

Configure Secure Malware Analytics Appliance RADIUS over DTLS Authentication for Console and OAdmin Portal

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Configuration](#)

[Verify](#)

[Troubleshoot](#)

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

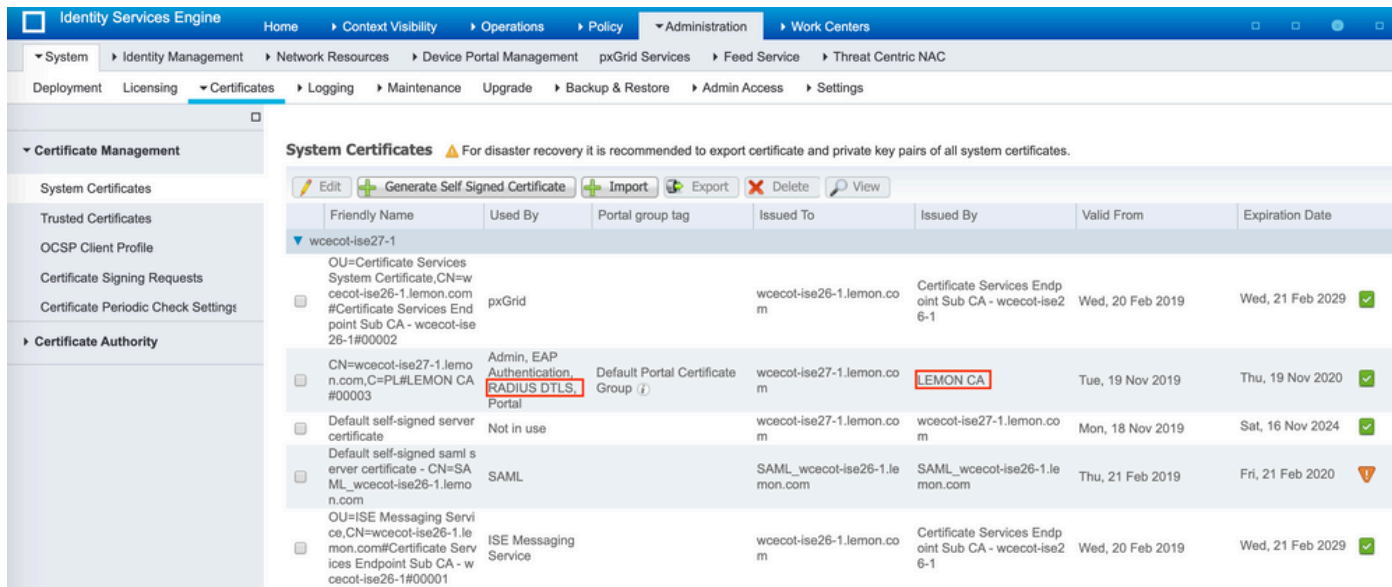
This section provides detailed instructions on how to configure Secure Malware Analytics Appliance and ISE for RADIUS Authentication feature.

 **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:



The screenshot shows the Identity Services Engine (ISE) Administration console. The navigation path is: Administration > System > Certificates > System Certificates. The page displays a table of system certificates. The second certificate, 'CN=wcecot-ise27-1.lemo n.com,C=PL#LEMON CA #00003', is highlighted. Its 'Used By' field is 'Admin, EAP Authentication, RADIUS DTLS, Portal', and its 'Issued By' field is 'LEMON CA'. The 'Valid From' date is 'Tue, 19 Nov 2019' and the 'Expiration Date' is 'Thu, 19 Nov 2020'. A red box highlights the 'LEMON CA' field in the 'Issued By' column.

System Certificates	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
<input type="checkbox"/>	wcecot-ise27-1 OU=Certificate Services System Certificate,CN=wcecot-ise26-1.lemo n.com #Certificate Services Endpoint Sub CA - wcecot-ise26-1#00002	pxGrid		wcecot-ise26-1.lemo n.com	Certificate Services Endpoint Sub CA - wcecot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029
<input type="checkbox"/>	CN=wcecot-ise27-1.lemo n.com,C=PL#LEMON CA #00003	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group (j)	wcecot-ise27-1.lemo n.com	LEMON CA	Tue, 19 Nov 2019	Thu, 19 Nov 2020
<input type="checkbox"/>	Default self-signed server certificate	Not in use		wcecot-ise27-1.lemo n.com	wcecot-ise27-1.lemo n.com	Mon, 18 Nov 2019	Sat, 16 Nov 2024
<input type="checkbox"/>	Default self-signed saml server certificate - CN=SAML_wcecot-ise26-1.lemo n.com	SAML		SAML_wcecot-ise26-1.lemo n.com	SAML_wcecot-ise26-1.lemo n.com	Thu, 21 Feb 2019	Fri, 21 Feb 2020
<input type="checkbox"/>	OU=ISE Messaging Service,CN=wcecot-ise26-1.lemo n.com#Certificate Services Endpoint Sub CA - wcecot-ise26-1#00001	ISE Messaging Service		wcecot-ise26-1.lemo n.com	Certificate Services Endpoint Sub CA - wcecot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029

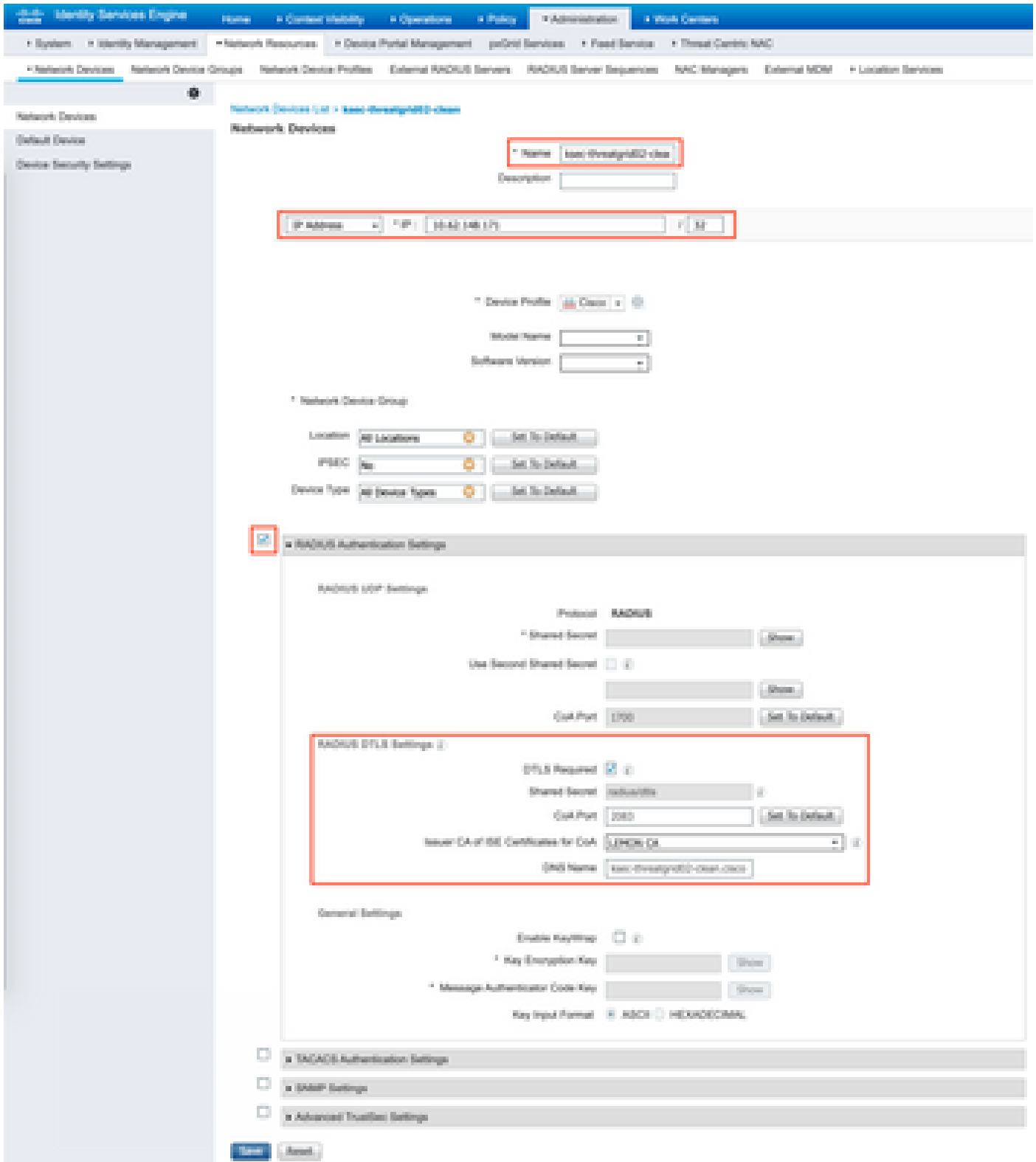
Step 2. Export the CA certificate from ISE.

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:

Friendly Name	Status	Issued For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
Baltimore CyberTrust Root	Enabled	Class Services	02 00 00 00	Baltimore CyberTrust Root	Baltimore CyberTrust Root	Fri, 12 May 2000	Tue, 12 May 2025
Class-CA-Manufacturing	Enabled	Endpoints Infrastructure administrators	04 00 07 03 00 00 ...	Class Manufacturing CA	Class Root-CA-2048	Sat, 11 Jun 2004	Mon, 14 May 2024
Class-ECI Root CA	Enabled	Class Services	01	Class ECI Root CA	Class ECI Root CA	Fri, 4 Apr 2014	Fri, 4 Apr 2024
Class-Learning Root CA	Enabled	Class Services	01	Class Learning Root CA	Class Learning Root CA	Fri, 20 May 2012	Sat, 20 May 2022
Class-Manufacturing CA 2048	Enabled	Endpoints Infrastructure administrators	02	Class Manufacturing CA	Class Root-CA-90	Mon, 12 Nov 2012	Thu, 12 Nov 2022
Class-Root-CA-2048	Enabled	Endpoints Infrastructure administrators	07 00 70 20 20 04 ...	Class Root CA 2048	Class Root-CA-2048	Fri, 04 May 2004	Mon, 14 May 2024
Class-Root-CA-2049	Enabled	Class Services	01 00 01 00 70 02 ...	Class Root CA 2049	Class Root-CA-2049	Tue, 9 Aug 2016	Mon, 11 Aug 2024
Class-Root-CA-90	Enabled	Class Services	00 00 00 70 07 00 ...	Class Root-CA-90	Class Root-CA-90	Tue, 08 Nov 2006	Fri, 08 Nov 2024
Class-Root-CA-901	Enabled	Endpoints Infrastructure administrators	01	Class Root-CA-90	Class Root-CA-90	Wed, 12 Nov 2014	Thu, 12 Nov 2024
Class-R02-02	Enabled	Class Services	01	Class R02-02	Class R02-02	Wed, 11 Jul 2014	Sat, 9 Jul 2024
Default self-signed server certificate	Enabled	Endpoints Infrastructure administrators	01 00 00 00 00 00 ...	localhost-1.localhost	localhost-1.localhost	Fri, 20 Feb 2015	Fri, 20 Feb 2025
Digicert Global Root CA	Enabled	Class Services	08 00 00 00 00 02 ...	Digicert Global Root CA	Digicert Global Root CA	Fri, 03 Nov 2000	Mon, 03 Nov 2024
Digicert Root CA	Enabled	Endpoints Infrastructure administrators	02 00 00 00 00 00 ...	Digicert High Assurance...	Digicert High Assurance...	Fri, 03 Nov 2000	Mon, 03 Nov 2024
Digicert 2048 High Assurance Server CA	Enabled	Endpoints Infrastructure administrators	04 00 07 04 00 00 ...	Digicert 2048 High Ass...	Digicert High Assurance...	Tue, 23 Oct 2012	Sat, 20 Oct 2024
DufaningerCA_01.01	Enabled	Endpoints Infrastructure administrators	01	DufaningerCA	DufaningerCA	Sat, 20 Mar 2010	Fri, 20 Mar 2024
007 Root CA (1) Certificate Authority	Enabled	Class Services	04 00 00 00 04 00 ...	007 Root CA (1)	007 Root CA (1)	Tue, 20 Sep 2000	Fri, 20 Sep 2024
Hydrex00-04-03-02	Enabled	Class Services	70 07 04 70 00 00 ...	Hydrex00-04-03-02	Quanta Root-CA-1	Tue, 17 Nov 2014	Sat, 07 Nov 2024
LTPM CA	Enabled	Class Services Endpoints Infrastructure administrators	02 00 00 70	LTPM CA	LTPM CA	Fri, 20 Jun 2017	Wed, 20 Jun 2024

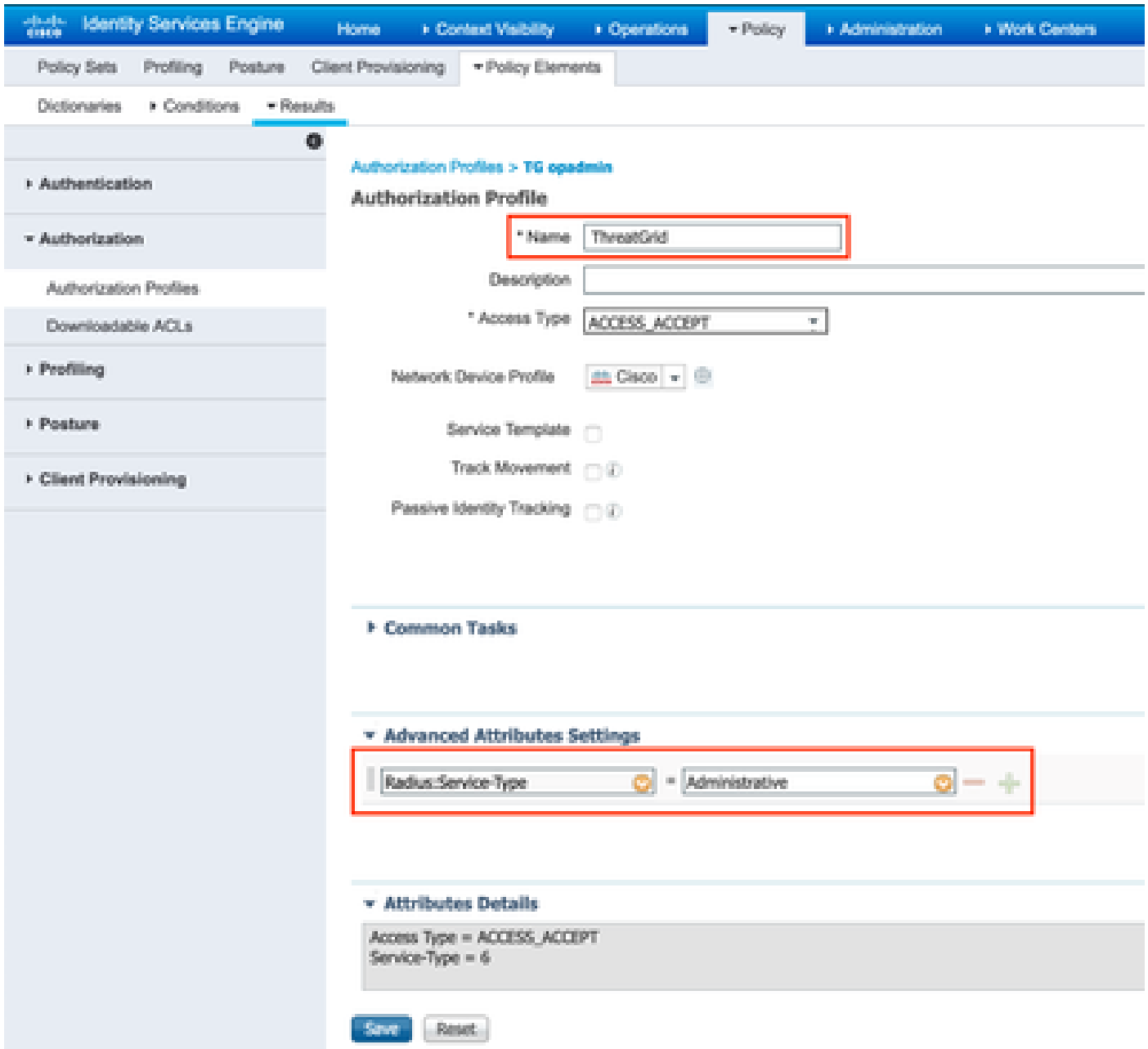
Step 3. Add Secure Malware Analytics Appliance as Network Access Device.

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:



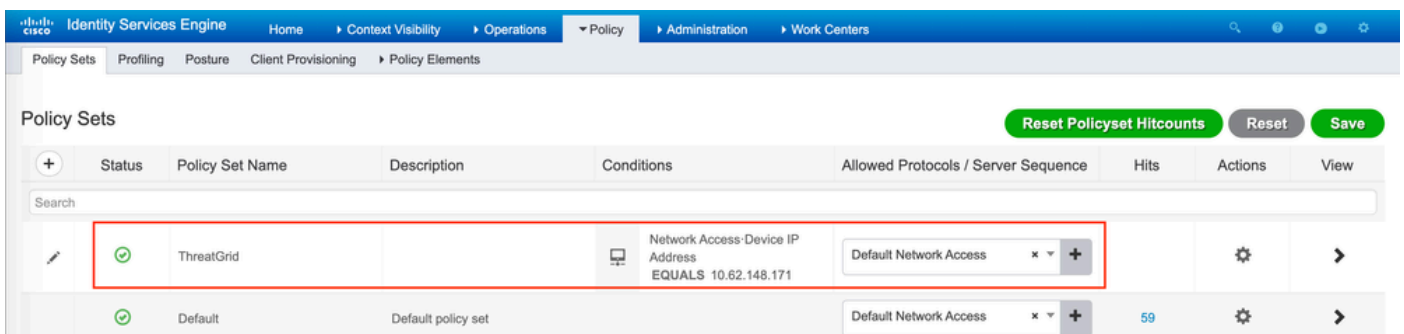
Step 4. Create an Authorization Profile for Authorization Policy.

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**:



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:




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**:



Authorization Policy (3)			Results		Hits	Actions
Status	Rule Name	Conditions	Profiles	Security Groups		
✓	ThreatGrid Admin	Radius-NAS-Identifier EQUALS Threat Grid Admin	ThreatGrid	Select from list	1	⚙️
✓	ThreatGrid Console	Radius-NAS-Identifier EQUALS Threat Grid UI	ThreatGrid	Select from list	1	⚙️
✓	Default		DenyAccess	Select from list	17	⚙️

 **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**:

RADIUS DTLS Configuration

Authentication Mode		<input type="text" value="Either System Or RADIUS Authentication"/>
RADIUS Host		<input type="text" value="10.48.17.135"/>
RADIUS DTLS Port	HELP	<input type="text" value="2083"/>
RADIUS CA Certificate	HELP	<input type="text" value="rV0covUhoHa7g+B
-----END CERTIFICATE-----"/>
RADIUS Client Certificate	HELP	<input type="text" value="GFtRNBHrKa
-----END CERTIFICATE-----"/>
RADIUS Client Key	HELP	<input type="text" value="2T0KEY4wskMClun==
-----END EC PRIVATE KEY-----"/>
Initial Application Admin Username	HELP	<input type="text" value="radius"/>

 **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@cisco.com
Integration	<input type="text" value="none"/>
Role	admin
Status	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
RADIUS Username	<input type="text" value="radek"/>
Default UI Submission	<input type="radio"/> Private <input type="radio"/> Public <input checked="" type="radio"/> Unset
Privacy	<input checked="" type="radio"/>
EULA Accepted	No
CSA Auto-Submit Types	Add...
Can Flag Entities	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> Unset
Enable Direct SSO Setup	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> 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.

Threat Grid Appliance Administration Portal

Support Help
Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

Authentication Mode	<input checked="" type="radio"/> Only RADIUS Authentication Permitted
RADIUS Host	<input type="text" value="10.48.17.135"/>

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

Authentication Required

Authenticate using RADIUS:



Authenticate

or

Authenticate using System Password:



Authenticate

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+



Threat Grid

 Use your RADIUS username and password.

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	Details	Repeat ...	Identity	Authentication Policy	Authorization Policy	Authorizati...	Network Device
				Identity	ThreatGrid	Authorization Policy	Authorization	Network Device
Feb 20, 2020 06:40:56,753 AM				nsfsk	ThreatGrid - Default	ThreatGrid - ThreatGrid Admin	TG-admin	ios-threatgrid-clear
Feb 20, 2020 06:40:58,293 AM				nsfsk	ThreatGrid - Default	ThreatGrid - ThreatGrid Console	TG-console	ios-threatgrid-clear

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
Service Type	Administrative
Network Device	ksec-threatgrid02-clean
Device Type	All Device Types
Location	All Locations
Authorization Profile	TG opadmin
Response Time	13 milliseconds

- 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 network and save to a file (up to 5 Minutes)

Status  Monitoring... (approximate file size: 8192 bytes) [Stop](#)

Host Name

Network Interface

Promiscuous Mode On Off

Filter
Example: 'ip host helios and not iceburg'

Format


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:

 **Threat Grid** Appliance Administration Portal

[Support](#) [Help](#)
[Logout](#)

[Configuration](#) [Operations](#) [Status](#) [Support](#)

We're sorry, but something went wrong.

The server experienced an error while processing your request. Please retry your request later.
If this problem persists, [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.