

## Configuring Protocol Handling (NSM Procedure)

The protocol anomaly detection methods identify traffic that deviates from RFC specifications. In general, you modify protocol thresholds and configuration settings only if you encounter false positives or performance issues.

To tune protocol anomaly detection thresholds:

1. In NSM Device Manager, double-click the IDP device that you want to modify. The device configuration editor appears.
2. Click **Sensor Settings**.
3. Click the **Protocol Thresholds and Configuration** tab.
4. Configure the protocol thresholds using Table 1.
5. Click **Apply**.
6. Click **OK**.

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings**

Setting	Description
AIM	<b>Maximum header length</b> —Raises a protocol anomaly if IDP detects a header containing more bytes than the specified maximum. The default is 10,000 bytes.
	<b>Maximum type-length-value length</b> —Raises a protocol anomaly if IDP detects an AIM/ICQ type-length-value (TLV) containing more bytes than the specified maximum. A TLV is a tuple used for passing typed information to the protocol. The default is 8000 bytes.
	<b>Maximum inter-client-message-block length</b> —Raises a protocol anomaly if IDP detects an AIM/ICQ inter-client-message-block (ICMB) containing more bytes than the specified maximum. The default is 2000 bytes.
	<b>Maximum filename length</b> —Raises a protocol anomaly if IDP detects an AIM/ICQ file name containing more bytes than the specified maximum. The default is 10,000 bytes.
DHCP	<b>Check to see if the source port of client's packets is 68</b> —Raises a protocol anomaly if IDP detects DHCP traffic that originates from a port other than 68. This setting is not enabled by default.

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
DNS	<p><b>Report unknown DNS parameters (high noise)</b>—Detects and reports unknown DNS parameters.</p> <p>You must also configure an IDP rulebase rule to detect DNS anomalies. This setting is not enabled by default.</p> <hr/> <p><b>Report unexpected DNS parameters (high noise)</b> —Detects and reports unexpected DNS parameters. This setting is not enabled by default.</p> <p>You must also configure an IDP rulebase rule to detect DNS anomalies.</p> <hr/> <p><b>Maximum length of a DNS UDP packet</b> —Raises a protocol anomaly if IDP detects a DNS UDP packet containing more bytes than the specified maximum. The default is 512 bytes.</p> <hr/> <p><b>Maximum size of a NXT resource record</b> —Raises a protocol anomaly if IDP detects an NXT resource record in a DNS request or response message of a greater size. The default is 4096 bytes.</p> <p>This setting tunes the following protocol anomaly attack object: DNS_BIND_NXT_OVERFLOW (key is DNS:OVERFLOW:NXT-OVERFLOW).</p> <hr/> <p><b>Maximum time of a dns cache</b> —Controls the maximum amount of time for a DNS query and reply. The default is 60 seconds.</p> <hr/> <p><b>Maximum number of logs in a session</b> —Controls the maximum number of DNS queries kept to match a reply. The default is 1000 queries.</p>
FTP	<p><b>Maximum Line length</b>—Raises a protocol anomaly if IDP detects an FTP username containing more bytes than the specified maximum. The default is 32 bytes.</p> <hr/> <p><b>Maximum Username length</b>—Raises a protocol anomaly if IDP detects an FTP password containing more bytes than the specified maximum. The default is 64 bytes.</p> <hr/> <p><b>Maximum Password length</b> —Raises a protocol anomaly if IDP detects an FTP pathname containing more bytes than the specified maximum. The default is 512 bytes.</p> <hr/> <p><b>Maximum Pathname length</b> —Raises a protocol anomaly if IDP detects an FTP pathname containing more bytes than the specified maximum. The default is 512 bytes.</p> <hr/> <p><b>Maximum Sitestring length</b> —Raises a protocol anomaly if IDP detects an FTP sitestring containing more bytes than the specified maximum. The default is 512 bytes.</p> <hr/> <p><b>Maximum number of login failures per-minute</b>—Raises a protocol anomaly if IDP detects more FTP login failures in one minute than the specified maximum. The default is 4 FTP login failures per minute.</p>
GNUTELLA	<p><b>Maximum TTL hops</b>—Raises a protocol anomaly if IDP detects a number of TTL hops that is higher than the specified maximum. The default is 8 TTL hops.</p> <hr/> <p><b>Maximum Line length</b>—Raises a protocol anomaly if IDP detects, in a Gnutella connection, a line that contains more bytes than the specified maximum. The default is 2048 bytes.</p> <hr/> <p><b>Maximum Query size</b>—Raises a protocol anomaly if IDP detects a Gnutella client query that contains more bytes than the specified maximum. The default is 256 bytes.</p>

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
GOPHER	<p><b>Maximum line length</b>—Raises a protocol anomaly if IDP detects, in a Gopher server-to-client connection, a line sent by a Gopher server to a client that contains more bytes than the specified maximum. The default is 512 bytes.</p>
	<p><b>Maximum hostname length</b>—Raises a protocol anomaly if IDP detects, in a Gopher server-to-client connection, a hostname that contains more bytes than the specified maximum. The default is 64 bytes.</p>
HTTP	<p><b>Maximum Request length</b>—Raises a protocol anomaly if IDP detects an HTTP request that contains more bytes than the specified maximum. The default is 8192 bytes.</p>
	<p><b>Maximum Header length</b>—Raises a protocol anomaly if IDP detects an HTTP header that contains more bytes than the specified maximum. The default is 8192 bytes.</p>
	<p><b>Maximum Cookie length</b> —Raises a protocol anomaly if IDP detects a cookie that contains more bytes than the specified maximum. The default is 8192 bytes.</p> <p>Cookies that exceed the cookie length setting can match the protocol anomaly "r;HTTP-HEADER-OVERFLOW" and produce unnecessary log records. If you are getting too many log records for the HTTP-HEADER-OVERFLOW protocol anomaly, increase the maximum cookie length.</p>
	<p><b>Maximum Authorization length</b>—Raises a protocol anomaly if IDP detects an HTTP header authorization line that contains more bytes than the specified maximum. The default is 512 bytes.</p> <p>Use this setting to tune results from the Auth Overflow attack object (key is HTTP:OVERFLOW:AUTH-OVFLW).</p>
	<p><b>Maximum Content-type length</b>—Raises a protocol anomaly if IDP detects an HTTP header content-type that contains more bytes than the specified maximum. The default is 512 bytes.</p>
	<p><b>Maximum User-agent length</b>—Raises a protocol anomaly if IDP detects an HTTP header user-agent that contains more bytes than the specified maximum. The default is 256 bytes.</p>
	<p><b>Maximum Host length</b>—Raises a protocol anomaly if IDP detects an HTTP header host that contains more bytes than the specified maximum. The default is 64 bytes.</p>
	<p><b>Maximum Referrer length</b> —Raises a protocol anomaly if IDP detects an HTTP header referrer that contains more bytes than the specified maximum. The default is 8192 bytes.</p>
	<p><b>Use alternate ports as http service</b>—If selected, the security module watches for HTTP traffic on the following ports in addition to tcp/80: 7001; 8000; 8001; 8100; 8200; 8080; 8888; 9080. This setting is enabled by default.</p>
	<p><b>Maximum number of login failures per-minute</b>—Raises a protocol anomaly if IDP detects, between a unique pair of hosts, more login failures than the specified maximum. The default is 4 HTTP authentication failures per minute.</p> <p>This setting tunes the BRUTE_FORCE attack object.</p>
<p><b>Maximum number of 301/403/404 or 405 errors per-minute</b>—Raises a protocol anomaly if IDP detects, between a unique pair of hosts, more 301/403/404/405 errors than the specified maximum. The default is 16 HTTP errors per minute.</p>	

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings** (continued)

Setting	Description
ICMP	<b>Maximum Packets per second to trigger a flood</b> —Raises a protocol anomaly if IDP detects more ICMP packets than the specified maximum. The default is 250 packets per second.
	<b>Minimum time interval (in seconds) between packets</b> —Raises a protocol anomaly if IDP detects ICMP packets that have less than the specified minimum time interval between them. The default is 1 second.
	Use this setting to tune the Flood attack object (ICMP:EXPLOIT:FLOOD).
IDENT	<b>Maximum requests per session</b> —Raises a protocol anomaly if IDP detects more IDENT (identification protocol) requests than the specified maximum. The default is 1 request per session.
	This setting tunes the Too Many Requests attack object (key is IDENT:OVERFLOW:REQUEST-NUM).
	<b>Maximum Request length</b> —Raises a protocol anomaly if IDP detects an IDENT request containing more bytes than the specified maximum. The default is 15 bytes.
	This setting tunes the Request Too Long attack object (key is IDENT:OVERFLOW:REQUEST).
IKE	<b>Maximum Reply length</b> —Raises a protocol anomaly if IDP detects an IDENT reply containing more bytes than the specified maximum. The default is 128 bytes.
	This setting tunes the Reply Too Long attack object (key is IDENT:OVERFLOW:REPLY).
IKE	<b>Maximum number of payloads in an IKE message</b> —Raises a protocol anomaly if IDP detects an IKE message with a higher number of payloads. The default is 57 payloads.
	This setting tunes detection with the TOO-MANY-PAYLOADS attack object (key is IKE:MALFORMED:2MANY-PAYLOAD).

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
IMAP	<b>Maximum Line length</b> —Raises a protocol anomaly if IDP detects an IMAP line containing more bytes than the maximum. The default is 2048 bytes.
	<b>Maximum Username length</b> —Raises a protocol anomaly if IDP detects an IMAP username containing more bytes than the maximum. The default is 64 bytes.
	<b>Maximum Password length</b> —Raises a protocol anomaly if IDP detects an IMAP password containing more bytes than the specified maximum. The default is 64 bytes.
	<b>Maximum Mailbox length</b> —Raises a protocol anomaly if IDP detects an IMAP mailbox containing more than the maximum. The default is 64 bytes.
	<b>Maximum Reference length</b> —Raises a protocol anomaly if IDP detects an IMAP reference containing more bytes than the specified maximum. The default is 64 bytes.
	<b>Maximum Flag length</b> —Raises a protocol anomaly if IDP detects an IMAP flag containing more bytes than the specified maximum. The default is 64 bytes.
	<p data-bbox="370 888 1421 1014"><b>Maximum Literal length</b>—Raises a protocol anomaly if IDP detects a literal with more octets than the specified maximum. In IMAP4 protocol, a string can be in one of two forms: literal and quoted. As defined in RFC 2060 4.3, a literal is a sequence of zero or more octets (including CR and LF), prefix-quoted with an octet count in the form of an open brace ("{"), the number of octets, close brace ("}"), and CRLF. Valid range is 1 to 1,67,77,215. The default is 65,535 bytes.</p> <p data-bbox="370 1045 1421 1098">This setting tunes detection with the <code>imap_literal_length_overflow</code> attack object (key is <code>IMAP:OVERFLOW:LIT_LENGTH_OFLOW</code>).</p> <p data-bbox="370 1129 1421 1192"><b>Maximum number of login failures per-minute</b>—Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the maximum. The default is 4 IMAP login failures per minute.</p>
IRC	<b>Maximum Password length</b> —Raises a protocol anomaly if IDP detects an Internet Relay Chat (IRC) password containing more bytes than the specified maximum. The default is 16 bytes.
	<b>Maximum Username length</b> —Raises a protocol anomaly if IDP detects an IRC username containing more bytes than the specified maximum. The default is 16 bytes.
	<b>Maximum Channel length</b> —Raises a protocol anomaly if IDP detects an IRC channel name containing more bytes than the specified maximum. The default is 64 bytes.
	<b>Maximum Nickname length</b> —Raises a protocol anomaly if IDP detects an IRC nickname containing more bytes than the specified maximum. The default is 16 bytes.

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
LDAP	<b>Maximum length of Integer representation in BER encoding</b> —Raises a protocol anomaly if IDP detects an integer field of the LDAP BER containing more bytes than the specified maximum. The default is 4 bytes.
	<b>Maximum number of left zeros for tag in BER encoding</b> —Raises a protocol anomaly if IDP detects more left zeros in any tag in LDAP BER encoding than the specified maximum. The default is 4 left zeros.
	<b>Maximum value of any LDAP tag in BER encoding</b> —Raises a protocol anomaly if IDP detects a value for a tag that can be seen in the LDAP BER encoding that is greater than the specified maximum. LDAP tags are represented using 1 byte, with the top 3 bits reserved. The default is 31.
	<b>Maximum number of left zeros for length in BER encoding</b> —Raises a protocol anomaly if IDP detects more left zeros in any length field in LDAP BER encoding than the specified maximum. The default is 64 left zeros.
	<b>Maximum number of search results requested by LDAP client</b> —Raises a protocol anomaly if IDP detects an LDAP client request for more matching entries than the specified maximum. The default is 0 (indicating no limit).
	<b>Maximum timelimit for search result requested by LDAP client</b> —Raises a protocol anomaly if IDP detects a time limit greater than the specified maximum. The time limit is the number of seconds before a client request times out waiting for a response from the server. The default is 0 (indicating no limit).
	<b>Maximum length of an LDAP Attribute Descriptor</b> —Raises a protocol anomaly if IDP detects a length of an attribute descriptor field in an LDAP message containing more bytes than the specified maximum. The default is 512 bytes.
	<b>Maximum length of an LDAP Distinguished Name</b> —Raises a protocol anomaly if IDP detects a length of a distinguished name field in the LDAP message containing more bytes than the specified maximum. The default is 512 bytes.
	<b>Maximum value of Message id in any LDAP Message</b> —Raises a protocol anomaly if IDP detects a message ID greater than the specified maximum. The default is 2,14,74,83,647.
	<b>Maximum length of an LDAP message</b> —Raises a protocol anomaly if IDP detects a LDAP message that will be processed by the LDAP subsystem larger than the specified maximum. The default is 8100 bytes.  This setting tunes the MESSAGE_TOO_LONG attack object. If IDP raises this anomaly, it logs the event and skips the message.
	<b>Maximum number of nested operators in an LDAP search request</b> —Raises a protocol anomaly if IDP detects a number of nested levels allowed in an LDAP search request filter argument greater than the specified maximum. The default is 8 nested operators.
<b>Maximum Number of login failures per-minute</b> —Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the maximum. The default is 4 LDAP login failures per minute.	

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
LPR	<p><b>Maximum Sub-command length in RECEIVE-JOB Command</b>—Raises a protocol anomaly if IDP detects in an Line Printer Protocol (LPR) control file a sub command line containing more bytes than the specified maximum. LPR is a TCP-based print server protocol used by line printer daemons (client and server) to communicate over networks. An LPR client uses the LPR protocol to send a print command to an LPR server (a line printer) at TCP/515. After the print command is received by the server, the client can issue subcommands to the server and send control and data files. Control files tell the line printer which functions to perform when printing the file; data files carry the payload. The default is 256 bytes.</p>
	<p><b>Maximum Reply length from server</b>—Raises a protocol anomaly if IDP detects an LPR control filename containing more bytes than the specified maximum. The default is 64 bytes.</p>
	<p><b>Maximum Control filename length</b>—Raises a protocol anomaly if IDP detects an LPR control filename containing more bytes than the specified maximum. The default is 64 bytes.</p>
	<p><b>Maximum Data filename length</b>—Raises a protocol anomaly if IDP detects a data filename containing more bytes than the specified maximum. The default is 64 bytes.</p>
	<p><b>Maximum Control file size</b>—Raises a protocol anomaly if IDP detects an LPR control file size greater than the specified maximum. The default is 1024 bytes.</p>
	<p><b>Maximum Data file size</b>—Raises a protocol anomaly if IDP detects an LPR data file size greater than the specified maximum. The default is 64 bytes.</p>
	<p><b>Maximum Banner string length</b>—Raises a protocol anomaly if IDP detects an LPR banner string containing more bytes than the specified maximum. A banner string is typically the filename of the print job. The default is 32 bytes.</p>
	<p><b>Maximum E-mail length</b> —Raises a protocol anomaly if IDP detects an LPR control file e-mail address containing more bytes than the specified maximum. After the file has printed, it is sent to the e-mail address specified in the control file. The default is 32 bytes.</p>
	<p><b>Maximum Symbolic link length</b> —Raises a protocol anomaly if IDP detects in an LPR control file a symbolic link containing more bytes than the specified maximum. A symbolic link is a file that points to another file (entry) in a UNIX file system, but does not contain the data in the target file. When the LPR protocol receives a symbolic link command in a control file, it records the symbolic link data for the print job filename to prevent directory entry changes from reprinting the file. The default maximum is 128 bytes.</p>
	<p><b>Maximum font length</b> —Raises a protocol anomaly if IDP detects in an LPR control file a font name containing more bytes than the specified maximum. The default is 64 bytes.</p>
<p><b>Maximum filename length for format related sub commands</b>—Raises a protocol anomaly if IDP detects in an LPR control file a format-related file name containing more bytes than the specified maximum. The default is 32 bytes.</p>	

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
MSN	<b>Maximum Username length</b> —Raises a protocol anomaly if IDP detects an MSN (Microsoft Instant Messaging) username containing more bytes than the specified maximum. The default is 84 bytes.
	<b>Maximum Display name length</b> —Raises a protocol anomaly if IDP detects an MSN display name containing more bytes than the specified maximum. The default is 128 bytes.
	<b>Maximum Group name length</b> —Raises a protocol anomaly if IDP detects an MSN group name containing more bytes than the specified maximum. The default is 84 bytes.
	<b>Maximum User state length</b> —Raises a protocol anomaly if IDP detects an MSN user state containing more bytes than the specified maximum. A user state is a three-letter code that indicates the status of the user's connection (online, offline, idle, and so on). The default is 10 bytes.
	<b>Maximum Phone number length</b> —Raises a protocol anomaly if IDP detects a phone number containing more bytes than the specified maximum. The default is 20 bytes.
	<b>Maximum Length of IP:port</b> —Raises a protocol anomaly if IDP detects an IP:port parameter containing more bytes than the specified maximum. An IP:port parameter indicates the IP address and port number of the MSN server for a switchboard session. The default is 30 bytes.
	<b>Maximum URL length</b> —Raises a protocol anomaly if IDP detects a URL containing more bytes than the specified maximum. The default is 1024 bytes.
MSRPC	<b>Maximum fragment length in MSRPC message</b> —Raises a protocol anomaly if IDP detects an MSRPC (Microsoft Remote Procedure Call) message with a fragment length greater than the specified maximum. The default is 8192.
	<b>Maximum tower data length in endpoint mapper messages</b> —Raises a protocol anomaly if IDP detects an endpoint mapper message with a tower data length greater than the specified maximum. The default is 8192.
	<b>Maximum number of entries in an insert message</b> —Raises a protocol anomaly if IDP detects an MSRPC insert message with more entries than the specified maximum. The default is 100 entries.
NFS	<b>Maximum Name length</b> —Raises a protocol anomaly if IDP detects an NFS packet name containing more bytes than the specified maximum. The default is 256 bytes.
	<b>Maximum Path length</b> —Raises a protocol anomaly if IDP detects an NFS packet pathname containing more bytes than the specified maximum. The default is 1024 bytes.
	<b>Maximum buffer length for read/write</b> —Raises a protocol anomaly if IDP detects an NFS read/writer buffer larger than the specified maximum. The default is 32,768 bytes.

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
NTP	<b>Minimum time (in seconds) between two requests</b> —Raises a protocol anomaly if IDP detects the time between two client-to-server NTP requests is greater than the specified maximum. Valid values range from 64 to 1024 seconds. The default is 0 seconds (which turns the feature off).
	<b>Maximum length for NTPv3 message</b> —Raises a protocol anomaly if IDP detects an NTPv3 message containing more bytes than the specified maximum. The default is 68 bytes.
	<b>Maximum length for NTPv4 message</b> —Raises a protocol anomaly if IDP detects an NTPv4 message containing more bytes than the specified maximum. The default is 68 bytes.
	<b>Maximum stratum value for any NTP peer</b> —Raises a protocol anomaly if IDP detects a stratum value larger than the specified maximum. The default is 15 bytes.
	<b>Maximum time since last update of Reference clock</b> —Raises a protocol anomaly if IDP detects that the NTP reference clock has not been updated in more time than the specified maximum. The default is 86,400 seconds.
	<b>Match timestamps on NTP request and response</b> —Enables IDP to perform timestamp matching on client requests and server responses. With this setting enabled, IDP expects the server response original timestamp to match the client request transmit timestamp; otherwise IDP considers the packet a possible protocol anomaly. This setting is enabled by default.
	<b>Maximum Authorization field length in NTP control message</b> —Raises a protocol anomaly if IDP detects that the length of the Authentication fields in an NTP control message is larger than the specified maximum. The default is 20 bytes.
	<b>Maximum length of any NTP control variable</b> —Raises a protocol anomaly if IDP detects that the length of NTP control data variable name is larger than the specified maximum. The default is 128 bytes.
	<b>Maximum length of any NTP variable value</b> —Raises a protocol anomaly if IDP detects that the length of any NTP control data variable value is larger than the specified maximum. The default is 255 bytes.
	<b>Maximum length of buffer to store between control packets</b> —NTP control messages can be split across multiple UDP packets. This setting is the maximum number of characters that IDP stores in memory to ensure continuity from one packet to the other. The default is 255 bytes.
<b>Maximum time for an NTP Symmetric passive association to dissolve</b> —A symmetric passive association between two NTP peers must be dissolved after sending one reply. This setting is the time in seconds after which IDP considers such an association as expired. The default is 900 seconds.	

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
POP3	<b>Maximum Line length</b> —Raises a protocol anomaly if IDP detects a POP3 line containing more bytes than the specified maximum. The default is 512 bytes.
	<b>Maximum Username length</b> —Raises a protocol anomaly if IDP detects a POP3 username containing more bytes than the specified maximum. The default is 64 bytes.
	<b>Maximum Password length</b> —Raises a protocol anomaly if IDP detects a POP3 password containing more bytes than the specified maximum. The default is 64 bytes.
	<b>Maximum APOP length</b> —Raises a protocol anomaly if IDP detects an APOP containing more bytes than the specified maximum. The default is 100 bytes.
	<b>Maximum message number</b> —Raises a protocol anomaly if IDP detects a POP3 message number that is higher than the specified maximum. The default is 10,00,000.
	<b>Maximum number of login failures per-minute</b> —Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 POP3 login failures per minute.
RADIUS	<b>Maximum number of authenticated failures per-minute</b> —Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 RADIUS login failures per minute.
SIP	<b>Max-Forwards threshold</b> —Raises a protocol anomaly if IDP detects maximum number of thresholds.
SMB	<b>Maximum registry key length</b> —Raises a protocol anomaly if IDP detects an SMB registry key containing more bytes than the specified maximum. The default is 8192 bytes.
	<b>Maximum number of login failures per-minute</b> —Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 SMB login failures per minute.

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
SMTP	<b>Maximum Number of mail recipients</b> —Raises a protocol anomaly if IDP detects an SMTP message containing more recipients than the specified maximum. The default is 100 recipients.
	<b>Maximum Username length in RCPT and MAIL</b> —Raises a protocol anomaly if IDP detects an SMTP message with a username containing more bytes than the specified maximum. The default is 256 bytes.
	<b>Maximum Domain name length in RCPT and MAIL</b> —Raises a protocol anomaly if IDP detects an SMTP message with a domain name containing more bytes than the specified maximum. The default is 64 bytes.
	<b>Maximum Path length in RCPT and MAIL</b> —Raises a protocol anomaly if IDP detects an SMTP message with a pathname containing more bytes than the specified maximum. The default is 256 bytes.
	<b>Maximum Command line length (before DATA)</b> —Raises a protocol anomaly if IDP detects an SMTP message with a command-line entry containing more bytes than the specified maximum. The default is 1024 bytes.
	<b>Maximum Reply line length from server (default)</b> —Raises a protocol anomaly if IDP detects an SMTP message with a reply line from the server containing more bytes than the specified maximum. The default is 512 bytes.
	<b>Maximum Text line length (after DATA)</b> —Raises a protocol anomaly if IDP detects an SMTP text line containing more bytes than the specified maximum. The default is 1024 bytes.
	<b>Maximum number of nested mime multi-part attachments</b> —Raises a protocol anomaly if IDP detects more nested attachments than the specified maximum. The default is 4 nested mime multi-part attachments.
	<b>Maximum number of base-64 bytes to decode</b> —Raises a protocol anomaly if IDP detects more bytes of encoded mime data than the specified maximum. The default is 64 bytes.
	<b>Maximum length of the value for content-type's name attribute</b> —Raises a protocol anomaly if IDP detects a name attribute in the content-type header containing more bytes than the specified maximum. The default is 128 bytes.
<b>Maximum length of the value for the content-disposition's filename attribute</b> —Raises a protocol anomaly if IDP detects a filename attribute in the content-disposition header containing more bytes than the specified maximum. The default is 128 bytes.	
	<b>Look for email headers in message data</b> —Controls whether IDP looks for e-mail headers in the message data, which can occur when a bounced email contains an attachment. This setting is not enabled by default.
SYSLOG	<b>Validate RFC-3164 compliant timestamp format</b> —If selected, the security module checks the timestamp in syslog traffic to ensure that it is compliant with RFC 3164. If the timestamp is not compliant, the security module considers the traffic a possibly anomaly. This setting is not enabled by default.
TELNET	<b>Maximum number of login failures per-minute</b> —Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 TELNET login failures per minute.
TFTP	<b>Maximum Filename length</b> —Raises a protocol anomaly if IDP detects a filename containing more bytes than the specified maximum. The default is 128 bytes.

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings** (continued)

Setting	Description
VNC	<b>Maximum Reason string length</b> —Raises a protocol anomaly if IDP detects a VNC (Virtual Network Computing) reason string length greater than the specified maximum. A reason string contains the text that describes why a connection between a VNC server and client failed. The default is 512 bytes.
	<b>Maximum Display name length</b> —Raises a protocol anomaly if IDP detects a VNC display name containing more bytes than the specified maximum. The default is 128 bytes.
	<b>Maximum cut text length</b> —Raises a protocol anomaly if IDP detects a VNC cut text buffer containing more bytes than the specified maximum. The default is 4096 bytes.
	<b>Verify message after the initial handshake</b> —Enables the security module to verify VNC connections after the initial handshake. This setting is not enabled by default.
	<b>Maximum number of login failures per-minute</b> —Raises a BRUTE_FORCE protocol anomaly if IDP detects more login failures than the specified maximum. The default is 4 VNC login failures per minute.
WHOIS	<b>Maximum Request length</b> —Raises a protocol anomaly if IDP detects a WHOIS request containing more bytes than the specified maximum. The default is 128 bytes.

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings (continued)**

Setting	Description
YMSG	<b>Maximum Message length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger message with a header that indicates more bytes for the total message than the specified maximum. The default is 8192 bytes.
	<b>Maximum Username length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger ID containing more bytes than the specified maximum. The default is 84 bytes.
	<b>Maximum Groupname length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger group name containing more bytes than the specified maximum. The default is 84 bytes.
	<b>Maximum Crypt length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger encrypted password containing more bytes than the specified maximum. The default is 124 bytes.
	<b>Maximum Instant message length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger message containing more bytes than the specified maximum. The default is 1024 bytes.
	<b>Maximum Activity string length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger activity data type containing more bytes than the specified maximum. The default is 8000 bytes.
	<b>Maximum Challenge length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger challenge containing more bytes than the specified maximum. The default is 15 bytes.
	<b>Maximum Cookie length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger cookie containing more bytes than the specified maximum. The default is 84 bytes.
	<b>Maximum URL length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger Web Name containing more bytes than the specified maximum. The default is 400 bytes.
	<b>Maximum Conference message length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger join conference message containing more bytes than the specified maximum. The default is 1024 bytes.
	<b>Maximum Conference name length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger conference name containing more bytes than the specified maximum. The default is 1024 bytes.
	<b>Maximum E-mail length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger new e-mail alert containing an e-mail that has more bytes than the specified maximum. The default is 84 bytes.
	<b>Maximum E-mail subject length</b> —Raises a protocol anomaly if IDP detects an Yahoo! Messenger subject line containing more bytes than the specified maximum. The default is 128 bytes.  This setting tunes the Mail Subject Overflow attack object (key is CHAT:YIM:OVERFLOW:MAIL-SUBJECT).
	<b>Maximum Filename length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger file transfer containing a filename that has more bytes than the specified maximum. The default is 1000 bytes.
	<b>Maximum Chatroom name length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger chat room name containing more bytes than the specified maximum. The default is 1024 bytes.
<b>Maximum Chatroom message length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger chat room message containing more bytes than the specified maximum. The default is 2000 bytes.	
<b>Maximum buddy list length</b> —Raises a protocol anomaly if IDP detects a Yahoo! Messenger buddy list containing more bytes than the specified maximum. The default is 8000 bytes.	

**Table 1: IDP Device Configuration: Protocol Thresholds and Configuration Settings** (continued)

Setting	Description
	<b>Maximum webcam key length</b> –Raises a protocol anomaly if IDP detects an Yahoo! Messenger Webcam key containing more bytes than the specified maximum. The default is 124 bytes.

- Related Topics**
- Updating the IDP Detector Engine (NSM Procedure)
  - Configuring Traffic Anomalies Rulebase Rules (NSM Procedure)

---

Published: 2009-08-20