                      | tenuer CA of BE Centificates for CoA (LINESS CA. +) 2   |
|                                      | (NO Name   two divergrafi)-dist.disc-   |
|                                      |   |
|                                      | General Bettings  |
|                                      | Enate KayImp 🗌 🛛  |
|                                      | * Kay Energeton Kay (Price)   |
|                                      | * Message Authenticator Code Key Show   |
|                                      | Kay Input Format (8: KBCIII) HEXINDECMIN,   |
|                                      | The ACE Automatication functions  |
|                                      |   |
|                                      |   |
|                                      | <ul> <li>Accuracy charges percept</li> </ul>  |
|                                      | term (Anne)   |

Step 4. Create an Authorization Profile for Authorization Policy.

Navigate to **Policy > Policy elements > Results > Authorization > Authorization Profiles** and click **Add**. Enter **Name** and select **Advanced Attributes Settings** as shown in the image and click **Save**:

| -de-de-<br>ence Identity Services Engine | Home + Context Visibility                    | Operations     Policy | Administration     Work Centers |
|--|--|-----------------------|---------------------------------|
| Policy Sets Profiling Posture C          | lient Provisioning Policy Element            | enta                  |                                 |
| Dictionaries + Conditions • Resul        | ts   |                       |                                 |
| 0  | Authorization Devilian > TG and              | dents                 |                                 |
| Authentication                           | Authorization Profile                        |                       |                                 |
| * Authorization                          | *Name  | ThreatGrid            |                                 |
| Authorization Profiles                   | Description                                  |                       |                                 |
| Downloadable ACLs                        | * Access Type                                | ACCESS_ACCEPT         | ¥.                              |
| Profiling                                | Network Device Profile                       | 🟥 Cisco 🔹 📵           |                                 |
| + Posture                                | Service Template                             | 0                     |                                 |
| Client Provisioning                      | Track Movement                               | 0.0                   |                                 |
|  | Passive Identity Tracking                    | 00                    |                                 |
|  |  |                       |                                 |
|  | Common Tasks                                 |                       |                                 |
|  |  |                       |                                 |
|  | · Advanced Attributes 5                      | iettings              |                                 |
|  | Radius:Service-Type                          | Administrative        | • - +                           |
|  |  |                       |                                 |
|  | * Attributes Details                         |                       |                                 |
|  | Access Type = ACCESS_ACC<br>Service-Type = 6 | IPT                   |                                 |
|  | Save Reset                                   |                       |                                 |

Step 5. Create an authentication policy.

Navigate to **Policy > Policy Sets** and click +. Enter Policy Set **Name** and set the condition to **NAD IP Address**, assigned to the Secure Malware Analytics Appliance's clean interface, click **Save** as shown in the image:

| cisco Ide  | ntity Service | es Engine Home 🔸          | Context Visibility | ▼Policy | Administration → V  | Vork Centers                        |                 | ् 🛛      | • •  |
|------------|---------------|---------------------------|--------------------|---------|---|-------------------------------------|-----------------|----------|------|
| Policy Set | s Profiling   | Posture Client Provisioni | ng                 |         |   |                                     |                 |          |      |
| Policy S   | ets           |                           |                    |         |   | Reset Po                            | licyset Hitcoun | ts Reset | Save |
| +          | Status        | Policy Set Name           | Description        | Con     | ditions   | Allowed Protocols / Server Sequence | Hits            | Actions  | View |
| Search     |               |                           |                    |         |   |                                     |                 |          |      |
| 1          | ø             | ThreatGrid                |                    | ₽       | Network Access Device IP<br>Address<br>EQUALS 10.62.148.171 | Default Network Access × × +        |                 | ۵        | >    |
|            | Ø             | Default                   | Default policy set |         |   | Default Network Access × × +        | 59              | ¢        | >    |

Step 6. Create an authorization policy.

Click the > to go to the authorization policy, expand the Authorization Policy, click + and configure as shown in the image, after you finish click **Save**:

| zation Polic | y (3)              |                                      |   |  |  |  |  |   |   |
|--------------|--------------------|--------------------------------------|---|--|--|--|--|---|---|
|              |                    |                                      |   | Results  |  |  |  |   |   |
| Status       | Rule Name          | Cor                                  | ditions   | Profiles   |  | Security Groups  |  | Hits  | Actions   |
|              |                    |                                      |   |  |  | _  |  |   |   |
| 0            | ThreatGrid Admin   | ÷                                    | Radius-NAS-Identifier EQUALS Threat Grid Admin  | × ThreatGrid   | +  | Select from list   | × +  | 1   | 0   |
| ø            | ThreatGrid Console | Ŧ                                    | Radius-NAS-Identifier EQUALS Threat Grid UI   | × ThreatGrid   | +  | Select from list   | - +  | 1   | ٥   |
| 0            | Default            |                                      |   | × DenyAccess   | +  | Select from list   | - +  | 17  | ¢   |
|              | Status             | Attaina Policy (3)  Status Rule Name | Itation Policy (3)       Status     Rule Name     Con       Image: Constraint of the state of t | tation Policy (3)       Status     Rule Name     Conditions       Image: Condition of the state | Radius NAS-Identifier EQUALS Threat Grid Uil     Results       Results     Results     Results       Image: Conditions     Conditions     Profiles | ation Policy (3)          Rule Name       Results         Rule Name       Conditions         Image: Conditions       Profiles         Image: Conditions       Profiles         Image: Conditions       Image: Conditions         Image: Co | ation Policy (3)<br>Status Rule Name Continues C | Rafus NAS-identifier EQUALS Threat Grid UI       Results         PrestGrid Console       Rafus NAS-identifier EQUALS Threat Grid UI       RTreatGrid       Results         Image: Construct Console       Rafus NAS-identifier EQUALS Threat Grid UI       Image: Console       Select from list       Image: Console         Image: Console       Default       Image: Console       Select from list       Image: Console       Select from list       Image: Console | ation Policy (3)          Rule Name       Results       Results |

**Tip**: You can create one authorization rule for all your users that match both conditions, Admin and UI.

Step 7. Create an identity certificate for Secure Malware Analytics Appliance.

Secure Malware Analytics Appliance's client certificate must be based on the Elliptic Curve key:

openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem

You must create CSR based on that key and then it has to be signed by the CA which ISE trusts. Check *Import the Root Certificates to the Trusted Certificate Store* page for more information of how to add CA certificate to ISE Trusted Certificate Store.

Step 8. Configure Secure Malware Analytics Appliance to use RADIUS.

Log in to admin portal, navigate to **Configuration > RADIUS**. In RADIUS CA Certificate paste the content of the PEM file collected from ISE, in Client Certificate paste PEM formatted certificate received from CA and in Client Key paste content of **private-ec-key.pem** file from the previous step as shown in the image. Click **Save**:

| Cisco Threat Grid Applance Administration Portal | E3 Support |
|--|------------|
| Configuration * Operations * Status * Support *  | jm -       |
| RADIUS DTLS Configuration                        |            |

| Authentication Mode                |               | 4, Ether System Or RADIUS Authentication •    |
|------------------------------------|---------------|---|
| RADIUS Host                        |               | 10.48.17.135                                  |
| RADIUS DTLS Port                   | O HELP        |   |
| RADIUS CA Certificate              | € HELP        | VCxvUhoHal7p+B     ·····END CERTIFICATE······ |
| RADIUS Client Certificate          | 0 ×0.P        | OFITRNBHIKA     OFITRNBHIKA     OFITRNBHIKA   |
| RADIUS Client Key                  | 0 HELP        | a, 2TOKEY4waktmChuw                           |
| initial Application Admin Username | <b>O</b> HELP | A radek                                       |

Note: You must reconfigure Secure Malware Analytics Appliance after you save RADIUS settings.

Step 9. Add RADIUS Username to console users.

In order to log in to console portal, you must add the RADIUS Username attribute to the respective user as shown in the image:

#### Details

|     | Login                            | radek                          |                 |       |
|-----|----------------------------------|--------------------------------|-----------------|-------|
|     | Name                             | radek /                        |                 |       |
|     | Title                            | Add /                          |                 |       |
|     | Email                            | roiszowy@c                     | cisco.com ,     | /     |
|     | Integration                      | none                           | $\sim$          |       |
|     | Role                             | admin                          |                 |       |
|     | Status                           | Active                         | Inactive        | 1     |
|     | DADU IC LINAMAN A                | C                              |                 |       |
|     | KADIUS Usemame                   | radek                          |                 | _     |
|     | Default UI Submission<br>Privacy | radek <br>Private              | Public          | Unset |
|     | EULA Accepted                    | Private<br>No                  | Public          | Unset |
| CSA | EULA Accepted Auto-Submit Types  | Private No Add                 | Public          | Unset |
| CSA | EULA Accepted Can Flag Entities  | Private<br>No<br>Add /<br>True | Public<br>False | Unset |

Step 10. Enable RADIUS only authentication.

After successful log in to the admin portal, a new option appears, which completely disables local system authentication and leaves the only RADIUS-based one.



## Verify

After Secure Malware Analytics Appliance has been reconfigured, log off and now the log in pages look like in the images, admin and console portal respectively:

# Threat Grid

| Authenticate using RADIUS: |    | Auth | anticata using Sustam Password- |
|----------------------------|----|------|---------------------------------|
| RADIUS Login               |    | Auto | Sustam Decouverd                |
| RADIUS Password            | or | -    | System Password                 |
| Authenticate               |    | Au   | thenticate                      |
|                            |    |      |                                 |

# Threat Grid



RADIUS username

RADIUS password

# Log In

# Forgot password?

## Troubleshoot

There are three components that could cause problems: ISE, network connectivity and Secure Malware Analytics Appliance.

• In ISE, ensure that it returns ServiceType=Administrative to Secure Malware Analytics Appliance's authentication requests. Navigate to **Operations** > **RADIUS** > **Live Logs** on ISE and check details:

| Time                         | Status | Ovtails | Repeat | klentity | Authentication Polic   | y. | Authorization Policy             | Authorizati  | Network Device      |
|------------------------------|--------|---------|--------|----------|------------------------|----|----------------------------------|--------------|---------------------|
|                              |        |         |        | low thy  | ThreatGrid             | ×  | Authorization Policy             | Autorization | Referent Device     |
| Feb 20, 2020 09:40:58,753 AW | 8      | 0       |        | radak    | Threat Grid 11 Default |    | ThreadGeld >> ThreadGeld Admin   | 15-spedmin   | loss finalgid2-dean |
| Feb 20, 2020 08:40 18,200 AW | 0      | 0       |        | radak.   | TreatOrie ++ Default   |    | ThreatGrid >> ThreatGrid Console | 10-conada    | lose finalgit? den  |

# **Authentication Details**

| Source Timestamp  | 2020-02-20 09:40:38.753   |
|---|---|
| Received Timestamp  | 2020-02-20 09:40:38.753   |
| Policy Server   | wcecot-ise27-1  |
| Event   | 5200 Authentication succeeded   |
| Username  | radek   |
| User Type   | User  |
| Authentication Identity Store   | Internal Users  |
| Authentication Method   | PAP_ASCII   |
|   |   |
| Authentication Protocol   | PAP_ASCII   |
| Authentication Protocol<br>Service Type   | PAP_ASCII<br>Administrative   |
| Authentication Protocol<br>Service Type<br>Network Device   | PAP_ASCII<br>Administrative<br>ksec-threatgrid02-clean  |
| Authentication Protocol<br>Service Type<br>Network Device<br>Device Type                                      | PAP_ASCII<br>Administrative<br>ksec-threatgrid02-clean<br>All Device Types                                |
| Authentication Protocol<br>Service Type<br>Network Device<br>Device Type<br>Location                          | PAP_ASCII<br>Administrative<br>ksec-threatgrid02-clean<br>All Device Types<br>All Locations               |
| Authentication Protocol<br>Service Type<br>Network Device<br>Device Type<br>Location<br>Authorization Profile | PAP_ASCII<br>Administrative<br>ksec-threatgrid02-clean<br>All Device Types<br>All Locations<br>TG opadmin |

<sup>•</sup> If you don't see these requests, do a packet capture on ISE. Navigate to **Operations > Troubleshoot > Diagnostic Tools > TCP Dump**, provide the IP in Filter field of the TG's **clean** interface, click **Start** 

and try to log in on Secure Malware Analytics Appliance:

#### TCP Dump

| Monitor the packet headers on the netwo | rk and save to a file (up to 5 Minutes) |
|---|---|
|---|---|

| Status            | Monitoring (approximate file size: 8192 bytes) Stop |  |
|-------------------|---|--|
| Host Name         | wcecot-ise27-1                                      |  |
| Network Interface | GigabitEthernet 0                                   |  |
| Promiscuous Mode  | ⊙On ⊖Off  |  |
| Filter            | ip host 10.62.148.171                               |  |
|                   | Example: 'ip host helios and not iceburg'           |  |
| Format            | Raw Packet Data                                     |  |
| Dump File         |   |  |
| Download Delete   |   |  |

You must see that number of bytes increased. Open pcap file in Wireshark for more information.

• If you see the error "We're sorry, but something went wrong" after you click **Save** in Secure Malware Analytics Appliance and the page looks like this:



#### We're sorry, but something went wrong.

The server experienced an error while processing your request. Please retry your request later. If this problem pensists, contact support.

That means that you most probably used RSA key for the client certificate. You must use ECC key with the parameters specified in step 7.