# l2 – lof


- l2tp tunnel hello （3 ページ）
- lacp max-bundle （5 ページ）
- lacp port-priority （7 ページ）
- lacp system-priority （10 ページ）
- ldap-attribute-map （12 ページ）
- ldap-base-dn （14 ページ）
- ldap-defaults （16 ページ）
- ldap-dn （18 ページ）
- ldap-group-base-dn （20 ページ）
- ldap-login-dn （22 ページ）
- ldap-login-password （24 ページ）
- ldap-naming-attribute （26 ページ）
- ldap-over-ssl （28 ページ）
- ldap-scope （31 ページ）
- leap-bypass （33 ページ）
- license （35 ページ）
- license-server address （38 ページ）
- license-server backup address （42 ページ）
- license-server backup backup-id （44 ページ）
- license-server backup enable （47 ページ）
- license-server enable （50 ページ）
- license-server port （54 ページ）
- license-server refresh-interval （56 ページ）
- license-server secret （58 ページ）
- license smart （60 ページ）
- license smart deregister （62 ページ）
- license smart register （64 ページ）
- license smart renew （66 ページ）
- license smart reservation （68 ページ）
- license smart reservation cancel （70 ページ）

- license smart reservation install （72 ページ）
- license smart reservation universal （74 ページ）
- license smart reservation return （76 ページ）
- lifetime（CA サーバー モード） （78 ページ）
- lifetime（IKEv2 ポリシー モード） （81 ページ）
- limit-resource （83 ページ）
- lmfactor （89 ページ）
- load-monitor （91 ページ）
- local-domain-bypass （93 ページ）
- local-unit （95 ページ）
- location-logging （97 ページ）

# l2tp tunnel hello

L2TP over IPsec 接続における hello メッセージ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。 |

## コマンド 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 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。 |

## 使用上のガイドライン

**l2tp tunnel hello** コマンドは、ASA による L2TP 接続の物理層に関する問題の検出を有効にします。デフォルトは 60 秒です。デフォルト設定を使用すると、L2TP トンネルが 180 秒後に切断されることが予想されます。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。L2TP の最大再試行回数は 3 回です。

## 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。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show vpn-sessiondb detail remote filter protocol L2TPOverIPsec** | L2TP 接続の詳細を表示します。 |

| コマンド | 説明 |
| --- | --- |
| **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。 |

# lacp max-bundle

EtherChannel チャネルグループで許可されるアクティブインターフェイスの最大数を指定するには、インターフェイス コンフィギュレーション モードで **lacp max-bundle** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

**lacp max-bundle** *number*
**no lacp max-bundle**

## 構文の説明

*number* このチャネル グループで許可されるアクティブ インターフェイスの最大数を 1 ～ 8 の範囲内で指定します。9.2(1) 以降では、最大数が 16 に引き上げられています。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。

## コマンド デフォルト

（9.1 以前）デフォルトは 8 です。

（9.2(1) 以降）デフォルトは 16 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 | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| インターフェイス 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(1) | このコマンドが追加されました。 |
| 9.2(1) | アクティブ インターフェイスの数が 8 から 16 に増加しました。 |

## 使用上のガイドライン

このコマンドは、ポートチャネル インターフェイスに対して入力します。チャネル グループあたりのアクティブ インターフェイスの最大数は 8 です。このコマンドは、最大数を減らす場合に使用します。

## 例

次に、EtherChannel のインターフェイスの最大数を 4 に設定する例を示します。

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| channel-group | EtherChannel にインターフェイスを追加します。 |
| **interface port-channel** | EtherChannel を設定します。 |
| **lacp max-bundle** | チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。 |
| **lacp port-priority** | チャネル グループの物理インターフェイスのプライオリティを設定します。 |
| **lacp system-priority** | LACP システム プライオリティを設定します。 |
| **port-channel load-balance** | ロード バランシング アルゴリズムを設定します。 |
| **port-channel min-bundle** | ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。 |
| **show lacp** | LACP情報（トラフィック統計情報、システムID、ネイバーの詳細など）が表示されます。 |
| **show port-channel** | EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。 |
| **show port-channel load-balance** | ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。 |

# lacp port-priority

EtherChannel における物理インターフェイスのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **lacp port-priority** コマンドを使用します。プライオリティをデフォルトに設定するには、このコマンドの **no** 形式を使用します。

**lacp port-priority** *number*
**no lacp port-priority**

## 構文の説明

*number* プライオリティ（1 ～ 65535）を設定します。数字が大きいほど、プライオリティは低くなります。

## コマンド デフォルト

デフォルトは 32768 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 | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| インターフェイス 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(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

このコマンドは、物理インターフェイスに対して入力します。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポート プライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID（スロット/ポート）で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。

あるインターフェイスについて、インターフェイス ID は大きいが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアクティブにするには、0/7 インターフェイスでのデフォルトの 32768 に対し、1/3 インターフェイスで **lacp port-priority** 値を 12345 にします。

EtherChannelの反対の端にあるデバイスのポートプライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。**lacp system-priority** コマンドを参照してください。

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。

## 例

次に、GigabitEthernet 0/2 のポート プライオリティの値を小さくして、EtherChannel で GigabitEthernet 0/0 および 0/1 よりも先に使用されるように設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode active
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| channel-group | EtherChannel にインターフェイスを追加します。 |
| **interface port-channel** | EtherChannel を設定します。 |
| **lacp max-bundle** | チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。 |
| **lacp port-priority** | チャネル グループの物理インターフェイスのプライオリティを設定します。 |
| **lacp system-priority** | LACP システム プライオリティを設定します。 |
| **port-channel load-balance** | ロード バランシング アルゴリズムを設定します。 |
| **port-channel min-bundle** | ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。 |
| **show lacp** | LACP情報（トラフィック統計情報、システムID、ネイバーの詳細など）が表示されます。 |
| **show port-channel** | EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。 |

| コマンド | 説明 |
| --- | --- |
| **show port-channel load-balance** | ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。 |

# lacp system-priority

EtherChannel の場合、ASA の LACP システムのプライオリティをグローバルに設定するには、グローバル コンフィギュレーション モードで **lacp system-priority** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

**lacp system-priority** *number*
**no lacp system-priority**

## 構文の説明

*number* LACP システム プライオリティを 1 ～ 65535 の範囲で設定します。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。このコマンドは、ASA に対してグローバルです。

## コマンド デフォルト

デフォルトは 32768 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 | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.4(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

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。EtherChannel 内でのインターフェイス プライオリティについては、**lacp port-priority** コマンドを参照してください。

## 例

次に、システムのプライオリティをデフォルトよりも高くする（小さい数値を設定する）例を示します。

```
ciscoasa(config)# lacp system-priority 12345
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| channel-group | EtherChannel にインターフェイスを追加します。 |
| **interface port-channel** | EtherChannel を設定します。 |
| **lacp max-bundle** | チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。 |
| **lacp port-priority** | チャネル グループの物理インターフェイスのプライオリティを設定します。 |
| **lacp system-priority** | LACP システム プライオリティを設定します。 |
| **port-channel load-balance** | ロード バランシング アルゴリズムを設定します。 |
| **port-channel min-bundle** | ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。 |
| **show lacp** | LACP情報（トラフィック統計情報、システムID、ネイバーの詳細など）が表示されます。 |
| **show port-channel** | EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。 |
| **show port-channel load-balance** | ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。 |

# ldap-attribute-map

既存のマッピング構成を LDAP ホストにバインドするには、AAA サーバー 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。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| AAA サーバー ホスト 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 |
|---|---|
| 7.1(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

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 サーバー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、未入力の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 コンフィギュレーション 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 コンフィギュレーション モードで **map-name** コマンドと **map-value** コマンドを使用して、属性マッピング構成に情報を入力します。
3. AAA サーバーホストモードで **ldap-attribute-map** コマンドを使用し、属性マップ構成を LDAP サーバーにバインドします。

## 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。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ldap attribute-map (global configuration mode)** | ユーザー定義の属性名を 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** | ユーザー定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。 |
| map-value | ユーザー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

サーバー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 サーバー 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 サーバー ホスト コンフィギュレーション モードは、AAA サーバー 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* サーバー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。

## コマンド 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| AAA サーバー ホスト 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

このコマンドは LDAP サーバーでのみ有効です。

## 例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバーを設定し、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。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
```

```
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host
)# ldap-base-dn starthere
ciscoasa
(config-aaa-server-host)#
exit
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa-server host** | AAA サーバー 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 サーバー パラメータを設定できるようにします。 |
| **ldap-scope** | サーバー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 サーバー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 サーバー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 サーバー 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、ASA は標準の LDAP ポート（389）を使用します。 |
| *server* | LDAP サーバーの 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ーが存在する場合、この値はそのサーバーによって上書きされます。 |

## コマンド 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | 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 | • 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。 |

## 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。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(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。 |

| コマンド | 説明 |
| --- | --- |
| **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 サーバーに 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 サーバー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。 |

## コマンド 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | 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。 |

## 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。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(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 サーバー 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* サーバーが検索を開始する 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。

## 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。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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| AAA サーバー ホスト コンフィギュレーション モード | • 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

**ldap-group-base-dn** コマンドは、LDAP を使用する Active Directory サーバーにのみ適用され、**show ad-groups** コマンドがグループ検索を開始するために使用する 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。

```
ciscoasa(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 サーバーからの応答を ASA が待機する時間を調整します。 |
| **show ad-groups** | Active Directory サーバー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 サーバー 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 サーバー ホスト コンフィギュレーション モードは、AAA サーバー 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。

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| AAA サーバー ホスト 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

このコマンドは LDAP サーバーでのみ有効です。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 サーバーなどの一部の LDAP サーバーでは、他の LDAP 動作の要求を受け入れる前に、ASA 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。ASA は、ログイン DN フィールドをユーザー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、ASA 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ー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 サーバーを設定し、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。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa-server host** | AAA サーバー 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 サーバー パラメータを設定できるようにします。 |
| **ldap-base-dn** | サーバー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 サーバーでのみ有効です。 |
| **ldap-naming-attribute** | LDAP サーバー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** | サーバー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 サーバーのログインパスワードを指定するには、AAA サーバー 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 サーバー ホスト コンフィギュレーション モードは、AAA サーバー 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。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| AAA サーバー ホスト 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

このコマンドは LDAP サーバーでのみ有効です。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 サーバーを設定し、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。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server)# timeout 9
```

```
ciscoasa
(config-aaa-server)# retry 7
ciscoasa(config-aaa-server)# ldap-login-password obscurepassword
ciscoasa
(config-aaa-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa-server host** | AAA サーバー 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 サーバー パラメータを設定できるようにします。 |
| **ldap-base-dn** | サーバー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 サーバー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** | サーバー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

相対識別名属性を指定するには、AAA サーバー 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 サーバー ホスト コンフィギュレーション モードは、AAA サーバー 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。この仕様を削除するには、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 サーバー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。

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| AAA サーバー ホスト 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

LDAP サーバー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）とユーザー ID（uid）です。

このコマンドは LDAP サーバーでのみ有効です。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 サーバーを設定し、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。

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

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa-server host** | AAA サーバー 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 サーバー パラメータを設定できるようにします。 |
| **ldap-base-dn** | サーバー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 サーバーでのみ有効です。 |
| **ldap-scope** | サーバー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 ASA と LDAP サーバーの間で確立するには、AAA サーバー 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 を無効にするには、このコマンドの **no** 形式を使用します。

**ldap-over-ssl** [ **enable** | **reference-identity** *ref_id_name* ]

**no ldap-over-ssl** *ref_id_name* [enable|reference-identity]

## 構文の説明

| | |
|---|---|
| **enable** | SSL で LDAP サーバーへの接続を保護することを指定します。 |
| **reference-identity** *ref_id_name* | LDAP サーバー ID を検証するための参照 ID 名を指定します。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| AAA サーバー ホスト 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 |
|---|---|
| 7.1(1) | このコマンドが追加されました。 |
| 9.18(1) | このコマンドは、LDAP サーバー ID を検証するように拡張されました。 |

## 使用上のガイドライン

このコマンドを使用して、SSL で ASA と LDAP サーバー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 command.** を参照してください。

## 例

次に、AAA サーバー ホスト コンフィギュレーション モードで、ASA と LDAP サーバー ldapsvr1（IP アドレスは 10.10.0.1）間の接続に対して SSL を有効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。

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

参照 ID 名を指定して LDAP サーバー ID を検証するには、**reference-identity** *ref_id_name* を使用します。参照 ID オブジェクトは、一致基準を指定し、**crypto ca reference-identity refidname** を使用して作成されます。LDAP AAA サーバー構成で参照 ID を設定すると、ASA は LDAP サーバー証明書と一致するホスト名を見つけようとします。ホストの解決に失敗するか、一致するものが見つからない場合、エラーメッセージが表示されて接続が終了します。

```
asa(config-aaa-server-host)# ldap-over-ssl ?

aaa-server-host mode commands/options:
  enable              Require an SSL connection to the LDAP server
  reference-identity  Enter reference-identity name to validate LDAP server identity

asa(config-aaa-server-host)# ldap-over-ssl reference-identity ?

aaa-server-host mode commands/options:
  WORD < 65 char  Enter reference-identity name to validate LDAP server identity
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname ?

aaa-server-host mode commands/options:
  <cr>
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname
```

show running-config aaa server は、設定された参照 ID 名をオプションの 1 つとして表示します。

```
asa(config-aaa-server-host)# show running-config aaa-server
aaa-server ldaps protocol ldap
aaa-server ldaps (manif) host 10.86.93.107
server-port 636
ldap-base-dn CN=Users,DC=BXBCASERVERS,DC=COM
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn CN=administrator,CN=Users,DC=BXBCASERVERS,DC=com
ldap-over-ssl enable
ldap-over-ssl reference-identity refidname
server-type microsoft
```

## 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ーの間に SASL 認証を指定します。 |

| コマンド | 説明 |
| --- | --- |
| **server-type** | LDAP サーバー ベンダーに Microsoft または Sun のいずれかを指定します。 |
| **ssl-client-certificate** | LDAPS を使用する場合に、ASA がクライアント証明書として LDAP サーバーに提示する証明書を指定します。 |
| **crypto ca reference-identity refidname** | 参照 ID オブジェクトを設定するには、次の手順を実行します。 |

# ldap-scope

サーバー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サーバー 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 サーバー ホスト コンフィギュレーション モードは、AAA サーバー 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* サーバー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。有効な値は次のとおりです。

- **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。

## コマンド 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| AAA サーバー ホスト 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

scope に **onelevel** を指定すると、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 サーバーでのみ有効です。

## 例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバーを設定し、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。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa-server host** | AAA サーバー 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 サーバー パラメータを設定できるようにします。 |
| **ldap-base-dn** | サーバー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 サーバーでのみ有効です。 |
| **ldap-naming-attribute** | LDAP サーバー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 バイパスを有効にするには、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 バイパスを無効にするには、**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。 |

## コマンド 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | 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

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、ユーザー認証の前に 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、ユーザー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、CLI 設定ガイド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

次の例は、「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方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(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ー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ーに対して、接続前に ASA に識別情報を示すように要求します。 |

# license

要求の送信元の組織を示すために ASA からクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定するには、scansafe 汎用オプション コンフィギュレーション モードで **license** コマンドを使用します。ライセ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。

**license***hex_key*
**no license** [ *hex_key* ]

## 構文の説明

| | |
|---|---|
| *hex_key* | 16 バイトの 16 進数の形式で認証キーを指定します。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.0(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

各 ASA は、クラウド Web セキュリティから取得した認証キーを使用する必要があります。クラウド Web セキュリティでは認証キーを使用して、Web 要求に関連付けられた会社を識別し、ASA が有効なお客様に関連付けられていることを確認できます。

ASA では、2 つの認証キー（企業キーおよびグループ キー）のいずれか 1 つを使用できます。

### 企業認証キー

企業認証キーは、同一企業内の複数の ASA で使用できます。このキーは、単に ASA のクラウド Web セキュリティ サービスを有効にします。管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。生成したキーは後で使用するために電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、https://www.cisco.com/c/ja_jp/products/index.html から入手できます。

### グループ認証キー

グループ認証キーは 2 つの機能を実行する各 ASA に固有の特別なキーです。

- 1 つの ASA のクラウド Web セキュリティ サービスを有効にします。
- ASA からのすべてのトラフィックが識別されるため、ASA ごとに ScanCenter ポリシーを作成できます。

管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。生成したキーは後で使用するために電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、https://www.cisco.com/c/ja_jp/products/index.html から入手できます。

## 例

次に、プライマリ サーバーのみを設定する例を示します。

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

## 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ー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ー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ー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 サーバーに送信する認証キーを設定します。 |
| **match user group** | ユーザー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ーをポーリングする前に ASA が待機する時間です。 |

| コマンド | 説明 |
|---|---|
| **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 サーバー 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 サーバー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** | サーバーが現在のアクティブ サーバー、バックアップ サーバー、または到達不能のいずれであるか、サーバーのステータスを表示します。 |
| **show scansafe statistics** | 合計と現在の http 接続を表示します。 |
| **user-identity monitor** | AD エージェントから指定したユーザーまたはグループ情報をダウンロードします。 |
| **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。 |

# license-server address

参加者が使用する共有ライセンスサーバーの IP アドレスと共有秘密を指定するには、グローバル コンフィギュレーション モードで **license-server address** コマンドを使用します。共有ライセンスへの参加を無効にするには、このコマンドの **no** 形式を使用します。共有ライセンスを使用すると、ASA の 1 台を共有ライセンスサーバーに、残りの ASA を共有ライセンス参加者として設定することで、多数の SSL VPN セッションを購入し、ASA のグループ間で必要に応じてセッションを共有できます。

**license-server address** *address* **secret** *secret* [ **port port** ]
**no license-server address** [ *address* **secret** *secret* [ **port port** ] ]

## 構文の説明

| | |
|---|---|
| *address* | 共有ライセンス サーバーの IP アドレスを指定します。 |
| **port** *port* | （任意）**license-server port** コマンドを使用してサーバー構成のデフォルトポートを変更した場合は、その変更に合わせてバックアップサーバーのポート（1 ～ 65535）を設定します。デフォルトのポートは 50554 です。 |
| **secret** *secret* | 共有秘密を指定します。共有秘密は、**license-server secret** コマンドを使用してサーバーに設定された秘密と一致する必要があります。 |

## コマンド デフォルト

デフォルトのポートは 50554 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 | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

共有ライセンス参加ユニットには、共有ライセンス参加キーが必要です。インストールされているライセンスを確認するには、**show activation-key** コマンドを使用します。

参加ユニットごとに共有ライセンス サーバーを 1 つのみ指定できます。

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバーとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバーのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバーを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （オプション）別の ASA を共有ライセンス バックアップ サーバーとして指定します。バックアップ サーバーには 1 台のみ指定できます。

（注） 共有ライセンス バックアップ サーバーに必要なのは参加ライセンスのみです。

1. 共有ライセンス サーバー上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
2. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバーに登録します。

（注） 参加者は IP ネットワークを経由してサーバーと通信できる必要がありますが、同じサブネット上にある必要はありません。

1. 共有ライセンス サーバーは、参加者がサーバーにポーリングするべき頻度の情報で応答します。
2. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバーに 50 セッション単位で追加セッションの要求を送信します。
3. 共有ライセンス サーバーは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

（注） 共有ライセンスサーバーは、ローカル セッションを使い果たした場合に共有ライセンス プールに参加もできます。参加には参加ライセンスもサーバー ライセンスも必要ありません。

1. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバーは使用可能な限りのセッション数で応答します。
2. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバーが要求に適切に対応できるまで続けます。
3. 参加者の負荷が減少した場合、参加者はサーバーに共有セッションを解放するようにメッセージを送信します。

（注） ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

### 参加者とサーバー間の通信問題

参加者とサーバー間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔3倍の時間が経過した後で、サーバーはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバーに到達できない場合、参加者はサーバーから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24時間を経過しても参加者がまだライセンス サーバーと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバーに再接続したが、サーバーが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバーは、参加者に再割り当てできる限りのセッション数で応答します。

## 例

次に、ライセンス サーバーの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバーの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **activation-key** | ライセンス アクティベーション キーを入力します。 |
| **clear configure license-server** | 共有ライセンス サーバー コンフィギュレーションをクリアします。 |
| clear shared license | 共有ライセンス統計情報をクリアします。 |
| **license-server backup address** | 参加者の共有ライセンス バックアップ サーバーを指定します。 |
| **license-server backup backup-id** | メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。 |
| **license-server backup enable** | 共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。 |
| **license-server enable** | 共有ライセンス サーバーになるユニットをイネーブルにします。 |

| コマンド | 説明 |
|---|---|
| **license-server port** | サーバーが参加者からの SSL 接続をリッスンするポートを設定します。 |
| **license-server refresh-interval** | サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。 |
| license-server secret | 共有秘密を共有ライセンス サーバーに設定します。 |
| **show activation-key** | インストールされている現在のライセンスを表示します。 |
| **show running-config license-server** | 共有ライセンス サーバー コンフィギュレーションを表示します。 |
| **show shared license** | 共有ライセンス統計情報を表示します。 |
| **show vpn-sessiondb** | VPN セッションのライセンス情報を表示します。 |

# license-server backup address

参加者が使用する共有ライセンス バックアップ サーバーの IP アドレスを特定するには、グローバル コンフィギュレーション モードで **license-server backup address** コマンドを使用します。バックアップサーバーの使用を無効にするには、このコマンドの **no** 形式を使用します。

**license-server backup address** *address*
**no license-server address**［ **address** ］

## 構文の説明

| | |
|---|---|
| *address* | 共有ライセンス バックアップ サーバーの IP アドレスを指定します。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

共有ライセンス バックアップ サーバーには、 **license-server backup enable** コマンドが設定されている必要があります。

## 例

次に、ライセンス サーバーの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバーの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **activation-key** | ライセンス アクティベーション キーを入力します。 |

| コマンド | 説明 |
|---|---|
| **clear configure license-server** | 共有ライセンス サーバー コンフィギュレーションをクリアします。 |
| clear shared license | 共有ライセンス統計情報をクリアします。 |
| **license-server address** | 共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。 |
| **license-server backup backup-id** | メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。 |
| **license-server backup enable** | 共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。 |
| **license-server enable** | 共有ライセンス サーバーになるユニットをイネーブルにします。 |
| **license-server port** | サーバーが参加者からの SSL 接続をリッスンするポートを設定します。 |
| **license-server refresh-interval** | サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。 |
| license-server secret | 共有秘密を共有ライセンス サーバーに設定します。 |
| **show activation-key** | インストールされている現在のライセンスを表示します。 |
| **show running-config license-server** | 共有ライセンス サーバー コンフィギュレーションを表示します。 |
| **show shared license** | 共有ライセンス統計情報を表示します。 |
| **show vpn-sessiondb** | VPN セッションのライセンス情報を表示します。 |

# license-server backup backup-id

メイン共有ライセンスサーバー構成で共有ライセンスバックアップサーバーを指定するには、グローバル コンフィギュレーション モードで **license-server backup backup-id** コマンドを使用します。バックアップサーバー構成を削除するには、このコマンドの **no** 形式を使用します。

**license-server backup** *address* **backup-id** *serial_number* [ **ha-backup-id** *ha_serial_number* ]
**no license-server backup** *address* [ **backup-id** *serial_number* [ **ha-backup-id** *ha_serial_number* ] ]

## 構文の説明

| | |
|---|---|
| *address* | 共有ライセンス バックアップ サーバーの IP アドレスを指定します。 |
| **backup-id***serial_number* | 共有ライセンスバックアップサーバーのシリアル番号を指定します。 |
| **ha-backup-id** *ha_serial_number* | バックアップサーバでフェールオーバーを使用する場合は、セカンダリ共有ライセンスバックアップサーバのシリアル番号を指定します。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

1 つのバックアップ サーバとそのオプションのスタンバイ ユニットのみを指定できます。

バックアップサーバーのシリアル番号を表示するには、**show activation-key** コマンドを入力します。

参加ユニットをバックアップサーバーとして有効にするには、**license-server backup enable** コマンドを使用します。

共有ライセンス バックアップ サーバーは、バックアップの役割を実行する前にメインの共有ライセンス サーバーへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバーは共有ライセンス情報に加えてサーバー設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サーバーとバックアップ サーバーは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバーはリロード後でもバックアップの役割を実行できます。

メイン サーバーがダウンすると、バックアップ サーバーがサーバー動作を引き継ぎます。バックアップ サーバーは継続して最大 30 日間動作できます。30 日を超えると、バックアップ サーバーは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン サーバーをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバーが復旧した場合、メイン サーバーはバックアップ サーバーと同期してから、サーバー動作を引き継ぎます。

バックアップ サーバーがアクティブでないときは、メインの共有ライセンス サーバーの通常の参加者として動作します。

（注） メインの共有ライセンス サーバーの初回起動時には、バックアップ サーバーは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メイン サーバーがその後短時間でもダウンした場合、バックアップ サーバーの動作制限は日ごとに減少します。メイン サーバーが復旧した場合、バックアップ サーバーは再び日ごとに増加を開始します。たとえば、メイン サーバーが 20 日間ダウンしていて、その期間中バックアップ サーバーがアクティブであった場合、バックアップ サーバーには、10 日間の制限のみが残っています。バックアップ サーバーは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **activation-key** | ライセンス アクティベーション キーを入力します。 |
| **clear configure license-server** | 共有ライセンス サーバー コンフィギュレーションをクリアします。 |
| clear shared license | 共有ライセンス統計情報をクリアします。 |
| **license-server address** | 共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。 |
| **license-server backup address** | 参加者の共有ライセンス バックアップ サーバーを指定します。 |
| **license-server backup enable** | 共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。 |
| **license-server enable** | 共有ライセンス サーバーになるユニットをイネーブルにします。 |
| **license-server port** | サーバーが参加者からの SSL 接続をリッスンするポートを設定します。 |
| **license-server refresh-interval** | サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。 |
| license-server secret | 共有秘密を共有ライセンス サーバーに設定します。 |
| **show activation-key** | インストールされている現在のライセンスを表示します。 |
| **show running-config license-server** | 共有ライセンス サーバー コンフィギュレーションを表示します。 |
| **show shared license** | 共有ライセンス統計情報を表示します。 |
| **show vpn-sessiondb** | VPN セッションのライセンス情報を表示します。 |

# license-server backup enable

このユニットを共有ライセンス バックアップ サーバーとして有効にするには、グローバル コンフィギュレーション モードで **license-server backup enable** コマンドを使用します。バックアップサーバーを無効にするには、このコマンドの **no** 形式を使用します。

**license-server backup enable** *interface_name*
**no license-server enable** *interface_name*

## 構文の説明

| | |
|---|---|
| *interface_name* | 参加ユニットがバックアップ サーバーとの通信に使用するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

バックアップ サーバーには、共有ライセンス参加キーが必要です。

共有ライセンス バックアップ サーバーは、バックアップの役割を実行する前にメインの共有ライセンス サーバーへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバーは共有ライセンス情報に加えてサーバー設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サーバーとバックアップ サーバーは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバーはリロード後でもバックアップの役割を実行できます。

メイン サーバーがダウンすると、バックアップ サーバーがサーバー動作を引き継ぎます。バックアップ サーバーは継続して最大 30 日間動作できます。30 日を超えると、バックアップ サーバーは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン

サーバーをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバーが復旧した場合、メイン サーバーはバックアップ サーバーと同期してから、サーバー動作を引き継ぎます。

バックアップ サーバーがアクティブでないときは、メインの共有ライセンス サーバーの通常の参加者として動作します。

（注） メインの共有ライセンス サーバーの初回起動時には、バックアップ サーバーは独立して 5 日間のみ動作できます。動作制限は30日に到達するまで日ごとに増加します。また、メインサーバーがその後短時間でもダウンした場合、バックアップサーバーの動作制限は日ごとに減少します。メイン サーバーが復旧した場合、バックアップ サーバーは再び日ごとに増加を開始します。たとえば、メイン サーバーが 20 日間ダウンしていて、その期間中バックアップ サーバーがアクティブであった場合、バックアップ サーバーには、10 日間の制限のみが残っています。バックアップ サーバーは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

## 例

次に、ライセンス サーバーと共有秘密を指定し、このユニットを内部インターフェイスと dmz インターフェイス上のバックアップ共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **activation-key** | ライセンス アクティベーション キーを入力します。 |
| **clear configure license-server** | 共有ライセンス サーバー コンフィギュレーションをクリアします。 |
| clear shared license | 共有ライセンス統計情報をクリアします。 |
| **license-server address** | 共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。 |
| **license-server backup address** | 参加者の共有ライセンス バックアップ サーバーを指定します。 |
| **license-server backup backup-id** | メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。 |

| コマンド | 説明 |
|---|---|
| **license-server enable** | 共有ライセンス サーバーになるユニットをイネーブルにします。 |
| **license-server port** | サーバーが参加者からの SSL 接続をリッスンするポートを設定します。 |
| **license-server refresh-interval** | サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。 |
| license-server secret | 共有秘密を共有ライセンス サーバーに設定します。 |
| **show activation-key** | インストールされている現在のライセンスを表示します。 |
| **show running-config license-server** | 共有ライセンス サーバー コンフィギュレーションを表示します。 |
| **show shared license** | 共有ライセンス統計情報を表示します。 |
| **show vpn-sessiondb** | VPN セッションのライセンス情報を表示します。 |

# license-server enable

このユニットを共有ライセンスサーバーとして指定するには、グローバル コンフィギュレーション モードで **license-server enable** コマンドを使用します。共有ライセンスサーバーを無効にするには、このコマンドの **no** 形式を使用します。共有ライセンスを使用すると、ASA の 1 台を共有ライセンスサーバーに、残りの ASA を共有ライセンス参加者として設定することで、多数の SSL VPN セッションを購入し、ASA のグループ間で必要に応じてセッションを共有できます。

**license-server enable** *interface_name*
**no license-server enable** *interface_name*

## 構文の説明

| | |
|---|---|
| *interface_name* | 参加ユニットがサーバーとの通信に使用するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | • 対応 | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

共有ライセンス サーバには、共有ライセンス サーバ キーが必要です。インストールされているライセンスを確認するには、**show activation-key** コマンドを使用します。

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバーとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバーのライセンスを購入します。

2. いずれの ASA を共有ライセンス バックアップ サーバーを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （オプション）別の ASA を共有ライセンス バックアップ サーバーとして指定します。バックアップ サーバーには 1 台のみ指定できます。

（注） 共有ライセンス バックアップ サーバーに必要なのは参加ライセンスのみです。

1. 共有ライセンス サーバー上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
2. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバーに登録します。

（注） 参加者は IP ネットワークを経由してサーバーと通信できる必要がありますが、同じサブネット上にある必要はありません。

1. 共有ライセンス サーバーは、参加者がサーバーにポーリングするべき頻度の情報で応答します。
2. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバーに 50 セッション単位で追加セッションの要求を送信します。
3. 共有ライセンス サーバーは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

（注） 共有ライセンスサーバーは、ローカル セッションを使い果たした場合に共有ライセンス プールに参加もできます。参加には参加ライセンスもサーバー ライセンスも必要ありません。

1. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバーは使用可能な限りのセッション数で応答します。
2. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバーが要求に適切に対応できるまで続けます。
3. 参加者の負荷が減少した場合、参加者はサーバーに共有セッションを解放するようにメッセージを送信します。

（注） ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

### 参加者とサーバー間の通信問題

参加者とサーバー間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔3倍の時間が経過した後で、サーバーはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバーに到達できない場合、参加者はサーバーから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24時間を経過しても参加者がまだライセンス サーバーと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバーに再接続したが、サーバーが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバーは、参加者に再割り当てできる限りのセッション数で応答します。

## 例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットをinsideインターフェイスおよびDMZインターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **activation-key** | ライセンス アクティベーション キーを入力します。 |
| **clear configure license-server** | 共有ライセンス サーバー コンフィギュレーションをクリアします。 |
| clear shared license | 共有ライセンス統計情報をクリアします。 |
| **license-server address** | 共有ライセンス サーバーのIPアドレスと参加者の共有秘密を指定します。 |
| **license-server backup address** | 参加者の共有ライセンスバックアップ サーバーを指定します。 |
| **license-server backup backup-id** | メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。 |
| **license-server backup enable** | 共有ライセンスバックアップ サーバーになるユニットをイネーブルにします。 |

| コマンド | 説明 |
|---|---|
| **license-server port** | サーバーが参加者からの SSL 接続をリッスンするポートを設定します。 |
| **license-server refresh-interval** | サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。 |
| license-server secret | 共有秘密を共有ライセンス サーバーに設定します。 |
| **show activation-key** | インストールされている現在のライセンスを表示します。 |
| **show running-config license-server** | 共有ライセンス サーバー コンフィギュレーションを表示します。 |
| **show shared license** | 共有ライセンス統計情報を表示します。 |
| **show vpn-sessiondb** | VPN セッションのライセンス情報を表示します。 |

# license-server port

共有ライセンスサーバーが参加者からの SSL 接続をリッスンするポートを設定するには、グローバル コンフィギュレーション モードで **license-server port** コマンドを使用します。デフォルトポートに戻すには、このコマンドの **no** 形式を使用します。

**license-server port** *port*
**no license-server port** [ *port* ]

## 構文の説明

*seconds* 参加ユニットからの SSL 接続をサーバーがリッスンするポート（1 ～ 65535）を設定します。デフォルトは、TCP ポート 50554 です。

## コマンド デフォルト

デフォルトのポートは 50554 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 | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

デフォルトポートを変更する場合は、**license-server address** コマンドを使用して、各参加者に同じポートを設定してください。

## 例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび DMZ インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

```
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **activation-key** | ライセンス アクティベーション キーを入力します。 |
| **clear configure license-server** | 共有ライセンス サーバー コンフィギュレーションをクリアします。 |
| clear shared license | 共有ライセンス統計情報をクリアします。 |
| **license-server address** | 共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。 |
| **license-server backup address** | 参加者の共有ライセンス バックアップ サーバーを指定します。 |
| **license-server backup backup-id** | メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。 |
| **license-server backup enable** | 共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。 |
| **license-server enable** | 共有ライセンス サーバーになるユニットをイネーブルにします。 |
| **license-server refresh-interval** | サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。 |
| license-server secret | 共有秘密を共有ライセンス サーバーに設定します。 |
| **show activation-key** | インストールされている現在のライセンスを表示します。 |
| **show running-config license-server** | 共有ライセンス サーバー コンフィギュレーションを表示します。 |
| **show shared license** | 共有ライセンス統計情報を表示します。 |
| **show vpn-sessiondb** | VPN セッションのライセンス情報を表示します。 |

# license-server refresh-interval

参加者が共有ライセンスサーバーと通信する頻度を設定するために参加者に提供されるリフレッシュ間隔を設定するには、グローバル コンフィギュレーション モードで **license-server refresh-interval** コマンドを使用します。デフォルトのリフレッシュ間隔に戻すには、このコマンドの **no** 形式を使用します。

**license-server refresh-interval** *seconds*
**no license-server refresh-interval** [ *seconds* ]

## 構文の説明

*seconds* リフレッシュ間隔（10 ～ 300 秒）を設定します。デフォルトは 30 秒です。

## コマンド デフォルト

デフォルトは 30 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

各参加ユニットは、SSL を使用して定期的に共有ライセンス サーバーと通信します。そのため、共有ライセンス サーバーは現在のライセンス使用状況を把握し、ライセンス要求を受信したりライセンス要求に応答できます。

## 例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

```
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **activation-key** | ライセンス アクティベーション キーを入力します。 |
| **clear configure license-server** | 共有ライセンス サーバー コンフィギュレーションをクリアします。 |
| clear shared license | 共有ライセンス統計情報をクリアします。 |
| **license-server address** | 共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。 |
| **license-server backup address** | 参加者の共有ライセンス バックアップ サーバーを指定します。 |
| **license-server backup backup-id** | メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。 |
| **license-server backup enable** | 共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。 |
| **license-server enable** | 共有ライセンス サーバーになるユニットをイネーブルにします。 |
| **license-server port** | サーバーが参加者からの SSL 接続をリッスンするポートを設定します。 |
| license-server secret | 共有秘密を共有ライセンス サーバーに設定します。 |
| **show activation-key** | インストールされている現在のライセンスを表示します。 |
| **show running-config license-server** | 共有ライセンス サーバー コンフィギュレーションを表示します。 |
| **show shared license** | 共有ライセンス統計情報を表示します。 |
| **show vpn-sessiondb** | VPN セッションのライセンス情報を表示します。 |

# license-server secret

共有ライセンスサーバーに共有秘密を設定するには、グローバル コンフィギュレーション モードで **license-server secret** コマンドを使用します。共有秘密を削除するには、このコマンドの **no** 形式を使用します。

**license-server secret** *secret*
**no license-server secret** *secret*

## 構文の説明

| | |
|---|---|
| *secret* | 共有秘密を 4 ～ 128 文字の ASCII 文字のストリングで設定します。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

この共有秘密を持つ、**license-server address** コマンドで指定された参加者は、ライセンスサーバーを使用できます。

## 例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **activation-key** | ライセンス アクティベーション キーを入力します。 |
| **clear configure license-server** | 共有ライセンス サーバー コンフィギュレーションをクリアします。 |
| clear shared license | 共有ライセンス統計情報をクリアします。 |
| **license-server address** | 共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。 |
| **license-server backup address** | 参加者の共有ライセンス バックアップ サーバーを指定します。 |
| **license-server backup backup-id** | メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。 |
| **license-server backup enable** | 共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。 |
| **license-server enable** | 共有ライセンス サーバーになるユニットをイネーブルにします。 |
| **license-server port** | サーバーが参加者からの SSL 接続をリッスンするポートを設定します。 |
| **license-server refresh-interval** | サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。 |
| **show activation-key** | インストールされている現在のライセンスを表示します。 |
| **show running-config license-server** | 共有ライセンス サーバー コンフィギュレーションを表示します。 |
| **show shared license** | 共有ライセンス統計情報を表示します。 |
| **show vpn-sessiondb** | VPN セッションのライセンス情報を表示します。 |

# license smart

スマートライセンス資格要求を設定するには、グローバル コンフィギュレーション モードで **license smart** コマンドを使用します。資格を削除してデバイスのライセンスを解除するには、このコマンドの **no** 形式を使用します。

（注） この機能は、ASA 仮想 およびシャーシのみでサポートされています。

**license smart**
**no license smart**

## 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

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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.3(2) | このコマンドは、ASA 仮想のサポートのために追加されました。 |
| 9.4(1.152) | Firepower 9300 のサポートが追加されました。 |
| 9.6(1) | Firepower 4100 シリーズのサポートが追加されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

## 使用上のガイドライン

このコマンドを使用すると、ライセンス スマート コンフィギュレーション モードになり、機能層やその他のライセンス資格を設定できます。ASA 仮想 の場合、初めて権限付与を要求したときは、変更を有効にするためにライセンス スマート コンフィギュレーション モードを終了する必要があります。

## 例

次に、機能階層を標準に設定し、スループット レベルを 2G に設定する例を示します。

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **call-home** | Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。 |
| **clear configure license** | スマート ライセンス設定をクリアします。 |
| **feature tier** | スマート ライセンスの機能層を設定します。 |
| **http-proxy** | スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。 |
| **license smart** | スマート ライセンスのライセンス権限付与を要求できます。 |
| **license smart deregister** | ライセンス認証局からデバイスを登録解除します。 |
| **license smart register** | デバイスをライセンス認証局に登録します。 |
| **license smart renew** | 登録またはライセンス権限を更新します。 |
| **service call-home** | Smart Call Home をイネーブルにします。 |
| **show license** | スマート ライセンスのステータスを表示します。 |
| **show running-config license** | スマート ライセンスの設定を表示します。 |
| **throughput level** | スマート ライセンスのスループット レベルを設定します。 |

# license smart deregister

Cisco License Authority に対するデバイスのスマートライセンス登録を解除するには、特権 EXEC モードで **license smart deregister** コマンドを使用します。

（注） この機能は、ASA 仮想 および Firepower 2100 だけでサポートされています。

**license smart deregister**

## 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

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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.3(2) | このコマンドは、ASA 仮想 のサポートのために追加されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

## 使用上のガイドライン

ASA の登録を解除すると、アカウントから ASA が削除されます。ASA のすべてのライセンス権限付与と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA に利用することもできます。このコマンドを実行すると、ASA がリロードします。

## 例

次に、デバイスの登録を解除する例を示します。

```
ciscoasa# license smart deregister
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **call-home** | Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。 |

| コマンド | 説明 |
|---|---|
| **clear configure license** | スマート ライセンス設定をクリアします。 |
| **feature tier** | スマート ライセンスの機能層を設定します。 |
| **http-proxy** | スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。 |
| **license smart** | スマート ライセンスのライセンス権限付与を要求できます。 |
| **license smart deregister** | ライセンス認証局からデバイスを登録解除します。 |
| **license smart register** | デバイスをライセンス認証局に登録します。 |
| **license smart renew** | 登録またはライセンス権限を更新します。 |
| **service call-home** | Smart Call Home をイネーブルにします。 |
| **show license** | スマート ライセンスのステータスを表示します。 |
| **show running-config license** | スマート ライセンスの設定を表示します。 |
| **throughput level** | スマート ライセンスのスループット レベルを設定します。 |

# license smart register

Cisco License Authority に対するデバイスのスマートライセンスを登録するには、特権 EXEC モードで **license smart register** コマンドを使用します。

（注） この機能は、ASA 仮想 および Firepower 2100 だけでサポートされています。

**license smart register idtoken** *id_token*［ **force** ］

## 構文の説明

| | |
|---|---|
| **idtoken** *id_token* | Smart Software Manager で、この ASA を追加するバーチャル アカウントの登録トークンを要求してコピーします。 |
| **force** | License Authority と同期されていない可能性がある登録済みの ASA を登録します。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.3(2) | このコマンドは、ASA 仮想のサポートのために追加されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

## 使用上のガイドライン

License Authority に ASA を登録すると、ASA と License Authority の間の通信に使用する ID 証明書が発行されます。また、該当するバーチャル アカウントに ASA が割り当てられます。通常、この手順は1回で済みます。ただし、通信の問題などが原因でアイデンティティ証明書の期限が切れた場合は、ASA の再登録が必要になります。

## 例

次に、登録トークンを使用して登録を行う例を示します。

```
ciscoasa# license smart register idtoken
```

YjE3NjcyMzYtMGQzMi00ODA4LWJhODItNzBhMGQ2NGRlYjUxLTE0MTQ5NDAy%0ADQzNzl8NXk2bzV3SDE0ZkgwQkdMRmZlNlNCNGlvRnBHUEpjcm02WlB4TU4w%0Ac2NrMD0%3D%0A

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **call-home** | Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。 |
| **clear configure license** | スマート ライセンス設定をクリアします。 |
| **feature tier** | スマート ライセンスの機能層を設定します。 |
| **http-proxy** | スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。 |
| **license smart** | スマート ライセンスのライセンス権限付与を要求できます。 |
| **license smart deregister** | ライセンス認証局からデバイスを登録解除します。 |
| **license smart register** | デバイスをライセンス認証局に登録します。 |
| **license smart renew** | 登録またはライセンス権限を更新します。 |
| **service call-home** | Smart Call Home をイネーブルにします。 |
| **show license** | スマート ライセンスのステータスを表示します。 |
| **show running-config license** | スマート ライセンスの設定を表示します。 |
| **throughput level** | スマート ライセンスのスループット レベルを設定します。 |

# license smart renew

スマートライセンスの登録またはソフトウェア利用資格の認証を更新するには、特権 EXEC モードで **license smart renew** コマンドを使用します。

（注） この機能は、ASA 仮想 および Firepower 2100 だけでサポートされています。

**license smart renew** { **id** | **auth** }

## 構文の説明

| | |
|---|---|
| **id** | デバイスの登録を更新します。 |
| **auth** | ライセンス資格を更新します。 |

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.3(2) | このコマンドは、ASA 仮想のサポートのために追加されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

## 使用上のガイドライン

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

## 例

次に、登録とライセンスの両方の認証を更新する例を示します。

```
ciscoasa# license smart renew id
ciscoasa# license smart renew auth
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **call-home** | Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。 |
| **clear configure license** | スマート ライセンス設定をクリアします。 |
| **feature tier** | スマート ライセンスの機能層を設定します。 |
| **http-proxy** | スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。 |
| **license smart** | スマート ライセンスのライセンス権限付与を要求できます。 |
| **license smart deregister** | ライセンス認証局からデバイスを登録解除します。 |
| **license smart register** | デバイスをライセンス認証局に登録します。 |
| **license smart renew** | 登録またはライセンス権限を更新します。 |
| **service call-home** | Smart Call Home をイネーブルにします。 |
| **show license** | スマート ライセンスのステータスを表示します。 |
| **show running-config license** | スマート ライセンスの設定を表示します。 |
| **throughput level** | スマート ライセンスのスループット レベルを設定します。 |

# license smart reservation

永続ライセンス予約を有効にするには、グローバル コンフィギュレーション モードで **license smart reservation** コマンドを使用します。永続ライセンス予約を無効にするには、このコマンドの **no** 形式を使用します。

**license smart reservation**
**no license smart reservation**

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

## 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 | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.5(2.200) | このコマンドは、ASA 仮想 のサポート用に導入されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

## 使用上のガイドライン

インターネットアクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます（https://software.cisco.com/#SmartLicensing-Inventory）。パーマネント ライセンスでは、すべての機能を最大限に使用できます。

ASA 仮想 の場合、**license smart reservation** コマンドを入力すると、次のコマンドが削除されます。

```
license smart
feature tier standard
throughput level {100M | 1G | 2G}
```

通常のスマート ライセンスを使用するには、このコマンドの **no** 形式を使用し、上記のコマンドを再入力します。その他の Smart Call Home 設定はそのまま維持されますが、使用されないため、それらのコマンドを再入力する必要はありません。

シャーシの場合、コンテキストライセンスなどのデフォルト以外のライセンスに対しては、**license smart**/**feature** コマンドを入力する必要があります。これらのコマンドは、ASA に機能の設定を許可するよう指定するために必要です。

（注） 永続ライセンスの予約については、ASA を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASA に再使用できません。**license smart reservation return** コマンドを参照してください。

## 例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **license smart reservation** | パーマネント ライセンスの予約をイネーブルにします。 |
| **license smart reservation cancel** | Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。 |
| **license smart reservation install** | 承認コードを入力します。 |
| **license smart reservation request universal** | Smart Software Manager に入力するライセンス コードを要求します。 |
| **license smart reservation return** | Smart Software Manager にライセンスを戻します。 |

# license smart reservation cancel

まだSmart Software Managerでコードを入力していない場合に永続ライセンス予約の要求をキャンセルするには、特権EXECモードで**license smart reservation cancel** コマンドを使用します。

**license smart reservation cancel**

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

## 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

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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.5(2.200) | このコマンドは、ASA仮想のサポート用に導入されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

## 使用上のガイドライン

**license smart reservation request universal** コマンドを使用して Smart Software Manager に入力するライセンスコードを要求した場合、そのコードをまだ Smart Software Manager に入力していなければ、**license smart reservation cancel** コマンドを使用して要求をキャンセルできます。

永続ライセンスの予約を無効にする（**no license smart reservation**）と、保留中のすべての要求がキャンセルされます。

すでに Smart Software Manager にコードを入力している場合は、ASA へのライセンスの適用を完了する必要があります。その時点から、**license smart reservation return** コマンドを使用してライセンスを返却できます。

## 例

次に、パーマネントライセンスの予約をイネーブルにして、Smart Software Managerに入力するライセンス コードを要求した後に、要求をキャンセルする例を示します。

```
ciscoasa(config)# license smart reservation
```

```
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa(config)# license smart reservation cancel
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **license smart reservation** | パーマネント ライセンスの予約をイネーブルにします。 |
| **license smart reservation cancel** | Smart Software Manager でコードを入力していない場合に、パーマネントライセンスの要求をキャンセルします。 |
| **license smart reservation install** | 承認コードを入力します。 |
| **license smart reservation request universal** | Smart Software Manager に入力するライセンス コードを要求します。 |
| **license smart reservation return** | Smart Software Manager にライセンスを戻します。 |

# license smart reservation install

Smart Software Manager から受け取った永続ライセンスの予約の承認コードを入力するには、特権 EXEC モードで **license smart reservation install** コマンドを使用します。

**license smart reservation install** *code*

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

**構文の説明**

*code* Smart Software Manager から受け取ったパーマネント ライセンスの予約の承認コード。

**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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 9.5(2.200) | このコマンドは、ASA 仮想 のサポート用に導入されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

**使用上のガイドライン**

インターネットアクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます（https://software.cisco.com/#SmartLicensing-Inventory）。**license smart reservation request universal** コマンドを使用して Smart Software Manager に入力するコードを要求します。Smart Software Manager にコードを入力するときは、受け取った承認コードをコピーして、**license smart reservation install** コマンドを使用して ASA に入力します。

**例**

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
```

```
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **license smart reservation** | パーマネント ライセンスの予約をイネーブルにします。 |
| **license smart reservation cancel** | Smart Software Manager でコードを入力していない場合に、パーマネントライセンスの要求をキャンセルします。 |
| **license smart reservation install** | 承認コードを入力します。 |
| **license smart reservation request universal** | Smart Software Manager に入力するライセンス コードを要求します。 |
| **license smart reservation return** | Smart Software Manager にライセンスを戻します。 |

# license smart reservation universal

Smart Software Manager に入力するライセンスコードを要求するには、特権 EXEC モードで **license smart reservation universal** コマンドを使用します。

**license smart reservation universal**

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

## 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

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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.5(2.200) | このコマンドは、ASA 仮想 のサポート用に導入されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

## 使用上のガイドライン

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。**license smart reservation request universal** コマンドを使用して Smart Software Manager に入力するコードを要求します。

ASA 仮想 の導入により、要求するライセンス（ASAv5/ASAv10/ASAv30）が決まります。

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、**license smart reservation cancel** コマンドを入力します。

パーマネントライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。**license smart reservation return** コマンドを参照してください。

承認コードを要求するには、Smart Software Manager のインベントリ画面（https://software.cisco.com/#SmartLicensing-Inventory）に移動して、[**Licenses**] タブをクリックします。**Licenses** タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。[**License Reservation**] をクリックして、ASA のコードをボックスに入力します。**Reserve License** をクリックします。Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[**License Reservation**] ボタンが表示されない場合、お使いのアカウントには永続ライセンスの予約が許可されていません。この場合、パーマネント ライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

**license smart reservation install** コマンドを使用して ASA に承認コードを入力します。

## 例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **license smart reservation** | パーマネント ライセンスの予約をイネーブルにします。 |
| **license smart reservation cancel** | Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。 |
| **license smart reservation install** | 承認コードを入力します。 |
| **license smart reservation request universal** | Smart Software Manager に入力するライセンス コードを要求します。 |
| **license smart reservation return** | Smart Software Manager にライセンスを戻します。 |

# license smart reservation return

Smart Software Managerにライセンスを戻すためのリターンコードを生成するには、特権EXECモードで **license smart reservation return** コマンドを使用します。

**license smart reservation return**

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

## 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

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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| 特権 EXEC | • 対応 | • 対応 | • 対応 | — | • 対応 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.5(2.200) | このコマンドは、ASA仮想のサポート用に導入されました。 |
| 9.8(2) | Firepower 2100 シリーズのサポートが追加されました。 |

## 使用上のガイドライン

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。永続ライセンスが不要になった場合（ASA を廃棄する場合や ASA 仮想 のモデルレベルの変更によって新しいライセンスが必要になった場合など）、ライセンスを正式に Smart Software Manager に返却する必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、他の場所で使用するために容易に解除できません。

**license smart reservation return** コマンドを入力すると、ASA がただちにライセンス未適用状態になり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンスを要求する（**license smart reservation request universal**）か、ASA 仮想 のモデルレベルを変更する（電源を切って vCPU/RAM を変更する）と、このコードは再表示できないことに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。

Smart Software Manager にコードを入力する前に、**show license udi** コマンドを使用して ASA のユニバーサル デバイス識別子（UDI）を表示すると、この ASA インスタンスを Smart Software

Manager で確認できます。Smart Software Manager インベントリ画面（https://software.cisco.com/#SmartLicensing-Inventory）に移動して、[**Product Instances**] タブをクリックします。[**Product Instances**] タブに、ライセンスが付与されているすべての製品が UDI で表示されます。ライセンスを解除する ASA 仮想 を確認し、[**Actions > Remove**] を選択して、ASA のリターンコードをボックスに入力します。**Remove Product Instance** をクリックします。パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

## 例

次に、ASA 仮想 でリターンコードを生成し、ASA 仮想 UDI を表示する例を示します。

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **license smart reservation** | パーマネント ライセンスの予約をイネーブルにします。 |
| **license smart reservation cancel** | Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。 |
| **license smart reservation install** | 承認コードを入力します。 |
| **license smart reservation request universal** | Smart Software Manager に入力するライセンス コードを要求します。 |
| **license smart reservation return** | Smart Software Manager にライセンスを戻します。 |

# lifetime（CA サーバー モード）

ローカル認証局（CA）証明書、各発行済み証明書、または証明書失効リスト（CRL）の有効期間を指定するには、CA サーバー 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*
**lifetime** { **ca-certificate** | **certificate** | **crl** }

## 構文の説明

| | |
|---|---|
| **ca-certificate** | ローカル CA サーバー証明書のライフタイムを指定します。 |
| **certificate** | CA サーバーが発行するすべてのユーザー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。有効範囲は 5 ～ 30 年です。デフォルトのライフタイム値は 15 年です。<br>発行されたすべてのユーザー証明書の有効範囲は 1 日 ～ 4 年です。デフォルトのライフタイム値は 2 年です。<br>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。 |

## コマンド 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：15 年
- 発行済み証明書：2 年
- 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| CA サーバー 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 |
|---|---|
| 8.0(2) | このコマンドが追加されました。 |
| 9.12(1) | lifetime ca-certificate で使用可能な値は、5 ～ 30 年に変更されており、デフォルトは 15 年です。<br>lifetime certificate で使用可能な値は、1 日 ～ 4 年に変更されており、デフォルトは 2 年です。 |

## 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。

**lifetime ca-certificate** コマンドは、ローカル CA サーバー証明書の初回生成時（初めてローカル CA サーバーを設定し、**no shutdown** コマンドを発行するとき）に有効になります。CA 証明書の期限が切れると、設定されたライフタイム値を使用して新しい CA 証明書が生成されます。既存の CA 証明書のライフタイム値は変更できません。

## 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。

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

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime crl 48
ciscoasa
(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 サーバー コンフィギュレーション モードのコマンド 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 セットを使用することで、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。 |

| コマンド | 説明 |
| --- | --- |
| **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 サーバー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。 |

# lifetime（IKEv2 ポリシー モード）

AnyConnect IPsec 接続に使用する IKEv2 セキュリティ アソシエーション（SA）の暗号化アルゴリズムを指定するには、IKEv2 ポリシー コンフィギュレーション モードで encryption コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

**lifetime** { { **seconds** *seconds* } | **none** }

## 構文の説明

| | |
|---|---|
| *seconds* | ライフタイムの秒数（120 ～ 2,147,483,647 秒）。デフォルトは 86,400 秒（24 時間）です。 |

## コマンド デフォルト

デフォルトは 86,400 秒（24 時間）です。

## 使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。crypto ikev2 policy コマンドを入力した後、**lifetime** コマンドを使用して SA ライフタイムを設定します。

このコマンドでは、IKEv2 SA のキーを再生成する間隔を設定します。none キーワードを使用すると、SA のキー再生成がディセーブルになります。ただし、引き続き セキュアクライアント で SA のキー再生成を実行できます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| グローバル コンフィギュレーション | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.4(1) | このコマンドが追加されました。 |

## 例

次に、IKEv2 ポリシー コンフィギュレーション モードを開始し、ライフタイムを 43,200 秒（12 時間）に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# lifetime 43200
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| encryption | AnyConnect IPsec 接続に対して IKEv2 SA の暗号化アルゴリズムを指定します。 |
| group | AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。 |
| **integrity** | AnyConnect IPsec 接続に対して IKEv2 SA の ESP 整合性アルゴリズムを指定します。 |
| **prf** | AnyConnect IPsec 接続に対して IKEv2 SA の疑似乱数関数を指定します。 |

# 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。ASA 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** [ **rate** ] { **all** | *resource_name* } *number* [ **%** ] }
**no limit-resource** [ **rate** ] { **all** | *resource_name* }

## 構文の説明

| | |
|---|---|
| **all** | すべてのリソースの制限を設定します。 |
| *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。リソースに制限がないことを示すには、制限を **0** に設定します。VPN リソース タイプの場合は、制限をなしに設定します。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 1 : リソース名および制限 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。この制限で、**all** に設定されている制限が上書きされます。 |

## コマンド デフォルト

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルトクラスに属します。コンテキストをデフォルトクラスに積極的に割り当てる必要はありません。

ほとんどのリソースについては、デフォルトクラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション：5 セッション。（コンテキストあたりの最大値）。
- SSH セッション：5 セッション。（コンテキストあたりの最大値）。
- ASDM セッション：5 セッション。（コンテキストあたりの最大値）。
- IPsec セッション：5 セッション。（コンテキストあたりの最大値）。
- MAC アドレス：65,535 エントリ。（コンテキストあたりの最大値）。
- AnyConnect ピア：0 セッション（AnyConnect ピアを許可するようにクラスを手動で設定する必要があります）。
- VPN サイトツーサイトトンネル：0 セッション（VPN セッションを許可するようにクラスを手動で設定する必要があります）。
- HTTPS セッション：6 セッション。（コンテキストあたりの最大値）。

（注） また、コンテキスト内で **quota management-session** コマンドを設定して最大管理セッション（SSH など）を設定した場合は、小さい方の値が使用されます。

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| クラス 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 |
|---|---|
| 7.2(1) | このコマンドが追加されました。 |
| 9.0(1) | 各コンテキストでのルーティング テーブル エントリの最大数を設定するために、新規リソース タイプ **routes** が作成されました。<br>各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するために、新しいリソースタイプ **vpn other** と **vpn burst other** が作成されました。 |
| 9.5(2) | 各コンテキストでの AnyConnect VPN ピアの最大数を設定するために、新しいリソースタイプ **vpn anyconnect** と **vpn burst anyconnect** が作成されました。 |
| 9.6(2) | 最大ストレージを設定するために、新しいリソースタイプ **storage** が作成されました。 |
| 9.12(1) | HTTPS 接続を制御するために、新しいリソースタイプ **http** が追加されました。 |

## 使用上のガイドライン

デフォルトでは、すべてのセキュリティ コンテキストは ASA のリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPN のリソース（デフォルトでディセーブルになっています）です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

表 1 : リソース名および制限 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。

表 *1*: リソース名および制限

| 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[1] | 説明 |
|---|---|---|---|---|
| **asdm** | 同時接続数 | 最小 1<br>最大 5 | 200 | ASDM 管理セッション。<br>（注） ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 200 の場合、HTTPS セッション数は 400 に制限されます。 |
| **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、CLI 設定ガイドを参照してください。<br>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）。 |
| **hosts** | 同時接続数 | 該当なし | 該当なし | ASA 経由で接続可能なホスト。 |
| **http** | 同時接続数 | 最小 1<br>最大 6 | 100 | 非 ASDM HTTPS セッション |
| **inspects** | 利率 | 該当なし | 該当なし | アプリケーション インスペクション。 |
| **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。 |
| **routes** | 同時接続数 | 該当なし | 該当なし | ダイナミック ルート。 |
| **ssh** | 同時接続数 | 最小 1<br>最大 5 | 100 | SSH セッション。 |
| **storage** | MB | 最大値は、指定するフラッシュ メモリのドライブによって異なります。 | 最大値は、指定するフラッシュ メモリのドライブによって異なります。 | コンテキストでのディレクトリのストレージ制限（MB 単位）。ドライブを指定するには、**storage-url** コマンドを使用します。 |
| **syslogs** | 利率 | 該当なし | 該当なし | システム ログ メッセージ。 |

| 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[1] | 説明 |
|---|---|---|---|---|
| **telnet** | 同時接続数 | 最小 1<br>最大 5 | 100 | Telnet セッション。 |
| **vpn burst anyconnect** | 同時接続数 | 該当なし | モデルに応じた AnyConnect Premium ピア数から、vpn anyconnect 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。 | **vpn anyconnect** でコンテキストに割り当てられた数を超えて許可される AnyConnect セッションの数。たとえば、使用するモデルで 5000 のピアがサポートされており、**vpn anyconnect** で割り当てたピア数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが **vpn burst anyconnect** に使用可能です。**vpn anyconnect** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst anyconnect** ではオーバーサブスクライブが可能で、すべてのコンテキストがバーストプールを先着順に使用できます。 |
| **vpn anyconnect** | 同時接続数 | 該当なし | モデルごとの使用可能な AnyConnect VPN ピア数については、CLI 設定ガイドの「モデルごとにサポートされている機能のライセンス」を参照してください。 | AnyConnect ピア。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたピアは、そのコンテキストに対して保証されます。 |
| **vpn burst other** | 同時接続数 | 該当なし | モデルに応じた Other VPN セッション数から、**vpn other** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。 | **vpn other** でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数。たとえば、使用するモデルで 5000 のセッションがサポートされており、**vpn other** で割り当てたセッションの合計が全コンテキストで 4000 の場合、残りの 1000 セッションを **vpn burst other** に使用できます。**vpn other** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst other** ではオーバーサブスクライブが可能で、すべてのコンテキストがバーストプールを先着順に使用できます。 |
| **vpn other** | 同時接続数 | 該当なし | モデルごとの使用可能な Other VPN セッション数については、CLI 設定ガイドの「モデルごとにサポートされている機能のライセンス」を参照してください。 | サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。 |

| 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[1] | 説明 |
|---|---|---|---|---|
| **xlates** | 同時接続数 | 該当なし | 該当なし | アドレス変換。 |

[1] この列に「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。

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。

```
ciscoasa(config)# class default
ciscoasa(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。

```
ciscoasa(config)# class gold
ciscoasa(config-class)#
limit-resource mac-addresses 10000
ciscoasa(config-class)#
limit-resource conns 15%
ciscoasa(config-class)#
limit-resource rate conns 1000
ciscoasa(config-class)#
limit-resource rate inspects 500
ciscoasa(config-class)#
limit-resource hosts 9000
ciscoasa(config-class)#
limit-resource asdm 5
ciscoasa(config-class)#
limit-resource ssh 5
ciscoasa(config-class)#
limit-resource rate syslogs 5000
ciscoasa(config-class)#
limit-resource telnet 5
ciscoasa(config-class)#
limit-resource xlates 36000
ciscoasa(config-class)#
limit-resource routes 700
```

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。 |

| コマンド | 説明 |
| --- | --- |
| 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の 20 にリセットするには、このコマンドの **no** 形式を使用します。

**lmfactor***value*
**nolmfactor**

## 構文の説明

| | |
|---|---|
| *value* | 0 ～ 100 の範囲の整数。 |

## コマンド 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | 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 | • 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

ASA 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。ASA 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。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
```

```
 cache
ciscoasa(config-webvpn-cache)# lmfactor 30
ciscoasa(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。 |
| **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。 |

# load-monitor

クラスタ トラフィック ロード モニタリングを設定するには、クラスタ コンフィギュレーション モードで **load-monitor** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

**load-monitor** [ **frequency** *seconds* ] [ **intervals** *intervals* ]
**no load-monitor** [ **frequency** *seconds* ] [ **intervals** *intervals* ]

## 構文の説明

| | |
|---|---|
| **frequency** *seconds* | （オプション）モニタリング メッセージの間隔を 10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。 |
| **intervals** *intervals* | （オプション）ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。 |

## 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。デフォルトの頻度は、20秒です。デフォルトの間隔は、30 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | 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

クラスタメンバのトラフィック負荷をモニターできます。対象には、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。たとえば、各シャーシに 3 つのセキュリティモジュールが搭載された Firepower 9300 のシャーシ間クラスタリングの場合、シャーシ内の 2 つのセキュリティモジュールがクラスタを離れると、そのシャーシに対する同じ量のトラフィックが残りのモジュールに送信され、過負荷になる可能性があります。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ユニットでクラスタリングを手動で無効にすることを選択できます。

トラフィック負荷を表示するには、**show cluster info load-monitor** コマンドを使用します。

## 例

次に、周波数を 50 秒に、間隔を 25 に設定する例を示します。

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
```

## 関連コマンド

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

# 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するには、Cisco Umbrella コンフィギュレーションモードで **local-domain-bypass** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**local-domain-bypass** { *regular_expression* | **regex class** *regex_classmap* }
**no local-domain-bypass** { *regular_expression* | **regex class** *regex_classmap* }

## 構文の説明

| | |
|---|---|
| *regular_expression* | バイパスするローカル ドメインを識別する正規表現。この正規表現は、ローカル ドメインのように単純にすることができます（たとえば、example.com）。最大 100 文字の正規表現を入力できます。<br>このオプションを使用する場合、**local-domain-bypass** コマンドを複数回入力して、複数のローカルドメインを定義できます。 |
| **regex class** *regex_classmap* | バイパスするローカル ドメイン名を定義する正規表現クラスの名前。クラス内の正規表現に一致する完全修飾ドメイン名に対するすべての DNS 要求は、Umbrella サーバーではなく、設定された DNS サーバーに直接送信されます。 |

## コマンド デフォルト

デフォルトでは、すべてのドメインに対する DNS 要求が Cisco Umbrella に送信されます。

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | コンテキスト | システム |
| Umbrella の設定 | • 対応 | • 対応 | • 対応 | • 対応 | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.12(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

このコマンドを使用する場合のガイドラインを次に示します。

- このコマンドを複数回入力して、ドメイン名の正規表現を直接定義することができます。
- 正規表現クラスを使用するときは、このコマンドを 1 回だけ入力できます。ただし、正規表現を直接使用する場合は、コマンドの単一の正規表現クラスバージョンと複数のインスタンスを組み合わせることができます。

## 例

次の例では、バイパスするローカルドメインとして example.com を定義しています。

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass example.com
```

次の例では、example.com と一致する正規表現を作成しています。これは、*example.com 上の完全修飾ドメイン名と一致します。次に、この例では、必要な正規表現クラスマップを作成して、Umbrella のローカル ドメイン バイパスとして使用しています。

```
ciscoasa(config)# regex example-com example.com

ciscoasa(config)# class-map type regex match-any umbrella-bypass

ciscoasa(config-cmap)# match regex example-com

ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass regex class umbrella-bypass
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **umbrella-global** | Cisco Umbrella グローバルパラメータを設定します。 |

# local-unit

このクラスタメンバーの名前を指定するには、クラスタ グループ コンフィギュレーション モードで **local-unit** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。

**local-unit** *unit_name*
**no local-unit** [ *unit_name* ]

## 構文の説明

*unit_name* このクラスタ メンバの固有の名前を、1 ～ 38 文字の ASCII 文字列で指定します。

## 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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | 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 |
|---|---|
| 9.0(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

各ユニットに固有の名前が必要です。クラスタ内の他のユニットと同じ名前を付けることはできません。

## 例

次に、このユニットに unit1 という名前を付ける例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clacp system-mac** | スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。 |

| コマンド | 説明 |
|---|---|
| cluster group | クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。 |
| **cluster-interface** | クラスタ制御リンク インターフェイスを指定します。 |
| **cluster interface-mode** | クラスタ インターフェイス モードを設定します。 |
| **conn-rebalance** | 接続の再分散をイネーブルにします。 |
| **console-replicate** | スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。 |
| **enable (cluster group)** | クラスタリングをイネーブルにします。 |
| **health-check** | クラスタのヘルスチェック機能（ユニットのヘルスモニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。 |
| **key** | クラスタ制御リンクの制御トラフィックの認証キーを設定します。 |
| **local-unit** | クラスタ メンバーに名前を付けます。 |
| **mtu cluster-interface** | クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。 |
| **priority (cluster group)** | マスター ユニット選定のこのユニットのプライオリティを設定します。 |

# location-logging

GTPインスペクションで、モバイルステーションの場所と場所の変更をログに記録するには、GTP インスペクションのポリシー マップ パラメータ コンフィギュレーション モードで **location-logging** コマンドを使用します。場所のロギングを無効にするには、このコマンドの **no** 形式を使用します。

**location-logging**［ **cell-id** ］
**no location-logging**［ **cell-id** ］

## 構文の説明

**cell-id** ユーザーが現在登録されているセル ID を含めるかどうかを指定します。セル ID は、セル グローバル識別（CGI）または E-UTRAN セル グローバル識別子（ECGI）から抽出されます。

## コマンド デフォルト

デフォルトでは、場所のロギング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。

| コマンドモード | ファイアウォールモード | | セキュリティコンテキスト | | |
|---|---|---|---|---|---|
| | ルーテッド | トランスペアレント | シングル | マルチ | |
| | | | | 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 モード | • 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) | このコマンドが導入されました。 |

## 使用上のガイドライン

GTPインスペクションを使用すると、モバイル端末の場所の変更を追跡できます。場所の変更を追跡すると、不正なローミング請求を特定するのに役立つ場合があります。たとえば、モバイル端末が、米国のセルから欧州のセルに 30 分以内に移動するなど、ある場所から別の場所にありえない時間で移動した場合などです。

場所のロギングを有効にすると、システムは International Mobile Subscriber Identity（IMSI）ごとに新しい場所または変更された場所の syslog メッセージを生成します。

- 324010 は新しい PDP コンテキストの作成を示し、携帯電話の国コード（MCC）、モバイル ネットワーク コード（MNC）、情報要素、および必要に応じてユーザーが現在登録さ

れているセルIDが含まれます。セルIDは、セル グローバル識別（CGI）またはE-UTRAN セル グローバル識別子（ECGI）から抽出されます。

- 324011 は、IMSI が PDP コンテキストの作成中に保存されたものから移動したことを示します。メッセージには、以前および現在の MCC/MNC および必要に応じてセル ID が表示されます。

デフォルトでは、syslog メッセージにタイムスタンプ情報は含まれません。これらのメッセージを分析してありえないローミングを識別する場合は、タイムスタンプも有効にする必要があります。タイムスタンプ ロギングは GTP インスペクション マップに含まれません。**logging timestamp** コマンドを使用します。

## 例

次の例では、タイムスタンプを syslog メッセージに追加してから、セルIDを使用して場所のロギングを有効にしています。

```
ciscoasa(config)# logging timestamp

ciscoasa(config)# policy-map type inspect gtp gtp-map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# location-logging cell-id
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **inspect gtp** | GTP アプリケーション インスペクションをイネーブルにします。 |
| **policy-map type inspect gtp** | GTP インスペクション ポリシー マップを作成または編集します。 |
| **show service-policy inspect gtp** | GTP 設定および統計情報を表示します。 |

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。