

配置SD-WAN上的OKTA單點登入(SSO)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景](#)

[設定](#)

[vManage配置](#)

[OKTA配置](#)

[常規設定](#)

[配置SAML](#)

[意見回饋](#)

[在OKTA中配置組](#)

[在OKTA中配置使用者](#)

[在應用程式中分配組和使用者](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹如何在軟體定義廣域網(SD-WAN)上整合OKTA單一啟用(SSO)。

必要條件

需求

思科建議您瞭解以下主題：

- SD-WAN概述
- 安全斷言標籤語言(SAML)
- 身份提供程式(IdP)
- 憑證

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco vManage 18.3.X版或更高版本
- Cisco vManage版本20.6.3

- Cisco vBond版本20.6.3
- 思科vSmart版本20.6.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

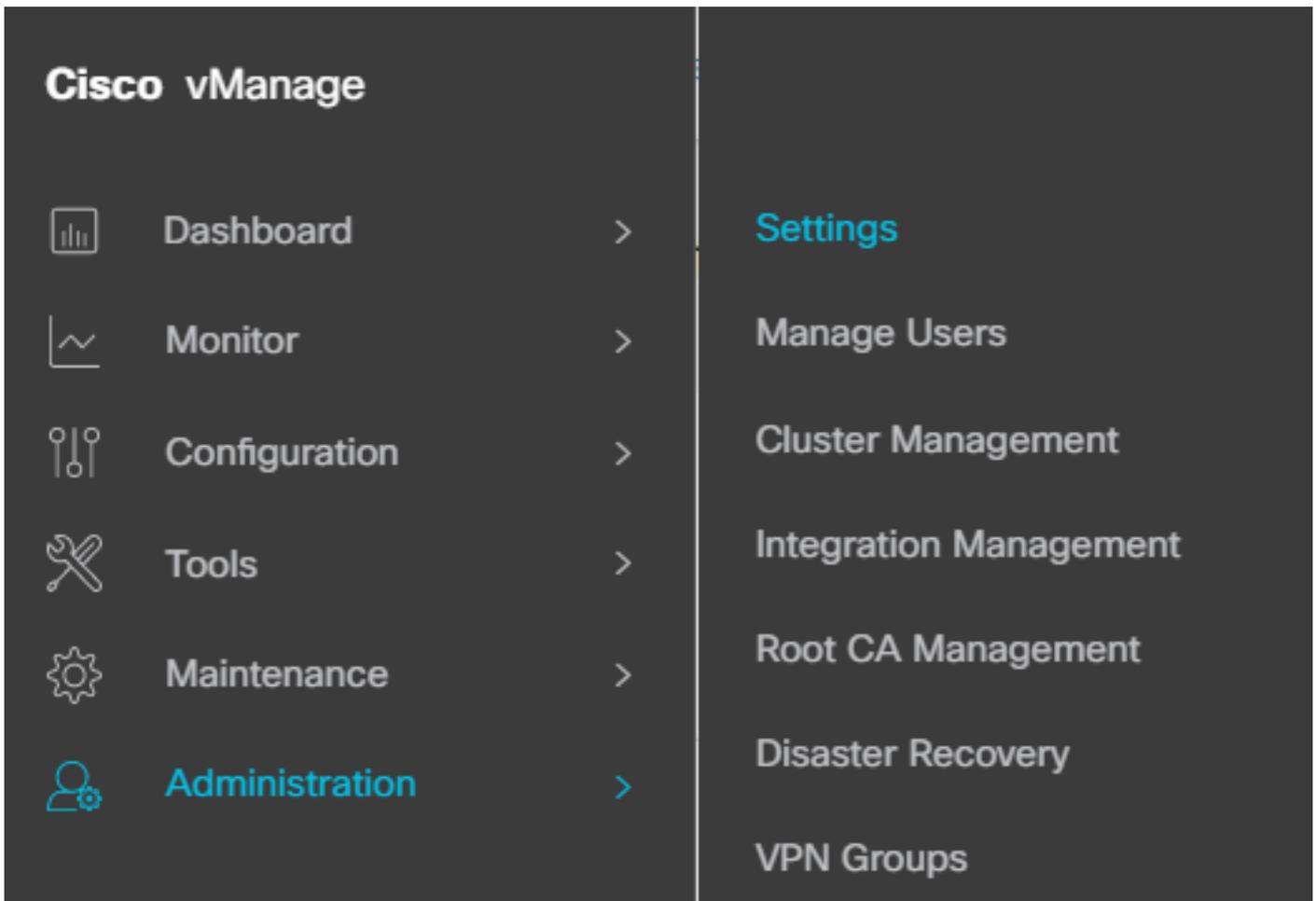
安全斷言標籤語言(SAML)是一種開放標準，用於在各方之間，尤其是在身份提供方與服務提供商之間交換身份驗證和授權資料。顧名思義，SAML是一種基於XML的安全宣告（服務提供商用來作出訪問控制決策的語句）標籤語言。

身份提供程式(IdP)是一個受信任的提供程式，可用於使用單一登入(SSO)來訪問其他網站。SSO減少了密碼疲勞，增強了可用性。它減少了潛在攻擊面，提供了更好的安全性。

設定

vManage配置

1. 在Cisco vManage中，導航到Administration > Settings > Identify Provider Settings > Edit。



2.按一下啟用。

3.按一下以下載SAML後設資料並將內容儲存到檔案中。這是OKTA方面所需要的。

Administration Settings

Identity Provider Settings

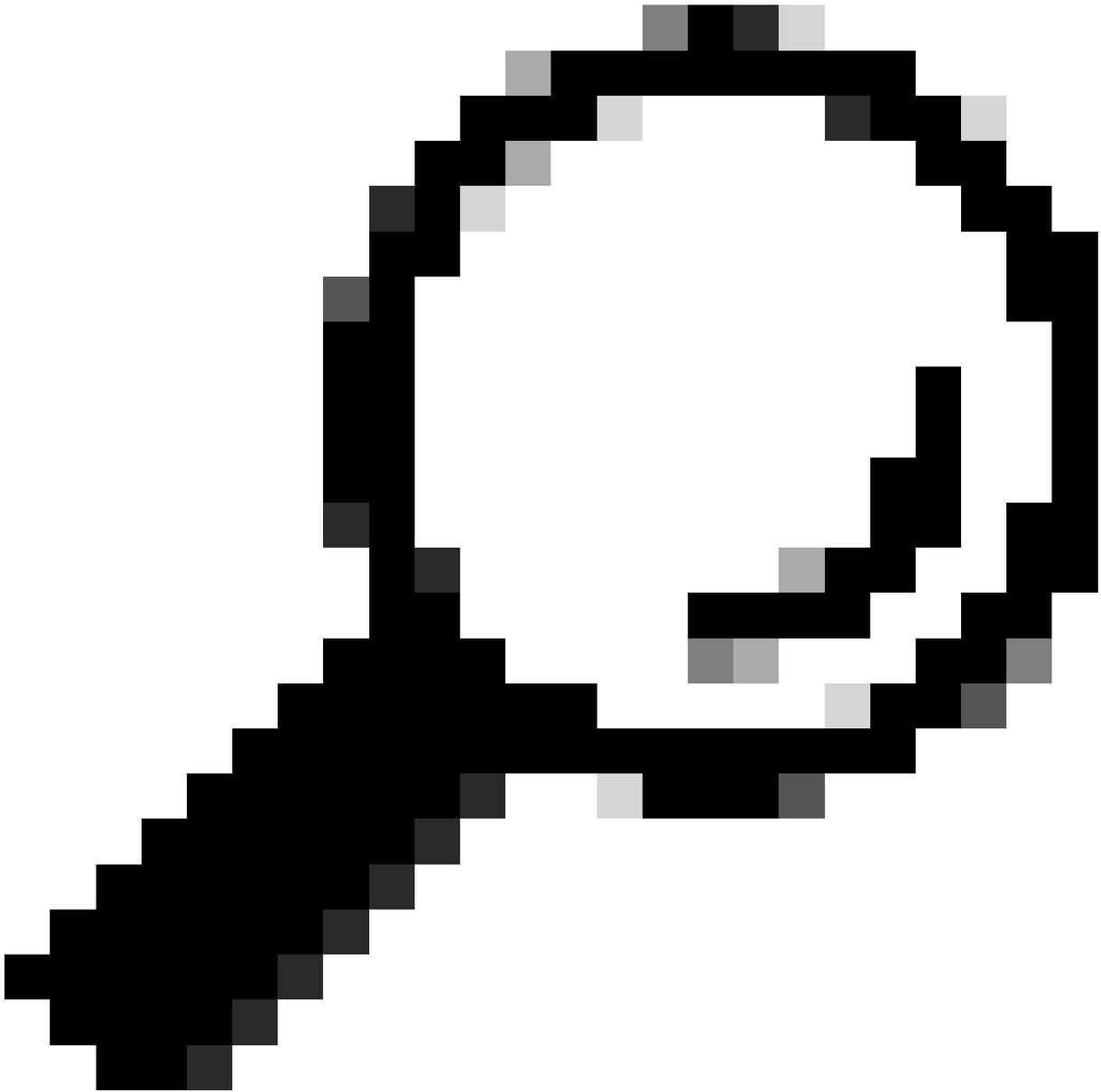
Disabled

Enable Identity Provider: Enabled Disabled

Upload Identity Provider Metadata

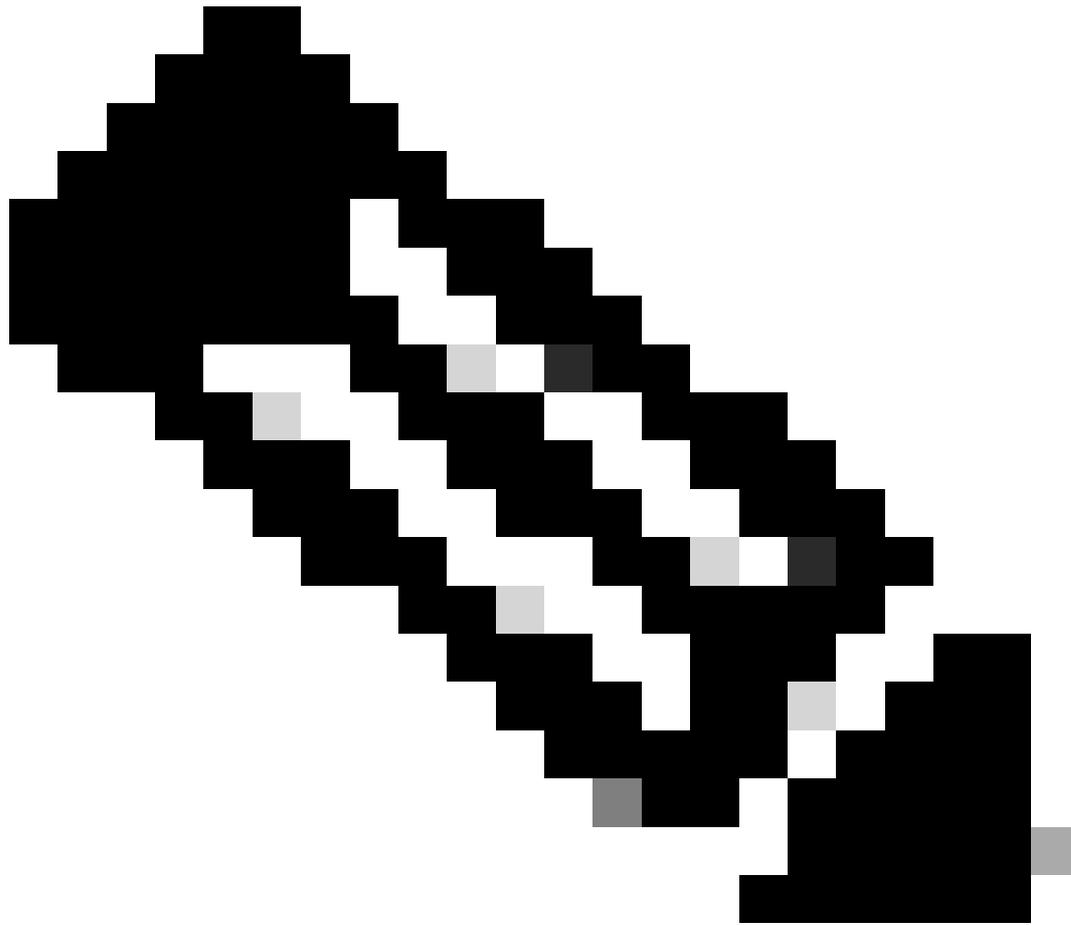
[↓ Click here to download SAML metadata](#)

下載SAML



提示：您需要來自METADATA的這些資訊才能使用Cisco vManage配置OKTA。

- a. 實體Id
 - b. 簽名證書
 - c. 加密證書
 - d. 註銷URL
 - e. 登入UR
-



附註：證書必須採用x.509格式並使用.CRT副檔名保存這些證書。

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIhAM8T9QVLqX/lp1oK/q2XNUbJcGhRmGvqdXxGTUkrKUBhMA0GCSqGSIb3
DQEBCwUAMHlxDDAKBgNVBAYTA1VTQTELMakGA1UECBMCQ0ExETAPBgNVBACTCFNhbiBkb3NlMRQw
EgYDVQQKEwtDSVNDT1JUUExBQjEUMBIGA1UECXMlQ01TQ09SVFBMQUIxIjAUBgNVBAMTDURlZmFl
bHRUZW5hbnQwHhcNMjAwNTI4MTQxMzQzWWhcNMjUwNTI4MTQxMzQzWjByMQwwCgYDVQQGEwNVU0Ex
CzAJBgNVBAgTAKNBMRwDwYDVQQHEWhTYW4gSm9zZTEUMBIGA1UEChMLQ01TQ09SVFBMQUIxIjFAS
BgNVBAsTC0NlU0NPUlRQTEFCMRywFAyDVQQDEw1EZWZhdWx0VGVuYW50MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAg9HOIwjWHD3pbkCB3wRUsn01PTsNAhCqRKOf5aY4QDWbu7U3+6gF
TzZgrB9189rLskkb7cEzRcE7ZbZ1a3zICVw76ZN8jj2BZMYpuTLS9LSGRq2FClYMAg6JU4Yc9prg
T6IcmJKHPfuFM3izXKVsrzfn8tDZ7UDHGIUNPs2kntamU4ZB7BRTE1zJXp+Zh3CvnfLE9g3aXK9
SM9qRFDjAaC8GhWphOYyK3RisQZ/bIZJ2vWkVo91p+6/kQy7/oxFKznK/2oAXaAe26P8HYw+XC0b
mkCwb3e9a1vCGrCmPJwJPjn9j09dX426/LbjdmDAo6HudjTEoQMZduD3Z9GU5QIDAQABMA0GCSqG
SIb3DQEBCwUAA4IBAQBbO/FdHT365rzOHpgHo8YWbxbYdhjAMrHUBbuXLq6MEaHvm4GoTYsgJzc9
Scy/Iwoa6krjBXHJPPtthBwzYYXvK6CJxh8J/rlednlmai0z9growg/sSEgbXPpuQw6qT9hM8s2i
FHlFchPoqiaZFldNF4iupuzFPTcD8kmzEC3mGlcxfm2TaVjLFDu7McRAMLZTV+yPY+WZXjuoMI8P
hXapKdUt0B6RrxzucBRac2ZB22g7HWDQuDZUzf966Q2k5Us1QxtNlpXLU5X+i+YDW011T2AP6+UUi
vrN1A6vFVPP3QtAd7ao7VziMeEvxfyTuK690b+ej4MntWIKdHneU+/YC
-----END CERTIFICATE-----
```

X.509憑證

OKTA配置

1. 登入[OKTA](#)帳戶。
2. 定位至「應用」>「應用」。

Applications



Applications

Self Service

Applications (應用) > Applications (應用)

3. 按一下 建立應用程式整合。

Applications

Create App Integration

建立應用程式

4. 按一下「SAML 2.0」和「next」。

Create a new app integration ×

Sign-in method

[Learn More](#) 

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

配置SAML2.0

常規設定

1. 輸入申請名稱。
2. 為應用程式新增徽標 (可選) 。
3. 應用可視性 (可選) 。
4. 按一下下一步。



1 General Settings

2 Configure SAML

App name

App logo (optional)

App visibility Do not display application icon to users

Cancel
Next

SAML 常規設定

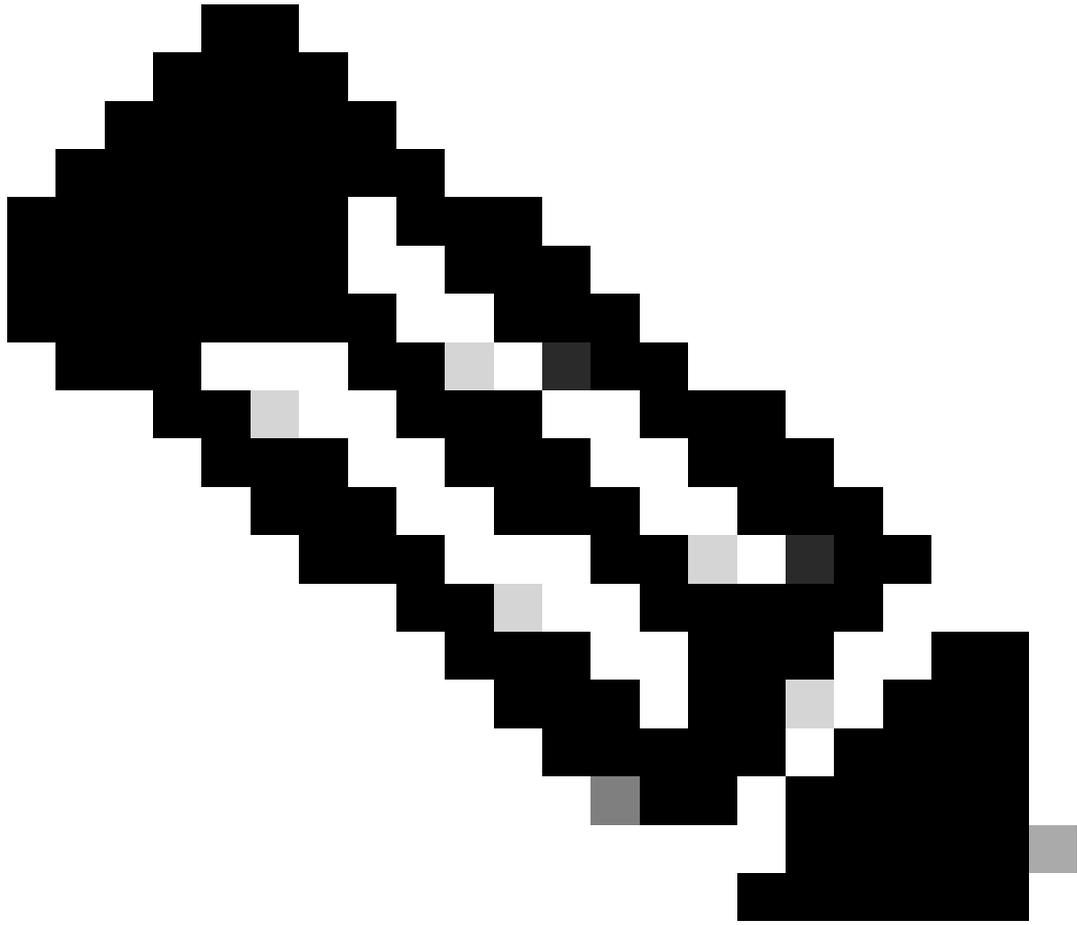
配置SAML

此表說明了該部分上必須配置的引數。

| 元件 | 價值 | 組態 |
|------------------------|---|----------------------------|
| 單一登入URL | https://XX.XX.XX.XX:XXXX/samlLoginResponse | 從後設資料中獲取。 |
| 訪問群體 URI (SP實體ID) | XX.XX.XX.XX | Cisco vManage的IP地址或 DNS |

| 元件 | 價值 | 組態 |
|--------------|---|------------------------|
| 預設RelayState | | 空 |
| 名稱ID格式 | | 根據您的偏好 |
| 應用程式使用者名稱 | | 根據您的偏好 |
| 更新應用程式使用者名稱 | 建立和更新 | 建立和更新 |
| 響應 | 已簽名 | 已簽名 |
| 斷言簽名 | 已簽名 | 已簽名 |
| 簽名演算法 | RSA-SHA256 | RSA-SHA256 |
| 摘要演算法 | SHA256 | SHA256 |
| 斷言加密 | 已加密 | 已加密 |
| 加密演算法 | AES256-CBC | AES256-CBC |
| 金鑰傳輸演算法 | RSA-OAEP | RSA-OAEP |
| 加密證書 | | 後設資料中的加密證書必須採用x.509格式。 |
| 啟用單一註銷 | | 必須檢查。 |
| 單一註銷URL | https://XX.XX.XX.XX:XXXX/samlLogoutResponse | 從後設資料獲取。 |
| SP頒發者 | XX.XX.XX.XX | 適用於vManage的IP位址或DNS |

| 元件 | 價值 | 組態 |
|--------------|--|--|
| 簽名證書 | | 後設資料中的加密證書必須採用x.509格式。 |
| 斷言內嵌掛接 | 無 (禁用) | 無 (禁用) |
| 身份驗證上下文類 | X.509憑證 | |
| 執行強制身份驗證 | 是 | 是 |
| SAML頒發者ID字串 | SAML頒發者ID字串 | 鍵入字串文本 |
| 屬性語句 (可選) | 名稱▶使用者名稱 未指定的名稱格式(▶選) 值▶user.login | 名稱▶使用者名稱 未指定的名稱格式(▶選) 值▶user.login |
| 組屬性語句 (可選) | 組▶稱 未指定的名稱格式(▶選) 篩選▶匹配regex ▶。 * | 組▶稱 名稱格式 (可選) ▶未指定 篩選▶匹配regex ▶。 * |



附註：必須使用Username和Groups，具體如CONFIGURE SAML表中所示。

1 General Settings

2 Configure SAML

A SAML Settings

General

Single sign-on URL ⓘ

https://XX.XX.XX.XX:XXXX/samlLoginResponse

Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ⓘ

XX.XX.XX.XX

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

EmailAddress ▼

Application username ⓘ

Okta username ▼

Update application username on

Create and update ▼

[Hide Advanced Settings](#)

Response ⓘ

Signed ▼

Assertion Signature ⓘ

Signed ▼

Signature Algorithm ⓘ

RSA-SHA256 ▼

Digest Algorithm ⓘ

SHA256 ▼

Assertion Encryption ⓘ

Encrypted ▼

Encryption Algorithm ⓘ

AES256-CBC ▼

Key Transport Algorithm ⓘ

RSA-OAEP ▼

Encryption Certificate ⓘ

Browse files...

Signature Certificate ⓘ

Browse files...

Enable Single Logout ⓘ

Allow application to initiate Single Logout

Signed Requests ⓘ

Validate SAML requests with signature certificates.

SAML request payload will be validated. SSO URLs will be read dynamically from the request. [Read more](#)

Other Requestable SSO URLs

URL

Index

[+ Add Another](#)

| | |
|---|---|
| Assertion Inline Hook | <input type="text" value="None (disabled)"/> |
| Authentication context class [?] | <input type="text" value="X.509 Certificate"/> |
| Honor Force Authentication [?] | <input type="text" value="Yes"/> |
| SAML Issuer ID [?] | <input type="text" value="http://www.example.com"/> |
| Maximum app session lifetime | <input type="checkbox"/> Send value in response Uses SessionNotOnOrAfter attribute |

Attribute Statements (optional) [LEARN MORE](#)

| Name | Name format (optional) | Value |
|---------------------------------------|--|---|
| <input type="text" value="Username"/> | <input type="text" value="Unspecified"/> | <input type="text" value="user.login"/> |

Group Attribute Statements (optional)

| Name | Name format (optional) | Filter |
|-------------------------------------|--|--|
| <input type="text" value="Groups"/> | <input type="text" value="Unspecified"/> | <input type="text" value="Matches regex"/> <input type="text" value=".*"/> |

- 按「Next」(下一步)。

意見回饋

1. 選擇其中一個選項作為首選項。
2. 按一下完成。

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

 Once you have a working SAML integration, submit it for Okta review to publish in the OIN. [Submit your app for review](#)

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

[Previous](#)

[Finish](#)

SMAL反饋

在OKTA中配置組

1. 導航至Directory > Groups。

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2. 按一下Add group並建立新組。

Groups

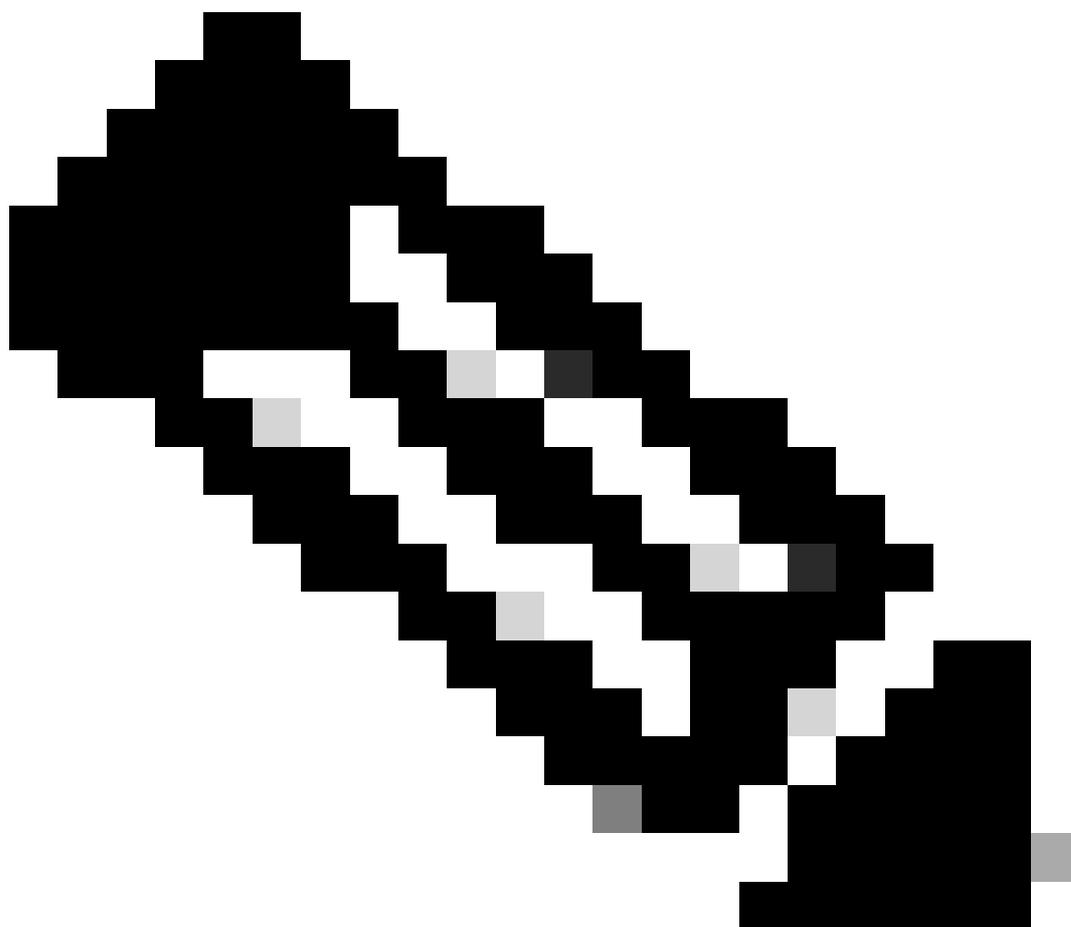
[Help](#)

All Rules

Search by group name

[Advanced search](#)

新增組



附註：組必須與Cisco vManage組匹配，並且它們需要大小寫更低。

在OKTA中配置使用者

1. 定位至Directory > People。

Directory



People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

2.按一下Add person，建立新使用者，將其分配給組並儲存。

Add Person

User type 

First name

Last name

Username

Primary email

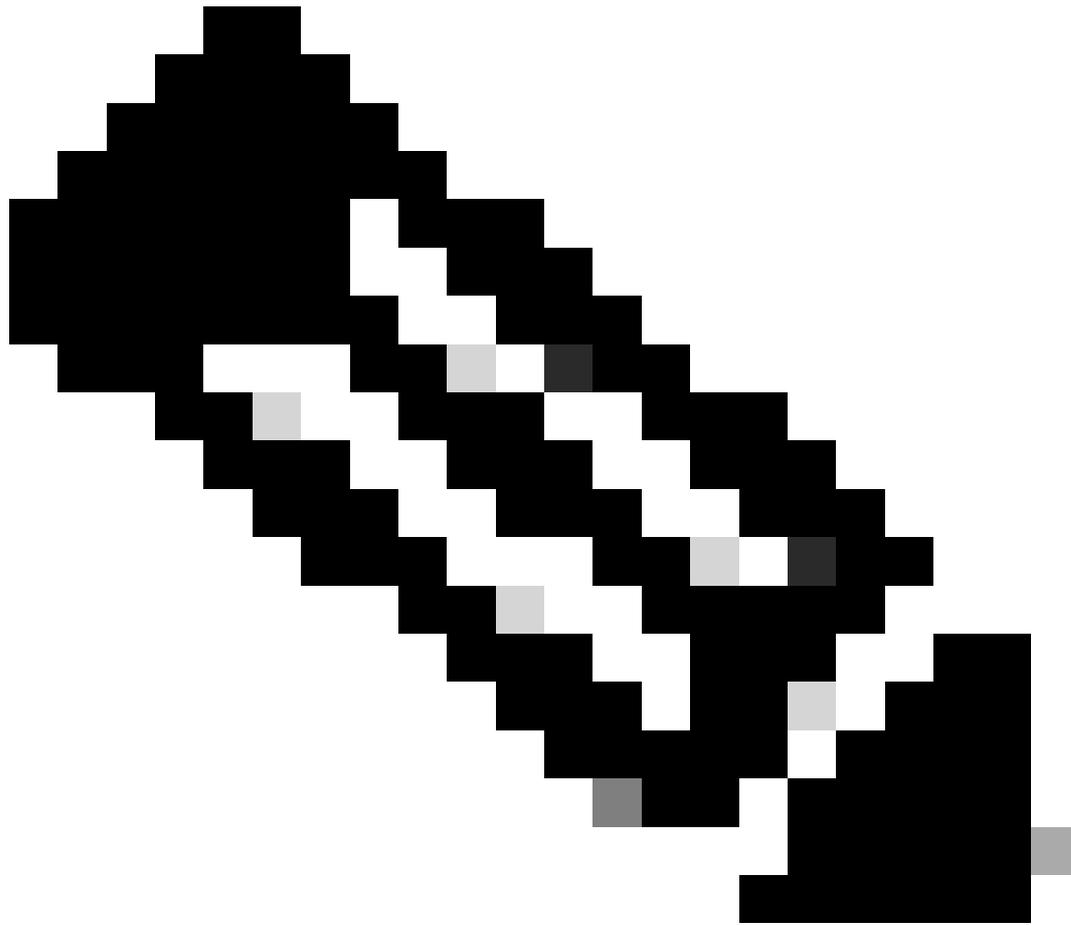
Secondary email (optional)

Groups (optional)

Activation

I will set password

新增使用者



附註：可使用Active Directory來代替OKTA使用者。

在應用程式中分配組和使用者

1. 定位至應用產品>應用產品>選擇新應用產品。
2. 按一下Assign > Assign to Groups。



Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

[Submit your app for review](#)[General](#)[Sign On](#)[Import](#)[Assignments](#)[Assign ▾](#)[Convert assignments ▾](#)[Groups ▾](#)[Assign to People](#)[Assign to Groups](#)

Assignment

Groups

01101110
01101111
01101100
01101000
01101001
01101110
01100111

No groups found

REPORTS

[Current Assignments](#)[Recent Unassignments](#)

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.

[Go to self service settings](#)

Requests Disabled

Approval N/A

[Edit](#)

應用程式>組

3.標識組，然後按一下分配 >完成。

Assign vManage to Groups



| | | |
|----------------------------------|---|----------|
| <input checked="" type="radio"/> | Everyone All users in your organization | Assign |
| <input checked="" type="radio"/> | netadmin | Assigned |

Done

分配組和使用者

4.現在必須向應用程式分配組和使用者。

驗證

完成配置後，您可以通過OKTA訪問Cisco vManage。

Connecting to

Sign-in with your cisco-org-958976 account to access vManage

okta



Sign In

Username

Password

Remember me

Sign In

Need help signing in?

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。