CHAPTER 18

l2tp tunnel hello コマンド～ log-adj-changes コマンド

l2tp tunnel hello

L2TP over IPSec 接続における hello メッセージ間の間隔を指定するには、グローバル コンフィギュレーション モードで **l2tp tunnel hello** コマンドを使用します。この間隔をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

構文の説明

interval	hello メッセージ間の間隔（秒）。デフォルトは 60 秒です。指定できる範囲は 10 ～ 300 秒です。

デフォルト

デフォルトは 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

l2tp tunnel hello コマンドは、セキュリティ アプライアンスによる L2TP 接続の物理層に関する問題の検出をイネーブルにします。デフォルトは 60 秒です。60 秒未満の値に設定すると、問題が発生している接続はより早く切断されます。

例

次に、hello メッセージ間の間隔を 30 秒に設定する例を示します。

```
hostname(config)# l2tp tunnel hello 30
```

関連コマンド

コマンド	説明
show vpn-sessiondbdetail remote filter protocol L2TPOverIPSec	L2TP 接続の詳細を表示します。
vpn-tunnel-protocol l2tp-ipsec	L2TP を特定のトンネル グループのトンネリング プロトコルとしてイネーブルにします。

ldap attribute-map

ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために LDAP 属性マップを作成し、名前を付けるには、グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

構文の説明

map-name	LDAP 属性マップのユーザ定義名を指定します。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ldap attribute-map コマンドを使用すると、ユーザ独自の属性名と値を Cisco 属性名にマッピングできます。その後、作成された属性マップを LDAP サーバにバインドできます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、何も入力されていない属性マップを作成します。このコマンドは LDAP 属性マップ モードを開始します。
2. LDAP 属性マップ モードで **map-name** コマンドと **map-value** コマンドを使用し、属性マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用し、属性マップを LDAP サーバにバインドします。このコマンドでは、ldap の後にハイフンを入力してください。

（注） 属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザ定義属性名と値を理解しておく必要があります。

例

次に、グローバル コンフィギュレーション モードで、情報を入力したり LDAP サーバにバインドする前に myldapmap という名前の LDAP 属性マップを作成するコマンドの例を示します。

```
hostname(config)# ldap attribute-map myldapmap
```

```
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP 属性マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP 属性名を Cisco LDAP 属性名にマッピングします。
map-value	ユーザ定義の属性値を Cisco 属性名にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

ldap-attribute-map（AAA サーバ ホスト モード）

既存のマッピング コンフィギュレーションを LDAP ホストにバインドするには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-attribute-map** コマンドを使用します。バインディングを削除するには、このコマンドの **no** 形式を使用します。

ldap-attribute-map *map-name*

no ldap-attribute-map *map-name*

構文の説明

map-name	LDAP 属性マッピング コンフィギュレーションを指定します。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シスコ定義の LDAP 属性名が使いやすさやその他の要件を満たしていない場合は、独自の属性名を作成し、それをシスコの属性にマッピングして、作成された属性コンフィギュレーションを LDAP サーバにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、何も入力されていない属性マップを作成します。このコマンドにより、LDAP 属性マップ モードが開始されます。このコマンドでは、「ldap」の後にハイフンを入力しないでください。
2. LDAP 属性マップ モードで **map-name** コマンドと **map-value** コマンドを使用して、属性マッピング コンフィギュレーションに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用して、LDAP サーバに属性マップ コンフィギュレーションをバインドします。

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、myldapmap という名前の既存の属性マップを ldapsvr1 という名前の LDAP サーバにバインドするコマンドの例を示します。

```
hostname(config)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-attribute-map myldapmap
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
map-name	ユーザ定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。
map-value	ユーザ定義の属性値をシスコ属性にマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP 属性マッピング コンフィギュレーションまたはすべての実行属性マッピング コンフィギュレーションを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

ldap-base-dn

サーバが認可要求を受信したときに検索を開始する、LDAP 階層内の位置を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-base-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除して、検索の開始位置をリストの先頭にリセットするには、このコマンドの **no** 形式を使用します。

ldap-base-dn *string*

no ldap-base-dn

構文の説明

string	サーバが認可要求を受信したときに検索を開始する LDAP 階層内の位置を指定する、最大 128 文字のストリング（たとえば、OU=Cisco）。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

デフォルト

リストの先頭から検索を開始します。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで変更された既存のコマンドです。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ベース DN を starthere に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。

ldap-defaults

LDAP デフォルト値を定義するには、crl 設定コンフィギュレーション モードで **ldap-defaults** 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、暗号 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。これらのデフォルト値は、LDAP サーバが必要とする場合にのみ使用されます。LDAP デフォルト値を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-defaults *server* [*port*]

no ldap-defaults

構文の説明

port	（任意）LDAP サーバ ポートを指定します。このパラメータが指定されていない場合、セキュリティ アプライアンスは標準の LDAP ポート（389）を使用します。
server	LDAP サーバの IP アドレスまたはドメイン名を指定します。CRL 配布ポイント内にサーバが存在する場合、この値はそのサーバによって上書きされます。

デフォルト

デフォルト設定は設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、デフォルト ポート（389）に LDAP デフォルト値を定義する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-defaults ldapdomain4 8389
```

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。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-dn

CRL 取得のために認証を要求する LDAP サーバに X.500 認定者名とパスワードを渡すには、crl 設定コンフィギュレーション モードで **ldap-dn** 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、暗号 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。これらのパラメータは、LDAP サーバで必要な場合のみ使用されます。LDAP DN を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-dn *x.500-name password*

no ldap-dn

構文の説明

password	この認定者名のパスワードを定義します。最大のフィールドの長さは 128 文字です。
x.500-name	この CRL データベースにアクセスするためのディレクトリ パスを定義します（たとえば、cn=crl,ou=certs,o=CAName,c=US）。最大のフィールドの長さは 128 文字です。

デフォルト

デフォルト値は設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、トラストポイント central の X.500 名として CN=admin,OU=devtest,O=engineering、パスワードとして xxzzyy を指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードを開始します。
crypto ca trustpoint	CA 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。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-group-base-dn

ダイナミック アクセス ポリシーによってグループ検索に使用される Active Directory 階層の基本グループを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-group-base-dn** コマンドを使用します。このコマンドを実行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** 形式を使用します。

ldap-group-base-dn [*string*]

no ldap-group-base-dn [*string*]

構文の説明

string	サーバが検索を開始する Active Directory 階層内の位置を指定する、最大 128 文字のストリング。大文字と小文字は区別されます。たとえば、ou=Employees を指定します。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。グループ検索 DN を指定しない場合、ベース DN から検索が開始されます。

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	透過	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 モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

ldap-group-base-dn コマンドは、LDAP を使用する Active Directory サーバにのみ適用され、**show ad-groups** コマンドがグループ検索を開始するときに使用する Active Directory 階層レベルを指定します。検索で取得されたグループは、ダイナミック グループ ポリシーによって特定のポリシーの選択基準として使用されます。

例

次に、組織の部門（ou）レベルの Employees から検索を開始するようにグループ ベース DN を設定する例を示します。

```
hostname(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

関連コマンド

コマンド	説明
group-search-timeout	グループのリストについて Active Directory サーバからの応答をセキュリティ アプライアンスが待機する時間を調整します。
show ad-groups	Active Directory サーバ上でリストされるグループを表示します。

ldap-login-dn

システムがバインドするディレクトリ オブジェクト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 **ldap-login-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル 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。

ldap-login-dn *string*

no ldap-login-dn

構文の説明

string	LDAP 階層内のディレクトリ オブジェクトの名前を指定する、最大 128 文字のストリング。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。サポートされるストリングの最大長は 128 文字です。

Microsoft Active Directory サーバなどの一部の LDAP サーバでは、他の LDAP 動作の要求を受け入れる前に、セキュリティ アプライアンスが認証済みバインディングを介してハンドシェイクを確立している必要があります。セキュリティ アプライアンスは、ログイン DN フィールドをユーザ認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。ログイン DN フィールドには、セキュリティ アプライアンスの認証特性が記述されます。これらの特性は、管理者特権を持つユーザの特性に対応している必要があります。

string 変数には、VPN コンセントレータの認証済みバインディングのディレクトリ オブジェクト名を入力します（たとえば、cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com）。匿名アクセスの場合は、このフィールドをブランクのままにします。

例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ログイン DN を myobjectname に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
```

```
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-login-dn myobjectname
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバでのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-login-password

LDAP サーバのログイン パスワードを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-login-password** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。このパスワード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。

ldap-login-password *string*

no ldap-login-password

構文の説明

string	最大 64 文字の英数字のパスワード。大文字と小文字は区別されます。パスワードにスペース文字を含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。パスワードの最大長は 64 文字です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ログイン パスワードを obscurepassword に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# ldap-login-password obscurepassword
hostname(config-aaa-server)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。

ldap-base-dn	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-naming-attribute

相対認定者名属性を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-naming-attribute** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル 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。

ldap-naming-attribute *string*

no ldap-naming-attribute

構文の説明

string	LDAP サーバ上のエントリを一意に識別する、最大 128 文字の英数字の相対認定者名属性を指定します。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LDAP サーバ上のエントリを一意に識別するための、相対認定者名属性を指定します。共通の命名属性は、一般名（cn）とユーザ ID（uid）です。

このコマンドは LDAP サーバでのみ有効です。サポートされるストリングの最大長は 128 文字です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP 命名属性を cn に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバでのみ有効です。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-over-ssl

セキュアな SSL 接続をセキュリティ アプライアンスと LDAP サーバの間で確立するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-over-ssl** コマンドを使用します。接続の SSL 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。

ldap-over-ssl enable

no ldap-over-ssl enable

構文の説明

enable	SSL で LDAP サーバへの接続を保護することを指定します。

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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、SSL でセキュリティ アプライアンスと LDAP サーバの間の接続を保護することを指定します。

（注） プレーン テキスト認証を使用している場合は、この機能をイネーブルにすることを推奨します。**sasl-mechanism** コマンドを参照してください。

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、セキュリティ アプライアンスと LDAP サーバ ldapsvr1（IP アドレスは 10.10.0.1）の間の接続に対して SSL をイネーブルにするコマンドの例を示します。PLAIN SASL 認証メカニズムも設定します。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
sasl-mechanism	LDAP クライアントとサーバの間に SASL 認証を指定します。
server-type	LDAP サーバ ベンダーに Microsoft または Sun のいずれかを指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

ldap-scope

サーバが認可要求を受信したときに検索する LDAP 階層内の範囲を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-scope** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードは、AAA サーバ プロトコル 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。

ldap-scope *scope*

no ldap-scope

構文の説明

scope	サーバが認可要求を受信したときに検索する LDAP 階層内のレベルの数を指定します。次の値が有効です。 • **onelevel**：ベース DN の 1 つ下のレベルのみを検索します。 • **subtree**：ベース DN の下のレベルをすべて検索します。

デフォルト

デフォルト値は **onelevel** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで変更された既存のコマンドです。

使用上のガイドライン

scope を **onelevel** と指定すると、ベース DN の 1 つ下のレベルのみが検索されるため、検索速度が向上します。**subtree** を指定すると、ベース DN の下のレベルがすべて検索されるため、検索速度が低下します。

このコマンドは LDAP サーバでのみ有効です。

例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP 範囲を subtree に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバでのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。

leap-bypass

LEAP バイパス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 **leap-bypass enable** コマンドを使用します。LEAP バイパスをディセーブルにするには、**leap-bypass 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 LEAP バイパス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。このオプションにより、別のグループ ポリシーから LEAP バイパスの値を継承できます。

leap-bypass {**enable | disable**}

no leap-bypass

構文の説明

disable	LEAP バイパスをディセーブルにします。
enable	LEAP バイパスをイネーブルにします。

デフォルト

LEAP バイパスはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LEAP バイパスをイネーブルにすると、VPN ハードウェア 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 トンネルを通過できます。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。デバイスは、ユーザ認証ごとに認証を再実行できます。

インタラクティブ ハードウェア クライアント認証をイネーブルにした場合、この機能は正常に動作しません。

詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

（注） 認証されていないトラフィックがトンネルを通過できるようにすると、セキュリティ リスクが発生する可能性があります。

例

次に、「FirstGroup」という名前のグループ ポリシーに LEAP バイパスを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# leap-bypass enable
```

関連コマンド

コマンド	説明
secure-unit-authentication	VPN ハードウェア 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します。
user-authentication	VPN 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、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

lifetime（CA サーバ モード）

ローカル Certificate Authority（CA; 認証局）証明書、各発行済み証明書、または Certificate Revocation List（CRL; 証明書失効リスト）の有効期間を指定するには、CA サーバ コンフィギュレーション モードで **lifetime** コマンドを使用します。パラメータをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

lifetime {ca-certificate | certificate | crl} *time*

no lifetime {**ca-certificate** | **certificate** | **crl**}

構文の説明

ca-certificate	ローカル CA サーバ証明書のライフタイムを指定します。
certificate	CA サーバが発行するすべてのユーザ証明書のライフタイムを指定します。
crl	CRL のライフタイムを指定します。
time	CA 証明書およびすべての発行済み証明書の場合、*time* はその証明書の有効日数を指定します。有効な範囲は、1 ～ 3650 日です。 CRL の場合、*time* は CRL の有効時間数を指定します。CRL の有効な範囲は、1 ～ 720 時間です。

デフォルト

デフォルトのライフタイムは次のとおりです。

- CA 証明書：3 年間
- 発行済み証明書：1 年間
- CRL：6 時間

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

証明書または CRL が有効である日数または時間数を指定すると、このコマンドは、証明書または CRL に含める有効期限を決定します。

例

次に、3 か月間有効な証明書を発行するように CA を設定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# lifetime certificate 90
```

```
hostname(config-ca-server))#
```

次に、2 日間有効な CRL を発行するように CA を設定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# lifetime crl 48
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める証明書失効リストの配布ポイント（CDP）を指定します。
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
show crypto ca server	ローカル CA コンフィギュレーションの詳細を ASCII テキストで表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

limit-resource

マルチ コンテキスト モードでクラスのリソース制限を指定するには、クラス コンフィギュレーション モードで **limit-resource** コマンドを使用します。制限をデフォルトに戻すには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスでは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

limit-resource {**all 0** | [**rate**] *resource_name number*[**%**]}

no limit-resource {**all** | [**rate**] *resource_name*}

構文の説明

all 0	すべてのリソースの制限を無制限として設定します。
number[**%**]	リソース制限を 1 以上の固定数、またはパーセント記号（%）付きのシステム制限のパーセンテージ（1 ～ 100）として指定します。無制限のリソースを指定するには、制限を **0** に設定します。システム制限がないリソースの場合は、パーセンテージ（%）を設定できません。絶対値のみを設定できます。
rate	リソースの 1 秒あたりのレートを設定することを指定します。1 秒あたりのレートを設定できるリソースについては、表 18-1 を参照してください。
resource_name	制限を設定するリソース名を指定します。この制限は、**all** に設定されている制限を上書きします。

デフォルト

すべてのリソースは無制限に設定されています。ただし、デフォルトでコンテキストごとに許可される最大値に設定される次の制限を除きます。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- IPSec セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

クラスのリソースを制限した場合、セキュリティ アプライアンスは、クラスに割り当てられた各コンテキストのためにリソースの一部を確保するのではなく、セキュリティ アプライアンスはコンテキストに上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。

表 18-1 に、リソース タイプと制限を示します。**show resource types** コマンドも参照してください。

（注） 「システム制限」カラムに「該当なし」と記述されている場合、そのリソースにはハード システム制限がないため、リソースのパーセンテージを設定できません。

表 18-1　リソース名と制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
mac-addresses	同時接続数	該当なし	65,535	トランスペアレント ファイアウォール モードでは、MAC アドレス テーブルで許可される MAC アドレス数。
conns	同時またはレート	該当なし	同時接続数：プラットフォームの接続制限については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。
inspects	レート	該当なし	該当なし	アプリケーション インスペクション。
hosts	同時接続数	該当なし	該当なし	セキュリティ アプライアンス経由で接続可能なホスト。
asdm	同時接続数	最小 1 最大 5	32	ASDM 管理セッション。 **（注）** ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。たとえば、ASDM セッションのシステム制限が 32 の場合、HTTPS セッション数は 64 に制限されます。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション
syslogs	レート	該当なし	該当なし	システム ログ メッセージ。
telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。
xlates	同時接続数	該当なし	該当なし	アドレス変換。

例

次に、接続のデフォルト クラスの制限に、無制限ではなく 10 % を設定する例を示します。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
member	コンテキストをリソース クラスに割り当てます。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

lmfactor

最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再検証ポリシーを設定するには、キャッシュ コンフィギュレーション モードで **lmfactor** コマンドを使用します。このようなオブジェクトを再検証するための新しいポリシーを設定するには、このコマンドを再度使用します。属性をデフォルト値 20 にリセットするには、このコマンドの **no** 形式を使用します。

lmfactor *value*

no lmfactor

構文の説明

value	0 ～ 100 の範囲の整数。

デフォルト

デフォルト値は 20 です。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、lmfactor の値を使用して、キャッシュされたオブジェクトを変更なしと見なす時間の長さを推定します。これは有効期限と呼ばれます。セキュリティ アプライアンスは、最終変更後の経過時間に lmfactor をかけることによって有効期限を推定します。

lmfactor を 0 に設定すると、ただちに再検証が強制されます。100 に設定すると、再検証までの時間は可能な限り長くなります。

例

次に、lmfactor を 30 に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# lmfactor 30
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。

コマンド	説明
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

log

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **log** コマンドを使用して、**match** コマンドまたはクラス マップに一致するパケットをログに記録します。このログ アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で使用できます。このアクション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。

log

no log

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを特定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照する）、**log** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するすべてのパケットをログに記録できます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットが http-traffic クラス マップに一致する場合にログを送信する例を示します。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# 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。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

log-adj-changes

OSPF ネイバーが起動または停止したときに syslog メッセージを送信するようにルータを設定するには、ルータ コンフィギュレーション モードで **log-adj-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

構文の説明

detail	（任意）ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信します。

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	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

log-adj-changes コマンドはデフォルトでイネーブルになっています。このコマンドの **no** 形式で削除しない限り、実行コンフィギュレーションに表示されます。

例

次に、OSPF ネイバーが起動または停止したときに syslog メッセージを送信しないようにする例を示します。

```
hostname(config)# router ospf 5
hostname(config-router)# no log-adj-changes
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。