Logging for Cisco ISE

NOTE: This is untested.

This only applies to Federation Operators and not to individual sites

Unfortunately ISE can't generate custom logs in the format required (FTICKS) but, fortunately, it can generate syslog logs with the right information, which can be sent to a syslog server and munged into a suitable format.

This approach assumes that the member sites are configured to include their Operator-Name in RADIUS Requests.

Configuring Cisco ISE

Enabling the Operator-Name attribute

- Go to **Policy** → **Policy Elements** → **Dictionaries**.
- Open up the **System** dropdown.
- Open up the **Radius** dropdown.
- Click on IETF.
- Click on unknown-126 and enter
 - Attribute Name as 'Operator-Name'
 - Data Type as STRING
 - Direction as IN
- Click Save

cisco Identity Services Engine Hom	ne	 Operations 	+ Policy Ad	Iministration	Work Centers	λ.
Policy Sets Policy Elements						
Dictionaries + Conditions + Results						
Dictionaries	Dictionaries > >	IETF > Operator-N	ame			
↓	<i>≩</i> .		* Attribute	Name Operation	stor-Name	
NT-Password-Hash		Dictionary Attrib	utes Desc	ription undefi	ined_attribute_126	
Operator-Name			* Dat	a Type STRIN	NG Enable MAC option	
Password-Retry				rection IN	*	
Proxy-State A Reply-Message				• ID 126	(0-255)	
Route-IPv6-Information						
Service-Type			Allow T	agging 🗌		
 Session-Timeout State 	Allov	v multiple instances	of this attribute in a	profile 🗹		
Stateful-IPv6-Address-Pool	Save Reset					

Logging

This has been done with ISE 2.6 but the principle should apply to other versions.

In Administration \rightarrow System \rightarrow Logging.

In **Remote Logging Targets** create a new Logging Target with the host name of your syslog server.

The *Facility Code* can be anything but make sure that it matches what the filters expect on the syslog server.

Maximum Length must be set higher than the default because the ISE log line exceeds 1024 bytes and gets split across multiple logs. 2048 seems to be high enough.

Enable Comply to RFC3164

	entre transformer aus reserves of the	Out many is seen in a provide station of
	Investigate Section - Rectinging Section	
and the second second	"Term Index for Indexes	here're alkining i
And a local division of the local division o	(receiptor	inter 🗰 manual (
THE OWNER WATCHING	10.7.000 XXXX	
dealer Time	144 (18	(and freque' a closed)
	Name Incol (2002) 1	
	The set of the	Table Respondence (1981)
	An and a second s	
	Name of the state	

In Logging Categories select Passed Authentications and add the new server to the Selected Targets.

cisco Identity Services Engine	Home + Context	Visibility + Operations	Policy Administration Work Center
System Identity Management	Network Resources	Device Portal Management	pxGrid Services
Deployment Licensing + Certification	les ▼Logging + Ma	intenance Upgrade + Ba	ckup & Restore → Admin Access → Settings
Cag Settings Remote Logging Targets Logging Calegories Message Catalog Dabug Log Configuration Collection Fillers		Passed Authentications	d.) Selected: LogCollector ProfilerRadiusProbe Syslog Proxy for Govroam

Configuring Syslog-NG

Syslog proxies

Here are two options for possible syslog servers and config but you set up any syslog server as long as it has the following behaviour:

- Uses the FTICKS format
- Proxies to utilities.govroam.uk on port 514/UDP with Facility local6
- Includes in the FTICKS '#FEDID=0X000#' where 0X000 is replaced by the Federation ID supplied by Jisc.
- Filters down the proxied log to just those for
 - Successful authentications
 - Only authentications between member sites (i.e. NOT those to or from the Jisc NRPS, or within an organisation)

The two options:

syslog-ng on Linux

```
source s remote udp {
  udp();
  unix-stream("/dev/log" max-connections(100));};
};
filter f local0 {
  facility(local0);
};
rewrite r realm {
  subst("@","",value("ISE.UserName"));
};
rewrite r_facility_6 {
  set-facility("local6");
};
destination d jisc {
  syslog("212.219.243.132"
        transport("udp")
        port("514")
        template("F-
TICKS/govroam/1.0#REALM=${ISE.UserName}#VISCOUNTRY=GB#VISINST=${ISE.Operator
-Name}#CSI=${ISE.Calling-Station-ID}#RESULT=OK#FEDID=XXXXX#")
  );
};
log {
        source(s remote udp);
        filter(f local0);
        parser {
            kv-parser (prefix("ISE."));
        };
        filter{ "${ISE.NetworkDeviceName}" != "NRPS NAME"};
        filter{ "${ISE.SelectedAccessService}" != "NRPS NAME"};
        rewrite(r_realm);
        rewrite(r_facility_6);
        destination(d jisc);
};
```

Replace the **XXXXX** with the Federation ID supplied.

Replace **NRPS NAME** with the NRPS name as defined in the *Network Devices* and the *External RADIUS Servers* respectively.

Last update: 2024/05/20 siteadmin:fticks_logging_for_cisco_ise https://wiki.govroam.uk/doku.php?id=siteadmin:fticks_logging_for_cisco_ise&rev=1716208484 12:34

NXLog on Windows

Install NXLog CE on Windows

```
• Use this configuration (with paths changed appropriately)
Panic Soft
#NoFreeOnExit TRUE
define ROOT C:\Program Files (x86)\nxlog
define CERTDIR %R00T%\cert
define CONFDIR %R00T%\conf
define LOGDIR
                %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%
Moduledir %R00T%\modules
CacheDir %R00T%\data
Pidfile
          %R00T%\data\nxlog.pid
SpoolDir %R00T%\data
<Extension _syslog>
    Module
                xm syslog
</Extension>
<Extension exec>
    Module
                xm exec
</Extension>
<Input tcp_ise>
    Module im tcp
    Host 10.10.10.10 # Set this to the address of the Windows syslog server
    Port 514
    <Exec>
      if $SyslogFacility != "local0" drop();
      if $raw event !~ /CISE Passed Authentications/ drop();
      $FedID="XXXXX"; # Set this to the Federation ID provided by Jisc
      $SyslogFacility = "local6";
    </Exec>
</Input>
## For future use
<Output syslog tls>
    Module
                om ssl
    Host
                212.219.243.132
    Port
                6514
#
     CAFile
                 c:/Program Files (x86)/nxlog/data/cacert.pem
#
                 c:/Program Files (x86)/nxlog/data/clientreg.pem
     CertFile
#
     CertKeyFile c:/Program Files (x86)/nxlog/data/clientkey.pem
    AllowUntrusted 1
```

5/6

OutputType Exec 	Syslog_TLS to_syslog_ietf();
<output syslog_<br="">Module Host Port OutputType Exec </output>	om_tcp 212.219.243.132 601
<route 1=""> Path </route>	tcp_ise => syslog_tcp

- Change XXXXX to the supplied Federation ID.
- Change the 'Host' in 'Input tcp_ise' to the address of the syslog server.
- (Ignore the syslog_tls part, that's for future use)
- Restart the Service

Untested Advanced Configuration

There's a limitation to the logging process which might be addressable.

Problem: Not all member organisations can or do set the Operater-Name attribute in their Requests. Ideally the RFO should be able to insert an O-N with a value set on behalf of your site but only some RADIUS servers are capable of doing this (FreeRADIUS, RadSecProxy, RADIATOR). The next best option is to insert a generic value for the Federation. i.e:

When an RFO, scarfolk.gov.uk, gets a request from a site, say arkham.nhs.uk:

- 1. If the Operator-Name is set to, say, 1arkham.nhs.uk then leave it as is.
- 2. If the Operator-Name is missing the insert an Operator-Name with the value 'larkham.nhs.uk' no matter which of the several holby,nhs.uk servers the request comes from.
- 3. If there's no way to set the Operator-Name as in (2) then just insert an Operator-Name of, say, '1scarfolk.gov.uk'.

This way the home site will, at best, see an Operator-Name with the source site's value or, at worst, with it set to the Federation's value.

However, this conditional setting of Operator-Name isn't something found in servers like ClearPass, ISE or NPS. NPS is completely incapable of setting the Operator-Name. ClearPass can't do any sort of conditional setting. ISE might be able to.

Conditional Setting of Operator-Name

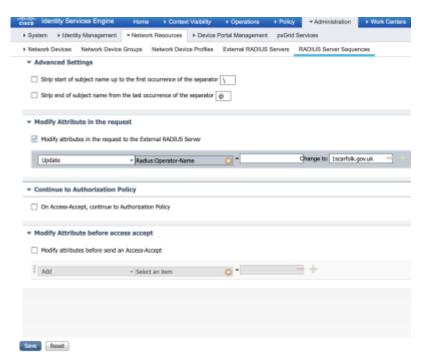
For each RADIUS Server Sequence dealing with proxying to a member organisation for authentication,

Last update: 2024/05/20 siteadmin:fticks_logging_for_cisco_ise https://wiki.govroam.uk/doku.php?id=siteadmin:fticks_logging_for_cisco_ise&rev=1716208484 12:34

go into the Advanced Attribute Settings and enable *Modify attributes in Request to External RADIUS Server*.

Set it to Update Radius:Operator-Name = "" 1scarfolk.gov.uk

which should replace the Operator-Name's value with 1scarfolk.gov.uk if it's empty.



Unfortunately, due to bugs in our ISE, we can't test this.

