

# Image Cover Sheet

**CLASSIFICATION**

UNCLASSIFIED

**SYSTEM NUMBER**

497167



**TITLE**

PROOF LOGGING USER MANUAL

**System Number:**

**Patron Number:**

**Requester:**

**Notes:**

**DSIS Use only:**

**Deliver to:** FF



# Proof Logging User Manual

TR-95-5471-04

Sentot Kromodimoeljo  
Bill Pase

Release date: JUNE 1995

ORA Canada  
267 Richmond Road, Suite 100  
Ottawa, Ontario K1Z 6X3  
CANADA

DSS Contract No. W2207-2-AF08/01-SV

© Her Majesty the Queen in right of Canada (1995)  
as represented by the Minister of National Defence

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Proof Logging</b>	<b>2</b>
2.1	Check All Proofs . . . . .	2
2.2	Check Proof . . . . .	2
2.3	Dump Log . . . . .	2
2.4	Log On . . . . .	2
2.5	Log Off . . . . .	3

## 1 Introduction

This report is the User Manual for proof logs in NEVER as they appear in EVES, version 2.4.2. It describes how to use the proof logging tool. For a technical description of Proof logs, the reader is referred to [1].

In keeping with recent releases of EVES, the User Manual is the same as the Online Help, except for this introduction and the references.

## 2 Proof Logging

```
proof_logging_command: check_all_proofs_command | check_proof_command
                      | dump_log_command | log_on_command | log_off_command
```

EVES has a proof-logging facility that enables proof steps to be logged in terms of very low-level inferences that can be used for the certification of proofs. The proof checker is used to formally certify proofs. A proof whose proof log is accepted by the proof checker has a high degree of assurance. The proof browser is used to informally certify proofs. A proof log can be browsed by the user to increase the credibility of a proof.

Initially, proof logging is disabled. It can be enabled or disabled at any time. This flexibility is useful for proof browsing during the development of a proof. For proof checking, it is usual to redo a completed proof with proof logging enabled so it can be checked by the proof checker. Proof logs can be checked either by the integrated proof checker, or dumped to a file for certification by an independent proof checker.

The log-on command is used to enable proof logging, while the log-off command is used to disable proof logging. Proof logs can be saved to a file using the dump-log command. The integrated proof checker can be invoked using the check-proof and check-all-proofs commands.

### 2.1 Check All Proofs

```
check_all_proofs_command: (CHECK-ALL-PROOFS)
```

The check-all-proofs command checks all proofs in the database. A report is displayed showing the results for each proof checked. The proof check will fail for any proof whose proof log was not fully recorded.

### 2.2 Check Proof

```
check_proof_command: (CHECK-PROOF [identifier])
```

The check-proof command checks the proof associated with *identifier* if specified or the proof associated with the current formula if none was specified. Proof logging must have been enabled during the entire proof for the proof check to succeed.

### 2.3 Dump Log

```
dump_log_command: (DUMP-LOG string)
```

The dump-log command saves the declarations and proof logs from the current theory into files for input to the independent proof checker. The declarations are saved into a file with a ".src" extension, while the proof logs are saved into a file with a ".plg" extension.

### 2.4 Log On

```
log_on_command: (LOG-ON)
```

This command enable's proof logging. It can be used at any time to begin recording proof logs. (Recording a log for part of a proof is not very useful.) Initially, proof logging is disabled.

## 2.5 Log Off

`log_off_command:` (LOG-OFF)

This command disable's proof logging. It can be used at any time to end recording proof logs. (Recording a log for part of a proof is not very useful.) Initially, proof logging is disabled.



## **References**

- [1] S. Kromodimoeljo, B. Pase, Proof Logs, TR-95-5471-03, ORA Canada, June 1995.

NO. OF COPIES NOMBRE DE COPIES 1	COPY NO. COPIE N° 1	INFORMATION SCIENTIST'S INITIALS INITIALES DE L'AGENT D'INFORMATION SCIENTIFIQUE
AQUISITION ROUTE FOURNI PAR ▶		
DATE ▶		
DSIS ACCESSION NO. NUMÉRO DSIS ▶		

DND 1158 (6-97)



National  
Défence

Défense  
nationale

*Sydney 497167*

**PLEASE RETURN THIS DOCUMENT  
TO THE FOLLOWING ADDRESS:**

DIRECTOR  
SCIENTIFIC INFORMATION SERVICES  
NATIONAL DEFENCE  
HEADQUARTERS  
OTTAWA, ONT. - CANADA K1A 0K2

**PRIÈRE DE RETOURNER CE DOCUMENT  
À L'ADRESSE SUIVANTE:**

DIRECTEUR  
SERVICES D'INFORMATION SCIENTIFIQUES  
QUARTIER GÉNÉRAL  
DE LA DÉFENSE NATIONALE  
OTTAWA, ONT. - CANADA K1A 0K2