

# Logging for Cisco ISE

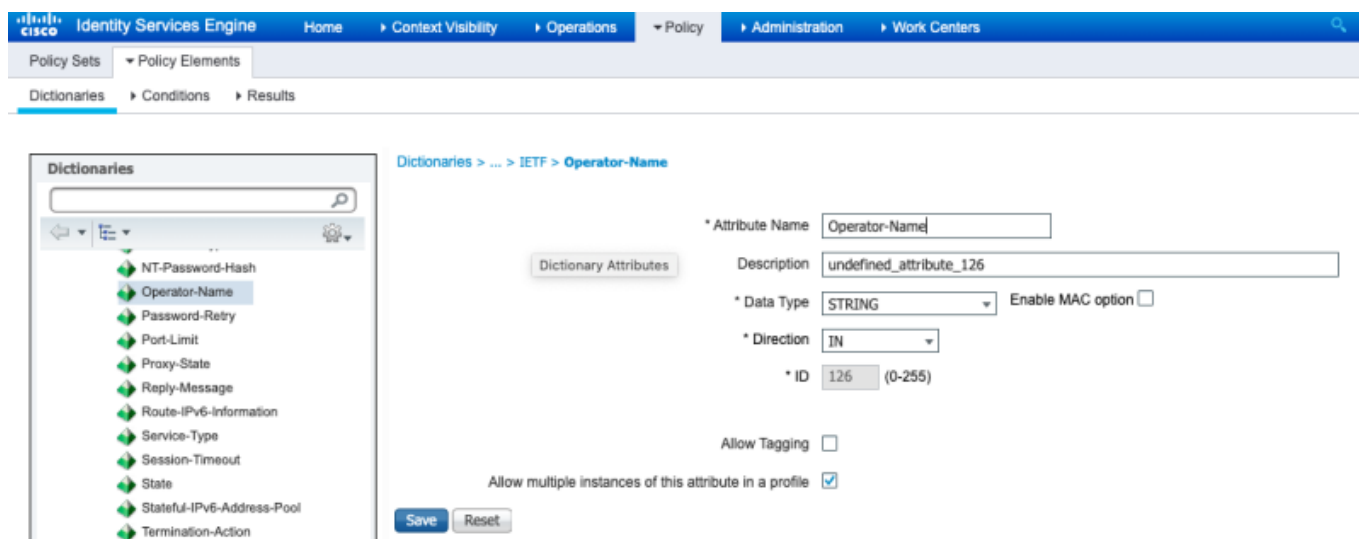
Unfortunately ISE can't generate custom logs in the format required (FTICKS) but, fortunately, it can generate syslog logs with the right information, which can be sent to a syslog server and munged into a suitable format.

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**



## Logging

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

In **Administration** → **System** → **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

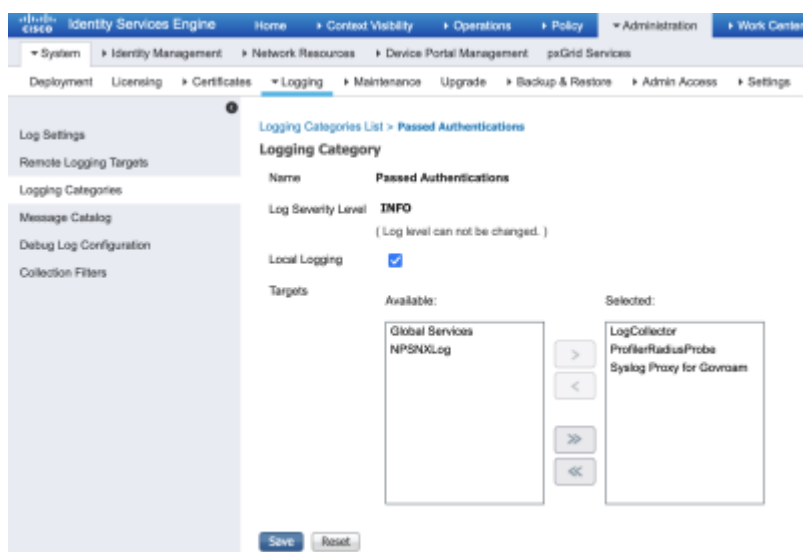
server.

*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*



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



## 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:

- Proxies to utilities.govroam.uk on port 601/TCP with Facility local6
- Includes in the FTICKS '#FEDID=0X000#' where 0X000 is replaced by the Federation ID supplied.
- 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)

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("tcp")
        port("601")
        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);
    filter{ match("Authentication succeeded" value ("MESSAGE"))};
    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 **XXXXXX** with the Federation ID supplied.

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

## 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   %ROOT%\cert
define CONFDIR   %ROOT%\conf
define LOGDIR    %ROOT%\data
define LOGFILE   %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data

<Extension _syslog>
    Module      xm_syslog
</Extension>

<Extension _exec>
    Module      xm_exec
</Extension>

<Input tcp_ise>
    Module im_tcp
    Host 10.10.10.10
    Port 514
    <Exec>
        if $SyslogFacility != "local6" drop();
        if $raw_event !~ /CISE_Passed_Authentications/ drop();
        $FedID="0X000";
    </Exec>
</Input>

<Output syslog_tls>
    Module      om_ssl
    Host        212.219.243.132
    Port        6514
#   CAFile      c:/Program Files (x86)/nxlog/data/cacert.pem
#   CertFile    c:/Program Files (x86)/nxlog/data/clientreq.pem
#   CertKeyFile c:/Program Files (x86)/nxlog/data/clientkey.pem
    AllowUntrusted 1
    OutputType  Syslog_TLS
    Exec        to_syslog_ietf();
```

```
</Output>

<Output syslog_tcp>
  Module      om_tcp
  Host        212.219.243.132
  Port        601
  OutputType  Syslog_TLS
  Exec        to_syslog_iETF();
  Exec        $SyslogFacility = "local6";
</Output>

<Route 1>
  Path        tcp_ise => syslog_tcp
</Route>
```

- Change 0X000 to the supplied Federation ID.
- Change the 'Host' in 'Input tcp\_ise' to the address of the ISE host.
- (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 Operator-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 holby.nhs.uk:

1. If the Operator-Name is set to, say, 1hobly.nhs.uk then leave it as is.
2. If the Operator-Name is missing the insert an Operator-Name with the value '1holby.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

Identity Services Engine

Home

Content Visibility

Operations

Policy

Administration

Work Center

System

Identity Management

Network Resources

Device Portal Management

paDMS Services

Deployment

License

Certificate

Logging

Maintenance

Upgrade

Backup & Restore

Admin Access

Settings

Click here to do wireless setup and visibility setup [Go not shown](#)

Log Settings

Remote Logging Targets

Logging Categories

Message Catalog

Debug Log Configuration

Collection Filters

Remove Logging Targets List

New Logging Target

Logging Target

\* Name

System Proxy for Scovision

Description

\* Host IP Address

10.30.18.18

\* Port

884

Facility Code

LOGG0

\* Maximum Length

2048

Target Type

syslog

Status

Enabled

Include Alarms For this Target

☐

Comply in RFC 3164

☒

Buttons

Cancel

(Valid Range 1 to 65535)

(Valid Range 255 to 8192)

From:  
<https://wiki.govroam.uk/> - Govroam

Permanent link:  
[https://wiki.govroam.uk/doku.php?id=siteadmin:fticks\\_logging\\_for\\_cisco\\_ise&rev=1715768067](https://wiki.govroam.uk/doku.php?id=siteadmin:fticks_logging_for_cisco_ise&rev=1715768067)

Last update: 2024/05/15 10:14

