CHAPTER 19

logging asdm コマンド～ logout message コマンド

logging asdm

システム ログ メッセージを ASDM ログ バッファに送信するには、グローバル コンフィギュレーション モードで **logging asdm** コマンドを使用します。ASDM ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	ASDM ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

ASDM のロギングはデフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

ASDM のログ バッファが満杯の場合、セキュリティ アプライアンス はメッセージを古いものから削除して、新しいメッセージのためのバッファ スペースを確保します。ASDM ログ バッファに保持されるシステム ログ メッセージの数を制御するには、**logging asdm-buffer-size** コマンドを使用します。

ASDM ログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは異なります。

例

ロギングをイネーブルにして、重大度レベル 0、1、2 のメッセージを ASDM ログ バッファに送信する例を示します。また、ASDM ログ バッファ サイズを 200 メッセージに設定する例も示します。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログ バッファに含まれているすべてのメッセージをクリアします。
logging asdm-buffer-size	ASDM ログ バッファに保持される ASDM メッセージの数を指定します。
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	ロギング設定を表示します。

logging asdm-buffer-size

ASDM ログ バッファに保持されるシステム ログ メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用します。ASDM ログ バッファをデフォルトのサイズの 100 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

構文の説明

num_of_msgs	ASDM ログ バッファでセキュリティ アプライアンスが保持するシステム ログ メッセージの数を指定します。

デフォルト

デフォルトの ASDM syslog バッファ サイズは 100 メッセージです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM のログ バッファが満杯の場合、セキュリティ アプライアンス はメッセージを古いものから削除して、新しいメッセージのためのバッファ スペースを確保します。ASDM ログ バッファへのロギングをイネーブルにするかどうかを制御するには、または ASDM ログ バッファに保持されるシステム ログ メッセージの種類を制御するには、**logging asdm** コマンドを使用します。

ASDM ログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは異なります。

例

ロギングをイネーブルにして、重大度レベル 0、1、2 のメッセージを ASDM ログ バッファに送信する例を示します。また、ASDM ログ バッファ サイズを 200 メッセージに設定する例も示します。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
```

```
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログ バッファに含まれているすべてのメッセージをクリアします。
logging asdm	ASDM ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging buffered

セキュリティ アプライアンスによってシステム ログ メッセージをログ バッファに送信できるようにするには、グローバル コンフィギュレーション モードで **logging buffered** コマンドを使用します。ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- バッファ サイズは 4 KB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

新しいメッセージは、バッファの最後に追加されます。バッファがいっぱいになると、セキュリティ アプライアンスはバッファを消去してから、メッセージの追加を続行します。ログ バッファがいっぱいになると、セキュリティ アプライアンスでは最も古いメッセージを削除して、バッファに新しいメッセージ用の領域を確保します。バッファの内容が「ラップ」されるたびにバッファの内容を自動的に保存することができます。これは、最後に保存されてから追加されたすべてのメッセージが新しいメッセージに置き換えられることを意味します。詳細については、**logging flash-bufferwrap** コマンドおよび **logging ftp-bufferwrap** コマンドを参照してください。

バッファの内容は、いつでもフラッシュ メモリに保存できます。詳細については、**logging savelog** コマンドを参照してください。

バッファに送信するシステム ログ メッセージは、**show logging** コマンドで確認できます。

例

次に、レベル 0 および 1 のイベントに対してバッファへのロギングを設定する例を示します。

```
hostname(config)# logging buffered alerts
hostname(config)#
```

次の例では、最大ロギング レベル 7 の notif-list というリストを作成し、notif-list リストで識別されるシステム ログ メッセージに対して、バッファへのロギングを設定します。

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging buffer-size

ログ バッファのサイズを指定するには、グローバル コンフィギュレーション モードで **logging buffer-size** コマンドを使用します。ログ バッファをデフォルトのサイズの 4 KB のメモリにリセットするには、このコマンドの **no** 形式を使用します。

logging buffer-size *bytes*

no logging buffer-size *bytes*

構文の説明

bytes	ログ バッファに使用するメモリ量をバイト単位で設定します。たとえば、8192 を指定した場合、セキュリティ アプライアンスによってログ バッファに 8 KB のメモリが使用されます。

デフォルト

ログ バッファ サイズは 4 KB メモリです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのバッファ サイズと異なるサイズのログ バッファがセキュリティ アプライアンスによって使用されているかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging buffer-size** コマンドが表示されない場合は、セキュリティ アプライアンスによって 4 KB のログ バッファが使用されています。

セキュリティ アプライアンスによるバッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次に、ロギングをイネーブルにし、ロギング バッファをイネーブルにして、セキュリティ アプライアンスがログ バッファに 16 KB のメモリを使用することを指定する例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging buffer-size 16384
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging class

メッセージ クラスに対して、ロギング先ごとの最大ロギング レベルを設定するには、グローバル コンフィギュレーション モードで **logging class** コマンドを使用します。メッセージ クラスのロギング レベル コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

logging class *class destination level* [*destination level . . .*]

no logging class *class*

構文の説明

class	ロギング先ごとの最大ロギング レベルのメッセージ クラスを指定します。class の有効な値については、後述する「使用上のガイドライン」を参照してください。
destination	*class* に対してロギング先を指定します。ロギング先について、*destination* に送信される最大ロギング レベルは *level* によって決まります。*destination* の有効な値については、後述する「使用上のガイドライン」を参照してください。
level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL

デフォルト

デフォルトでは、セキュリティ アプライアンス はロギング先およびメッセージ クラス単位ではロギング レベルを適用しません。ロギング先をイネーブルに設定したときに指定したロギング リストまたはレベルに基づいて決定されたロギング レベルで、イネーブルの各ロギング先が全クラスのメッセージを受け取ります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	有効な class の値に **eigrp** が追加されました。

使用上のガイドライン

class の有効な値は次のとおりです。

- **auth**：ユーザ認証
- **bridge**：トランスペアレント ファイアウォール
- **ca**：PKI 認証局
- **config**：コマンド インターフェイス
- **eap**：Extensible Authentication Protocol（EAP; 拡張認証プロトコル）ネットワーク アドミッション コントロールをサポートする、EAP セッション状態の変更、EAP ステータスのクエリー イベントといったタイプのイベント、および EAP ヘッダーおよびパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：Extensible Authentication Protocol（EAP; 拡張認証プロトコル）over UDP ネットワーク アドミッション コントロールをサポートする EAPoUDP のイベントをログに記録し、EAPoUDP ヘッダーおよびパケット内容の完全な記録を生成します。
- **eigrp**：EIGRP ルーティング
- **email**：電子メール プロキシ
- **ha**：フェールオーバー
- **ids**：侵入検知システム
- **ip**：IP スタック
- **nac**：ネットワーク アドミッション コントロール 初期化、例外リスト照合、ACS トランザクション、クライアントレス認証、デフォルト ACL 適用、および再評価といったタイプのイベントのログを記録します。
- **np**：ネットワーク プロセッサ
- **ospf**：OSPF ルーティング
- **rip**：RIP ルーティング
- **session**：ユーザ セッション
- **snmp**：SNMP
- **sys**：システム
- **vpn**：IKE および IPSec
- **vpnc**：VPN クライアント

- **vpnfo**：VPN フェールオーバー
- **vpnlb**：VPN ロード バランシング

有効なロギング先は、次のとおりです。

- **asdm**：このロギング先については、**logging asdm** コマンドを参照してください。
- **buffered**：このロギング先については、**logging buffered** コマンドを参照してください。
- **console**：このロギング先については、**logging console** コマンドを参照してください。
- **history**：このロギング先については、**logging history** コマンドを参照してください。
- **mail**：このロギング先については、**logging mail** コマンドを参照してください。
- **monitor**：このロギング先については、**logging monitor** コマンドを参照してください。
- **trap**：このロギング先については、**logging trap** コマンドを参照してください。

例

次に、フェールオーバー関連メッセージについて、ASDM ログ バッファの最大ロギング レベルが 2、システム ログ バッファの最大ロギング レベルが 7 であることを指定する例を示します。

```
hostname(config)# logging class ha asdm 2 buffered 7
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging console

セキュリティ アプライアンスでシステム ログ メッセージをコンソール セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。コンソール セッションへのシステム ログ メッセージの表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging console [*logging_list* | *level*]

no logging console

（注） バッファ オーバーフローが原因で多数のシステム ログ メッセージがドロップされる可能性があるため、このコマンドは使用しないことを推奨します。詳細については、後述する「使用上のガイドライン」を参照してください。

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	コンソール セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトでは、セキュリティ アプライアンスでシステム ログ メッセージはコンソール セッションに表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コンソールにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

注意　**logging console** コマンドを使用すると、システム パフォーマンスが大幅に低下する可能性があります。代わりに、**logging buffered** コマンドを使用してロギングを開始し、**show logging** コマンドを使用してメッセージを表示します。最新のメッセージをより簡単に表示するには、**clear logging buffer** コマンドを使用してバッファをクリアします。

例

次に、ロギング レベル 0、1、2、および 3 のシステム ログ メッセージをコンソール セッションに表示できるようにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging console errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging debug-trace

デバッグ メッセージを重大度レベル 7 で発行されるシステム ログ メッセージ 711001 としてログにリダイレクトするには、グローバル コンフィギュレーション モードで **logging debug-trace** コマンドを使用します。デバッグ メッセージのログへの送信を停止するには、このコマンドの **no** 形式を使用します。

logging debug-trace

no logging debug-trace

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはデバッグ出力をシステム ログ メッセージに含めません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ メッセージは重大度レベル 7 のメッセージとして生成されます。システム ログ メッセージ番号 711001 でログに表示されますが、モニタリング セッションには表示されません。

例

次に、ロギングをイネーブルに設定し、システム ログ バッファにログ メッセージを送信し、ログにデバッグ出力を転送し、ディスク動作のデバッグをオンにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

ログに示されるデバッグ メッセージの例は、次のとおりです。

```
%PIX-7-711001: IFS: Read: fd 3, bytes 4096
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging device-id

EMBLEM 形式でないシステム ログ メッセージにデバイス ID を含めるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **logging device-id** コマンドを使用します。デバイス ID の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

no logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

構文の説明

context-name	現在のコンテキストの名前をデバイス ID として指定します。
hostname	セキュリティ アプライアンスのホスト名をデバイス ID として指定します。
ipaddress *interface_name*	デバイス ID または *interface_name* のインターフェイスの IP アドレスを指定します。**ipaddress** キーワードを使用すると、外部サーバに送信されるシステム ログ メッセージには、外部サーバへのログ データの送信にセキュリティ アプライアンスで使用されるインターフェイスに関係なく、指定したインターフェイスの IP アドレスが含まれます。
string *text*	最大 16 文字の *text* で指定された文字をデバイス ID として指定します。スペースおよび次の文字は使用できません。 • &：アンパサンド • '：一重引用符 • "：二重引用符 • <：未満 • >：より大きい • ?：疑問符

デフォルト

システム ログ メッセージにデフォルトのデバイス ID は使用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ipaddress キーワードを使用すると、メッセージが送信されるインターフェイスに関係なく、デバイス ID は指定したセキュリティ アプライアンス インターフェイスの IP アドレスとなります。このキーワードにより、そのデバイスから送信されるすべてのメッセージに対して、単一の一貫したデバイス ID が指定されます。

例

次の例は、secappl-1 というホストを設定する方法を示しています。

```
hostname(config)# logging device-id hostname
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

ホスト名は、次のメッセージなどのシステム ログ メッセージの先頭に表示されます。

```
secappl-1 %PIX-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging emblem

syslog サーバ以外のロギング先に送信されるシステム ログ メッセージに EMBLEM 形式を使用するには、グローバル コンフィギュレーション モードで **logging emblem** コマンドを使用します。EMBLEM 形式の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging emblem

no logging emblem

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスでシステム ログ メッセージに EMBLEM 形式は使用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが **logging host** コマンドと無関係になるように変更されました。

使用上のガイドライン

logging emblem コマンドを使用すると、syslog サーバ以外のすべてのロギング先に対して、EMBLEM 形式のロギングをイネーブルにすることができます。**logging timestamp** キーワードもイネーブルにする場合、タイム スタンプが付与されたメッセージが送信されます。

syslog サーバに対して EMBLEM 形式のロギングをイネーブルにするには、**logging host** コマンドで **format emblem** オプションを使用します。

例

次に、ロギングをイネーブルにし、syslog サーバを除くすべてのロギング先へのロギングに対して EMBLEM 形式の使用をイネーブルにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging emblem
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging enable

設定済みの出力場所すべてに対してロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **logging enable** コマンドを使用します。ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging enable

no logging enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ロギングはデフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**logging on** コマンドから変更されました。

使用上のガイドライン

logging enable コマンドを使用すると、サポートされている任意のロギング先へのシステム ログ メッセージの送信をイネーブルまたはディセーブルにすることができます。**no logging enable** コマンドを使用して、すべてのロギングを停止できます。

次のコマンドを使用して、個別のロギング先へのロギングをイネーブルにすることができます。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

例

次に、ロギングをイネーブルにする例を示します。**show logging** コマンドの出力は、使用可能な各ロギング先を個別にイネーブルにする必要がある状況を示しています。

```
hostname(config)# logging enable
```

```
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging facility

syslog サーバに送信されるメッセージに使用するロギング ファシリティを指定するには、グローバル コンフィギュレーション モードで **logging facility** コマンドを使用します。ロギング ファシリティをデフォルトの 20 にリセットするには、このコマンドの **no** 形式を使用します。

logging facility *facility*

no logging facility

構文の説明

facility	ロギング ファシリティを指定します。有効な値は、16 ～ 23 です。

デフォルト

デフォルトのファシリティは 20（LOCAL4）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。例外については、「構文の説明」を参照してください。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

syslog サーバでは、メッセージはメッセージの *facility* 番号に基づいてファイルされます。使用可能なファシリティには、16（LOCAL0）～ 23（LOCAL7）の 8 つがあります。

例

この例では、セキュリティ アプライアンスでシステム ログ メッセージのロギング ファシリティを 16 に指定する例を示します。**show logging** コマンドの出力には、セキュリティ アプライアンスによって使用されているファシリティが含まれます。

```
hostname(config)# logging facility 16
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
```

```
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging flash-bufferwrap

未保存のメッセージでログ バッファがいっぱいになるたびに、セキュリティ アプライアンスでバッファをフラッシュ メモリに書き込めるようにするには、グローバル コンフィギュレーション モードで **logging flash-bufferwrap** コマンドを使用します。フラッシュ メモリへのログ バッファの書き込みをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging flash-bufferwrap

no logging flash-bufferwrap

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- フラッシュ メモリへのログ バッファの書き込みはディセーブルです。
- バッファ サイズは 4 KB です。
- フラッシュ メモリの最小の空き容量は 3 MB です。
- バッファ ロギングに対するフラッシュ メモリの最大割り当て容量は 1 MB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスによってログ バッファがフラッシュ メモリに書き込まれるようにするには、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに書き込まれません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスはフラッシュ メモリにログ バッファの内容を書き込んでいる間も、新しいイベント メッセージをログ バッファに格納し続けます。

セキュリティ アプライアンスは、次のようなデフォルトのタイムスタンプ形式を使用した名前のログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

logging flash-bufferwrap コマンドを使用する場合、フラッシュ メモリの可用性が、セキュリティ アプライアンスによるシステム ログ メッセージの保存方法に影響します。詳細については、**logging flash-maximum-allocation** コマンドおよび **logging flash-minimum-free** コマンドを参照してください。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにし、セキュリティ アプライアンスによるフラッシュ メモリへのログ バッファの書き込みをイネーブルにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
copy	TFTP サーバまたは FTP サーバを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ ファイルなどのファイルをディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-maximum-allocation	ログ バッファの内容の書き込みに使用できるフラッシュ メモリの最大量を指定します。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するために、セキュリティ アプライアンスで使用可能にする必要があるフラッシュ メモリの最小量を指定します。
show logging	イネーブルなロギング オプションを表示します。

logging flash-maximum-allocation

ログ データを保管するためにセキュリティ アプライアンスで使用するフラッシュ メモリの最大量を指定するには、グローバル コンフィギュレーション モードで **logging flash-maximum-allocation** コマンドを使用します。この目的に使用するフラッシュ メモリの最大量をデフォルト サイズの 1 MB にリセットするには、このコマンドの **no** 形式を使用します。

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

構文の説明

kbytes	ログ バッファ データを保存するためにセキュリティ アプライアンスで使用できるフラッシュ メモリの最大量（KB 単位）。

デフォルト

ログ データ用のデフォルトの最大フラッシュ メモリ割り当ては 1 MB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで使用できるフラッシュ メモリの量が決まります。

logging savelog または **logging flash-bufferwrap** で保存されるログ ファイルにより、ログ ファイル用のフラッシュ メモリの使用が **logging flash-maximum-allocation** コマンドで指定された最大量を超える場合、セキュリティ アプライアンスによって最も古いログ ファイルが削除され、新しいログ ファイル用に十分なメモリが解放されます。削除するファイルがない場合や、古いファイルをすべて削除しても空きメモリが新しいログ ファイルには小さすぎる場合は、セキュリティ アプライアンスで新しいログ ファイルを保存できません。

デフォルトのサイズとは異なるサイズの最大フラッシュ メモリ割り当てがセキュリティ アプライアンスにあるかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging flash-maximum-allocation** コマンドが表示されない場合、セキュリティ アプライアンスでは保存されるログ バッファ データに対して最大 1 MB が使用されています。割り当てられたメモリは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドの両方に使用されます。

セキュリティ アプライアンスによるログ バッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにし、セキュリティ アプライアンスによるフラッシュ メモリへのログ バッファの書き込みをイネーブルにし、ログ ファイルの書き込みに使用されるフラッシュ メモリの最大量を約 1.2 MB に設定する例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-maximum-allocation 1200
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するために、セキュリティ アプライアンスで使用可能にする必要があるフラッシュ メモリの最小量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging flash-minimum-free

セキュリティ アプライアンスで新しいログ ファイルを保存する前に存在している必要があるフラッシュ メモリの最小空き領域を指定するには、グローバル コンフィギュレーション モードで **logging flash-minimum-free** コマンドを使用します。このコマンドは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドによって作成されたログ ファイルをセキュリティ アプライアンスで保存する前に存在している必要があるフラッシュ メモリの空き領域に影響します。フラッシュ メモリの必要最小空き領域をデフォルト サイズの 3 MB にリセットするには、このコマンドの **no** 形式を使用します。

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

構文の説明

kbytes	セキュリティ アプライアンスで新しいログ ファイルを保存する前に使用可能にしておく必要のあるフラッシュ メモリの最小量（KB 単位）。

デフォルト

フラッシュ メモリのデフォルトの最小の空き容量は 3 MB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

logging flash-minimum-free コマンドでは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンド用に常に保持しておく必要があるフラッシュ メモリの量を指定します。

logging savelog または **logging flash-bufferwrap** で保存されるログ ファイルにより、フラッシュ メモリの空き領域が **logging flash-minimum-free** コマンドで指定された制限を下回る場合、セキュリティ アプライアンスによって最も古いログ ファイルが削除され、新しいログ ファイルの保存後も最小量のメモリが空きのまま残るようにします。削除するファイルがない場合や、古いファイルをすべて削除しても空きメモリがまだ制限を下回る場合、セキュリティ アプライアンスで新しいログ ファイルを保存できません。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにし、セキュリティ アプライアンスによるフラッシュ メモリへのログ バッファの書き込みをイネーブルにし、フラッシュ メモリの最小空き領域が 4000 KB である必要があることを指定する例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-minimum-free 4000
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-maximum-allocation	ログ バッファの内容の書き込みに使用できるフラッシュ メモリの最大量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging from-address

セキュリティ アプライアンスによって送信されるシステム ログ メッセージの送信元電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging from-address** コマンドを使用します。送信されるすべてのシステム ログ メッセージは、指定したアドレスから送信されたように表示されます。送信元電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。

logging from-address *from-email-address*

no logging from-address *from-email-address*

構文の説明

from-email-address	送信元電子メール アドレス。つまり、システム ログ メッセージの送信元として表示される電子メール アドレス（cdb@example.com など）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

電子メールによるシステム ログ メッセージの送信は、**logging mail** コマンドでイネーブルにします。

このコマンドで指定するアドレスは、既存の電子メール アカウントに対応している必要はありません。

例

ロギングをイネーブルにし、システム ログ メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定するには、次の基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
hostname(config)# logging enable
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
```

```
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging mail	セキュリティ アプライアンスの電子メールによるシステム ログ メッセージの送信をイネーブルにし、電子メールで送信するメッセージを決定します。
logging recipient-address	システム ログ メッセージの送信先の電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging ftp-bufferwrap

未保存のメッセージでログ バッファがいっぱいになるたびに、セキュリティ アプライアンスが FTP サーバにログ バッファを送信できるようにするには、グローバル コンフィギュレーション モードで **logging ftp-bufferwrap** コマンドを使用します。FTP サーバへのログ バッファの送信をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging ftp-bufferwrap

no logging ftp-bufferwrap

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- FTP サーバへのログ バッファの送信はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

logging ftp-bufferwrap をイネーブルにすると、セキュリティ アプライアンスにより、ログ バッファ データは **logging ftp-server** コマンドで指定した FTP サーバに送信されます。セキュリティ アプライアンスは FTP サーバにログ データを送信しているいる間も、新しいイベント メッセージをログ バッファに格納し続けます。

セキュリティ アプライアンスによってログ バッファの内容が FTP サーバに送信されるようにするには、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに書き込まれません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスは、次のようなデフォルトのタイムスタンプ形式を使用した名前のログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにして、FTP サーバを指定し、セキュリティ アプライアンスが FTP サーバにログ バッファを書き込めるようにする例を示します。この例では、ホスト名が logserver-352 である FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs でアクセスできます。ログ ファイルは、/syslogs ディレクトリに格納されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-server	**logging ftp-bufferwrap** コマンドで使用する FTP サーバ パラメータを指定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging ftp-server

logging ftp-bufferwrap がイネーブルの場合にセキュリティ アプライアンスによってログ バッファ データが送信される FTP サーバの詳細を指定するには、グローバル コンフィギュレーション モードで **logging ftp-server** コマンドを使用します。FTP サーバの詳細をすべて削除するには、このコマンドの **no** 形式を使用します。

logging ftp-server *ftp_server path username* [*0* | *8*] *password*

no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

構文の説明

0	（任意）暗号化されていない（クリア テキストの）ユーザ パスワードが続くことを指定します。
8	（任意）暗号化されたユーザ パスワードが続くことを指定します。
ftp-server	外部 FTP サーバの IP アドレスまたはホスト名。 **（注）** ホスト名を指定する場合は、ネットワーク上で DNS が正しく動作していることを確認してください。
password	指定したユーザ名のパスワード。
path	ログ バッファ データが保存される FTP サーバ上のディレクトリ パス。このパスは、FTP ルート ディレクトリに対する相対パスです。次に例を示します。 `/security_appliances/syslogs/appliance107`
username	FTP サーバへのログインに有効なユーザ名。

デフォルト

デフォルトでは、FTP サーバは指定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(5)	パスワード暗号化のサポートが追加されました。

使用上のガイドライン

FTP サーバは 1 つのみ指定できます。ロギング FTP サーバがすでに指定されている場合、**logging ftp-server** コマンドを使用すると、その FTP サーバ コンフィギュレーションが、入力した新しいコンフィギュレーションに置き換えられます。

セキュリティ アプライアンス は、指定された FTP サーバ情報を確認しません。詳細を誤って設定した場合、セキュリティ アプライアンスによってログ バッファ データを FTP サーバに送信できません。

セキュリティ アプライアンスの起動時またはアップグレード時に、1 桁のパスワードや、1 桁の数値で始まりその後に空白が指定されたパスワードはサポートされません。たとえば、0 pass や 1 は不正なパスワードです。

例

次に、ロギングをイネーブルにし、ログ バッファをイネーブルにして、FTP サーバを指定し、セキュリティ アプライアンスが FTP サーバにログ バッファを書き込めるようにする例を示します。この例では、ホスト名が logserver-352 である FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs でアクセスできます。ログ ファイルは、/syslogs ディレクトリに格納されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
```

次に、暗号化されたパスワードを入力する例を示します。

```
hostname(config)# logging ftp-server logserver /path1 user1 8 JPAGWzIIFVlheXv2I9nglfytOzHU
```

次に、暗号化されていない（クリア テキストの）パスワードを入力する例を示します。

```
hostname(config)# logging ftp-server logserver /path1 user1 0 pass1
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging history

SNMP ロギングをイネーブルにし、SNMP サーバに送信するメッセージを指定するには、グローバル コンフィギュレーション モードで **logging history** コマンドを使用します。SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging history [*logging_list* | *level*]

no logging history

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	SNMP サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトでは、セキュリティ アプライアンスによって SNMP サーバにロギングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging history コマンドを使用すると、SNMP サーバへのロギングをイネーブルにし、SNMP メッセージ レベルまたはイベント リストを設定できます。

例

次に、SNMP ロギングをイネーブルにし、ロギング レベル 0、1、2、および 3 のメッセージが設定した SNMP サーバに送信されることを指定する例を示します。

```
hostname(config)# logging enable
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。
snmp-server	SNMP サーバの詳細を指定します。

logging host

syslog サーバを定義するには、グローバル コンフィギュレーション モードで **logging host** コマンドを使用します。syslog サーバ定義を削除するには、このコマンドの **no** 形式を使用します。

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**] [**permit-hostdown**]

logging host *interface_name syslog_ip*

[**no**] **logging host** *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**]

[**no**] **logging host** *interface_name syslog_ip*

構文の説明

format emblem	（任意）syslog サーバに対して EMBLEM 形式のロギングをイネーブルにします。
interface_name	syslog サーバが配置されているインターフェイスを指定します。
permit-hostdown	syslog サーバがダウンしているか、または到達不能である場合に、適応型セキュリティ アプライアンスが TCP ロギングを続行できるようにします。
port	syslog サーバがメッセージをリッスンするポートを指定します。有効なポート値は、いずれのプロトコルの場合も 1025 ～ 65535 です。
secure	リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 **（注）** セキュアなロギング接続は、SSL/TLS 対応の syslog サーバとのみ確立できます。SSL/TLS 接続を確立できない場合、新しい接続はすべて拒否されます。このデフォルトの動作は、**logging permit-hostdown** コマンドを入力して変更できます。
syslog_ip	syslog サーバの IP アドレスを指定します。
tcp	セキュリティ アプライアンスによって syslog サーバへのメッセージの送信に TCP が使用されることを指定します。
udp	セキュリティ アプライアンスによって syslog サーバへのメッセージの送信に UDP が使用されることを指定します。

デフォルト

デフォルト プロトコルは UDP です。

デフォルトのポート番号は次のとおりです。

- UDP：514
- TCP：1470

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
8.0(2)	**secure** キーワードが追加されました。

使用上のガイドライン

logging host *ip_address* **format emblem** コマンドを使用すると、各 syslog サーバに対して EMBLEM 形式のロギングをイネーブルにすることができます。EMBLEM 形式のロギングは、UDP システム ログ メッセージのみに使用できます。EMBLEM 形式のロギングを特定の syslog サーバに対してイネーブルにすると、メッセージはそのサーバに送信されます。**logging timestamp** キーワードもイネーブルにする場合、タイム スタンプが付与されたメッセージが送信されます。

複数の **logging host** コマンドを使用して、追加サーバを指定できます。それらすべてでシステム ログ メッセージが受信されます。ただし、UDP と TCP 両方ではなく、いずれかのシステム ログ メッセージのみが受信されるようにサーバを指定できます。

（注） **logging host** コマンドで **tcp** オプションを使用すると、syslog サーバに到達できない場合、ファイアウォールを通過する接続は適応型セキュリティ アプライアンスによってドロップされます。

以前入力した *port* と *protocol* の値だけを表示するには、**show running-config logging** コマンドを使用して、リストからコマンドを見つけます（TCP は 6、UDP は 17 として表示されます）。TCP ポートは syslog サーバのみで機能します。*port* は、syslog サーバがリッスンするポートと同じである必要があります。

（注） **logging host** コマンドと **secure** キーワードを UDP で使用しようとすると、エラー メッセージが表示されます。

PIX セキュリティ アプライアンスは **secure** キーワードをサポートしません。

例

次の例は、デフォルトのプロトコルとポート番号を使用する内部インターフェイス上の syslog サーバに、重大度 0、1、2、および 3 のシステム ログ メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging list

さまざまな基準（ログ レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するために、他のコマンドで使用するロギング リストを作成するには、グローバル コンフィギュレーション モードで **logging list** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[**-***end_id*]}

no logging list *name*

構文の説明

class *event_class*	（任意）システム ログ メッセージのイベントのクラスを設定します。指定したレベルについて、指定したクラスのシステム ログ メッセージのみがコマンドによって識別されます。クラスのリストについては、「使用上のガイドライン」を参照してください。
level *level*	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
message *start_id*[**-***end_id*]	メッセージ ID または ID の範囲を指定します。メッセージのデフォルト レベルを検索するには、**show logging** コマンドを使用するか、または『*Cisco ASA 5500 Series System Log Messages*』を参照してください。
name	ロギング リスト名を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

リストを使用できるロギング コマンドは、次のとおりです。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

event_class で使用できる値は、次のとおりです。

- **auth**：ユーザ認証
- **bridge**：トランスペアレント ファイアウォール
- **ca**：PKI 認証局
- **config**：コマンド インターフェイス
- **eap**：Extensible Authentication Protocol（EAP; 拡張認証プロトコル）ネットワーク アドミッション コントロールをサポートする、EAP セッション状態の変更、EAP ステータスのクエリー イベントといったタイプのイベント、および EAP ヘッダーおよびパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：Extensible Authentication Protocol（EAP; 拡張認証プロトコル）over UDP ネットワーク アドミッション コントロールをサポートする EAPoUDP のイベントをログに記録し、EAPoUDP ヘッダーおよびパケット内容の完全な記録を生成します。
- **email**：電子メール プロキシ
- **ha**：フェールオーバー
- **ids**：侵入検知システム
- **ip**：IP スタック
- **nac**：ネットワーク アドミッション コントロール 初期化、例外リスト照合、ACS トランザクション、クライアントレス認証、デフォルト ACL 適用、および再評価といったタイプのイベントのログを記録します。
- **np**：ネットワーク プロセッサ
- **ospf**：OSPF ルーティング
- **rip**：RIP ルーティング
- **session**：ユーザ セッション
- **snmp**：SNMP
- **sys**：システム
- **vpn**：IKE および IPSec
- **vpnc**：VPN クライアント
- **vpnfo**：VPN フェールオーバー

- **vpnlb**：VPN ロード バランシング

例

次に、logging list コマンドの使用例を示します。

```
hostname(config)# logging list my-list message 100100-100110
hostname(config)# logging list my-list level critical
hostname(config)# logging list my-list level warning class vpn
hostname(config)# logging buffered my-list
```

上の例では、指定した基準に一致するシステム ログ メッセージがロギング バッファに送信されるように指定しています。この例で指定されている基準は、次のとおりです。

- 100100 ～ 100110 の範囲内のシステム ログ メッセージ ID
- 重大度が critical 以上（emergency、alert、または critical）のすべてのシステム ログ メッセージ
- warning レベル以上（emergency、alert、critical、error、または warning）にある VPN クラスのすべてのシステム ログ メッセージ

システム ログ メッセージがこれらの条件のいずれかを満たしている場合、そのメッセージはバッファにロギングされます。

（注） リストの条件を設定するときには、条件が重なり合うメッセージ セットを指定できます。複数の基準と一致するシステム ログ メッセージも正常にロギングされます。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging mail

セキュリティ アプライアンスでシステム ログ メッセージを電子メールで送信できるようにし、電子メールで送信するメッセージを判別できるようにするには、グローバル コンフィギュレーション モードで **logging mail** コマンドを使用します。システム ログ メッセージの電子メール送信をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	電子メールの受信者に送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

電子メールへのロギングは、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　電子メールで送信されるシステム ログ メッセージは、送信された電子メールの件名欄に表示されます。

例

電子メールでシステム ログ メッセージを送信するようにセキュリティ アプライアンスを設定するには、次のような基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	電子メールで送信されるシステム ログ メッセージの送信元として表示される電子メール アドレスを指定します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
logging recipient-address	電子メールで送信されるシステム ログ メッセージの送信先の電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging message

システム ログ メッセージのログ レベルを指定するには、グローバル コンフィギュレーション モードで **logging message** コマンドを **level** キーワードとともに使用します。メッセージのログ レベルをデフォルトのレベルにリセットするには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスで特定のシステム ログ メッセージを生成しないようにするには、グローバル コンフィギュレーション モードで **logging message** コマンドの **no** 形式を使用します（**level** キーワードは指定しません）。セキュリティ アプライアンスで特定のシステム ログ メッセージを生成できるようにするには、**logging message** コマンドを使用します（**level** キーワードは指定しません）。これら 2 つのバージョンの **logging message** コマンドは、並行して使用できます。後述する「例」を参照してください。

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

構文の説明

level *level*	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
syslog_id	イネーブルまたはディセーブルにするシステム ログ メッセージまたは重大度レベルを変更する syslog メッセージの ID。メッセージのデフォルト レベルを検索するには、**show logging** コマンドを使用するか、または『*Cisco ASA 5500 Series System Log Messages*』を参照してください。

デフォルト

デフォルトでは、すべてのシステム ログ メッセージはイネーブルであり、すべてのメッセージの重大度レベルはデフォルトのレベルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging message コマンドは、次の 2 つの目的で使用できます。

- メッセージをイネーブルにするかディセーブルにするかを制御します。
- メッセージの重大度レベルを制御します。

show logging コマンドを使用して、メッセージに現在割り当てられている重大度レベルや、メッセージがイネーブルかどうかを判別できます。

例

次に、**logging message** コマンドの一連の使用例を示します。これらの例では、メッセージをイネーブルにするかどうか、およびメッセージの重大度レベルの両方を制御しています。

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

関連コマンド

コマンド	説明
clear configure logging	すべてのロギング コンフィギュレーションまたはメッセージ コンフィギュレーションのみをクリアします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging monitor

セキュリティ アプライアンスでシステム ログ メッセージを SSH セッションおよび Telnet セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging monitor** コマンドを使用します。SSH セッションおよび Telnet セッションへのシステム ログ メッセージの表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging monitor [*logging_list* | *level*]

no logging monitor

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	SSH セッションまたは Telnet セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトでは、セキュリティ アプライアンスによってシステム ログ メッセージは SSH セッションおよび Telnet セッションに表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging monitor コマンドにより、現在のコンテキストのすべてのセッションに対してシステム ログ メッセージがイネーブルになります。ただし、各セッションでは **terminal** コマンドによって、システム ログ メッセージがそのセッションに表示されるかどうかが制御されます。

例

次に、コンソール セッションでシステム ログ メッセージの表示をイネーブルにする例を示します。**errors** キーワードの使用は、ロギング レベル 0、1、2、および 3 のメッセージが SSH セッションおよび Telnet セッションに表示されることを示しています。**terminal** コマンドを使用すると、現在のセッションでメッセージを表示できます。

```
hostname(config)# logging enable
hostname(config)# logging monitor errors
hostname(config)# terminal monitor
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。
terminal	端末回線のパラメータを設定します。

logging permit-hostdown

TCP ベースの syslog サーバのステータスを新しいユーザ セッションと無関係にするには、グローバル コンフィギュレーション モードで **logging permit-hostdown** コマンドを使用します。TCP ベースの syslog サーバが使用できないときにセキュリティ アプライアンスで新しいユーザ セッションを拒否するには、このコマンドの **no** 形式を使用します。

logging permit-hostdown

no logging permit-hostdown

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、TCP 接続を使用する syslog サーバへのロギングをイネーブルにした場合、何らかの理由で syslog サーバが使用できないときに、セキュリティ アプライアンスでは新しいネットワーク アクセス セッションを許可しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

syslog サーバへメッセージを送信するためのロギング トランスポート プロトコルとして TCP を使用している場合、セキュリティ アプライアンスが syslog サーバに到達できないときに、セキュリティ アプライアンスではセキュリティ対策として新しいネットワーク アクセス セッションを拒否します。**logging permit-hostdown** コマンドを使用して、この制限を削除できます。

例

次に、TCP ベースの syslog サーバのステータスを、セキュリティ アプライアンスで新しいセッションが許可されるかどうかと無関係にする例を示します。**logging permit-hostdown** コマンドの出力に **show running-config logging** コマンドが含まれている場合、TCP ベースの syslog サーバのステータスは、新しいネットワーク アクセス セッションと無関係です。

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging queue

ロギング コンフィギュレーションに従って処理する前にセキュリティ アプライアンスのキューに保持できるシステム ログ メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging queue** コマンドを使用します。ロギング キューのサイズをデフォルトの 512 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging queue *queue_size*

no logging queue *queue_size*

構文の説明

queue_size	処理前の syslog メッセージを保管するために使用されるキューで許可される syslog メッセージの数。有効な値は、プラットフォームの種類に応じて 0 ～ 8192 メッセージです。ロギング キューが 0 に設定されている場合、プラットフォームに応じて、キューは設定可能な最大サイズ（8192 メッセージ）になります。ASA-5505 では、最大キュー サイズは 1024 です。ASA-5510 では 2048 です。その他のすべてのプラットフォームでは 8192 です。

デフォルト

デフォルトのキュー サイズは 512 メッセージです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

トラフィックが多いためにキューがいっぱいになった場合、セキュリティ アプライアンスによってメッセージが廃棄される場合があります。ASA-5505 では、キューの最大サイズは 1024 です。ASA-5510 では 2048 です。その他のすべてのプラットフォームでは 8192 です。

例

次に、**logging queue** コマンドおよび **show logging queue** コマンドの出力を表示する例を示します。

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

この例では、**logging queue** コマンドは 0 に設定されています。つまり、キューは最大の 8192 に設定されます。キュー内のシステム ログ メッセージは、セキュリティ アプライアンスによって、ロギング コンフィギュレーションで指定された方法で処理されます。たとえば、システム ログ メッセージをメールの受信者に送信したり、フラッシュ メモリに保存したりします。

この例の **show logging queue** コマンドの出力には、5 つのメッセージがキューにあり、セキュリティ アプライアンスが最後に起動されてから同時にキューにあった最大メッセージ数は 3513 メッセージであり、1 つのメッセージが廃棄されたことが示されています。キューは無制限として設定されていますが、キューにメッセージを追加するためのブロック メモリがなかったため、メッセージが廃棄されました。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging rate-limit

システム ログ メッセージの生成レートを制限するには、特権 EXEC モードで **logging rate-limit** コマンドを使用します。レート制限をディセーブルにするには、特権 EXEC モードでこのコマンドの **no** 形式を使用します。

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

[no] logging rate-limit [**unlimited** | {*num* [*interval*]}} **message** *syslog_id*] **level** *severity_level*

構文の説明

interval	（任意）メッセージの生成レートを測定するために使用する時間間隔（秒単位）。*interval* 値の有効な範囲は、0 ～ 2147483647 です。
level *severity_level*	設定されたレート制限を、特定の重大度レベルに属するすべてのシステム ログ メッセージに適用します。指定した重大度レベルのすべてのシステム ログ メッセージは、個別にレート制限されます。*severity_level* の有効な範囲は、1 ～ 7 です。
message	このシステム ログ メッセージのレポートを抑制します。
num	指定した時間間隔中に生成できるシステム メッセージ数。*num* 値の有効な範囲は、0 ～ 2147483647 です。
syslog_id	抑制されるシステム ログ メッセージの ID。有効な値の範囲は 100000 ～ 999999 です。
unlimited	レート制限をディセーブルにします。これは、ロギング レートが制限されないことを意味します。

デフォルト

interval のデフォルト設定は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

システム メッセージの重大度は次のとおりです。

•0：システム使用不可

•1：ただちに対応

•2：重大な状況

•3：エラー メッセージ

•4：警告メッセージ

•5：通知だけ、重要な状況ではない

•6：Informational（情報）

•7：デバッグ メッセージ

例

システム ログ メッセージの生成レートを制限するには、特定のメッセージ ID を入力します。次に、特定のメッセージ ID と時間間隔を使用してシステム ログ メッセージの生成レートを制限する例を示します。

```
hostname(config)# logging rate-limit 100 600 message 302020
```

この例では、指定した 600 秒の間隔でレート制限 100 に達すると、システム ログ メッセージ 302020 はホストに送信されなくなります。

システム ログ メッセージの生成レートを制限するには、特定の重大度レベルを入力します。次に、特定の重大度レベルと時間間隔を使用してシステム ログ メッセージの生成レートを制限する例を示します。

```
hostname(config)# logging rate-limit 1000 600 level 6
```

この例では、重大度レベル 6 未満のすべてのシステム ログ メッセージが、指定した 600 秒の時間間隔で指定したレート制限 1000 に抑制されます。重大度 6 のシステム ログ メッセージのレート制限はそれぞれ 1000 です。

関連コマンド

コマンド	説明
clear running-config logging rate-limit	ロギング レート制限の設定をデフォルトにリセットします。
show logging	現在内部バッファ内にあるメッセージを表示するか、ロギング コンフィギュレーションの設定を表示します。
show running-config logging rate-limit	現在のロギング レート制限の設定を表示します。

logging recipient-address

セキュリティ アプライアンスによって送信されるシステム ログ メッセージの受信者の電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging recipient-address** コマンドを使用します。受信者の電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。最大 5 つの受信者アドレスを設定できます。必要に応じて、受信者アドレスごとに、**logging mail** コマンドで指定されたメッセージ レベルとは異なるメッセージ レベルを指定できます。

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

構文の説明

address	システム ログ メッセージを電子メールで送信する際の受信者の電子メール アドレスを指定します。
level	ロギング レベルがこの後に続くことを示します。
level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL **（注）** **logging recipient-address** コマンドで 3 より大きいレベルを使用することは推奨できません。ロギング レベルを大きくすると、バッファ オーバーフローによってシステム ログ メッセージがドロップされる可能性があります。 **logging recipient-address** コマンドで指定されたメッセージ レベルは、**logging mail** コマンドで指定されたメッセージ レベルを上書きします。たとえば、**logging recipient-address** コマンドでロギング レベル 7 を指定すると、**logging mail** コマンドでレベル 3 を指定していても、セキュリティ アプライアンスはロギング レベル 4、5、6、および 7 を含め、すべてのメッセージを受信側に送信します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

電子メールによるシステム ログ メッセージの送信は、**logging mail** コマンドでイネーブルにします。

最大 5 つの **logging recipient-address** コマンドを設定できます。コマンドごとに異なるロギング レベルを指定できます。このコマンドは、緊急性の高いメッセージを緊急性の低いメッセージよりも多くの受信者に送信する場合に便利です。

例

電子メールでシステム ログ メッセージを送信するようにセキュリティ アプライアンスを設定するには、次のような基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	システム ログ メッセージの送信元として表示される電子メール アドレスを指定します。
logging mail	セキュリティ アプライアンスの電子メールによるシステム ログ メッセージの送信をイネーブルにし、電子メールで送信するメッセージを決定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging savelog

ログ バッファをフラッシュ メモリに保存するには、特権 EXEC モードで **logging savelog** コマンドを使用します。

logging savelog [*savefile*]

構文の説明

savefile	（任意）保存するフラッシュ メモリ ファイルの名前。ファイル名を指定しない場合は、次に示すように、ログ ファイルはセキュリティ アプライアンスによってデフォルトのタイムスタンプ フォーマットを使用して保存されます。 LOG-*YYYY-MM-DD-HHMMSS*.TXT *YYYY* は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

デフォルト

デフォルトの設定は次のとおりです。

- バッファ サイズは 4 KB です。
- フラッシュ メモリの最小の空き容量は 3 MB です。
- バッファ ロギングに対するフラッシュ メモリの最大割り当て容量は 1 MB です。
- デフォルトのログ ファイル名については、「構文の説明」を参照してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ログ バッファをフラッシュ メモリに保存する前に、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに保存されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

（注）　**logging savelog** コマンドによってバッファはクリアされません。バッファをクリアするには、**clear logging buffer** コマンドを使用します。

例

次に、ロギングとログ バッファを有効にし、グローバル コンフィギュレーション モードを終了して、フラッシュ メモリへファイル名 latest-logfile.txt を使用してログ バッファを保存する例を示します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# exit
hostname# logging savelog latest-logfile.txt
hostname#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべてのシステム ログ メッセージをクリアします。
copy	TFTP サーバまたは FTP サーバを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ ファイルなどのファイルをディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。

logging standby

フェールオーバー スタンバイセキュリティ アプライアンスでこのセキュリティ アプライアンスのシステム ログ メッセージをロギング先に送信できるようにするには、グローバル コンフィギュレーション モードで **logging standby** コマンドを使用します。システム ログのメッセージングおよび SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging standby

no logging standby

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

logging standby コマンドは、デフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging standby をイネーブルにして、フェールオーバーの発生時にフェールオーバー スタンバイセキュリティ アプライアンスのシステム ログ メッセージを同期されたままにすることができます。

（注） **logging standby** コマンドを使用すると、syslog サーバ、SNMP サーバ、FTP サーバなどの共有ロギング先でのトラフィックは 2 倍になります。

例

次に、セキュリティ アプライアンスでシステム ログ メッセージをフェールオーバー スタンバイ セキュリティ アプライアンスに送信できるようにする例を示します。**show logging** コマンドの出力から、この機能がイネーブルであることがわかります。

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
```

```
Monitor logging: disabled
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

関連コマンド

コマンド	説明
failover	フェールオーバー機能をイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging timestamp

メッセージが生成された日付と時刻をシステム ログ メッセージに含めることを指定するには、グローバル コンフィギュレーション モードで **logging timestamp** コマンドを使用します。日付と時刻をシステム ログ メッセージから削除するには、このコマンドの **no** 形式を使用します。

logging timestamp

no logging timestamp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

セキュリティ アプライアンスでは、デフォルトでは日付と時刻はシステム ログ メッセージに含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logging timestamp コマンドを使用すると、セキュリティ アプライアンスによってすべてのシステム ログ メッセージにタイムスタンプが含まれます。

例

次に、すべてのシステム ログ メッセージにタイムスタンプ情報が含まれるようにする例を示します。

```
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging trap

セキュリティ アプライアンスによって syslog サーバに送信されるシステム ログ メッセージを指定するには、グローバル コンフィギュレーション モードで **logging trap** コマンドを使用します。コンフィギュレーションからこのコマンドを削除するには、このコマンドの **no** 形式を使用します。

logging trap [*logging_list* | *level*]

no logging trap

構文の説明

level	システム ログ メッセージの最大レベルを設定します。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 3、2、1、および 0 のシステム ログ メッセージを送信します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システム使用不可 • **1** または **alerts**：ただちに対応 • **2** または **critical**：重大な状況 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：通知だけ、重要な状況ではない • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、および WWW URL
logging_list	syslog サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトのシステム ログ メッセージのトラップは定義されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ロギング トランスポート プロトコルとして TCP を使用している場合、セキュリティ アプライアンスが syslog サーバに到達できないか、syslog サーバが誤って設定されているか、ディスクがいっぱいになると、セキュリティ アプライアンスではセキュリティ対策として新しいネットワーク アクセス セッションを拒否します。

UDP ベースのロギングでは、syslog サーバに障害が発生しても、セキュリティ アプライアンスによるトラフィックの送信は停止されません。

例

次の例は、内部インターフェイス上に存在し、デフォルトのプロトコルとポート番号を使用する syslog サーバに、ロギング レベル 0、1、2、および 3 のシステム ログ メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

login

ローカル ユーザ データベースを使用して特権 EXEC モードにログインするか（username コマンドを参照）、ユーザ名を変更するには、ユーザ EXEC モードで **login** コマンドを使用します。

login

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ユーザ EXEC モードから、**login** コマンドを使用して、ローカル データベース内の任意のユーザ名として特権 EXEC モードにログインできます。認証をオンにした場合、**login** コマンドは **enable** コマンドと類似しています（**aaa authentication console** コマンドを参照）。enable 認証と異なり、**login** コマンドではローカル ユーザ名データベースのみを使用でき、認証が常に必要です。CLI モードから **login** コマンドを使用して、ユーザを変更することもできます。

ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、**aaa authorization コマンド**を参照してください。

注意　CLI にアクセスできるユーザや特権 EXEC モードを開始できないようにするユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、RADIUS または TACACS+ 認証を使用できます。あるいは、すべてのローカル ユーザをレベル 1 に設定して、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御できます。

例

次に、**login** コマンドを入力した後のプロンプトの例を示します。

```
hostname> login
Username:
```

関連コマンド

コマンド	説明
aaa authorization command	CLI アクセスのためのコマンド認可をイネーブルにします。
aaa authentication console	コンソール、Telnet、HTTP、SSH、または **enable** コマンド アクセスに対して認証を要求します。
logout	CLI からログアウトします。
username	ユーザをローカル データベースに追加します。

login-button

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログイン ボックスのログイン ボタンをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **login-button** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

login-button {**text** | **style**} *value*

[**no**] **login-button** {**text** | **style**} *value*

構文の説明

style	スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン ボタン テキストは「Login」です。

デフォルトのログイン ボタン スタイルは、次のとおりです。

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ログイン ボタンをテキスト「OK」でカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-button text OK
```

関連コマンド

コマンド	説明
login-title	WebVPN ページ ログイン ボックスのタイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワードをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。

login-message

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン メッセージをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **login-message** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

login-message {**text** | **style**} *value*

[**no**] **login-message** {**text** | **style**} *value*

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン メッセージは、「Please enter your username and password」です。

デフォルトのログイン メッセージのスタイルは、background-color:#CCCCCC;color:black です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次の例では、ログイン メッセージのテキストは「username and password」に設定されます。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-message text username and password
```

関連コマンド

コマンド	説明
login-title	WebVPN ページのログイン ボックスのタイトルをカスタマイズします。
username-prompt	WebVPN ページ ログインのユーザ名プロンプトをカスタマイズします。
password-prompt	WebVPN ページ ログインのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ページ ログインのグループ プロンプトをカスタマイズします。

login-title

WebVPN ユーザに表示される WebVPN ページのログイン ボックスのタイトルをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **login-title** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

login-title {**text** | **style**} *value*

[**no**] **login-title** {**text** | **style**} *value*

構文の説明

text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン テキストは「Login」です。

ログイン タイトルのデフォルトの HTML スタイルは、background-color: #666666; color: white です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ログイン タイトルのスタイルを設定する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

関連コマンド

コマンド	説明
login-message	WebVPN ログイン ページのログイン メッセージをカスタマイズします。
username-prompt	WebVPN ログイン ページのユーザ名プロンプトをカスタマイズします。
password-prompt	WebVPN ログイン ページのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ログイン ページのグループ プロンプトをカスタマイズします。

logo

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのロゴをカスタマイズするには、webvpn カスタマイゼーション モードで **logo** コマンドを使用します。コンフィギュレーションからロゴを削除してデフォルト（Cisco ロゴ）にリセットするには、このコマンドの **no** 形式を使用します。

logo {**none** | **file** {*path value*}}

[**no**] **logo** {**none** | **file** {*path value*}}

構文の説明

file	ロゴを含むファイルを指定することを示します。
none	ロゴがないことを指定します。ヌル値を設定して、ロゴを拒否します。ロゴを継承しないようにします。
path	ファイル名のパス。可能なパスは、disk0:、disk1:、または flash: です。
value	ロゴのファイル名を指定します。最大長は 255 文字です（スペースを含めることはできません）。ファイル タイプは JPG、PNG、または GIF であり、100 KB 未満である必要があります。

デフォルト

デフォルトのロゴは Cisco ロゴです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

指定したファイル名が存在しない場合は、エラー メッセージが表示されます。ロゴ ファイルを削除したが、コンフィギュレーションがまだそのファイルを指している場合、ロゴは表示されません。

ファイル名にスペースを含めることはできません。

例

次の例では、ファイル cisco_logo.gif にカスタム ロゴが含まれています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

関連コマンド

コマンド	説明
title	WebVPN ページのタイトルをカスタマイズします。
page style	Cascading Style Sheet（CSS; カスケーディング スタイル シート）パラメータを使用して WebVPN ページをカスタマイズします。

logout

CLI を終了するには、ユーザ EXEC モードで **logout** コマンドを使用します。

logout

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

logout コマンドを使用すると、セキュリティ アプライアンスからログアウトできます。**exit** コマンドまたは **quit** コマンドを使用して、ユーザ モードに戻ることができます。

例

次に、セキュリティ アプライアンスからログアウトする例を示します。

```
hostname> logout
```

関連コマンド

コマンド	説明
login	ログイン プロンプトを開始します。
exit	アクセス モードを終了します。
quit	コンフィギュレーション モードまたは特権モードを終了します。

logout-message

WebVPN ユーザが WebVPN サービスからログアウトするときに表示される WebVPN ログアウト画面のログアウト メッセージをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **logout-message** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

logout-message {**text** | **style**} *value*

[**no**] **logout-message** {**text** | **style**} *value*

構文の説明

style	スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログアウト メッセージ テキストは「Goodbye」です。

デフォルトのログアウト メッセージのスタイルは、background-color:#999999;color:black です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ログアウト メッセージのスタイルを設定する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# logout-message style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style:
italic; font-weight: bold
```

関連コマンド

コマンド	説明
logout-title	WebVPN ページのログアウト タイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワードをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。