SSD コマンド

この章は、次の項で構成されています。

ssd config

セキュア センシティブ データ（SSD）コマンド モードを開始するには、グローバル コンフィギュレーション モードで **ssd config** を使用します。このコマンド モードでは、管理者はデバイス上のセンシティブ データ（キーやパスワードなど）をどのように保護するかを設定できます。

構文

ssd config

パラメータ

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 モード

グローバル コンフィギュレーション モード

使用上のガイドライン

十分な権限を持つユーザのみが、このコマンドを使用して、SSD設定を編集および表示できます。これらの権限の説明については、ssd rule （4 ページ） を参照してください。

例

```
switchxxxxxx(config)# ssd config
switchxxxxxx(config-ssd)#
```

passphrase

システムのパスフレーズを変更するには、SSD コンフィギュレーション モードで **passphrase** を使用します。デバイスは、パスフレーズから生成されたキーを使用して自身のセンシティブ データを暗号化して保護します。

パスフレーズをデフォルトのパスフレーズにリセットするには、**no passphrase** を使用します。

構文

passphrase *{passphrase}*

encrypted passphrase *{encrypted-passphrase}*

no passphrase

パラメータ

- **passphrase**：新しいシステム パスフレーズ。
- **encrypted-passphrase**：その暗号化形式のパスフレーズ。

デフォルトの使用

このコマンドを入力しない場合は、デフォルトのパスフレーズが使用されます。

コマンド モード

SSD コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用するには、passphrase と Enter を入力します。確認メッセージが表示され、ユーザはパスフレーズを変更する意思を確認する必要があります。その後、パスフレーズを入力することができます（例を参照）。

パスフレーズの暗号化は、スタートアップ コンフィギュレーション ファイルにコピーされるソース ファイルの SSD 制御ブロックでのみ許可されます（ユーザがこのコマンドを手動で入力することはできません）。

パスフレーズを生成する場合、ユーザは4種類の文字クラスを使用する必要があります（強力なパスワード/パスワードの複雑さに似ています）。標準のキーボードから入力できる大文字、小文字、数値、および特殊文字を使用できます。

例

次の例では、パスフレーズの復号化を定義しています。

```
switchxxxxxx(config-ssd)# passphrase
This operation will change the system SSD passphrase. Are you sure? (Y/N)[N] Y
Please enter SSD passphrase:**********
Please reenter SSD passphrase:**********
```

ssd rule

SSD ルールを設定するには、SSD コンフィギュレーション モードで **ssd rule** を使用します。デバイスは、SSD ルールに基づいてユーザにセンシティブ データの読み取りアクセス許可を付与します。**Both** または **Plaintext** 読み取りアクセス許可を付与されているユーザは、SSD コンフィギュレーション モードを開始する権限も付与されます。

ユーザ定義のルールを削除し、デフォルトのルールに戻すには、**no ssd rule** を使用します。

構文

[encrypted] SSD rule {***all*** **|** *level-15* **|** *default-user* **|** *user user-name*}

{***secure*** **|** *insecure* | ***secure-xml-snmp*** **|** *insecure-xml-snmp}*

permission {***encrypted-only*** **| plaintext-only | both |** *exclude*}

default*-read* **{***encrypted* | ***plaintext*** **|** *exclude*}

no ssd rule [{***all*** **|** *level-15* **|** *default-user* **|** *user user-name*}

{***secure*** **|** *insecure* | ***secure-xml-snmp*** **|** *insecure-xml-snmp*}]

コマンド モード

SSD コンフィギュレーション モード。

デフォルト ルール

デバイスには、次のような工場出荷時のデフォルト ルールがあります。

表 *1:* デフォルトの *SSD* ルール

ルール キー		規則アクション	
ユーザ	チャネル	読み取り権限	デフォルト読み取りモード
level-15	secure-xml-snmp	プレーンテキストのみ	Plaintext
level-15	secure	Both	暗号化
level-15	insecure	Both	Encrypted
all	insecure-xml-snmp	Exclude	Exclude
all	secure	Encrypted Only	暗号化
all	insecure	Encrypted Only	暗号化

使用上のガイドライン

ユーザ定義のルールを削除したり、変更したデフォルトルールをデフォルトに戻したりするには、**no ssd rule** を使用します。

すべての SSD ルールを削除し、デフォルトの SSD ルールに戻すには、**no ssd rule**（パラメータなし）を使用します。確認メッセージが表示され、これを行うための権限が求められます。特定のルールを削除するには（対象となるのはユーザ定義のルール）、パラメータを使用してチャネルのユーザおよびセキュリティを指定します。

encrypted SSD rule は、安全な方法によりデバイス間で SSD ルールをコピーするために使用します。

デフォルトの SSD ルールは、変更することはできますが削除することはできません。次に、SSD ルールが適用される順序を示します。

- 指定した *users* に対する SSD ルール。
- **default-user**（**cisco**）に対する SSD ルール。
- **level-15** ユーザの SSD ルール。
- **all** に対する残りの SSD ルール。

ユーザは、コマンドを任意の順序で入力できます。順序付けは、デバイスによって暗黙的に行われます。

例 1：次の例では、ルールを変更しています。

```
switchxxxxxx(config-ssd)# ssd rule level-15 secure permission encrypted-only default-read
 encrypted
```

例 2：次の例では、ルールを追加しています。

```
switchxxxxxx(config-ssd)# ssd rule user james secure permission both default-read encrypted
```

例 3：次の例では、ルールを暗号化形式として追加しています。

```
switchxxxxxx(config-ssd)# encrypted ssd rule iurwe874jho32iu9ufjo32i83232fdefsd
```

例 4：次の例では、デフォルトルールを削除しています。

```
switchxxxxxx(config-ssd)# no ssd rule all secure
```

例 5：次の例では、ユーザ定義のルールを削除しています。

```
switchxxxxxx(config-ssd)# no ssd rule user james secure
```

例 6：次の例では、すべてのルールを削除しています。

```
switchxxxxxx(config-ssd)# no ssd rule
This operation will delete all user-defined rules and retrieve the default rules instead.
Are you sure (Y/N): N
```

show SSD

現在のSSDのルールを表示するには（ルールはプレーンテキストとして表示されます）、SSD コンフィギュレーション モードで **show ssd rules** を使用します。

構文

show SSD [***rules*** | ***brief***]

パラメータ

- **rules**：（任意）SSD ルールのみを表示します。
- **brief**：（任意）暗号化パスフレーズ、ファイル パスフレーズ制御、およびファイル整合性の属性を表示します。

コマンド モード

SSD コンフィギュレーション モード

デフォルト設定

すべての SSD 情報を表示します。

例 1：次の例では、すべての SSD 情報を表示しています。

```
switchxxxxxx(config-ssd)# show ssd
SSD current parameters:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
SSD parameters after reset:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
 User Type   User Name      Channel      Read Permission Default Read    Type
------------ --------- ----------------- --------------- ------------ -----------
  Specific    admin11       secure            Both        Encrypted   User-Define
  Specific    admin2        secure       Encrypted-Only   Encrypted   User-Define
  Level-15              secure-xml-snmp  Plaintext-Only   Plaintext     Default
  Level-15                  secure            Both        Encrypted     Default
  Level-15                 insecure           Both        Encrypted     Default
    All                     secure       Encrypted-Only   Encrypted     Default
    All                    insecure      Encrypted-Only   Encrypted     Default
    All                insecure-xml-snmp Plaintext-Only   Plaintext    *Default
* Modified default entry
```

例 2：次の例では、SSD ルールを表示しています。

```
switchxxxxxx(config-ssd)# show ssd rules
 User Type   User Name      Channel      Read Permission Default Read    Type
------------ --------- ----------------- --------------- ------------ -----------
  Specific    admin11       secure            Both        Encrypted   User-Define
  Specific    admin2        secure       Encrypted-Only   Encrypted   User-Define
  Level-15              secure-xml-snmp  Plaintext-Only   Plaintext     Default
```

```
  Level-15                  secure            Both        Encrypted     Default
  Level-15                insecure            Both        Encrypted     Default
    All                     secure       Encrypted-Only   Encrypted     Default
    All                   insecure       Encrypted-Only   Encrypted     Default
    All               insecure-xml-snmp Plaintext-Only    Plaintext    *Default
* Modified default entry
```

例 3：次の例では、SSD 属性を表示しています。

```
switchxxxxxx(config-ssd)# show ssd brief
SSD current parameters:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
SSD parameters after reset:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
```

ssd session read

現在のセッションにおける SSD 読み取りの現在のデフォルトをオーバーライドするには、グローバル コンフィギュレーション モードで **ssd session read** を使用します。

構文

ssd session read {***encrypted*** | ***plaintext*** | ***exclude***}

no **ssd session** read

パラメータ

- **encrypted**：SSD のデフォルトのオプションを encrypted にオーバーライドします。
- **plaintext**：SSD のデフォルトのオプションを plaintext にオーバーライドします。
- **exclude**：SSD のデフォルトのオプションを exclude にオーバーライドします。

コマンド モード

グローバル コンフィギュレーション モード。

デフォルト

このコマンド自体にデフォルトはありません。ただし、セッション自体の読み取りモードは、デフォルトではデバイスがセッションのユーザに SSD 権限を付与するために使用する SSD ルールのデフォルトの読み取りモードに設定されます。

使用上のガイドライン

SSD ルールの読み取りオプションをデフォルトに戻すには、**no ssd session read** を使用します。この設定が許可されるのは、現在のセッションのユーザが十分な読み取りアクセス許可を持っている場合のみです。それ以外の場合、コマンドは失敗し、エラーが表示されます。設定は、ただちに有効になり、ユーザが設定を元に戻すかセッションを終了すると終了します。

例

```
switchxxxxxx(config)# ssd session read plaintext
```

show ssd session

現在のセッションのユーザに対する SSD 読み取りアクセス許可およびデフォルトの読み取りモードを表示するには、特権 EXEC モードで **show ssd session** を使用します。

構文

show ssd session

コマンド モード

特権 EXEC モード

デフォルト

なし

例

```
switchxxxxxx# show ssd session
User Name/Level: James / Level 15
User Read Permission:  Both
Current Session Read mode: Plaintext
```

ssd file passphrase control

コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルにコピーするときに保護のレベルを高めるには、SSD コンフィギュレーション モードで **ssd file passphrase control** を使用します。コンフィギュレーション ファイル内のパスフレーズは、常にデフォルトのパスフレーズ キーで暗号化されます。

構文

ssd file passphrase control {***restricted*** | ***unrestricted***}

no ssd file passphrase control

パラメータ

- **Restricted**：このモードでは、デバイスは自身のパスフレーズがコンフィギュレーション ファイルにエクスポートされるのを制限します。制限モードは、パスフレーズがないデバイスからコンフィギュレーション ファイル内の暗号化されたセンシティブ データを保護します。このモードは、ユーザがコンフィギュレーション ファイルにパスフレーズを公開しないようにする場合に使用します。
- **Unrestricted**：このモードでは、デバイスはコンフィギュレーション ファイルを作成するときに自身のパスフレーズを含めます。これにより、コンフィギュレーション ファイルを受け入れるすべてのデバイスがそのファイルからパスフレーズを学習できます。

デフォルト

デフォルトは **unrestricted** です。

コマンド モード

SSD コンフィギュレーション モード。

使用上のガイドライン

デフォルトの状態に戻すには、**no ssd file passphrase control** コマンドを使用します。

デバイスを工場出荷時の設定にリセットすると、そのローカル パスフレーズがデフォルトのパスフレーズに設定されることに注意してください。そのため、このままではデバイスは自身のコンフィギュレーション ファイルにあるユーザ定義のパスフレーズ キーで暗号化されたセンシティブ データを復号化できません。これを行うには、ユーザ パスフレーズで再度デバイスを手動で設定するか、コンフィギュレーション ファイルを無制限モードで作成します。

無制限モードのユーザ定義のパスフレーズを設定する場合は、SSD ファイル整合性制御を有効にすることを強く推奨します。SSD ファイル整合性制御を有効にすると、コンフィギュレーション ファイルを改ざんから保護できます。

例

```
console(ssd-config)# ssd file passphrase control restricted
console(ssd-config)# no ssd file passphrase control
```

ssd file integrity control

暗号化されたセンシティブ データが含まれている新規生成のコンフィギュレーション ファイルを改ざんから保護するようにデバイスに指示するには、SSD コンフィギュレーション モードで **ssd file integrity control** コマンドを使用します。

Integrity Control を無効にするには、**no ssd file integrity control** を使用します。

構文

ssd file integrity control ***enabled***

no ssd file integrity control

パラメータ

- **enabled**：ファイル整合性制御を有効にして、新規生成のコンフィギュレーション ファイルを改ざんから保護します。

デフォルト

デフォルトのファイル入力制御は**無効**になっています。

コマンド モード

SSD コンフィギュレーション モード。

使用上のガイドライン

TAユーザは、ファイル整合性制御を有効にしたファイルを作成することで、コンフィギュレーション ファイルを改ざんから保護できます。ファイル パスフレーズ制御を無制限にしたユーザ定義のパスフレーズをデバイスで使用する場合には、ファイル整合性制御を有効にすることを推奨します。

デバイスは、コンフィギュレーションファイルでファイル整合性制御コマンドを調べて、コンフィギュレーションファイルの整合性が保護されているかどうかを判別します。ファイルの整合性を保護するようになっているのに、ファイルの整合性が維持されていないことをデバイスが検出した場合、デバイスはファイルを拒否します。そうでない場合、ファイルは受け入れられて、さらに処理が加えられることになります。

例

```
switchxxxxxx(config-ssd)#  ssd file integrity control enabled
```

File Integrityが有効である場合、コンフィギュレーション ファイル全体の末尾に内部のダイジェストコマンドを追加します。これは、スタートアップ コンフィギュレーションにコンフィギュレーション ファイルをダウンロードする場合に使用します。

```
config-file-digest 0AC78001122334400AC780011223344
```

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。