uc-ime コマンド～ username-prompt コマンド

uc-ime（非推奨）

Cisco Intercompany Media Engine プロキシ インスタンスを作成するには、グローバル コンフィギュレーション モードで **uc-ime** コマンドを使用します。このプロキシ インスタンスを削除するには、このコマンドの **no** 形式を使用します。

uc-ime *uc-ime_name*

no uc-ime *uc-ime_name*

構文の説明

uc-ime_name	ASA 上で設定されている Cisco Intercompany Media Engine プロキシのインスタンス名を指定します。*name* は 64 文字までに制限されています。 ASA に設定できる Cisco Intercompany Media Engine プロキシは 1 つだけです。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.4(1)	このコマンドは廃止されました。

使用上のガイドライン

Cisco Intercompany Media Engine プロキシを設定します。Cisco Intercompany Media Engine により、企業はインターネット経由での相互接続をオンデマンドで行うことが可能になり、VoIP テクノロジーによる高度な機能を利用できます。Cisco Intercompany Media Engine では、ピアツーピア、セキュリティ、および SIP プロトコルを使用してビジネス間にダイナミック SIP トランクを作成することにより、異なる企業内の Cisco Unified Communications Manager クラスタの間で企業間フェデレーションを実現できます。企業の集合は、最終的にそれらの間にクラスタ間トランクが存在する 1 つの大きなビジネスであるかのように連携します。

メディア ターミネーション インスタンスは、Cisco Intercompany Media Engine プロキシで指定する前に作成する必要があります。

ASA に設定できる Cisco Intercompany Media Engine プロキシは 1 つだけです。

例

次に、**uc-ime** コマンドを使用して Cisco Intercompany Media Engine プロキシを設定する例を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

関連コマンド

コマンド	説明
fallback	接続の整合性が低下する場合に VoIP から PSTN へのフォールバックに Cisco Intercompany Media Engine が使用するフォールバック タイマーを設定します。
show uc-ime	フォールバック通知、マッピング サービス セッション、およびシグナリング セッションに関する統計情報または詳細情報を表示します。
ticket	Cisco Intercompany Media Engine プロキシのチケット エポックおよびパスワードを設定します。
ucm	Cisco Intercompany Media Engine プロキシの接続先の Cisco UCM を設定します。

ucm（廃止）

Cisco Intercompany Media Engine プロキシの接続先の Cisco Unified Communications Manager（UCM）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 **ucm** コマンドを使用します。Cisco Intercompanuy Media Engine プロキシに接続されている Cisco UCMs を削除するには、このコマンドの **no** 形式を使用します。

ucm address *ip_address* **trunk-security-mode** {**nonsecure** | **secure**}

no ucm address *ip_address* **trunk-security-mode** {**nonsecure** | **secure**}

構文の説明

address	Cisco Unified Communications Manager（UCM）の IP アドレスを設定するキーワードです。
ip_address	Cisco UCM の IP アドレスを指定します。IP アドレスは IPv4 形式で入力します。
nonsecure	Cisco UCM クラスタまたは Cisco UCM クラスタが非セキュア モードで動作するように指定します。
secure	Cisco UCM クラスタまたは Cisco UCM クラスタがセキュア モードで動作するように指定します。
trunk-security-mode	Cisco UCM クラスタまたは Cisco UCM クラスタのセキュリティ モードを設定するキーワードです。

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	トランスペアレント	シングル	コンテキスト	システム
UC-IME コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **uc-ime** モード コマンドとともに廃止されました。

使用上のガイドライン

企業内の Cisco UCM サーバを指定します。

Cisco Intercompany Media Engine プロキシの **ucm** コマンドを複数入力できます。

（注） Cisco Intercompany Media Engine の SIP トランクがイネーブルになっているクラスタ内の各 Cisco UCM に対してエントリを追加する必要があります。

Cisco UCM または Cisco UCM に **secure** を指定することは、Cisco UCM または Cisco UCM クラスタが TLS を開始することを意味します。したがって、コンポーネントに TLS を設定する必要があります。

secure オプションは、この作業で設定することも、後で企業の TLS を設定するときに更新することもできます。

企業内の TLS は、ASA から見た Cisco Intercompany Media Engine トランクのセキュリティ ステータスを参照します。

Cisco UCM で Cisco Intercompany Media Engine トランクの転送セキュリティを変更する場合は、適応型セキュリティ アプライアンスでも変更する必要があります。一致していないと、コールは失敗します。適応型セキュリティ アプライアンスは、非セキュア IME トランクを持つ SRTP をサポートしません。適応型セキュリティ アプライアンスは、SRTP がセキュア トランクで許可されることを前提としています。したがって、TLS が使用される場合は、IME トランクに対して [SRTP Allowed] をオンにする必要があります。ASA は、セキュア IME トランク コールに対して SRTP から RTP へのフォールバックをサポートしています。

プロキシは企業のエッジに置かれ、企業間で作成される SIP トランク間の SIP シグナリングを検査します。プロキシはインターネットから TLS シグナリングを終端し、TCP または TLS を Cisco UCM に対して開始します。

Transport Layer Security（TLS）は、インターネットなどのネットワーク経由の通信にセキュリティを提供する暗号化プロトコルです。TLS によって、トランスポート層エンドツーエンドでのネットワーク接続のセグメントが暗号化されます。

この作業は、内部ネットワーク内で TCP が許可されている場合は必要ありません。

ローカルの企業内で TLS を設定するための主要な手順を次に示します。

- ローカルの ASA で、自己署名証明書の別の RSA キーおよびトラストポイントを作成します。
- ローカル Cisco UCM とローカルの ASA 間で証明書をエクスポートおよびインポートします。
- ASA でローカル Cisco UCM のトラストポイントを作成します。

TLS を介した認証：N 社の企業のために ASA がポートとして機能するためには、Cisco UCM は ASA からの証明書の受け入れを許可する必要があります。この処理は、Cisco UCM が証明書からサブジェクト名を抽出してセキュリティ プロファイルで設定されている名前と比較するため、ASA によって示されるサブジェクト名と同じものが含まれている同じ SIP セキュリティ プロファイルにすべての UC IME SIP トランクを関連付けることによって実行できます。

例

次に、UCM プロキシに接続する例を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

包括的

DNS インスペクション エンジンが DNS ルックアップ要求を Cisco Umbrella へリダイレクトできるようにするには、DNS インスペクション ポリシーマップ パラメータ コンフィギュレーション モードで **umbrella** コマンドを使用します。Cisco Umbrella 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。

umbrella [**tag** *umbrella_policy*] [**fail-open**]

no umbrella [**tag** *umbrella_policy*] [**fail-open**]

構文の説明

fail-open	Cisco Umbrella DNS サーバが使用できない場合は、このポリシーマップで Umbrella に自身を無効にさせて、DNS 要求をシステムに設定されている他の DNS サーバ（ある場合）に移動できるようにします。Umbrella DNS サーバが再度使用可能になると、ポリシーマップはそれらの使用を再開します。 このオプションが含まれていない場合、DNS 要求は到達不能の Umbrella リゾルバへ移動し続けるので、応答は取得されません。
tag *umbrella_policy*	（任意）Cisco Umbrella に定義され、デバイスに適用される、エンタープライズ セキュリティ ポリシーの名前。ポリシーを指定しない場合、または入力した名前が Cisco Umbrella に存在しない場合、デフォルトのポリシーが指定されます。

デフォルト

タグを指定しないと、デバイス登録は、デフォルトのエンタープライズ セキュリティ ポリシーを指定します。

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	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。
9.12(1)	**fail-open** キーワードが追加されました。

使用上のガイドライン

DNS インスペクション ポリシーマップを設定する際に、次のコマンドを使用します。

アクティブな DNS インスペクション ポリシーマップのこのコマンドのプレゼンスは、Cisco Umbrella 登録サーバの登録プロセスを開始します。HTTPS 経由で行われる登録と接続を確立するには、登録サーバの CA 証明書をインストールしておく必要があります。

グローバル コンフィギュレーション モードで **umbrella-global** コマンド使用して、グローバル パラメータを設定する必要もあります。

例

次の例では、デフォルト ポリシーを使用して Umbrella を有効にし、グローバル DNS インスペクションで使用されるデフォルトのインスペクション ポリシーマップで DNScrypt も有効にします。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

次の例では、デフォルト ポリシーを使用して Umbrella のフェール オープンを有効にし、グローバル DNS インスペクションで使用されるデフォルトのインスペクション ポリシーマップで DNScrypt も有効にします。タグをすでに登録していて、**fail-open** オプションのみを追加する場合は、コマンドに同じタグを含める必要があります。そうしない場合、タグなしでデバイスを再登録することになります。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

関連コマンド

コマンド	説明
dnscrypt	デバイスと Cisco Umbrella 間の接続で DNScrypt 暗号化を有効にします。
inspect dns	DNS インスペクションをイネーブルにします。
policy-map type inspect dns	DNS インスペクション ポリシー マップを作成します。
public-key	Cisco Umbrella で使用する公開キーを設定します。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

umbrella-global

Cisco Umbrella ポータルにデバイスを接続するために必要なグローバル設定を設定するために、Umbrella コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **umbrella-global** コマンドを使用します。グローバル Umbrella 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。

umbrella-global

no umbrella-global

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

デフォルトのグローバル Umbrella コンフィギュレーションはありません。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco Umbrella サービスに登録する場合は、デバイスを Cisco Umbrella に登録するように設定できます。

Umbrella グローバル設定は、主に、Cisco Umbrella にデバイスを登録するために必要な API トークンを定義します。Cisco Umbrella ダッシュボードからトークンを取得します。

グローバル設定が Umbrella を有効にするために十分ではありません。パラメータ コンフィギュレーション モードで umbrella コマンドを使用して、DNS インスペクション ポリシーマップで Umbrella を有効にする必要もあります。

例

次の例では、グローバル Umbrella 設定を構成し、デフォルトの DNS インスペクション ポリシーマップで Umbrella を有効にする方法についても説明します。

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license

ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

関連コマンド

コマンド	説明
dnscrypt	デバイスと Cisco Umbrella 間の接続で DNScrypt 暗号化を有効にします。
local-domain-bypass	DNS 要求が Cisco Umbrella をバイパスする必要があるローカル ドメインを設定します。
public-key	Cisco Umbrella で使用する公開キーを設定します。
resolver	DNS 要求を解決する Cisco Umbrella DNS サーバのアドレスを設定します。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。
umbrella	DNS インスペクション エンジンで、DNS ルックアップ要求を Cisco Umbrella にリダイレクトできるようにします。

undebug

現在のセッションでデバッグ情報の表示をディセーブルにするには、特権 EXEC モードで **undebug** コマンドを使用します。

undebug {*command* | **all**}

構文の説明

all	すべてのデバッグ出力をディセーブルにします。
command	指定したコマンドのデバッグをディセーブルにします。サポートされるコマンドの詳細については、「使用上のガイドライン」を参照してください。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。**debug** キーワードが追加されました。

使用上のガイドライン

次のコマンドは、**undebug** コマンドで使用できます。特定のコマンドのデバッグ、または特定の **debug** コマンドに関連付けられた引数とキーワードの詳細については、**debug** コマンドのエントリを参照してください。

- aaa：AAA 情報
- acl：ACL 情報
- all：すべてのデバッグ
- appfw：アプリケーション ファイアウォール情報
- arp：NP オペレーションを含む ARP
- asdm：ASDM 情報
- auto-update：Auto-update 情報
- boot-mem：ブート メモリの計算と設定
- cifs：CIFS 情報
- cmgr：CMGR 情報

- context：コンテキスト情報
- cplane：CP 情報
- crypto：クリプト情報
- ctiqbe：CTIQBE 情報
- ctl-provider：CTL プロバイダーのデバッグ情報
- dap：DAP 情報
- dcerpc：DCERPC 情報
- ddns：ダイナミック DNS 情報
- dhcpc：DHCP クライアント情報
- dhcpd：DHCP サーバ情報
- dhcprelay：DHCP リレー情報
- disk：ディスク情報
- dns：DNS 情報
- eap：EAP 情報
- eigrp：EIGRP プロトコル情報
- email：電子メール情報
- entity：エンティティ MIB 情報
- eou：EAPoUDP 情報
- esmtp：ESMTP 情報
- fips：FIPS 140-2 情報
- fixup：フィックスアップ情報
- fover：フェールオーバー情報
- fsm：FSM 情報
- ftp：FTP 情報
- generic：その他の情報
- gtp：GTP 情報
- h323：H323 情報
- http：HTTP 情報
- icmp：ICMP 情報
- igmp：インターネット グループ管理プロトコル
- ils：LDAP 情報
- im：IM インスペクション情報
- imagemgr：Image Manager 情報
- inspect：デバッグ情報のインスペクション
- integrityfw：Integrity ファイアウォール情報
- ip：IP 情報
- ipsec-over-tcp：IPsec over TCP 情報
- IPSec-pass-thru：ipsec-pass-thru 情報のインスペクション

- ipv6：IPv6 情報
- iua-proxy：IUA プロキシ情報
- kerberos：KERBEROS 情報
- l2tp：L2TP 情報
- ldap：LDAP 情報
- mfib：マルチキャスト転送情報ベース
- mgcp：MGCP 情報
- module-boot：サービス モジュール ブート情報
- mrib：マルチキャスト ルーティング情報ベース
- nac-framework：NAC-FRAMEWORK 情報
- netbios-inspect：NETBIOS インスペクション情報
- npshim：NPSHIM 情報
- ntdomain：NT ドメイン情報
- ntp：NTP 情報
- ospf：OSPF 情報
- p2p：P2P インスペクション情報
- parser：パーサー情報
- pim：Protocol Independent Multicast
- pix：PIX 情報
- ppp：PPP 情報
- pppoe：PPPoE 情報
- pptp：PPTP 情報
- radius：RADIUS 情報
- redundant-interface：冗長インターフェイス情報
- rip：RIP 情報
- rtp：RTP 情報
- rtsp：RTSP 情報
- sdi：SDI 情報
- sequence：シーケンス番号の追加
- session-command：セッション コマンド情報
- sip：SIP 情報
- skinny：Skinny 情報
- sla：IP SLA モニタ デバッグ
- smtp-client：電子メール システムのログ メッセージ
- splitdns：スプリット DNS 情報
- sqlnet：SQLNET 情報
- ssh：SSH 情報
- sunrpc：SUNRPC 情報

- tacacs：TACACS 情報
- tcp：WebVPN の TCP
- tcp-map：TCP マップ情報
- timestamps：タイムスタンプの追加
- track：スタティック ルート トラッキング
- vlan-mapping：VLAN マッピング情報
- vpn-sessiondb：VPN セッション データベース情報
- vpnlb：VPN ロード バランシング情報
- wccp：WCCP 情報
- webvpn：WebVPN 情報
- xdmcp：XDMCP 情報
- xml：XML パーサー情報

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべてのデバッグ出力をディセーブルにする例を示します。

```
ciscoasa(config)# undebug all
```

関連コマンド

コマンド	説明
debug	選択したコマンドに関するデバッグ情報を表示します。

unit join-acceleration

クラスタ結合の高速化を有効にするには、クラスタ コンフィギュレーション モードで **unit joint-acceleration** コマンドを使用します。この機能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。

unit join-acceleration

no unit join-acceleration

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。

コマンド デフォルト

このコマンドは、デフォルトでイネ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	トランスペアレント	シングル	コンテキスト	システム
クラスタ構成	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

スレーブ ユニットがマスター ユニットと同じ構成の場合、構成の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、マスターからスレーブには複製されません。

(注) 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。互換性のない設定を表示するには、**show cluster info unit-join-acceleration incompatible-config** コマンドを使用します。

例

次に、クラスタ結合の高速化を無効にする例を示します。

```
ciscoasa(config)# cluster cluster1
ciscoasa(cfg-cluster)# no unit join-acceleration
```

関連コマンド

コマンド	説明
クラスタ	クラスタ コンフィギュレーション モードを開始します

unit parallel-join

Firepower 9300 シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されていることを確認するには、クラスタ グループ コンフィギュレーション モードで **unit parallel-join** コマンドを使用します。並行参加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。

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*

no unit parallel-join [*num_of_units* **max-bundle-delay** *max_delay_time*]

構文の説明

num_of_units	モジュールがクラスタに参加する前に準備する必要がある同じシャーシ内のモジュールの最小数(1 ～ 3)を指定します。デフォルトは 1 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。たとえば、値を 3 に設定した場合、各モジュールは *max_delay_time* の間、または 3 つすべてのモジュールの準備が完了するまで待機してからクラスタに参加します。3 のすべてのモジュールがほぼ同時にクラスタの参加を要求し、同時期にトラフィックの受信を開始します。
max-bundle-delay *max_delay_time*	最大遅延時間を分単位(0 ～ 30 分)で指定します。この時間が経過すると、モジュールは他のモジュールの準備が完了するのを待つことをやめて、クラスタに参加します。デフォルトは 0 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。*num_of_units* を 1 に設定した場合、この値は 0 にする必要があります。*num_of_units* を 2 または 3 に設定した場合、この値は 1 以上にする必要があります。このタイマーはモジュールごとのタイマーですが、最初のモジュールがクラスタに参加すると、その他すべてのモジュールのタイマーが終了し、残りのモジュールがクラスタに参加します。 たとえば、*num_of_units* を 3、*max_delay_time* を 5 分に設定します。モジュール 1 が起動すると、その 5 分間のタイマーが開始されます。モジュール 2 が 2 分後に起動すると、その 5 分間のタイマーが開始されます。モジュール 3 が 1 分後に起動し、すべてのモジュールが 4 分符号でクラスタに参加します。モジュールはタイマーが完了するまで待機しません。モジュール 3 が起動しない場合、モジュール 1 は 5 分間タイマーの終了時にクラスタに参加し、モジュール 2 も参加します。モジュール 2 はタイマーがまだ 2 分残っていますが、タイマーが完了するまで待機しません。

コマンド デフォルト

この機能はデフォルトで無効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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.10(1)	コマンドが追加されました。

使用上のガイドライン　他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。

例　次の例では、モジュールの数を 2 に、最大遅延時間を 6 分に設定します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# unit parallel-join 2 max-bundle-delay 6
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループ コンフィギュレーション モードを開始します。

unix-auth-gid

UNIX グループ ID を設定するには、グループ ポリシー webvpn コンフィギュレーション モードで **unix-auth-gid** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

unix-auth-gid *identifier*

no storage-objects

構文の説明

identifier	0 ～ 4294967294 の範囲の整数を指定します。

デフォルト

デフォルトは 65534 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

文字列でネットワーク ファイル システム（NetFS）の場所を指定します。SMB プロトコルおよび FTP プロトコルだけがサポートされています。たとえば、smb://（NetFS の場所）または ftp://（NetFS の場所）。この場所の名前を **storage-objects** コマンドで使用します。

例

次に、UNIX グループ ID を 4567 に設定する例を示します。

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# unix-auth-gid 4567
```

関連コマンド

コマンド	説明
unix-auth-uid	UNIX ユーザ ID を設定します。

unix-auth-uid

UNIX ユーザ ID を設定するには、グループ ポリシー webvpn コンフィギュレーション モードで **unix-auth-uid** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

unix-auth-gid *identifier*

no storage-objects

構文の説明

identifier	0 ～ 4294967294 の範囲の整数を指定します。

デフォルト

デフォルトは 65534 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

文字列でネットワーク ファイル システム（NetFS）の場所を指定します。SMB プロトコルおよび FTP プロトコルだけがサポートされています。たとえば、smb://（NetFS の場所）または ftp://（NetFS の場所）。この場所の名前を **storage-objects** コマンドで使用します。

例

次に、UNIX ユーザ ID を 333 に設定する例を示します。

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# unix-auth-gid 333
```

関連コマンド

コマンド	説明
unix-auth-gid	UNIX グループ ID を設定します。

unsupported

ソフトウェアで直接サポートされていない Diameter 要素をロギングするには、ポリシー マップ パラメータ コンフィギュレーション モードで **unsupported** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

unsupported {**application-id** | **avp** | **command-code**} **action log**

no unsupported {**application-id** | **avp** | **command-code**} **action log**

構文の説明

application-id	アプリケーション ID が直接サポートされていない Diameter メッセージをロギングします。
avp	直接サポートされていない属性値ペア（AVP）が含まれている Diameter メッセージをロギングします。
command-code	直接サポートされていないコマンド コードが含まれている Diameter メッセージをロギングします。

デフォルト

デフォルトでは、ロギングなしで要素が許可されています。

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。

	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	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

Diameter インスペクション ポリシー マップを設定する場合に、このコマンドを使用します。

これらのオプションでは、ソフトウェアで直接サポートされていないアプリケーション ID、コマンド コード、および AVP が指定されます。デフォルトでは、ロギングなしで要素が許可されています。コマンドを 3 回入力して、すべての要素のロギングを有効にできます。

例

次に、サポートされていないすべてのアプリケーション ID、コマンド コード、および AVP をロギングする例を示します。

```
ciscoasa(config)# policy-map type inspect diameter diameter-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# unsupported application-id action log
ciscoasa(config-pmap-p)# unsupported command-code action log
ciscoasa(config-pmap-p)# unsupported avp action log
```

関連コマンド

コマンド	説明
inspect diameter	Diameter インスペクションを有効にします。
policy-map type inspect diameter	Diameter インスペクション ポリシー マップを作成します。

upgrade rommon

ASA 5506-X および ASA 5508-X シリーズ セキュリティ アプライアンスをアップグレードするには、特権 EXEC モードで **upgrade rommon** コマンドを使用します。

upgrade rommon [disk0 | disk1 | flash]:/[*path*] *filename*

構文の説明

disk0:/[*path*/]*filename*	このオプションは内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。
disk1:/[*path*/]*filename*	このオプションは外部フラッシュ メモリ カードを示します。
flash:/[*path*/]*filename*	このオプションは、内部フラッシュ カードを示します。**flash** は **disk0** のエイリアスです。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

コマンドにファイル名を指定すると、コマンドによってファイルが確認され、アップグレードを確認するよう求められます。設定情報を保存していない場合、リロードを開始する前に情報を保存するように促されます。確認すると、ASA は ROMMON になり、アップグレード手順が開始されます。

例

次に、ASA 5506-X および ASA 5508-X シリーズ セキュリティ アプライアンスをアップグレードする例を示します。

```
ciscoasa# upgrade rommon disk0:/kenton_rommon_1-0-19_release.SPA
Verifying file integrity of disk0:/kenton_rommon_1-0-19_release.SPA

Computed Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
                      9ef1fa4c3892f04b2e71a6b19ddb64c4
```

```
Embedded Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
                      9ef1fa4c3892f04b2e71a6b19ddb64c4


Digital signature successfully validated
File Name                     : disk0:/kenton_rommon_1-0-19_release.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 54232BC5
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

upload-max-size

（注） **upload-max-size** コマンドは機能しません。使用しないでください。ただし、実行コンフィギュレーションでは表示される場合があり、CLI で使用できます。

アップロードするオブジェクトの最大許容サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **upload-max-size** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

upload-max-size *size*

no upload-max-size

構文の説明

size	アップロードされるオブジェクトの最大許容サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

関連コマンド

コマンド	説明
post-max-size	ポストするオブジェクトの最大サイズを指定します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

srv-id

参照 ID オブジェクトに URI ID を設定するには、*ca-reference-identity* モードで **uri-id** コマンドを使用します。URI ID を削除するには、このコマンドの **no** 形式を使用します。最初に、**crypto ca reference-identity** コマンドを入力して参照 ID オブジェクトを設定することで、*ca-reference-identity* モードにアクセスできます。

srv-id *value*

no srv-id *value*

構文の説明

value	各参照 ID の値。
srv-id	RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。

コマンド 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	トランスペアレント	シングル	コンテキスト	システム
ca-reference-identity	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

例

次に、syslog サーバの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
crypto ca reference-identity	参照 ID オブジェクトを設定します。
cn-id	参照 ID オブジェクトのコモン ネーム ID を設定します。
dns-id	参照 ID オブジェクトの DNS ドメイン名 ID を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギング サーバを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバを設定します。

uri-non-sip

Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別するには、パラメータ コンフィギュレーション モードで **uri-non-sip** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能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。

uri-non-sip action {**mask** | **log**} [**log**]

no uri-non-sip action {**mask** | **log**} [**log**]

構文の説明

ログ	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。
mask	SIP 以外の URI をマスクします。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップの Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別する例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# uri-non-sip action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

url（crl 設定）（廃止）

CRL を取得するためのスタティック URL のリストを維持するには、crl 設定コンフィギュレーション モードで **url** コマンドを使用します。crl 設定コンフィギュレーション モードは、**クリプト CA トラストポイント** コンフィギュレーション モードからアクセスできます。既存の URL を削除するには、このコマンドの **no** 形式を使用します。

url *index url*

no url *index url*

構文の説明

index	リスト内の各 URL のランクを決定する 1 ～ 5 の値を指定します。ASA は、インデックス 1 から URL を試行します。
url	CRL の取得元となる URL を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.13(1)	このコマンドは削除されました。**match certificate** コマンドを参照してください。

使用上のガイドライン

既存の URL は上書きできません。既存の URL を置き換えるには、まずこのコマンドの **no** 形式を使用して、その URL を削除します。

例

次に、crl コンフィギュレーション モードを開始し、CRL 取得用の URL リストを作成およびメンテナンスするために インデックス 3 を設定し、CRL の取得元となる URL https://example.com を設定する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# url 3 https://example.com
ciscoasa(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
ポリシー	CRL の取得元を指定します。

url（SAML IDP）

サイン インまたはサイン アウト用に SAML IdP URL を設定するには、SAML IDP コンフィギュレーション モードで **url** コマンドを使用します。SAML IDP コンフィギュレーション モードにアクセスするには、まず **webvpn** コマンドを入力します。URL を削除するには、このコマンドの **no** 形式を使用します。

url {**sign-in** | **sign-out**} **value** *url*

no url *url*

構文の説明

url	CRL の取得元となる URL を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
SAML IDP コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

既存の URL は上書きできません。既存の URL を置き換えるには、まずこのコマンドの **no** 形式を使用して、その URL を削除します。

url-block

フィルタリング サーバからのフィルタリング決定を待機する間、Web サーバの応答に使用される URL バッファを管理するには、**url-block** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

url-block block *block_buffer*

no url-block block *block_buffer*

url-block mempool-size *memory_pool_size*

no url-block mempool-size *memory_pool_size*

url-block url-size *long_url_size*

no url-block url-size *long_url_size*

構文の説明

block *block_buffer*	フィルタリング サーバからのフィルタリング決定を待機している間に Web サーバの応答を保存する HTTP 応答バッファを作成します。指定できる値は 1 ～ 128 です。これは、1550 バイトのブロック数を示します。
mempool-size *memory_pool_size*	URL バッファ メモリ プールの最大サイズをキロバイト（KB）単位で設定します。指定できる値は 2 ～ 10240 です。これは、2 ～ 10240 KB の URL バッファ メモリ プールを示します。
url-size *long_url_size*	バッファに保存する長い各 URL の最大許容 URL サイズを KB 単位で設定します。最大 URL サイズとして指定できる値は、Websense では 2、3、または 4（それぞれ 2 KB、3 KB、4 KB を表す）、Secure Computing では 2 または 3（それぞれ 2 KB、3 KB を表す）です。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Websense フィルタリング サーバの場合、**url-block url-size** コマンドを使用すると、最大 4 KB の長い URL をフィルタリングできます。Secure Computing の場合は、**url-block url-size** コマンドを使用して、最大 3 KB の長い URL をフィルタリングできます。Websense フィルタリング サーバおよび N2H2 フィルタリング サーバの場合、**url-block block** コマンドを使用すると、ASA は、URL フィルタリング サーバからの応答を待機している間、Web クライアント要求への応答として Web サーバから受信したパケットをバッファに保存します。これにより、Web クライアントのパフォーマンスがデフォルトの ASA 動作よりも向上します。デフォルトの動作では、パケットをドロップし、接続か許可された場合に Web サーバにパケットの再送信を要求します。

url-block block コマンドを使用し、フィルタリング サーバが接続を許可した場合、ASA はブロックを HTTP 応答バッファから Web クライアントに送信し、バッファからブロックを削除します。フィルタリング サーバが接続を拒否した場合、ASA は拒否メッセージを Web クライアントに送信し、HTTP 応答バッファからブロックを削除します。

url-block block コマンドを使用して、フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答のバッファリングに使用するブロック数を指定します。

url-block url-size コマンドを **url-block mempool-size** コマンドとともに使用して、フィルタリングする URL の最大長と URL バッファに割り当てる最大メモリを指定します。Websense サーバまたは Secure-Computing サーバに、1159 バイトよりも長く、最大 4096 バイトまでの URL を渡す場合は、これらのコマンドを使用します。**url-block url-size** コマンドは、1159 バイトよりも長い URL をバッファに保存し、その URL を（TCP パケット ストリームを使用して）Websense サーバまたは Secure-Computing サーバに渡します。これにより、Websense サーバまたは Secure-Computing サーバでは、その URL へのアクセスを許可または拒否できます。

例

次に、URL フィルタリング サーバからの応答をバッファに保存するために 1550 バイトのブロックを 56 個割り当てる例を示します。

```
ciscoasa#(config)# url-block block 56
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファの使用状況カウンタをクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

url-cache

Websense サーバから受信した URL 応答の URL キャッシングをイネーブルにし、キャッシュのサイズを設定するには、グローバル コンフィギュレーション モードで **url-cache** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

no url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

構文の説明

dst	URL 宛先アドレスに基づくキャッシュ エントリ。すべてのユーザが Websense サーバ上で同一の URL フィルタリング ポリシーを共有している場合に、このモードを選択します。
size *kbytes*	キャッシュ サイズの値を 1 ～ 128 KB の範囲で指定します。
src_dst	URL 要求の送信元アドレスと URL 宛先アドレスの両方に基づくキャッシュ エントリ。このモードは、Websense サーバ上でユーザが同じ URL フィルタリング ポリシーを共有しない場合に選択します。
statistics	**statistics** オプションを使用すると、キャッシュ ルックアップの回数やヒット率などの追加の URL キャッシュ統計情報が表示されます。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

url-cache コマンドには、URL サーバからの応答をキャッシュするコンフィギュレーション オプションが用意されています。

url-cache コマンドは、URL キャッシングのイネーブル化、キャッシュ サイズの設定、およびキャッシュ統計情報の表示を行う場合に使用します。

(注) N2H2 サーバ アプリケーションは、URL フィルタリングでこのコマンドをサポートしません。

キャッシングにより、URL アクセス権限が ASA 上のメモリに保存されます。ホストが接続を要求すると、ASA は要求を Websense サーバに転送するのではなく、一致するアクセス権限を URL キャッシュ内で探します。キャッシングをディセーブルにするには、**no url-cache** コマンドを使用します。

(注) Websense サーバで設定を変更した場合は、**no url-cache** コマンドでキャッシュをディセーブルにした後、**url-cache** コマンドで再度イネーブルにします。

URL キャッシュを使用しても、Websense プロトコル バージョン 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル バージョン 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。目的のセキュリティ要求を満たす使用プロファイルを取得したら、**url-cache** をイネーブルにしてスループットを増大させます。Websense プロトコル バージョン 4 の URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログが更新されます。

例

次に、送信元アドレスと宛先アドレスに基づいてすべての発信 HTTP 接続をキャッシュする例を示します。

```
ciscoasa(config)# url-cache src_dst 128
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド ステートメントを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-server	**filter** コマンドで使用する Websense サーバを指定します。

url-entry

ポータル ページで HTTP/HTTPS URL を入力する機能をイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **url-entry** コマンドを使用します。

url-entry enable | disable

enable | disable	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

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	トランスペアレント	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、Finance という DAP レコードで URL 入力をイネーブルにする例を示します。

```
ciscoasa (config) config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dynamic-access-policy-record)# url-entry enable
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-entry	アクセス先のファイル サーバの名前を入力する機能をイ ネーブルまたはディセーブルにします。

url-length-limit

RTSP メッセージで許可される URL の最大長を設定するには、パラメータ コンフィギュレーション モードで **url-length-limit** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能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。

url-length-limit *length*

no url-length-limit *length*

構文の説明

length	URL の長さ制限（バイト単位）。値の範囲は、0 ～ 6000 です。

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	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、RTSP インスペクション ポリシー マップで URL の長さ制限を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# url-length-limit 50
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

url-list

WebVPN サーバと URL のリストを特定のユーザまたはグループ ポリシーに適用するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **url-list** コマンドを使用します。**url-list none** コマンドを使用して作成したヌル値を含む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。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。URL リストが継承されないようにするには、**url-list none** コマンドを使用します。次回このコマンドを使用すると、前回までの設定が上書きされます。

url-list {**value** *name* | **none**} [*index*]

no url-list

構文の説明

index	ホームページ上の表示のプライオリティを指定します。
none	URL リストにヌル値を設定します。デフォルトまたは指定したグループ ポリシーからリストが継承されないようにします。
value *name*	設定済み URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

デフォルト

デフォルトの URL リストはありません。

コマンド モード

次の表に、このコマンドを入力す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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

次回このコマンドを使用すると、前回までの設定が上書きされます。

webvpn モードで **url-list** コマンドを使用してユーザまたはグループ ポリシーの WebVPN ホームページに表示する URL リストを指定する前に、XML オブジェクトでリストを作成する必要があります。グローバル コンフィギュレーション モードで **import** コマンドを使用して、URL リストをセキュリティ アプライアンスにダウンロードします。次に、url-list コマンドを使用して、リストを特定のグループ ポリシーまたはユーザに適用します。

例

次に、FirstGroupURLs という名前の URL リストを FirstGroup という名前のグループ ポリシーに適用し、このリストを 1 番めの URL リストに指定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# url-list value FirstGroupURLs 1
```

関連コマンド

コマンド	説明
clear configure url-list	すべての url-list コマンドをコンフィギュレーションから削除します。リスト名を含めると、ASA はそのリストのコマンドだけを削除します。
show running-configuration url-list	現在設定されている一連の **url-list** コマンドを表示します。
webvpn	webvpn モードを開始します。これは、webvpn コンフィギュレーション モード、グループ ポリシー webvpn コンフィギュレーション モード（特定のグループ ポリシーの webvpn 設定を行う場合）、またはユーザ名 webvpn コンフィギュレーション モード（特定のユーザの webvpn 設定を行う場合）のいずれかです。

url-server

filter コマンドで使用する N2H2 サーバまたは Websense サーバを指定するには、グローバル コンフィギュレーション モードで **url-server** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

N2H2

url-server [(*if_name*)] **vendor** {**smartfilter** | **n2h2**} **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** [connections *number*]} | **UDP**]

no url-server [(*if_name*)] **vendor** {**smartfilter** | **n2h2**} **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** [**connections** *number*]} | **UDP**]

Websense

url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]

no url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | *version*]

構文の説明

N2H2

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに作成される TCP 接続の最大数を指定します。この数はサーバごとであるため、複数のサーバに異なる接続値を指定できます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	(任意)認証サーバが存在するネットワーク インターフェイス。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。
port *number*	N2H2 サーバ ポート。ASA は、UDP 応答のリッスンもこのポート上で行います。デフォルトのポート番号は 4005 です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP です。
timeout *seconds*	許容される最大アイドル時間で、この時間が経過すると、ASA は指定した次のサーバに切り替わります。デフォルトは 30 秒です。
vendor	「smartfilter」または「n2h2」(下位互換性を維持するため)を使用して URL フィルタリング サービスを指定します。ただし、「smartfilter」はベンダー文字列として保存されます。

Websense

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに作成される TCP 接続の最大数を指定します。この数はサーバごとであるため、複数のサーバに異なる接続値を指定できます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	認証サーバが存在するネットワーク インターフェイス。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。
timeout *seconds*	許容される最大アイドル時間で、この時間が経過すると、ASA は指定した次のサーバに切り替わります。デフォルトは 30 秒です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP プロトコル バージョン 1 です。
vendor websense	URL フィルタリング サービスのベンダーが Websense であることを示します。
version	プロトコル バージョン **1** または **4** を指定します。デフォルトは TCP プロトコル バージョン 1 です。TCP は、バージョン 1 またはバージョン 4 を使用して設定できます。UDP は、バージョン 4 を使用してのみ設定できます。

デフォルト

このコマンドは、デフォルトで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	トランスペアレント	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	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

url-server コマンドでは、N2H2 または Websense URL フィルタリング アプリケーションを実行しているサーバを指定します。URL サーバ数の上限は、シングル コンテキスト モードでは 16、マルチ コンテキスト モードでは 4 ですが、一度に使用できるアプリケーションは、N2H2 または Websense のいずれか 1 つのみです。さらに、ASA 上でコンフィギュレーションを変更しても、アプリケーション サーバ上のコンフィギュレーションは更新されないため、ベンダーの指示に従って別途更新する必要があります。

HTTPS および FTP に対して **filter** コマンドを発行するには、事前に **url-server** コマンドを設定する必要があります。すべての URL サーバがサーバ リストから削除されると、URL フィルタリングに関連するすべての **filter** コマンドも削除されます。

サーバを指定した後、**filter url** コマンドを使用して URL フィルタリング サービスをイネーブルにします。

サーバの統計情報（到達不能サーバを含む）を表示するには、**show url-server statistics** コマンドを使用します。

次の手順を実行して、URL フィルタリングを行います。

ステップ 1 ベンダー固有の **url-server** コマンドの適切な形式を使用して、URL フィルタリング アプリケーション サーバを指定します。

ステップ 2 **filter** コマンドを使用して、URL フィルタリングをイネーブルにします。

ステップ 3 （任意）**url-cache** コマンドを使用して、URL キャッシングをイネーブルにし、認識される応答時間を短縮します。

ステップ 4 （任意）**url-block** コマンドを使用して、長い URL および HTTP バッファリングのサポートをイネーブルにします。

ステップ 5 **show url-block block statistics**、**show url-cache statistics**、または **show url-server statistics** コマンドを使用して、実行情報を表示します。

N2H2 によるフィルタリングの詳細については、次の N2H2 の Web サイトを参照してください。

http://www.n2h2.com

Websense フィルタリング サービスの詳細については、次の Web サイトを参照してください。

http://www.websense.com/

例

次に、N2H2 の使用時に 10.0.2.54 ホストからの接続を除くすべての発信 HTTP 接続をフィルタリングする例を示します。

```
ciscoasa(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、Websense の使用時に 10.0.2.54 ホストからの接続を除くすべての発信 HTTP 接続をフィルタリングする例を示します。

```
ciscoasa(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報をクリアします。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。

urgent-flag

TCP ノーマライザを通して URG ポインタを許可またはクリアするには、tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

構文の説明

allow	TCP ノーマライザを通して URG ポインタを許可します。
clear	TCP ノーマライザを通して URG ポインタをクリアします。

デフォルト

緊急フラグおよび緊急オフセットはデフォルトでクリアされます。

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	トランスペアレント	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用して、緊急フラグを許可します。

URG フラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCP RFC では、URG フラグの正確な解釈を明確化していません。したがって、エンド システムにおいては緊急オフセットがさまざまな方法で処理されます。このため、エンド システムが攻撃を受けやすくなります。デフォルトの動作では、URG フラグとオフセットはクリアされます。

例

次に、緊急フラグを許可する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 513
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

user

アイデンティティ ファイアウォール機能をサポートするユーザ グループ オブジェクトでユーザを作成するには、ユーザ グループ オブジェクト コンフィギュレーション モードで **user** コマンドを使用します。オブジェクトからユーザを削除するには、このコマンドの **no** 形式を使用します。

user [*domain_nickname*\]*user_name*

[no] user [*domain_nickname*\]*user_name*

構文の説明

domain_nickname	(オプション)ユーザを追加するドメインを指定します。
user_name	ユーザの名前を指定します。ユーザ名には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。ユーザ名にスペースを含める場合は、名前全体を引用符で囲みます。 **user** キーワードとともに指定する *user_name* 引数には ASCII ユーザ名が含まれ、IP アドレスは指定されません。

デフォルト

domain_nickname 引数を指定しない場合、ユーザはアイデンティティ ファイアウォール機能用に設定された LOCAL ドメインに作成されます。

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	トランスペアレント	シングル	コンテキスト	システム
オブジェクト グループ ユーザ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、Active Directory ドメイン コントローラでグローバルに定義されているユーザ グループについて、Active Directory サーバに LDAP クエリーを送信します。これらのグループは、ASA によりアイデンティティ ファイアウォール機能用にインポートされます。ただし、ローカライズされたセキュリティ ポリシーを持つローカル ユーザ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル ユーザ グループには、Active Directory からインポートされる、ネストされたグループおよびユーザ グループを含めることができます。ASA は、ローカル グループおよび Active Directory グループを統合します。ユーザは、ローカル ユーザ グループと Active Directory からインポートされたユーザ グループに属することができます。

ASA は、最大 256 のユーザ グループをサポートします(インポートされたユーザ グループとローカル ユーザ グループを含む)。

アクセス グループ、キャプチャ、またはサービス ポリシー内に含めることによって、ユーザ グループ オブジェクトをアクティブにします。

ユーザ グループ オブジェクト内で、次のオブジェクト タイプを定義できます。

- **ユーザ**:オブジェクト グループ ユーザに単一のユーザを追加します。ユーザは、ローカル ユーザまたはインポートされたユーザを追加できます。

  インポートされたユーザの名前は、一意でない可能性がある一般名(cn)ではなく、一意の sAMAccountName にする必要があります。ただし、一部の Active Directory サーバ管理者は、sAMAccountName と cn を同一にすることが必要な場合があります。この場合、ASA によって **show user-identity ad-group-member** コマンドの出力に表示される cn を、ユーザ オブジェクトで定義したインポートされたユーザに使用できます。

- **ユーザ グループ**:Microsoft Active Directory サーバなどの外部ディレクトリ サーバによって定義されたインポートされたユーザ グループをグループ オブジェクト ユーザに追加します。

  ユーザ グループのグループ名は、一意でない可能性がある cn ではなく、一意の sAMAccountName にする必要があります。ただし、一部の Active Directory サーバ管理者は、sAMAccountName と cn を同一にすることが必要な場合があります。この場合、ASA によって **show user-identity ad-group-member** コマンドの出力に表示される cn を、*user-group* キーワードで指定される **user_group_name** 引数で使用できます。

  (注) *domain_nickname**user_group_name* または *domain_nickname**user_ name* を最初にオブジェクトで指定せずに、ユーザ グループ オブジェクト内に直接追加できます。*domain_nickname* が AAA サーバに関連付けられている場合、ユーザ オブジェクト グループがアクティブ化されると、ASA は詳細なネストされたユーザ グループおよび Microsoft Active Directory サーバなどの外部ディレクトリ サーバで定義されたユーザを ASA にインポートします。

- **グループ オブジェクト**:ASA でローカルに定義されたグループをオブジェクト グループ ユーザに追加します。

  (注) オブジェクト グループ ユーザ オブジェクト内にオブジェクト グループを含める場合、ACL 最適化をイネーブルにした場合にも、ASA はアクセス グループ内のオブジェクト グループを拡張しません。**show object-group** コマンドの出力には、ヒット数は表示されません。ヒット数は、ACL 最適化がイネーブルの場合に、通常のネットワーク オブジェクト グループについてのみ取得できます。

- **説明**:オブジェクト グループ ユーザの説明を追加します。

例

次に、**user** コマンドを **user-group object** コマンドとともに使用して、アイデンティティ ファイアウォール機能で使用するユーザ グループ オブジェクトにユーザを追加する例を示します。

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
```

```
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

関連コマンド

コマンド	説明
description	**object-group user** コマンドで作成されたグループに説明を追加します。
group-object	ローカルで定義されたオブジェクト グループをアイデンティティ ファイアウォール機能で使用するために **object-group user** コマンドで作成されたユーザ オブジェクト グループに追加します。
object-group user	アイデンティティ ファイアウォール機能用のユーザ グループ オブジェクトを作成します。
user-group	Microsoft Active Directory からインポートされたユーザ グループを **object-group user** コマンドで作成されたグループに追加します。
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

user-alert

現在のアクティブ セッションのすべてのクライアントレス SSL VPN ユーザに対して、緊急メッセージのブロードキャストをイネーブルにするには、特権 EXEC モードで **user-alert** コマンドを使用します。メッセージ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。

user-alert *string cancel*

no user-alert

構文の説明

cancel	ポップアップ ブラウザ ウィンドウの起動を取り消します。
string	英数字。

デフォルト

メッセージなし。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを発行すると、設定されたメッセージを含むポップアップ ブラウザ ウィンドウがエンドユーザに表示されます。このコマンドでは、ASA コンフィギュレーション ファイルは変更されません。

例

次の例は、DAP トレース デバッグをイネーブルにする方法を示しています。

```
ciscoasa # We will reboot the security appliance at 11:00 p.m. EST time. We apologize for
any inconvenience.
ciscoasa #
```

user-authentication

ユーザ認証をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **user-authentication enable** コマンドを使用します。ユーザ認証をディセーブルにするには、**user-authentication disable** コマンドを使用します。実行コンフィギュレーションからユーザ認証属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーからユーザ認証の値を継承できます。

ユーザ認証をイネーブルにすると、ハードウェア クライアントの背後にいる個々のユーザは、トンネルを介してネットワークにアクセスするために認証を受けることが必要となります。

user-authentication {**enable** | **disable**}

no user-authentication

構文の説明

disable	ユーザ認証をディセーブルにします。
enable	ユーザ認証をイネーブルにします。

デフォルト

ユーザ認証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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

個々のユーザは、設定した認証サーバの順序に従って認証されます。

プライマリ ASA でユーザ認証が必要な場合は、バックアップ サーバでも同様にユーザ認証を設定する必要があります。

例

次の例は、「FirstGroup」という名前のグループ ポリシーのユーザ認証をイネーブルにする方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# user-authentication enable
```

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を行わずに IP 電話に接続できるようにします。セキュア ユニット認証は有効なままです。
leap-bypass	イネーブルにすると、VPN クライアントの背後にある無線デバイスからの LEAP パケットは、ユーザ認証の前に VPN トンネルを通過します。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。その後、ユーザ認証ごとに再度認証を行います。
secure-unit-authentication	VPN クライアントに、トンネルを開始するたびにユーザ名とパスワードによる認証を要求することによって、セキュリティを強化します。
user-authentication-idle-timeout	個々のユーザのアイドル タイムアウトを設定します。アイドル タイムアウト期間内にユーザ接続上で通信アクティビティが行われない場合、ASA によって接続が切断されます。

user-authentication-idle-timeout

ハードウェア クライアントの背後にいる個々のユーザに対してアイドル タイムアウトを設定するには、グループ ポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを使用します。アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーからアイドル タイムアウト値を継承できます。アイドル タイムアウト値が継承されないようにするには、**user-authentication-idle-timeout none** コマンドを使用します。

アイドル タイムアウト期間内にハードウェア クライアントの背後にいるユーザによって通信アクティビティが行われない場合、ASA によって接続が切断されます。

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

構文の説明

minutes	アイドル タイムアウト期間の分数を指定します。指定できる範囲は 1 ～ 35791394 分です。
none	無制限のアイドル タイムアウト期間を許可します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトまたは指定したグループ ポリシーからユーザ認証のアイドル タイムアウト値が継承されないようにします。

デフォルト

30 分。

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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

最小値は 1 分、デフォルトは 30 分、最大値は 10,080 分です。

このタイマーは、VPN トンネル自体ではなく、VPN トンネルを通過するクライアントのアクセスだけを終了します。

show uauth コマンドへの応答で示されるアイドル タイムアウトは、常に Cisco Easy VPN リモート デバイスのトンネルを認証したユーザのアイドル タイムアウト値になります。

例

次の例は、「FirstGroup」という名前のグループ ポリシーに 45 分のアイドル タイムアウト値を設定する方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# user-authentication-idle-timeout 45
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前に ASA に識別情報を示すように要求します。

user-group

Microsoft Active Directory からインポートされたユーザ グループをアイデンティティ ファイアウォール機能で使用するために **object-group user** コマンドで作成されたグループに追加するには、**ユーザ グループ オブジェクト** コンフィギュレーション モードで **user-group** コマンドを使用します。オブジェクトからユーザ グループを削除するには、このコマンドの **no** 形式を使用します。

user-group [*domain_nickname*\]*user_group_name*

[no] user-group [*domain_nickname*\]*user_group_name*

構文の説明

domain_nickname	(オプション)ユーザ グループを作成するドメインを指定します。
user_group_name	ユーザ グループの名前を指定します。グループ名には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。グループ名にスペースを含める場合は、名前全体を引用符で囲みます。

デフォルト

domain_nickname 引数を指定しない場合、ユーザ グループはアイデンティティ ファイアウォール機能用に設定された LOCAL ドメインに作成されます。

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	トランスペアレント	シングル	コンテキスト	システム
オブジェクト グループ ユーザ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、Active Directory ドメイン コントローラでグローバルに定義されているユーザ グループについて、Active Directory サーバに LDAP クエリーを送信します。これらのグループは、ASA によりアイデンティティ ファイアウォール機能用にインポートされます。ただし、ローカライズされたセキュリティ ポリシーを持つローカル ユーザ グループを必要とする、グローバルに定義されていないネットワーク リソースが ASA によりローカライズされている場合があります。ローカル ユーザ グループには、Active Directory からインポートされる、ネストされたグループおよびユーザ グループを含めることができます。ASA は、ローカル グループおよび Active Directory グループを統合します。ユーザは、ローカル ユーザ グループと Active Directory からインポートされたユーザ グループに属することができます。

ASA は、最大 256 のユーザ グループをサポートします(インポートされたユーザ グループとローカル ユーザ グループを含む)。

アクセス グループ、キャプチャ、またはサービス ポリシー内に含めることによって、ユーザ グループ オブジェクトをアクティブにします。

ユーザ グループ オブジェクト内で、次のオブジェクト タイプを定義できます。

- **ユーザ**:オブジェクト グループ ユーザに単一のユーザを追加します。ユーザは、ローカル ユーザまたはインポートされたユーザを追加できます。

  インポートされたユーザの名前は、一意でない可能性がある一般名(cn)ではなく、一意の sAMAccountName にする必要があります。ただし、一部の Active Directory サーバ管理者は、sAMAccountName と cn を同一にすることが必要な場合があります。この場合、ASA によって **show user-identity ad-group-member** コマンドの出力に表示される cn を、ユーザ オブジェクトで定義したインポートされたユーザに使用できます。

- **ユーザ グループ**:Microsoft Active Directory サーバなどの外部ディレクトリ サーバによって定義されたインポートされたユーザ グループをグループ オブジェクト ユーザに追加します。

  ユーザ グループのグループ名は、一意でない可能性がある cn ではなく、一意の sAMAccountName にする必要があります。ただし、一部の Active Directory サーバ管理者は、sAMAccountName と cn を同一にすることが必要な場合があります。この場合、ASA によって **show user-identity ad-group-member** コマンドの出力に表示される cn を、*user-group* キーワードで指定される **user_group_name** 引数で使用できます。

  (注) *domain_nickname**user_group_name* または *domain_nickname**user_ name* を最初にオブジェクトで指定せずに、ユーザ グループ オブジェクト内に直接追加できます。*domain_nickname* が AAA サーバに関連付けられている場合、ユーザ オブジェクト グループがアクティブ化されると、ASA は詳細なネストされたユーザ グループおよび Microsoft Active Directory サーバなどの外部ディレクトリ サーバで定義されたユーザを ASA にインポートします。

- **グループ オブジェクト**:ASA でローカルに定義されたグループをオブジェクト グループ ユーザに追加します。

  (注) オブジェクト グループ ユーザ オブジェクト内にオブジェクト グループを含める場合、ACL 最適化をイネーブルにした場合にも、ASA はアクセス グループ内のオブジェクト グループを拡張しません。**show object-group** コマンドの出力には、ヒット数は表示されません。ヒット数は、ACL 最適化がイネーブルの場合に、通常のネットワーク オブジェクト グループについてのみ取得できます。

- **説明**:オブジェクト グループ ユーザの説明を追加します。

例

次に、**user-group** コマンドを **user-group object** コマンドとともに使用して、アイデンティティ ファイアウォール機能で使用するユーザ グループ オブジェクトにユーザ グループを追加する例を示します。

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
```

```
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

関連コマンド

コマンド	説明
description	**object-group user** コマンドで作成されたグループに説明を追加します。
group-object	ローカルで定義されたオブジェクト グループをアイデンティティ ファイアウォール機能で使用するために **object-group user** コマンドで作成されたユーザ オブジェクト グループに追加します。
object-group user	アイデンティティ ファイアウォール機能用のユーザ グループ オブジェクトを作成します。
user	**object-group user** コマンドで作成されたオブジェクト グループにユーザを追加します。
user-identity enable	Cisco Identity Firewall インスタンスを作成します。

user-identity action ad-agent-down

Active Directory エージェントが応答不能の場合の Cisco Identity Firewall インスタンスに対するアクションを設定するには、グローバル コンフィギュレーション モードで **user-identity action ad-agent-down** コマンドを使用します。アイデンティティ ファイアウォール インスタンスに対するこのアク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。

user-identity action ad-agent-down disable-user-identity-rule

no user-identity action ad-agent-down disable-user-identity-rule

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、このコマンド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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

AD エージェントが応答していない場合のアクションを指定します。

AD エージェントがダウンし、**user-identity action ad-agent-down** コマンドが設定されている場合、ASA はそのドメインのユーザに関連付けられたユーザ アイデンティティ ルールをディセーブルにします。さらに、**show user-identity user** コマンドによって表示される出力では、そのドメイン内のすべてのユーザ IP アドレスがディセーブルとマークされます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションをイネーブルにする例を示します。

```
ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity action domain-controller-down

Active Directory ドメイン コントローラが応答不能の場合の Cisco Identity Firewall インスタンスに対するアクションを設定するには、グローバル コンフィギュレーション モードで **user-identity action domain-controller-down** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**

no user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**

構文の説明

domain_nickname	アイデンティティ ファイアウォールのドメイン名を指定します。

デフォルト

デフォルトでは、このコマンド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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

Active Directory ドメイン コントローラが応答しないためにドメインがダウンしている場合のアクションを指定します。

ドメインがダウンし、**disable-user-identity-rule** キーワードが設定されている場合、ASA はそのドメインのユーザ アイデンティティと IP アドレスのマッピングをディセーブルにします。さらに、**show user-identity user** コマンドによって表示される出力では、そのドメイン内のすべてのユーザ IP アドレスがディセーブルとマークされます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションを設定する例を示します。

```
ciscoasa(config)# user-identity action domain-controller-down SAMPLE
disable-user-identity-rule
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity action mac-address-mismatch

ユーザの MAC アドレスが ASA デバイス IP アドレスと一致しないことが明らかになった場合の Cisco Identity Firewall インスタンスに対するアクションを設定するには、グローバル コンフィギュレーション モードで **user-identity action mac-address mismatch** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

user-identity action mac-address mismatch remove-user-ip

no user-identity action mac-address mismatch remove-user-ip

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、このコマンドが指定されている場合、ASA は **remove-user-ip** を使用します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ユーザの MAC アドレスが、そのアドレスに現在マッピングされている ASA デバイス IP アドレスと一致しないことが明らかになった場合のアクションを指定します。このアクションは、ユーザ アイデンティティ ルールの効果を無効にします。

user-identity action mac-address-mismatch コマンドが設定されている場合、ASA はそのクライアントのユーザ アイデンティティと IP アドレスのマッピングを削除します。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity action mac-address-mismatch remove-user-ip
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity action netbios-response-fail

クライアントが NetBIOS プローブに応答しない場合の Cisco Identity Firewall インスタンスに対するアクションを設定するには、グローバル コンフィギュレーション モードで **user-identity action netbios-response-fail** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

user-identity action netbios-response-fail remove-user-ip

no user-identity action netbios-response-fail remove-user-ip

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、このコマンド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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

クライアントが NetBIOS プローブに応答しない場合のアクションを指定します。このような状況には、そのクライアントへのネットワーク接続がブロックされている場合やクライアントがアクティブでない場合などがあります。

user-identity action remove-user-ip コマンドを設定すると、ASA は、そのクライアントのユーザアイデンティティと IP アドレスのマッピングを削除します。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity ad-agent aaa-server

Cisco Identity Firewall インスタンスの AD エージェントのサーバ グループを定義するには、AAA サーバ ホスト コンフィギュレーション モードで **user-identity ad-agent aaa-server** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*

no user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*

構文の説明

aaa_server_group_tag	アイデンティティ ファイアウォールに関連付けられた AAA サーバ グループを指定します。

デフォルト

このコマンドには、デフォルトはありません。

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	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

aaa_server_group_tag 変数に定義する最初のサーバがプライマリ AD エージェントとなり、次に定義するサーバがセカンダリ AD エージェントとなります。

アイデンティティ ファイアウォールでは、2 つの AD エージェント ホストのみ定義できます。

プライマリ AD エージェントがダウンしていることを ASA が検出し、セカンダリ AD エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの AAA サーバは通信プロトコルとして RADIUS を使用するため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

例

次に、アイデンティティ ファイアウォールの AD エージェントの AAA サーバ ホストを定義する例を示します。

```
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity ad-agent active-user-database

ASA が Cisco Identity Firewall インスタンスの AD エージェントからユーザ アイデンティティと IP アドレスのマッピング情報を取得する方法を定義するには、グローバル コンフィギュレーション モードで **user-identity ad-agent active-user-database** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

user-identity ad-agent active-user-database {**on-demand** | **full-download**}

no user-identity ad-agent active-user-database {**on-demand** | **full-download**}

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、ASA 5505 は on-demand オプションを使用します。それ以外の ASA プラットフォームは full-download オプションを使用します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA が AD エージェントからユーザ アイデンティティと IP アドレスのマッピング情報を取得する方法を定義します。

- **full-download**：ASA が、ASA の起動時に IP/ユーザ マッピング テーブル全体をダウンロードし、ユーザのログインおよびログアウト時に増分 IP/ユーザ マッピングを受信するように指示する要求を AD エージェントに送信することを指定します。
- **on-demand**：ASA が新しい接続を必要とするパケットを受信し、その送信元 IP アドレスのユーザがユーザ アイデンティティ データベースに含まれていない場合に、ASA が AD エージェントから IP アドレスのユーザ マッピング情報を取得することを指定します。

デフォルトでは、ASA 5505 は on-demand オプションを使用します。それ以外の ASA プラットフォームは full-download オプションを使用します。

フル ダウンロードはイベント ドリブンです。つまり、2 回目以降のデータベース ダウンロード要求は、ユーザ アイデンティティと IP アドレス マッピング データベースの更新内容だけを送信します。

ASA が変更要求を AD エージェントに登録すると、AD エージェントは新しいイベントを ASA に送信します。

例

次に、アイデンティティ ファイアウォールに対してこのオプションを設定する例を示します。

```
ciscoasa(config)# user-identity ad-agent active-user-database full-download
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity ad-agent hello-timer

ASA と Cisco Identity Firewall インスタンスの AD エージェントとの間のタイマーを定義するには、グローバル コンフィギュレーション モードで **user-identity ad-agent hello-timer** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

no user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

構文の説明

number	タイマーのリトライ回数を指定します。
seconds	タイマーの時間の長さを指定します。

デフォルト

デフォルトでは、Hello タイマーは間隔が 30 秒、リトライ回数が 5 回に設定されます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA と AD エージェントとの間の Hello タイマーを定義します。

ASA と AD エージェントとの間の Hello タイマーは、ASA が hello パケットを交換する頻度を定義します。ASA は、hello パケットを使用して、ASA 複製ステータス（in-sync または out-of-sync）とドメイン ステータス（up または down）を取得します。ASA は、AD エージェントから応答を受信しなかった場合、指定された間隔が経過した後、hello パケットを再送信します。

デフォルトでは、Hello タイマーは間隔が 30 秒、リトライ回数が 5 回に設定されます。

例

次に、アイデンティティ ファイアウォールに対してこのオプションを設定する例を示します。

```
ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity ad-agent event-timestamp-check

認可変更リプレイ アタックから ASA を保護するために RADIUS イベント タイムスタンプ チェック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 **user-identity ad-agent event-timestamp-check** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

user-identity ad-agent event-timestamp-check

no user-identity ad-agent event-timestamp-check

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

デフォルト設定では無効になっています。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ASA が受信する各 ID の最後のイベントのタイムスタンプを追跡し、イベントのタイムスタンプが ASA のクロックより 5 分以上古い場合、またはメッセージのタイムスタンプが最後のイベントのタイムスタンプよりも前の場合にメッセージを廃棄することを可能にします。

最後のイベントのタイムスタンプの情報を持たない新しく起動した ASA の場合、ASA は自身のクロックとイベントのタイムスタンプを比較します。イベントから少なくとも 5 分以上経過している場合、ASA はメッセージを受け入れません。

（注） NTP を使用して、ASA、Active Directory、および Active Directory エージェントをそれらのクロックが相互に同期するように設定することを推奨します。

例

次に、アイデンティティ ファイアウォールにイベント タイムスタンプ チェックを設定する例を示します。

```
ciscoasa(config)# user-identity ad-agent event-timestamp-check
```

関連コマンド

コマンド	説明
user-identity ad-agent hello-timer	ASA と Cisco Identity Firewall インスタンスの AD エージェントとの間のタイマーを定義します。

user-identity default-domain

Cisco Identity Firewall インスタンスのデフォルト ドメインを指定するには、グローバル コンフィギュレーション モードで **user-identity default-domain** コマンドを使用します。デフォルト ドメインを削除するには、このコマンドの **no** 形式を使用します。

user-identity default-domain *domain_NetBIOS_name*

no user-identity default-domain *domain_NetBIOS_name*

構文の説明

domain_NetBIOS_name	アイデンティティ ファイアウォールのデフォルト ドメインを指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

domain_NetBIOS_name には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.] で構成される最大 32 文字の名前を入力します。ただし、先頭に「.」と「 」(スペース) を使用することはできません。ドメイン名にスペースを含める場合は、名前全体を引用符で囲みます。ドメイン名では、大文字と小文字が区別されません。

デフォルト ドメインは、ユーザまたはグループにドメインが明示的に設定されていない場合に、すべてのユーザおよびユーザ グループで使用されます。デフォルト ドメインを指定しない場合、ユーザおよびグループのデフォルト ドメインは LOCAL となります。マルチ コンテキスト モードでは、システム実行スペース内だけでなく、各コンテキストについてデフォルト ドメイン名を設定できます。

（注） 指定するデフォルト ドメイン名は、Active Directory ドメイン コントローラに設定された NetBIOS ドメイン名と一致している必要があります。ドメイン名が一致しない場合、AD エージェントは、ユーザ アイデンティティと IP アドレスのマッピングを ASA の設定時に入力されたドメイン名に誤って関連付けます。NetBIOS ドメイン名を表示するには、任意のテキスト エディタで Active Directory ユーザ イベント セキュリティ ログを開きます。

アイデンティティ ファイアウォールは、ローカルに定義されたすべのユーザ グループまたはユーザに対して LOCAL ドメインを使用します。Web ポータル（カットスルー プロキシ）経由でログインしたユーザは、認証された Active Directory ドメインに属すると見なされます。VPN 経由でログインしたユーザは、VPN が Active Directory で LDAP によって認証される場合を除き、LOCAL ドメインに属するユーザと見なされます。これにより、アイデンティティ ファイアウォールはユーザをそれぞれの Active Directory ドメインに関連付けることができます。

例

次に、アイデンティティ ファイアウォールのデフォルト ドメインを設定する例を示します。

```
ciscoasa(config)# user-identity default-domain SAMPLE
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity domain

Cisco Identity Firewall インスタンスのドメインを関連付けるには、グローバル コンフィギュレーション モードで **user-identity domain** コマンドを使用します。ドメインの関連付けを削除するには、このコマンドの **no** 形式を使用します。

user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*

no user-identity *domain_nickname* **aaa-server** *aaa_server_group_tag*

構文の説明

aaa_server_group_tag	アイデンティティ ファイアウォールに関連付けられた AAA サーバ グループを指定します。
domain_nickname	アイデンティティ ファイアウォールのドメイン名を指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

AAA サーバでユーザ グループ クエリーのインポート用に定義された LDAP パラメータをドメイン名に関連付けます。

domain_nickname には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_=+[]{};,.] で構成される最大 32 文字の名前を入力します。ただし、先頭に「.」と「 」(スペース)を使用することはできません。ドメイン名にスペースを含める場合は、スペースを引用符で囲む必要があります。ドメイン名では、大文字と小文字が区別されません。

例

次に、アイデンティティ ファイアウォールのドメインを関連付ける例を示します。

```
ciscoasa(config)# user-identity domain SAMPLE aaa-server ds
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity enable

Cisco Identity Firewall インスタンスを作成するには、グローバル コンフィギュレーション モードで **user-identity enable** コマンドを使用します。アイデンティティ ファイアウォール インスタンス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。

user-identity enable

no user-identity 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

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、アイデンティティ ファイアウォールをイネーブルにします。

例

次に、アイデンティティ ファイアウォールをイネーブルにする例を示します。

```
ciscoasa(config)# user-identity enable
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity inactive-user-timer

Cisco Identity Firewall インスタンスでユーザがアイドル状態であると見なされるまでの時間を指定するには、グローバル コンフィギュレーション モードで **user-identity inactive-user-timer** コマンドを使用します。タイマーを削除するには、このコマンドの **no** 形式を使用します。

user-identity inactive-user-timer minutes *minutes*

no user-identity inactive-user-timer minutes *minutes*

構文の説明

minutes	ユーザがアイドル状態であると見なされるまでの時間を分単位で指定します。これは、ASA が指定された時間にわたりユーザの IP アドレスからトラフィックを受信しなかった場合を意味します。

デフォルト

デフォルトでは、アイドル タイムアウトは 60 分に設定されます。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

タイマーの期限が切れると、ユーザの IP アドレスが非アクティブとマークされ、ローカル キャッシュ内のユーザ アイデンティティと IP アドレスのマッピング データベースから削除されます。ASA は、この IP アドレスの削除を AD エージェントに通知しません。既存のトラフィックは通過を許可されます。このコマンドを指定すると、ASA は NetBIOS ログアウト プローブが設定されている場合でも非アクティブ タイマーを実行します。

(注) アイドル タイムアウト オプションは VPN ユーザまたはカットスルー プロキシ ユーザには適用されません。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity inactive-user-timer minutes 120
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity logout-probe

Cisco Identity Firewall インスタンスに対する NetBIOS プローブ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 **user-identity logout-probe** コマンドを使用します。プローブを削除して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。

user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed | match-any | exact-match**]

no user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed | match-any | exact-match**]

構文の説明

minutes	プローブ間隔を分単位で指定します。
seconds	リトライ インターバルの時間の長さを指定します。
times	プローブのリトライ回数は、次のように指定してください。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

NetBIOS パケットを最小限に抑えるために、ASA は、ユーザが指定された分数を超えてアイドル状態である場合のみ NetBIOS プローブをクライアントに送信します。

NetBIOS プローブ タイマーを 1 ～ 65535 分に設定し、リトライ インターバルを 1 ～ 256 回に設定します。プローブのリトライ回数は、次のように指定してください。

- **match-any**：クライアントからの NetBIOS 応答に IP アドレスに割り当てられたユーザのユーザ名が含まれている場合、ユーザ アイデンティティは有効と見なされます。このオプションを指定するためには、クライアントで Messenger サービスがイネーブルになっており、WINS サーバが設定されている必要があります。

- **exact-match**：NetBIOS 応答に IP アドレスに割り当てられたユーザのユーザ名だけが含まれている必要があります。そうでない場合、その IP アドレスのユーザ アイデンティティは無効と見なされます。このオプションを指定するためには、クライアントで Messenger サービスがイネーブルになっており、WINS サーバが設定されている必要があります。
- **user-not-needed**：ASA がクライアントから NetBIOS 応答を受信した場合、ユーザ アイデンティティは有効と見なされます。

アイデンティティ ファイアウォールは、少なくとも 1 つのセキュリティ ポリシーに存在するアクティブ状態のユーザ アイデンティティに対してのみ NetBIOS プローブを実行します。ASA は、ユーザがカットスルー プロキシ経由または VPN を使用してログインするクライアントについては、NetBIOS プローブを実行しません。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10
retry-interval seconds 10 retry-count 2 user-not-needed
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity monitor

クラウド Web セキュリティのために、指定されたユーザまたはグループの情報を AD エージェントからダウンロードするには、グローバル コンフィギュレーション モードで user-identity monitor コマンドを使用します。モニタリングを停止にするには、このコマンドの **no** 形式を使用します。

user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*}

no user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*}

構文の説明

object-group-user *object-group-name*	オブジェクト グループ ユーザ名を指定します。このグループには、複数のグループを含めることができます。
user-group [*domain-name*\\] *group-name*	グループ名をインラインで指定します。ドメインとグループの間に 2 つのバックスラッシュ (\\) を指定しますが、ASA は、クラウド Web セキュリティへの送信時に、クラウド Web セキュリティの表記規則に準拠するようにバックスラッシュが 1 つのみ含まれるように名前を変更します。

コマンド 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォール機能を使用する場合、ASA は、アクティブな ACL に含まれるユーザおよびグループの AD サーバからのユーザ アイデンティティ情報のみをダウンロードします。ACL は、アクセス ルール、AAA ルール、サービス ポリシー ルール、またはアクティブと見なされるその他の機能で使用する必要があります。クラウド Web セキュリティでは、そのポリシーがユーザ アイデンティティに基づくことができるため、すべてのユーザに対する完全なアイデンティティ ファイアウォール カバレッジを取得するには、アクティブな ACL の一部ではないグループをダウンロードする必要があります。たとえば、ユーザおよびグループを含む ACL を使用するようにクラウド Web セキュリティ サービス ポリシー ルールを設定し、関連するグループをアクティブ化できますが、これは必須ではありません。IP アドレスのみに基づく ACL を使用できます。ユーザ アイデンティティ モニタ機能では、AD エージェントからグループ情報を直接ダウンロードすることができます。

ASA は、ユーザ アイデンティティ モニタ用に設定されたグループ、アクティブな ACL によってモニタされているグループも含めて 512 以下のグループモニタできます。

例

次に、CISCO\\Engineering ユーザ グループをモニタする例を示します。

```
ciscoasa(config)# user-identity monitor user-group CISCO\\Engineering
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。

コマンド	説明
show scansafe statistics	合計と現在の HTTP 接続を表示します。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

user-identity poll-import-user-group-timer

ASA が Active Directory サーバに Cisco Identity Firewall インスタンスのユーザ グループ情報を問い合わせるまでの時間を指定するには、グローバル コンフィギュレーション モードで **user-identity poll-import-user-group-timer** コマンドを使用します。タイマーを削除するには、このコマンドの **no** 形式を使用します。

user-identity poll-import-user-group-timer hours *hours*

no user-identity poll-import-user-group-timer hours *hours*

構文の説明

hours	poll タイマーの時間を設定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA が Active Directory サーバにユーザ グループ情報を問い合わせるまでの時間を指定します。

Active Directory グループでユーザが追加または削除されると、ASA はグループ インポート タイマーの実行後に更新されたユーザ グループを受け取ります。

デフォルトでは、poll タイマーは 8 時間です。

ユーザ グループ情報をただちに更新するには、**user-identity update import-user** コマンドを入力します。

例

次に、アイデンティティ ファイアウォールを設定する例を示します。

```
ciscoasa(config)# user-identity poll-import-user-group-timer hours 1
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity static user

新しいユーザと IP アドレスのマッピングを作成するか、Cisco Identity Firewall 機能でユーザの IP アドレスを非アクティブに設定するには、グローバル コンフィギュレーション モードで **user-identity static user** コマンドを使用します。アイデンティティ ファイアウォールでこの設定を削除するには、このコマンドの **no** 形式を使用します。

user-identity static user [*domain*\] *user_name host_ip*

no user-identity static user [*domain*\] *user_name host_ip*

構文の説明

domain	新しいユーザと IP アドレスのマッピングを作成するか、指定したドメインのユーザの IP アドレスを非アクティブに設定します。
host_ip	新しいユーザと IP アドレスのマッピングを作成するか、非アクティブに設定するユーザの IP アドレスを指定します。
user_name	新しいユーザと IP アドレスのマッピングを作成するか、IP アドレスを非アクティブに設定するユーザのユーザ名を指定します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには使用上のガイドラインはありません。

例

次に、user1 の静的マッピングを作成する例を示します。

```
ciscoasa(config)# user-identity static user SAMPLE\user1 192.168.1.101
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity update active-user-database

Active Directory エージェントからアクティブ ユーザ データベース全体をダウンロードするには、グローバル コンフィギュレーション モードで **user-identity update active-user-database** コマンドを使用します。

user-identity update active-user-database [**timeout minutes** *minutes*]

構文の説明

minutes	タイムアウトの分数を指定します。

デフォルト

デフォルトのタイムアウトは 5 分です。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Active Directory エージェントからアクティブ ユーザ データベース全体をダウンロードします。

このコマンドは、更新処理を開始し、更新開始ログを生成して即座に返します。更新処理が終了するか、タイマーの期限切れで中断すると、別の syslog メッセージが生成されます。1 つの未処理の更新処理だけが許可されます。コマンドを再実行すると、エラー メッセージが表示されます。

コマンドの実行が終了すると、ASA によってコマンド プロンプトに [Done] が表示され、syslog メッセージが生成されます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションをイネーブルにする例を示します。

```
ciscoasa# user-identity update active-user-database
ERROR: one update active-user-database operation is already in progress
[Done] user-identity update active-user-database
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity update import-user

Active Directory エージェントからアクティブ ユーザ データベース全体をダウンロードするには、グローバル コンフィギュレーション モードで **user-identity update active-user-database** コマンドを使用します。

user-identity update import-user [[*domain_nickname*\\] *user_group_name* [**timeout seconds** *seconds*]]

構文の説明

domain_nickname	更新するグループのドメインを指定します。
seconds	タイムアウトの秒数を指定します。
user_group_name	*user_group_name* を指定した場合、指定したインポート ユーザ グループだけが更新されます。アクティブ化されたグループのみ(たとえば、アクセス グループ、アクセス リスト、キャプチャ、サービス ポリシー内のグループ)を更新することができます。 指定したグループがアクティブ化されていない場合、このコマンドは処理を拒否します。指定したグループに複数の階層レベルがある場合は、再帰 LDAP クエリーが実行されます。 *user_group_name* を指定しない場合、ASA は LDAP 更新サービスを即座に開始し、すべてのアクティブ化されたグループの更新を定期的に試行します。

デフォルト

ASA は更新を最大 5 回再試行し、必要に応じて警告メッセージを生成します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ポーリング インポート ユーザ グループ タイマーの満了を待たずに即時に Active Directory サーバを照会して、指定されたインポート ユーザ グループ データベースを更新します。ローカル ユーザ グループで設定が変更されるたびにグループ ID データベースが更新されるため、ローカル ユーザ グループを更新するコマンドはありません。

このコマンドは、コンソールが LDAP クエリーの戻りを待機することを妨げません。

このコマンドは、更新処理を開始し、更新開始ログを生成して即座に返します。更新処理が終了するか、タイマーの期限切れで中断すると、別の syslog メッセージが生成されます。1 つの未処理の更新処理だけが許可されます。コマンドを再実行すると、エラー メッセージが表示されます。

LDAP クエリーが成功した場合、ASA は取得したユーザ データをローカル データベースに保存し、ユーザ/グループの関連付けを必要に応じて変更します。更新処理が成功した場合、**show user-identity user-of-group** *domain**group* コマンドを実行して、このグループの下に保存されたすべてのユーザを一覧表示できます。

ASA は、各アップデート後に、インポートされたすべてのグループをチェックします。アクティブ化された Active Directory グループが Active Directory に存在しない場合、ASA は syslog メッセージを生成します。

user_group_name を指定しない場合、ASA は LDAP 更新サービスを即座に開始し、すべてのアクティブ化されたグループの更新を定期的に試行します。LDAP 更新サービスはバックグラウンドで実行され、Active Directory サーバで LDAP クエリーによってインポート ユーザ グループを定期的に更新します。

システムのブートアップ時に、アクセス グループで定義されたインポート ユーザ グループがある場合、ASA は LDAP クエリーによってユーザ/グループ データを取得します。更新中にエラーが発生した場合、ASA は更新を最大 5 回再試行し、必要に応じて警告メッセージを生成します。

コマンドの実行が終了すると、ASA によってコマンド プロンプトに [Done] が表示され、syslog メッセージが生成されます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションをイネーブルにする例を示します。

```
ciscoasa# user-identity update import-user group.sample-group1
ERROR: Update import-user group is already in progress
[Done] user-identity update import-user group.sample-group1
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-identity user-not-found

Cisco Identity Firewall インスタンスの user-not-found 追跡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 **user-identity user-not-found** コマンドを使用します。アイデンティティ ファイアウォール インスタンスでこの追跡を削除するには、このコマンドの **no** 形式を使用します。

user-identity user-not-found enable

no user-identity user-not-found 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

デフォルトでは、このコマンド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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

最後の 1024 個の IP アドレスだけがトラッキングされます。

例

次に、アイデンティティ ファイアウォールに対してこのアクションをイネーブルにする例を示します。

```
ciscoasa(config)# user-identity user-not-found enable
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

user-message

DAP レコードが選択されたときに表示するテキスト メッセージを指定するには、ダイナミック アクセス ポリシー レコード モードで user-message コマンドを使用します。このメッセージを削除するには、このコマンドの **no** 形式を使用します。同じ DAP レコードに対してコマンドを複数回使用した場合、前のメッセージは新しいメッセージに置き換えられます。

user-message *message*

no user-message

構文の説明

message	この DAP レコードに割り当てられているユーザに対するメッセージ。最大 128 文字を入力できます。メッセージにスペースを含める場合は、メッセージを二重引用符で囲みます。

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	トランスペアレント	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

SSL VPN 接続に成功すると、ポータル ページに、クリック可能な点滅するアイコンが表示されます。ユーザはそのアイコンをクリックして、接続に関連付けられているメッセージを確認できます。DAP ポリシーからの接続が終了し（アクション = 終了）、その DAP レコードにユーザ メッセージが設定されている場合は、そのメッセージがログイン画面に表示されます。

複数の DAP レコードが接続に適用される場合、ASA は該当するユーザ メッセージを組み合わせて 1 つのストリングとして表示します。

例

次に、Finance という DAP レコードに「Hello Money Managers」というユーザ メッセージを設定する例を示します。

```
ciscoasa (config) config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# user-message "Hello Money Managers"
ciscoasa(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

user-parameter

SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求パラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **user-parameter** を使用します。

user-parameter *name*

(注) HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	HTTP POST 要求に含まれているユーザ名パラメータの名前。名前の最大の長さは 128 文字です。

デフォルト

デフォルトの値や動作はありません。

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	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

これは HTTP フォームのコマンドを使用した SSO です。ASA の WebVPN サーバは、SSO サーバにシングル サインオン認証要求を送信することに HTTP POST 要求を使用します。要求されたコマンド **user-parameter** は、HTTP POST 要求に SSO 認証用のユーザ名パラメータを含める必要があることを指定します。

(注) ログイン時に、ユーザは実際の名前を入力します。この名前は、HTTP POST 要求に入力されて認証 Web サーバに渡されます。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、SSO 認証に使用される HTTP POST 要求にユーザ名パラメータ userid を含めることを指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# user-parameter userid
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。

user-statistics

MPF によるユーザ統計情報の収集をアクティブ化し、アイデンティティ ファイアウォールの検索アクションを一致させるには、ポリシー マップ コンフィギュレーション モードで **user-statistics** コマンドを使用します。ユーザ統計情報の収集を削除するには、このコマンドの **no** 形式を使用します。

user-statistics [**accounting** | **scanning**]

no user-statistics [**accounting** | **scanning**]

構文の説明

accounting	（オプション）ASA が送信パケット数、送信ドロップ数、および受信パケット数を収集することを指定します。
scanning	（オプション）ASA が送信ドロップ数のみを収集することを指定します。

デフォルト

デフォルトでは、このコマンド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	トランスペアレント	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ユーザ統計情報を収集するようポリシー マップを設定すると、ASA は選択したユーザの詳細な統計情報を収集します。**accounting** または **scanning** キーワードを指定せずに **user-statistics** コマンドを指定した場合、ASA はアカウンティング統計情報とスキャンの統計情報の両方を収集します。

例

次に、アイデンティティ ファイアウォールに対してユーザ統計情報をアクティブ化する例を示します。

```
ciscoasa(config)# class-map c-identity-example-1
ciscoasa(config-cmap)# match access-list identity-example-1
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map p-identity-example-1
ciscoasa(config-pmap)# class c-identity-example-1
ciscoasa(config-pmap)# user-statistics accounting
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy p-identity-example-1 interface outside
```

関連コマンド

コマンド	説明
policy-map	モジュラ ポリシー フレームワークの使用時に、レイヤ 3/4 クラスマップで特定したトラフィックにアクションを割り当てます。
service-policy（グローバル）	すべてのインターフェイスまたは対象のインターフェイスでポリシー マップをグローバルにアクティブ化します。
show service-policy [**user-statistics**]	アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合、設定されたサービス ポリシーのユーザ統計情報を表示します。
show user-identity ip-of-user [**detail**]	アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合、指定したユーザの IP アドレスについて受信パケット、送信パケット、およびドロップ統計情報を表示します。
show user-identity user active [**detail**]	アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合、アクティブ ユーザについて指定期間の受信パケット、送信パケット、およびドロップ統計情報を表示します。
show user-identity user-of-ip [**detail**]	アイデンティティ ファイアウォールのユーザ統計情報スキャンまたはアカウンティングをイネーブルにした場合、指定した IP アドレスのユーザの受信パケット、送信パケット、およびドロップ統計情報を表示します。
user-identity enable	アイデンティティ ファイアウォール インスタンスを作成します。

user-storage

クライアントレス SSL VPN セッション間で設定された個人ユーザ情報を保存するには、グループ ポリシー webvpn コンフィギュレーション モードで **user storage** コマンドを使用します。ユーザ ストレージ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。

user-storage *NETFS-location*

no user-storage]

構文の説明

NETFS-location	ファイル システムの宛先を proto://user:password@host:port/path の形式で指定します。 ユーザ名とパスワードが NETFS-location に組み込まれている場合、パスワード入力はクリアとして扱われます。

デフォルト

ユーザストレージ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	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.4(6)	**show run** の実行時にパスワードがクリア テキストで表示されないようになりました。

使用上のガイドライン

ユーザ ストレージを使用すると、キャッシュされた資格情報およびクッキーを、ASA フラッシュ以外の場所に保存できます。このコマンドは、クライアントレス SSL VPN ユーザの個人用ブックマークにシングル サイン オンを提供します。ユーザ資格情報は、複合できない <user_id>.cps ファイルとして FTP/CIFS/SMB サーバに暗号化形式で保存されます。

ユーザ名、パスワード、および事前共有キーがコンフィギュレーションに示されていますが、ASA ではこの情報が内部アルゴリズムを使用して暗号化された形式で格納されるため、セキュリティのリスクは発生しません。

データが外部の FTP サーバまたは SMB サーバで暗号化されている場合は、ブックマークの追加を選択してポータル ページ内に個人用ブックマークを定義できます（例：user-storage cifs://jdoe:test@10.130.60.49/SharedDocs）。すべてのプラグイン プロトコルにも個人用 URL を作成できます。

（注） すべてが同じ FTP/CIFS/SMB サーバを参照して同じ「ストレージ キー」を使用する ASA のクラスタがある場合は、クラスタ内のどの ASA を介してもブックマークにアクセスできます。

例

次に、anyfiler02a/new_share というパス、anyshare というファイル共有で、パスワードが 12345678 の newuser というユーザとして、ユーザ ストレージを設定する例を示します。

```
ciscoasa(config)# wgroup-policy DFLTGrpPolicy attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
ciscoasa(config-group_webvpn)#
```

関連コマンド

コマンド	説明
storage-key	セッション間で保管されたデータを保護するためのストレージ キーを指定します。
storage-objects	セッションとセッションの間に保存されたデータのストレージ オブジェクトを設定します。

username

ユーザを ASA ローカル データベースに追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除するユーザ名を指定して、このコマンドの **no** 形式を使用します。

username *name* [**password** *password* [**pbkdf2** | **mschap** | **encrypted** | **nt-encrypted**] | **nopassword**] [**privilege** *priv_level*]

no username *name* [**password** *password* [**pbkdf2** | **mschap** | **encrypted** | **nt-encrypted**] | **nopassword**] [**privilege** *priv_level*]

構文の説明

encrypted	9.6 以前の場合は、32 文字以内のパスワードは暗号化されることを示します（**mschap** を指定しなかった場合）。**username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するとき MD5 ハッシュを作成します。**show running-config** コマンドを入力しても、**username** コマンドによって実際のパスワードは表示されません。暗号化されたパスワードと、その後に **encrypted** キーワードが表示されます。たとえば、"test" というパスワードを入力した場合、**show running-config** コマンドの出力は次のように表示されます。 `username pat password rvEdRh0xPC8bel7s encrypted` CLI で実際に **encrypted** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストして、同じパスワードを使用する場合だけです。 9.7 以降では、すべての長さのパスワードで PBKDF2 を使用します。
mschap	パスワードを入力後に Unicode に変換し、MD4 を使用してハッシュすることを指定します。このキーワードは、ユーザを MSCHAPv1 または MSCHAPv2 を使用して認証する場合に使用します。
name	3 ～ 64 文字のスペースと疑問符を除く任意の ASCII 印刷可能文字を使用して、ユーザ名を指定します。
nopassword	このユーザの*任意の*パスワードを入力できることを示します。これは安全な設定ではないため、このキーワードの使用には注意してください。 (9.6(2) 以降）パスワードなしでユーザ名を作成するには、**password** または **nopassword** キーワードを入力しないでください。たとえば、**ssh authentication** コマンドを使用すると、ASA に公開キーをインストールして、SSH クライアントでプライベート キーを使用できます。そのため、パスワード設定が不要な場合があります。

nt-encrypted	パスワードを MSCHAPv1 または MSCHAPv2 で使用するために暗号化することを示します。ユーザを追加するときに **mschap** キーワードを指定した場合は、**show running-config** コマンドを使用してコンフィギュレーションを表示すると、**encrypted** キーワードではなくこのキーワードが表示されます。 **username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **nt-encrypted** キーワードが示されます。たとえば、"test" というパスワードを入力した場合、**show running-config** コマンドの表示は次のようになります。 `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` CLI で実際に **nt-encrypted** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストし、かつ、同じパスワードを使用する場合のみです。
password *password*	3 ～ 32 文字（9.5 以前）または 127 文字（9.6 以降）の、スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）でパスワードを設定します。
pbkdf2	パスワードの暗号化を指定します。9.6 以前の場合、PBKDF2（パスワードベースのキー派生関数 2）ハッシュは、パスワードの長さが 32 文字を超える場合にのみ使用されます。9.7 以降では、すべてのパスワードで PBKDF2 を使用します。**username** コマンド内のパスワードを定義すると、ASA はセキュリティを維持するため、そのパスワードをコンフィギュレーションに保存するときに PBKDF2 ハッシュを作成します。**show running-config** コマンドを入力すると、**username** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **pbkdf2** キーワードが示されます。たとえば、長いパスワードを入力した場合、**show running-config** コマンドの出力は次のように表示されます。 `username pat password rvEdRh0xPC8bel7s pbkdf2` CLI で実際に **pbkdf2** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストして、同じパスワードを使用する場合だけです。 新しいパスワードを入力しない限り、既存のパスワードは MD5 ベースのハッシュを使用し続けることに注意してください。
privilege *priv_level*	使用する特権レベルを 0（最低）～ 15（最高）の範囲で設定します。デフォルトの特権レベルは 2 です。この特権レベルは、コマンド認可で使用されます。

デフォルト　デフォルトの特権レベルは 2 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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが追加されました。
7.2(1)	**mschap** キーワードと **nt-encrypted** キーワードが追加されました。
9.6(1)	パスワードの長さが 127 文字に増加し、**pbkdf2** キーワードが追加されました。
9.6(2)	**password** または **nopassword** キーワードを使用せずにユーザ名を作成できるようになりました。
9.7(1)	すべての長さのパスワードが PBKDF2 ハッシュを使用してコンフィギュレーションに保存されるようになりました。

使用上のガイドライン

login コマンドでは、このデータベースを認証用に使用します。

CLI にアクセスできるユーザや特権モードを開始できないユーザをローカル データベースに追加する場合は、コマンド認可をイネーブルにする必要があります（**aaa authorization command** コマンドを参照してください）。コマンド許可がない場合、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、AAA 認証を使用してユーザが **login** コマンドを使用できないようにするか、すべてのローカル ユーザをレベル 1 に設定して **enable** パスワードで特権 EXEC モードにアクセスできるユーザを制御できます。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。**username attributes** コマンドを使用して、明示的にすべての値を設定する必要があります。

パスワード認証ポリシーがイネーブルの場合、**username** コマンドを使用して自身のパスワードを変更したり、自身のアカウントを削除したりできません。ただし、パスワードは **change-password** コマンドを使用して変更できます。

ユーザ名パスワード日付を表示するには、**show running-config all username** コマンドを使用します。

例

次に、パスワードが 12345678、特権レベルが 12 の「anyuser」という名前のユーザを設定する例を示します。

```
ciscoasa(config)# username anyuser password 12345678 privilege 12
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
clear config username	特定のユーザまたはすべてのユーザのコンフィギュレーションをクリアします。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username attributes	ユーザ名属性モードを開始し、特定のユーザの属性を設定できるようにします。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

username attributes

ユーザ名属性モードを開始するには、ユーザ名コンフィギュレーション モードで **username attributes** コマンドを使用します。特定のユーザの属性をすべて削除するには、このコマンドの **no** 形式を使用し、ユーザ名を付加します。すべてのユーザの属性をすべて削除するには、ユーザ名を付加せずに、このコマンドの **no** 形式を使用します。属性モードを使用すると、指定したユーザに対して属性値ペアを設定できます。

username *name* **attributes**

no username *name* **attributes**

構文の説明

name	ユーザの名前を指定します。

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	トランスペアレント	シングル	コンテキスト	システム
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	**service-type** 属性が追加されました。
9.1(2)	**ssh authentication** {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]} 属性が追加されました。

使用上のガイドライン

内部ユーザ認証データベースは、**username** コマンドを使用して入力されたユーザで構成されています。**login** コマンドでは、このデータベースを認証用に使用します。ユーザ名属性は、**username** コマンドまたは **username attributes** コマンドを使用して設定できます。

ユーザ名コンフィギュレーション モードのコマンド構文には、一般に次の特性があります。

- **no** 形式を使用すると、実行コンフィギュレーションから属性が削除されます。
- **none** キーワードを使用しても、実行コンフィギュレーションから属性が削除されます。ただし、このキーワードでは、属性をヌル値に設定し、継承されないようにすることによって、このことを行います。
- ブール型属性には、イネーブルおよびディセーブルの設定用に明示的な構文があります。

username attributes コマンドは、ユーザ名属性モードを開始し、次の属性を設定できるようにします。

属性	機能
group-lock	ユーザが接続する必要がある既存のトンネル グループを指定します。
password-storage	クライアント システムでのログイン パスワードの保存をイネーブルまたはディセーブルにします。
service-type [**remote-access** | **admin** | **nas-prompt**]	コンソール ログインを制限し、適切なレベルが割り当てられているユーザのログインをイネーブルにします。**remote-access** オプションでは、リモート アクセスのための基本的な AAA サービスを指定します。**admin** オプションは、AAA サービス、ログイン コンソール特権、EXEC モード特権、イネーブル特権、および CLI 特権を指定します。**nas-prompt** オプションは、AAA サービス、ログイン コンソール特権、および EXEC モード特権を指定しますが、イネーブル特権は指定しません。

属性	機能
ssh authentication {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]}	公開キー認証をユーザ単位でイネーブルにします。*key* 引数の値は次のいずれかになります。 • *key* 引数が指定され、ハッシュされたタグが指定されていない場合、キーの値は、SSH-RSA の未処理キーを生成することのできる SSH キー生成ソフトウェアによって生成される Base 64 で符号化された公開キーである必要があります(つまり、証明書は使用しません)。Base 64 エンコード公開キーを送信すると、そのキーは SHA-256 によりハッシュ化され、それ以降のすべての比較では対応する 32 バイト ハッシュが使用されます。 • *key* 引数が指定され、ハッシュされたタグを指定した場合は、キーの値は、SHA-256 で事前にハッシュされている必要があります。長さは 32 バイトで、各バイトはコロンで区切られている必要があります(解析のため)。 **pkf** オプションを使用すると、4096 ビットの RSA キーを SSH 公開キー ファイル(PKF)として使用して認証を行うことができます。このオプションは、4096 ビットの RSA キーに制限されず、4096 ビット RSA キー未満の任意のサイズに使用できます。 **nointeractive** オプションは、SSH 公開キー形式のキーをインポートするときにすべてのプロンプトを抑制します。この非インタラクティブ データ入力モードは ASDM での使用のみを目的としています。 *key* フィールドおよび **hashed** キーワードは **publickey** オプションでのみ使用でき、**nointeractive** キーワードは **pkf** オプションでのみ使用できます。 設定を保存すると、ハッシュされたキー値はコンフィギュレーションに保存され、ASA のリブート時に使用されます。 (注) PKF オプションはフェールオーバーがイネーブルの場合に使用できますが、PKF データはスタンバイ システムに自動的に複製されません。**write standby** コマンドを入力して、フェールオーバー ペアのスタンバイ システムに PKF 設定を同期する必要があります。
vpn-access-hours	設定済みの時間範囲ポリシーの名前を指定します。
vpn-filter	ユーザ固有の ACL の名前を指定します。
vpn-framed-ip-address	クライアントに割り当てる IP アドレスとネットマスクを指定します。
vpn-group-policy	属性の継承元となるグループ ポリシーの名前を指定します。
vpn-idle-timeout [**alert-interval**]	アイドルタイムアウト期間を分単位で指定するか、または **none** を指定してディセーブルにします。任意で、タイムアウト前のアラート間隔を指定します。
vpn-session-timeout [**alert-interval**]	最大ユーザ接続時間を分単位で指定するか、または **none** を指定して時間を無制限にします。任意で、タイムアウト前のアラート間隔を指定します。

属性	機能
vpn-simultaneous-logins	許可される同時ログインの最大数を指定します。
vpn-tunnel-protocol	使用できるトンネリング プロトコルを指定します。
webvpn	ユーザ名 webvpn コンフィギュレーション モードを開始し、WebVPN 属性を設定できるようにします。

ユーザ名の webvpn モード属性を設定するには、ユーザ名 webvpn コンフィギュレーション モードで **username attributes** コマンドを入力してから、**webvpn** コマンドを入力します。詳細については **webvpn** コマンド（グループ ポリシー属性モードおよびユーザ名属性モード）を参照してください。

例

次に、「anyuser」という名前のユーザのユーザ名属性コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)#
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースをクリアします。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username	ASA データベースにユーザを追加します。
webvpn	webvpn コンフィギュレーション モードを開始し、指定したグループの WebVPN 属性を設定できるようにします。

username-from-certificate

認可のためのユーザ名として、証明書内のいずれのフィールドを使用するかを指定するには、トンネル グループ一般属性モードで **username-from-certificate** コマンドを使用します。認可のためのユーザ名として使用するピア証明書の DN。

属性をコンフィギュレーションから削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no username-from-certificate

構文の説明

primary-attr	証明書から認可クエリーのユーザ名を取得するために使用する属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
secondary-attr	(任意)デジタル証明書から認証または認可クエリーのユーザ名を取得するためにプライマリ属性とともに使用する追加の属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。
use-entire-name	ASA では、完全なサブジェクト DN(RFC1779)を使用して、デジタル証明書から認可クエリーの名前を取得する必要があることを指定します。
use-script	ASDM によって生成されたスクリプト ファイルを使用して、ユーザ名として使用する DN フィールドを証明書から抽出することを指定します。

デフォルト

プライマリ属性のデフォルト値は CN(一般名)です。

セカンダリ属性のデフォルト値は OU(組織の部門)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	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ユーザ名として使用する証明書内のフィールドを選択します。このコマンドは、リリース 8.0(4) 以降で廃止された **authorization-dn-attributes** コマンドに代わるものです。**username-from-certificate** コマンドは、セキュリティ アプライアンスに、指定した証明書フィールドをユーザ名/パスワード認可のためのユーザ名として使用するように強制します。

ユーザ名/パスワード認証または認可のために、証明書からのユーザ名の事前充填機能で、取得されたこのユーザ名を使用するには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドも設定する必要があります。つまり、ユーザ名の事前充填機能を使用するには、両方のコマンドを設定する必要があります。

プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

属性	定義
C	Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
CN	Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	E-mail Address（電子メール アドレス）。
GENQ	Generational Qualifier（世代修飾子）。
GN	Given Name（名）。
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。
use-entire-name	DN 名全体を使用します。セカンダリ属性としては使用できません。
use-script	ASDM によって生成されたスクリプト ファイルを使用します。

例

グローバル コンフィギュレーション モードで入力される次の例では、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成して、Common Name（CN; 通常名）をプライマリ属性として使用し、認可クエリー用の名前をデジタル証明書から生成するために使用するセカンダリ属性として OU を使用することを指定します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN OU
ciscoasa(config-tunnel-general)#
```

次に、トンネル グループ属性を変更し、事前入力ユーザ名を設定する例を示します。

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザ名機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

username-from-certificate-choice

プライマリ認証または許可用として事前入力ユーザ名フィールドにユーザ名を使用する必要がある証明書を選択するには、**username-from-certificate-choice** コマンドを使用します。このコマンドは tunnel-group general-attributes モードで使用します。デフォルトの証明書で使用されているユーザ名を使用するには、このコマンドの **no** 形式を使用します。

username-from-certificate-choice {**first-certificate** | **second-certificate**}

no username-from-certificate-choice {**first-certificate** | **second-certificate**}

構文の説明

first-certificate	マシン証明書のユーザ名を、プライマリ認証の事前入力ユーザ名フィールドで使用するように SSL または IKE で送信するかどうかを指定します。
second-certificate	ユーザ証明書のユーザ名を、プライマリ認証の事前入力ユーザ名フィールドで使用するようにクライアントから送信するかどうかを指定します。

デフォルト

デフォルトでは、事前入力するユーザ名は 2 つ目の証明書から取得されます。

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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

複数証明書オプションを使用すると、証明書を通じたマシンとユーザ両方の証明書認証が可能になります。事前入力ユーザ名フィールドでは、証明書のフィールドを解析し、AAA および証明書認証済み接続で以降の（プライマリまたはセカンダリ）AAA 認証に使用することができます。事前入力のユーザ名は、常にクライアントから受信した 2 つ目の（ユーザ）証明書から取得されます。

9.14(1) 以降、ASA では、最初の証明書（マシン証明書）または 2 つ目の証明書（ユーザ証明書）のどちらを使用して事前入力ユーザ名フィールドに使用するユーザ名を取得するかを選択できます。

このコマンドは、認証タイプ（AAA、証明書、または複数証明書）に関係なく、任意のトンネルグループに使用および設定できます。ただし、設定は、複数証明書認証（複数証明書または AAA 複数証明書）に対してのみ有効となります。このオプションが複数証明書認証に使用されない場合は、2 つ目の証明書がデフォルトとして認証または許可の目的で使用されます。

例

次に、プライマリおよびセカンダリ認証または許可の事前入力ユーザ名に使用する証明書を設定する方法の例を示します。

```
ciscoasa(config)#tunnel-group tg1 type remote-access
ciscoasa(config)#tunnel-group tg1 general-attributes
ciscoasa(config-tunnel-general)# address-pool IPv4
ciscoasa(config-tunnel-general)# secondary-authentication-server-group LOCAL/<Auth-Server>
ciscoasa(config-tunnel-general)# username-from-certificate-choice first-certificate
ciscoasa(config-tunnel-general)# secondary-username-from-certificate-choice
first-certificate

ciscoasa(config)# tunnel-group tg1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication aaa multiple-certificate
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client
```

関連コマンド

コマンド	説明
secondary-username-from-certificate-choice	セカンダリ認証の証明書オプションを指定します。

username password-date

システムがブート時または実行コンフィギュレーションへのファイルのコピー時にパスワード作成日付を復元できるようにするには、非インタラクティブ コンフィギュレーション モードで **username pasword-date** コマンドを入力します。言い換えると、このコマンドは、このコマンドがすでに存在しているときにコンフィギュレーション ファイルをブート アップする場合にのみ使用できます。CLI プロンプトにこのコマンドを入力することはできません。

username *name* **password-date** *date*

構文の説明

name	3 ～ 64 文字のスペースと疑問符を除く任意の ASCII 印刷可能文字を使用して、ユーザ名を指定します。
date	ブートアップ時にユーザ名が読み込まれるときに、システムがパスワード作成日付を復元できるようにします。存在しない場合、パスワード日付は現在の日付に設定されます。日付の形式は、mmm-dd-yyyy です。

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	トランスペアレント	シングル	コンテキスト	システム
非インタラクティブ	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

ユーザ名パスワード日付を表示するには、**show running-config all username** コマンドを使用します。

CLI プロンプトから **username password-date** 値を入力することはできません。パスワード日付は、パスワード ポリシーの有効期間がゼロでない場合にだけスタートアップ コンフィギュレーションに保存されます。これは、パスワードの有効期限が設定されている場合に限り、パスワード日付が保存されることを意味します。ユーザがパスワード作成日を変更することを防ぐために **username password-date** コマンドを使用することはできません。

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
clear config username	特定のユーザまたはすべてのユーザのコンフィギュレーションをクリアします。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username attributes	ユーザ名属性モードを開始し、特定のユーザの属性を設定できるようにします。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

username-prompt

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 ボックスのユーザ名プロンプト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 **username-prompt** 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。

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**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

ユーザ名プロンプトのデフォルト テキストは「USERNAME:」です。

ユーザ名プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right 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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

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、テキストを「Corporate Username:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# username-prompt text Corporate Username:
ciscoasa(config-webvpn-custom)# username-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。