

# MultiNet/TCPware Intrusion Prevention System

## Event Description Guide

5-Sep-2009

This document describes the events that can be logged to the Intrusion Prevention System (IPS) that in MultiNet V5.3 and TCPware V5.9 and later. This includes not only events reported by MultiNet and TCPware components, but also those events that can be reported by PMDF V6.4 and later (running on a MultiNet or TCPware platform where IPS is configured).

### FTP Events (MultiNet and TCPware)

FTP_TIMEOUT	The user failed to login within MULTINET_FTP_MAXIMUM_IDLE_TIME.
FTP_INVALIDUSER	The user logging in didn't exist in the VMS UAF file, so LOGINOUT returned a value of SS\$_NOSUCHUSER or LGI\$_NOTVALID.
FTP_USERAUTH	LOGINOUT returned couldn't read the user's UAF record.
FTP_AUTHFAILED	The user was denied access due to one of the following reasons: <ul style="list-style-type: none"><li>• Account or user is disabled</li><li>• Account has expired</li><li>• Account is restricted</li><li>• Password authentication failed</li></ul>

### IMAP Events (MultiNet and TCPware)

IMAP_TIMEOUT	Session timed out before login was complete.
IMAP_INVALIDUSER	The username specified wasn't valid or didn't exist in the UAF file.
IMAP_USERAUTH	LOGINOUT could not read the user's UAF record.
IMAP_AUTHFAILED	The user was denied access due to one of the following reasons: <ul style="list-style-type: none"><li>• Account or user is disabled</li><li>• Account has expired</li><li>• Account is restricted</li><li>• User's password has expired</li><li>• An invalid password was entered</li></ul>

### **POP3 Server Events (MultiNet and TCPware)**

POP3_ABORT	A status of SS\$_ABORT that does not come from the POP3 routines was encountered.
POP3_INVALIDUSER	The username specified wasn't valid or didn't exist in the UAF file.
POP3_USERAUTH	LOGINOUT could not read the user's UAF record.
POP3_AUTHFAILED	The user was denied access due to one of the following reasons: <ul style="list-style-type: none"><li>• Account or user is disabled</li><li>• Account has expired</li><li>• Account is restricted</li><li>• User's password has expired</li><li>• An invalid password was entered</li></ul>

### **R-Services (MultiNet and TCPware)**

<service>_BAD_PORT	The client is not on a privileged port
<service>_TIMEOUT	Session timeout or abort.
<service>_LOGIN_DISABLED	User logins are currently disabled.
<service>_USERAUTH	LOGINOUT could not read the user's UAF record.

Note: *REXEC*, *RUSER* and *RSHELL* are common, though the names vary with the service.

### **SMTP Events (MultiNet and TCPware)**

SMTP_REJECT_822	SMTP_REJECT_822 is due to RFC 822 header matching with the filter file.
SMTP_INVALID_DOMAIN	SMTP_INVALID_DOMAIN is due to DNS returning NXDOMAIN.
SMTP_FLAG_REJECT	SMTP_FLAG_REJECT is due to reject file (MULTINET_SMTP_SERVER_REJECT_FILE) matching.
SMTP_FLAG_REJECT_QUIET	SMTP_FLAG_REJECT_QUIET is due to reject file (MULTINET_SMTP_SERVER_REJECT_FILE) matching.

### **SNMP Events (MultiNet and TCPware)**

SNMP_BADCOMMUNITY	The community name specified does not match the request.
SNMP_AUTHENERR	The community name does not match one for the address that the request comes from.

### **SSH Events (MultiNet and TCPware)**

SSH_BOGUS_ID	An invalid or incomplete identification message was sent to the SSH server by the SSH client. This could be caused by a port scanner.
SSH_AUTHFAILED	The user was denied access due to the following reasons: <ul style="list-style-type: none"><li>• Account or user is disabled</li><li>• Account has expired</li><li>• Account is restricted</li><li>• Password authentication failed</li><li>• Password has expired and must be reset by the system manager</li></ul>
SSH_USERAUTH	Publickey and/or hostbased authentication failed.
SSH_INVALIDUSER	User has no UAF record.

### **TELNET Events (MultiNet and TCPware)**

TELNET_TIMEOUT	The user login session timed out.
TELNET_INVALIDUSER	The username specified wasn't valid or didn't exist in the UAF file.
TELNET_USERAUTH	LOGINOUT could not read the user's UAF record.
TELNET_AUTHFAILED	The user was denied access due to one of the following reasons: <ul style="list-style-type: none"><li>• Account or user is disabled</li><li>• Account has expired</li><li>• Account is restricted</li><li>• User's password has expired</li><li>• An invalid password was entered</li></ul>

### **PMDF IMAP Server Events (PMDF only)**

PMDF_IMAP_AUTHFAILED	User authentication failed (e.g. invalid password, disabled account, expired account, etc).
PMDF_IMAP_INVALIDUSER	The username specified wasn't valid or didn't exist.
PMDF_IMAP_ABORTLOGIN	A connection abort happened during the login process.
PMDF_IMAP_SENDRECVERR	IMAP got an error on a send or recv call on the connection.
PMDF_IMAP_EXCEEDLIFE	A session exceeded the SESSION_LIFETIME option value.
PMDF_IMAP_MININTERVAL	A client connected again in less than the MIN_LOGIN_INTERVAL option value.
PMDF_IMAP_FORCEKILL	A connection was killed after shutdown based on the FORCE_KILL_TIMEOUT option.
PMDF_IMAP_OTHERERR	Some other error occurred on the connection or with the mailbox.

### **PMDF POP3 Server Events (PMDF only)**

PMDF_POP3_AUTHFAILED	User authentication failed (e.g. invalid password, disabled account, expired account, etc).
PMDF_POP3_INVALIDUSER	The username specified wasn't valid or didn't exist.
PMDF_POP3_ABORTLOGIN	A connection abort happened during the login process.
PMDF_POP3_SENDRECVERR	POP3 got an error on a send or recv call on the connection.
PMDF_POP3_EXCEEDLIFE	A session exceeded the SESSION_LIFETIME option value.
PMDF_POP3_MININTERVAL	A client connected again in less than the MIN_LOGIN_INTERVAL option value.
PMDF_POP3_FORCEKILL	A connection was killed after shutdown based on the FORCE_KILL_TIMEOUT option.
PMDF_POP3_OTHERERR	Some other error occurred on the connection or with the mailbox.

### **PMDF SMTP Server Events (PMDF only)**

PMDF_SMTP_AUTHFAILED	User authentication failed.
PMDF_SMTP_REJECT	Rejected via a mapping table.

## **Notes**

1. Though not currently in all of the services, in the future FTP, POP3, REXEC, RUSER, RSHELL, TELNET and IMAP can also log an event of "unexpected status <hex value>" so that failure status values that were not expected can be used. One possible source of these values is external authentication.