

# TACACS.net™

## Configuration Guide

### Enhanced Logging

## 1. Introduction

TACACS.net version 2.1.0 introduces Enhanced Logging. This new logging functionality was added based on feedback from Enterprise customers who needed more flexibility to work with log aggregators and SIEM (Security Information and Event Management) tools. This new functionality is configured in a new configuration file; logging.xml. We have added structured logging, TCP transport for better reliability, CSV logging to make the logs easier to read and export, removed redundant information, changed to ISO standard time stamps, made better use of Syslog severities, collapsed the Startup log into the System log, and split System and Accounting into different logs.

## 2. Deployment Scenarios

This new functionality gives the Administrator a lot of options when configuring logging. The Security team may want to see all information logged to SIEM. The NOC may only want to see Error level System events sent to their logging server. The Production Networking Team may want to see Warning level System events for the devices they manage. Management or Compliance teams may wish to have Informational level Accounting events sent to their logging system. This new functionality enables these scenarios and can send different types of logs with different severity levels sent to different servers, each with their own settings.

## 3. Log files

### 3.1. System log

The System log is for server related events such licensing errors, start/restart, or reloading configuration files. In previous versions, there was a separate Startup log that showed events as the Server started up. The Startup log has been deprecated and these events are now sent to the System log.

### 3.2. Accounting log

The Accounting log shows events are sent by the TACACS+ client. This will typically include all commands sent to the client, depending on the type of client and how it is configured.

### 3.3. Debug log

The Debug log shows events from the Server's perspective. The System log says what happened, the Debug log shows *why* it happened. The Debug log is only written locally. The Default settings will rollover this log daily and automatically purge logs weekly to prevent them from taking up a lot of space on the server.

## 4. Structured Logging

Unstructured logging can create headaches for Administrators because they can be difficult to understand, difficult for log aggregation tools to parse, and take up lots of disk space. Structured events are written for the gathering of analytics, but are also readable by humans. Structured logging is simpler to query and analyze, easier to automate parsing of the data, and easier to correlate log entries from multiple sources.

## 5. CSV File Format

System and Accounting logs are now written in CSV format. These log files are created with appropriate header lines to make them easier to read, sort, and filter. See example below.

## TACACS.net™ Enhanced Logging Configuration Guide

TimeStamp	Severity	ConnectionId	SessionId	NAS_IP	NAS_HostName	NAS_Port	RemAddr	RemPort	User	Message
2016-01-15T00:25:11.18-05:00	I									No errors found in configuration files
2016-01-15T00:25:11.22-05:00	I									Server started.
2016-01-15T00:25:12.46-05:00	I									License information: License is valid;Printing individual license parts...Nodeid MVMMPGHRYLXN6N matches current computer;Hostname: TACSERVER1;Licensed to: test
2016-01-15T00:25:13.93-05:00	I	1		10.0.0.3	TACSERVER1	52670	10.0.0.1	23232		New client connection opened
2016-01-15T00:25:13.99-05:00	D	1	946092898	10.0.0.4	TACSERVER1	52670	10.0.0.2	23232	user1	Authentication message: Trying to authenticate user against group MISDept.
2016-01-15T00:25:15.02-05:00	D	1	946092898	10.0.0.5	TACSERVER1	52670	10.0.0.3	23232	user1	Authentication message: Result of authentication user against group MISDept is InvalidUserOrPassword. Trying to authenticate against next group in list.
2016-01-15T00:25:15.02-05:00	D	1	946092898	10.0.0.6	TACSERVER1	52670	10.0.0.4	23232	user1	Authentication message: Trying to authenticate user against group Tech Support.
2016-01-15T00:25:16.03-05:00	D	1	946092898	10.0.0.7	TACSERVER1	52670	10.0.0.5	23232	user1	Authentication message: Result of authentication user against group Tech Support is InvalidUserOrPassword. Trying to authenticate against next group in list.
2016-01-15T00:25:16.03-05:00	D	1	946092898	10.0.0.8	TACSERVER1	52670	10.0.0.6	23232	user1	Authentication message: Trying to authenticate user against group Network Engineering.
2016-01-15T00:25:16.03-05:00	D	1	946092898	10.0.0.9	TACSERVER1	52670	10.0.0.7	23232	user1	Authentication message: Authentication for user user1 passed against group Network Engineering - Passed.
2016-01-15T00:25:16.03-05:00	I	1	946092898	10.0.0.10	TACSERVER1	52670	10.0.0.8	23232	user1	Authentication passed.

Figure 1: CSV Formatted log file with headers

The Debug log is used for troubleshooting and has information which does not fit a CSV format appropriately.

## 6. Logging.xml

Logging.xml is a new configuration file that is included with TACACS.net version 2.1.0 and later. If this file is found in in the Configuration directory, it will override the settings in tacplus.xml. If this file is found in installations of versions earlier than 2.1.0, it will be ignored, and the settings in tacplus.xml will be used.

### 6.1. Local Logs

This section defines the local logs; System, Accounting, and Debug. The Startup log from previous versions has been eliminated and the data has been moved into the System log. If this section is commented out or deleted, the server will still send the minimal amount of logging to operate the server and delete these logs daily to minimize disk space.

#### 6.1.1. RolloverDays

This specifies how many days before starting a new log file. The default is 30.

#### 6.1.2. RolloverMB

This specifies how large the file can be before starting a new log. The default is 10 MB.

#### 6.1.3. DeleteDays

This specifies how long to keep a file before deleting it. The default is 90 days for System and Accounting and 7 days for the Debug log.

#### 6.1.4. Severity

This specifies what severity of events to send. Supported levels are: Critical, Error, Warning, Informational, or Debug. The server will send that level and higher severities. For example, if you set it to Warning, it will send Warning, Error, and Critical events. Refer to the table below to see what information is sent at each level. Most log types are set to Informational by default. The Debug log only uses the debug level.

### 6.2. Remote Syslog

This section defines the logs that you can send to other systems. Only the Accounting and System logs can be sent to other central logging servers. You can define multiple entries that send the same or different information to multiple servers.

#### 6.2.1. Host Name

This is the host name of the syslog server or log aggregator. This is relevant only to this configuration file. It can be the systems DNS name, a team name, or any other name that will help the TACACS+ Administrator distinguish between different log destinations.

#### 6.2.2. Address

The IP address or FQDN of the remote log collector. If there is no address specified, no syslog will be sent.

#### 6.2.3. Protocol

This can be UDP or TCP. Some administrators choose TCP for more reliable transport.

### 6.2.4. Port

This can be any port number. The default UDP port is 514, the default TCP port is 601.

### 6.2.5. Facility

The default facility is 4. You can change this to a different facility if needed for your logging server.

### 6.2.6. RFC

This determines the formatting of the Syslog message. The options are rfc3164 which does not support structured data (default), and rfc5424, which does support structured data. RFC 5424 is the newer format and should be used if your logging system supports it.

### 6.2.7. MaxLength


This sets the maximum message length support. Use the default (1000) unless your log destination requires a different number.

### 6.2.8. Type

This can be either Accounting or System.

#### 6.2.1. Severity

This specifies what severity of events to send. Supported levels are: Critical, Error, Warning, Informational, or Debug. The server will send that level and higher severities. For example, if you set it to Warning, it will send Warning, Error, and Critical events. Refer to the table below to see what information is sent at each level.

	When the Debug severity is chosen, it can generate a large amount of log data. This can degrade performance, particularly for System logs in Remote Syslog settings, so use this severity level with caution.
--	---

## 7. Log settings and severity

The following table shows the logging events that are sent at each severity level.

VALUE	SEVERITY	DESCRIPTION	SYSTEM	ACCOUNTING
2	Critical	Critical conditions	TACACS.net can't start because of file syntax or other error.	
3	Error	Error conditions	Authentication, authorization failure, Licensing threshold exceeded. Time synch mismatch. Bad packets received from clients.	Authentication or authorization failures sent from the client.
4	Warning	An error will occur if action is not taken.	AD/LDAP error, RADIUS errors, invalid client/user, remote address or shared secret. Google MFA errors, User lockout. Invalid packet or shared secret.	
6	Informational	Normal operational messages that require no action.	Authentication, authorization success, reloading config files. Server startup, shutdown, License verification. TACVerify.	Authentication, authorization success sent from the client.
7	Debug	Information useful for debugging the application	Everything	Everything

Table 1: Syslog events and severities