管理員指南

Sun™ ONE Portal Server, Secure Remote Access

版本 6.2

817-4737-10
2003 年 11 月

目錄

圖目錄

表目錄

程序目錄

關於本指南

本指南會解釋如何管理 Sun™ Open Net Environment (Sun™ ONE) Portal Server，Secure Remote Access。

Sun™ ONE Portal Server，Secure Remote Access 讓遠端使用者可以透過網際網路安全地存取他們組織的網路及服務。此外，還能爲您的組織提供安全的網際網路入口網站，並供任何目標族群 - 員工、事業夥伴或一般大眾存取內容、應用程式及資料等。

Secure Remote Access 在 Solaris™ 8.0 和 9.0 作業系統中執行。本指南包含有關配置與管理 「Secure Remote Access」的說明。

本前言包含下列各節：

誰應該閱讀本指南

本指南假設您是網路或系統管理員，對於管理 UNIX® 系統和 TCP/IP 網路有豐富的經驗。您負責安裝、配置與管理 Secure Remote Access。

您對於要安裝的機器必須要有 root 存取權限，才能安裝各種不同的 Secure Remote Access 元件。您也需要必要的管理權限才能執行其他作業，例如配置使用者與服務。

您需要知道的事項

在您管理 Secure Remote Access 之前，您必須先熟悉下列資訊：

- 基本的 Solaris 管理程序
- LDAP
- Sun™ ONE Directory Server
- Sun™ ONE Web Server
- Sun™ ONE Portal Server

您也需要具備下列條件才能撰寫 Rewriter 規則：

- 瞭解 HTML 和 HTML 標籤
- 相當了解 JavaScript
- 了解基本 XML

本指南的編排方式

本指南包含下列章節與索引：

關於本指南 (本章)

第 1 章，「Sun ONE Portal Server, Secure Remote Access 簡介」

本章會介紹 Sun™ ONE Portal Server，Secure Remote Access 產品和 Sun™ ONE Portal Server 產品與 Secure Remote Access 元件之間的關係。本章同時也提供有關管理和配置 Secure Remote Access 的資訊。

第 2 章，「閘道」

本章會說明與閘道相關的概念，與順利執行閘道所需的資訊。

第 3 章，「Rewriter」

本章會介紹 Rewriter 並提供規則範例以及最佳實務。

第 4 章，「NetFile」

本章會介紹 NetFile 並詳細說明其操作。

第 5 章，「Netlet」

本章會介紹如何使用 Netlet 在使用者遠端入口網站桌面以及在您的企業內部網站中執行應用程式的伺服器之間，以安全的方式執行應用程式。

第 6 章，「PDC 與 Netlet 搭配使用」

本章會介紹如何配置用戶端瀏覽器的 Java Plugin，使得 Netlet 能夠和 PDC 搭配使用。

第 7 章，「證書」

本章會介紹證書管理並解釋如何安裝自簽的證書或是來自認證機構的證書。

第 8 章，「配置 URL 存取控制」

本章會介紹如何允許或拒絕透過特定 URL 的閘道存取一般使用者。

第 9 章，「配置閘道」

本章會介紹如何透過 Sun™ ONE Identity Server 管理主控台來配置「閘道」屬性。

第 10 章，「配置 NetFile」

本章會介紹如何透過 Sun™ ONE Identity Server 管理主控台來配置 NetFile。

第 11 章，「配置 Netlet」

本章會介紹如何透過 Sun™ ONE Identity Server 管理主控台來配置 Netlet 屬性。

附錄 A，「配置 SSL 加速器」

本章說明如何爲 Sun™ Portal Server，Secure Remote Access 配置不同的加速器。

附錄 B，「國家代碼」

本附錄列出了二字母國家代碼，在證書管理期間您需要指定這個國家代碼。

附錄 C，「配置屬性」

本附錄列出了您在 Sun™ ONE Identity Server 管理主控台中爲 Sun™ Portal Server，Secure Remote Access 所設定的屬性。

本指南中所使用的文件慣例

固定間距字型

固定間距字型是用於出現在電腦螢幕上的任何文字或是您應該鍵入的文字。它也用於檔案名稱、區別名稱、功能和範例。

斜體字型

*斜體字型*是用來表示您使用對安裝而言唯一的資訊 (例如變數) 所輸入的文字。它適用於伺服器路徑、名稱以及帳戶 ID。

方括弧或中括弧

方 (或中) 括弧 [] 是用來隔開選用參數。例如在本文件中，您會看到 xx 指令的用法，其說明如下：

```
xx [options] [action] [component]
```

[options]、[arguments] 和 [component] 的出現表示在 xx 指令之後可以加入選擇性參數。

指令行提示

指令行提示 (例如，用於 C-Shell 的 %，或是用於 Korn 或 Bourne shell 的 $) 不會在範例中顯示。根據您在使用的作業系統環境，將會看見各種不同的指令行提示。然而除非是特別註明，您應該依照文件中出現的指令輸入。

哪裡可以找到相關資訊

Secure Remote Access 文件

下方列出的是其他的 Secure Remote Access 文件。

- *Sun ONE Portal Server，Secure Remote Access 6.2 Deployment Guide*
- *Sun ONE Portal Server，Secure Remote Access Attribute Online Help*
- *Sun ONE Portal Server，Secure Remote Access Netlet Online Help*
- *Sun ONE Portal Server，Secure Remote Access NetFile Java1 Online Help*
- *Sun ONE Portal Server，Secure Remote Access NetFile Java2 Online Help*

Portal Server 文件

Sun™ ONE Portal Server 文件套裝包括了下列文件：

- *Sun ONE Portal Server 6.2 安裝指南*
- *Sun ONE Portal Server 6.2 管理員指南*
- *Sun ONE Portal Server 6.2 Migration Guide*
- *Sun ONE Portal Server 6.2 Desktop Customization Guide*
- *Sun ONE Portal Server 6.2 Developer's Guide*

本指南中所參考的文件

本指南中所參考的其他文件：

- *Sun ONE Identity Server 管理員指南*
- *Sun Crypto Accelerator 1000 Board Installation and User's Guide*

  本指南可以在以下網址中找到：
  http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-10.pdf

相關協力廠商網站參考

您可以透過下列網址存取 Sun 的線上技術文件：docs.sun.com。您可以瀏覽歸檔或是搜尋特定的書籍名稱或主題。

備註	Sun 不保證在此文件中提及的協力廠商網站的有效性。Sun 不爲此類網站或資源上的內容、廣告、產品或其他資料背書及負責。由於使用或信任此類網站或資源上可取得的內容、商品或服務所造成的實質或宣稱的傷害或損失，Sun 並不負擔任何責任。

在線上何處尋找本指南

您可以透過下列網址存取 Sun 的線上技術文件：http://docs.sun.com。您可以瀏覽歸檔或是搜尋特定的書籍名稱或主題。

第 1 章

Sun ONE Portal Server, Secure Remote Access 簡介

本章會介紹 Sun™ ONE Portal Server, Secure Remote Access 產品以及 Sun™ ONE Portal Server 產品與 Secure Remote Access 元件之間的關係。本章同時也提供有關管理和配置 Secure Remote Access 的資訊。

本章涵蓋下列主題：

Secure Remote Access 概述

Secure Remote Access 讓遠端使用者可以透過網際網路安全地存取他們組織的網路及服務。此外，還能爲您的組織提供安全的網際網路入口網站，並供任何目標族群 - 員工、事業夥伴或一般大眾存取內容、應用程式及資料等。

Secure Remote Access 提供以瀏覽器爲基礎的安全遠端存取，使用者可從任何遠端裝置存取入口網站內容與服務。這是一個有成本效益的安全存取解決方案。使用者可以從任何裝有啓用 Java 技術瀏覽器的裝置進行遠端存取，消除了對用戶端軟體的需求。與 Sun™ ONE Portal Server 軟體的整合能確保使用者可安全加密的存取他們有權存取的內容與服務。

Secure Remote Access 的用戶群體爲部署高度安全遠端存取入口網站的企業。這些入口網站重視企業內部網路資源的安全性、保護與隱私權。Secure Remote Access 結構恰恰適用於這些類型的入口網站。Secure Remote Access 的閘道、NetFile 與 Netlet 元件能讓使用者安全的經由網際網路存取企業內部網路資源，而無需在網際網路上顯露這些資源。

閘道，位於非軍事區 (DMZ)，提供至所有企業內部網路 URL、檔案系統與應用程式的單一安全存取點。所有其他非 Secure Remote Access 服務例如階段作業、認證與入口網站桌面皆位於 DMZ 之後的安全的內部網路中。用戶端瀏覽器至閘道的通訊將使用 HTTPS 加密。閘道至伺服器與內部網路資源的通訊可使用 HTTP 或 HTTPS 加密。

Secure Remote Access 使用兩種方法

Netlet 與 NetFile applet 將下載至用戶端機器，支援檔案可能位於閘道或 Portal Server 主機。

Portal Server 可以在兩個模式中執行：

- 開放模式
- 安全模式

開放模式

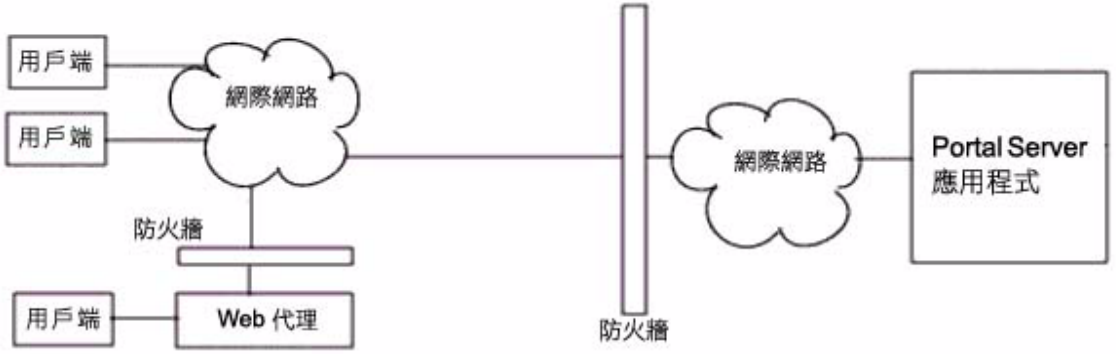
在開放模式中，Portal Server 安裝時未安裝 Secure Remote Access。雖然這個模式下可以使用 HTTPS 通訊，但卻不可以使用安全遠端存取。這表示使用者無法存取安全遠端檔案系統與應用程式。

開放入口網站與安全入口網站的主要不同爲，由開放入口網站提供的服務通常會位於非軍事區 (DMZ) 而不會位於安全內部網路中。DMZ 是一個位於公用網際網路與私人內部網路之間的小型受保護網路，通常由兩端的防火牆劃分界線。

若入口網站沒有包含敏感的資訊 (部署了公用資訊與允許存取任意應用程式)，則對於多數使用者存取請求的回應將會快於使用安全模式。

圖 1-1 示意了開放模式中的 Portal Server。此處，Portal Server 爲安裝於防火牆後的單一伺服器。多個用戶端透過網際網路經由單一防火牆存取 Portal Server。

圖 1-1 開放模式下的 Portal Server



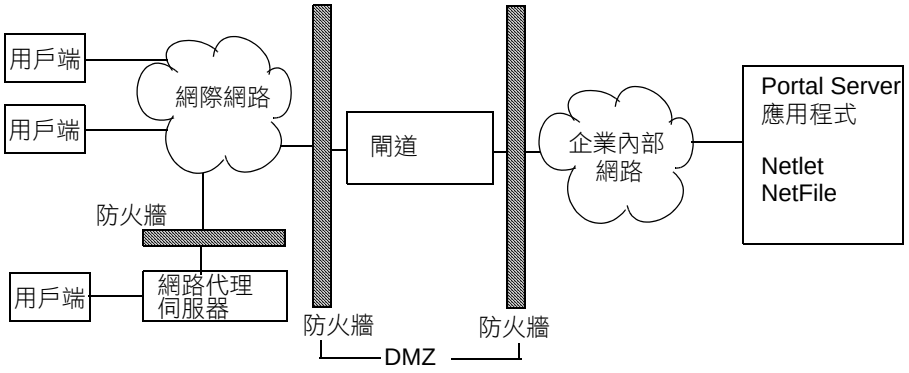
安全模式

安全模式可讓使用者安全遠端存取需要的企業內部網路檔案系統與應用程式。

閘道位於非軍事區域 (DMZ)。閘道提供至所有內部網路 URL 與應用程式的單一安全存取點，如此會減少將在防火牆中被開放的連接埠數。所有其他 Portal Server 服務例如階段作業、認證與入口網站桌面皆位於 DMZ 之後的安全的企業內部網路中。用戶端瀏覽器至閘道的通訊將使用 HTTPS 透過安全套接層 (SSL) 加密。閘道至伺服器與內部網路資源的通訊可使用 HTTP 或 HTTPS 加密。

圖 1-2 顯示了包含 Secure Remote Access 的 Portal Server。SSL 將用於加密網際網路上用戶端與 Portal Server 閘道之間的連線。SSL 也可以用於加密閘道與伺服器之間的連線。企業內部網路與網際網路之間的閘道將延伸用戶端與 Portal Server 之間的安全路徑。

圖 1-2 安全模式下的 Portal Server (含有 Secure Remote Access)



可以新增其他伺服器與閘道以擴大站台。Secure Remote Access 元件可以基於業務需求用不同方式配置。

Secure Remote Access 元件

Secure Remote Access 擁有四個主要元件：

- 閘道
- Rewriter
- NetFile
- Netlet

閘道

Secure Remote Access 閘道在源自網際網路的遠端使用者階段作業與您的企業內部網路之間提供了介面與安全的屏障。透過單一介面給遠端使用者，閘道可經由內部網路伺服器和應用程式伺服器安全地顯示內容。

網路伺服器使用以網路爲基礎的資源例如 HTML、JavaScript 與 XML 以在用戶端與閘道之間進行通訊。Rewriter 是用於使網路內容可用的閘道元件。

應用程式伺服器會使用二進制通訊協定例如 telnet 與 FTP 以在用戶端與閘道之間進行通訊。位於「閘道」的 Netlet 就是基於這個目的而使用。有關詳細資訊，請參閱第 2 章「閘道」。

Rewriter

Rewriter 會讓一般使用者可以瀏覽企業內部網路並使得那些頁面的連結與其他 URL 參照正確作業。Rewriter 會在網路瀏覽器位置欄位中前置閘道 URL，藉此經由閘道重新導向內容請求。有關詳細資料，請參閱第 3 章「Rewriter」。

NetFile

NetFile 是一個檔案管理員應用程式，其允許遠端存取與操作檔案系統與目錄。NetFile 包括 NetFile Java™, 以 Java 爲基礎的使用者介面。此適用 Java 1 與 Java 2。有關詳細資訊，請參閱第 4 章「NetFile」。

Netlet

Netlet 方便了以安全方式在遠端桌面執行熱門應用程式與公司特定應用程式的功能。在站台實施 Netlet 之後，使用者可以安全執行共用的 TCP/IP 服務，例如 Telnet 與 SMTP，和以 HTTP 爲基礎的應用程式例如 pcANYWHERE 或 Lotus Notes。有關詳細資料，請參閱第 5 章「Netlet」。

管理 Secure Remote Access

Secure Remote Access 具有兩個管理介面：

- Sun™ ONE Identity Server 管理主控台
- 指令行

大部分管理作業會經由以網路爲基礎的 Sun™ ONE Identity Server 管理主控台執行。管理主控台可以本機存取或從網路瀏覽器遠端存取。然而，例如修改檔案的作業必須經由 UNIX 指令行介面管理。

配置 Secure Remote Access 屬性

您可以在組織、角色與使用者層級中，配置與 Secure Remote Access 相關的屬性，以下屬性除外：

- 在使用者層級中無法設定「衝突解析層級」。在「服務配置」標籤中也無法設定。請參閱第 33 頁的「設定衝突解析」。
- MIME 類型配置檔案位置屬性只可以在組織層級中設定。請參閱第 278 頁的「指定 MIME 類型配置檔案位置」。

組織下所有的角色與使用者會繼承在組織層級設定的值。在使用者層級設定的值會覆寫在組織或角色層級設定的值。

大多數屬性可以在 Identity Server 標籤或 Identity Server 上的「服務配置」標籤上設定。「服務配置」層級設定的屬性可用作範本。任何新建立的組織或使用者會依預設繼承這些值。

您可以在「服務配置」層級變更屬性值。這些新值僅會在新增新組織時有所體現。變更「服務配置」標籤屬性值不會影響現有組織或使用者。有關詳細資訊，請參閱 *Sun ONE Identity Server 管理員指南*。

您可在 Identity Server 管理主控台的「SRA 配置」下使用下列服務配置 Secure Remote Access 屬性：

- 存取清單

  這個服務可讓您允許或拒絕存取特定的 URL 並管理單次登入功能。有關詳細資訊，請參閱第 8 章「配置 URL 存取控制」。

- 閘道

  這個服務可讓您配置所有與閘道相關的屬性，例如代理伺服器管理、cookie 管理、記錄、Rewriter 管理與密碼。有關詳細資訊，請參閱第 9 章「配置閘道」。

- NetFile

  這個服務可讓您配置所有與 NetFile 相關的屬性，例如共用主機、MIME 類型並存取不同類型的主機。有關詳細資訊，請參閱第 10 章「配置 NetFile」。

- Netlet

  這個服務可讓您配置所有與 Netlet 相關的屬性，例如 Netlet 規則、存取需要的規則、組織與主機以及預設演算法。有關詳細資訊，請參閱第 11 章「配置 Netlet」。

注意 閘道在執行時不會接收屬性變更的通知。

重新啓動閘道以確保閘道使用的是更新的設定檔屬性 (屬於閘道或其他任何服務)。請參閱第 68 頁的 「使用認證鏈接」。

設定衝突解析

➤ **若要設定衝突解析層級**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取 「識別管理」標籤。
3. 從 「檢視」下拉式清單中選取 「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從 「檢視」下拉式清單中選取 「服務」。
6. 按一下 「SRA 配置」之下適當服務 (存取清單、NetFile 或 Netlet) 旁的箭頭。
7. 在 「衝突解析層級」欄位下拉式清單中選取需要的層級。
8. 按一下 NetFile 頁面頂端或底部的 「儲存」記錄變更。

支援的應用程式

Secure Remote Access 支援下列應用程式

- MS Exchange 2000 SP3 installation of Outlook Web Access (OWA).

  OWA 頁面需要的規則集會使用 `exchange_2000sp3_owa_ruleset` 名稱安裝於方塊之外。若要檢視 OWA 的專案研究，請參閱第 253 頁的 「Outlook Web Access 的規則集」。

- i Notes - Notes 5.0.11
- 行事曆 - Sun™ ONE Calendar Server Release 5.1.1 與 Sun™ ONE Calendar Server Release 6.0
- Messenger Express - iPlanet Messaging Server 5.2 與 Sun™ ONE Messaging Server 6.0

第 2 章

閘道

本章說明與閘道相關的概念，與順利執行閘道時所需的資訊。關於配置閘道的資訊，請參閱第 9 章，「配置閘道」。

本章涵蓋下列主題：

- 閘道簡介
- 建立閘道設定檔
- 了解 platform.conf 檔案
- 啓動和停止閘道
- 重新啓動閘道
- 指定代理伺服器以聯絡 Identity Server
- 在 chroot 環境中執行閘道
- 建立閘道的多個實例
- 使用網路代理伺服器
- 使用 Netlet 代理伺服器
- 使用 Rewriter 代理伺服器
- 取得用戶端資訊
- 使用認證鏈接
- 使用萬有字元證書
- 停用瀏覽器快取
- 自訂閘道服務使用者介面
- 使用聯合管理

閘道簡介

閘道在源自網際網路的遠端使用者階段作業與您的企業內部網路之間提供了介面與安全界線。透過單一介面給遠端使用者，閘道可經由內部網路伺服器和應用程式伺服器安全地顯示內容。

建立閘道設定檔

閘道設定檔包含與閘道配置相關的所有資訊，例如閘道傾聽的連接埠、SSL 選項與代理伺服器選項。

當您安裝閘道時，如果您選擇預設值，則會建立名爲「default」的預設閘道設定檔。與預設設定檔對應的配置檔會出現在：

`/etc/opt/SUNWps/platform.conf.default`

其中 `/etc/opt/SUNWps` 是所有 `platform.conf.*` 檔案的預設位置。

請參閱第 37 頁的「了解 platform.conf 檔案」以取得更多關於 `platform.conf` 檔案內容的資訊。

您可以：

- 建立多個設定檔，定義每個設定檔的屬性，並視需要指定這些設定檔給不同的閘道。
- 在不同的機器上指定單一設定檔給閘道安裝。
- 指定不同的設定檔給在相同機器上執行的單一閘道實例。

注意 不要指定相同的設定檔給在相同機器上執行的閘道不同實例。這將會造成衝突，因爲連接埠號碼會一樣。

不要在不同的設定檔 (建立給相同的閘道) 中指定相同的連接埠號碼。以同樣的連接埠執行相同閘道的多個實例會造成衝突。

➤ 建立閘道設定檔

1. 以管理員的身份登入 Sun™ ONE Identity Server 管理主控台。
2. 選取「服務配置」標籤。

3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   閘道頁面會顯示在右邊的窗格中。

4. 按一下「新增」。

   建立新閘道設定檔頁面會顯示。

5. 輸入新「閘道設定檔」名稱。

6. 選取欲使用的設定檔，以在下拉式清單中建立新設定檔。

   在預設情況下，您建立的任何新設定檔都是以預先封裝的預設設定檔爲基礎。如果您已經建立自訂的設定檔，則可以從下拉清單中選擇該設定檔。新的設定檔會繼承所選設定檔的所有屬性。

7. 按一下「建立」。

   會建立新的設定檔，而您會回到「閘道」頁面，新的設定檔會列在此處。

8. 如果您想要讓變更生效，請使用新的閘道設定檔名稱重新啓動閘道：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

若要配置閘道，請參閱第 9 章，「配置閘道」。

了解 platform.conf 檔案

`platform.conf` 檔案位於：

`/etc/opt/SUNWps`

`platform.conf` 檔案包含閘道所需的詳細資訊。本節提供一個範例 `platform.conf` 檔案，並說明所有的項目。

在配置檔中包含所有機器特定詳細資料的優點，就是共用的設定檔可以被在多個機器上執行的閘道共享。

範例如下：

```
#
# Copyright 11/28/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf1.38 00/11/28 Sun Microsystems"
#
gateway.user=noaccess
gateway.jdk.dir=/usr/java_1.3.1_06
```

```
gateway.dsame.agent=http://pserv2.iportal.com:8080/sunportal/RemoteConfigS
ervlet
portal.server.protocol=http
portal.server.host=pserv2.iportal.com
portal.server.port=8080
gateway.protocol=https
gateway.host=siroe.india.sun.com
gateway.port=333
gateway.trust_all_server_certs=true
gateway.trust_all_server_cert_domains=false
gateway.virtualhost=siroe1.india.sun.com 10.13.147.81
gateway.virtualhost.defaultOrg=o=root,dc=test,dc=com
gateway.notification.url=/notification
gateway.retries=6
gateway.debug=error
gateway.debug.dir=/var/opt/SUNWps/debug
gateway.logdelimiter=&&
gateway.external.ip=10.12.147.71
gateway.certdir=/etc/opt/SUNWps/cert/portal
gateway.allow.client.caching=true
gateway.userProfile.cacheSize=1024
gateway.userProfile.cacheSleepTime=60000
gateway.userProfile.cacheCleanupTime=300000
gateway.bindipaddress=10.12.147.71
gateway.sockretries=3
gateway.enable.accelerator=false
gateway.enable.customurl=false
gateway.httpurl=http://siroe.india.sun.com
gateway.httpsurl=https://siroe.india.sun.com
gateway.favicon=https://siroe.india.sun.com
```

```
gateway.logging.password=ALKJDF123SFLKJJSDFU
```

表 2-1 列出並說明在 platform.conf 檔中所有的欄位。此表格具有三個欄。第一欄列出檔案中的項目，第二欄提供預設值 (如果有的話)，第三欄提供該欄位的簡單說明。

表 2-1 platform.conf 檔案屬性

項目	預設值	說明
gateway.user	noaccess	閘道以此使用者執行。 閘道必須以根使用者啟始，在安裝後會遺失根使用者的特權而變成此使用者。
gateway.jdk.dir		這是閘道所使用之 JDK 目錄的位置。
gateway.dsame.agent		當閘道啟動要取得其設定檔時，這是閘道會聯絡的識別伺服器 URL。
portal.server.protocol portal.server.host portal.server.port		這是預設 Portal Server 安裝使用的通訊協定、主機和連接埠。
gateway.protocol gateway.host gateway.port		這是閘道的通訊協定、主機和連接埠。這些值與您在安裝時所指定的模式和連接埠相同。這些值用於建立通知 URL。
gateway.trust_all_server_certs	true	這表示閘道必須相信所有的伺服器證書，或僅相信在閘道證書資料庫中的伺服器證書。
gateway.trust_all_server_cert_domains	false	無論何時在閘道和伺服器之間都會有個 SSL 通訊，並且會提供伺服器證書給閘道。在預設情況下，閘道會檢查伺服器主機名稱是否與伺服器證書 CN 相同。 如果屬性值設定為 true，則閘道會停用它收到之伺服器證書的網域名稱檢查。
gateway.virtualhost		如果閘道機器有配置多個主機名稱，您可以在此欄位指定不同的名稱和識別提供者位址。

表 2-1 platform.conf 檔案屬性

項目	預設值	說明
gateway.virtualhost.defaultOrg=org		這會指定預設的 Org 給將登入的使用者。 例如假設虛擬主機欄位項目如下所示： gateway.virtualhost=test.com employee.test.com Managers.test.com 含有預設的 org 項目為： test.com.defaultOrg = o=root,dc=test,dc=com employee.test.com.defaultOrg = o=employee,dc=test,dc=com Manager.test.com.defaultOrg = o=Manager,dc=test,dc=com 使用者可以使用 https://manager.test.com 而非 https://test.com/o=Manager,dc=test,dc=com 以登入管理員的 org。 注意：virtualhost 和 defaultOrg 在 platform.conf file 中區分大小寫，但用於 URL 時則沒有區分。
gateway.notification.url		閘道主機、通訊協定和連接埠的組合，用於建立通知 URL。用於從 Identity Server 接收階段作業通知。 請確定通知 URL 和任何組織的名稱不相同。如果通知 URL 和組織名稱相同，則使用者在嘗試連結到該組織時會看到空白頁面而非登入的頁面。
gateway.retries		此數字是在啟動時，閘道嘗試連絡 Portal Server 的次數。

表 2-1 platform.conf 檔案屬性

項目	預設值	說明
gateway.debug	error	設定閘道的除錯層級。除錯檔案位於 *debug-directory*/files。除錯檔案位置指定在 gateway.debug.dir 項目中。 除錯層級為： error - 只會在除錯檔案中記錄幾個錯誤。在此種錯誤發生時，閘道通常會停止運作。 warning - 會記錄警告訊息。 message - 會記錄所有的除錯訊息。 on - 會在主控台顯示所有的除錯訊息。 除錯檔案為： srapGateway.*gateway-profile-name* - 包含閘道的除錯訊息。 Gateway_to_from_server.*gateway-profile-name* - 在訊息模式下，此檔案包含閘道和內部伺服器之間所有的需求和回應標頭。 要產生此檔案，請變更 /var/opt/SUNWps/debug 目錄的寫入權限。 Gateway_to_from_browser.*gateway-profile-name* - 在訊息模式下，此檔案包含閘道和內部伺服器之間所有的需求和回應標頭。 要產生此檔案，請變更 /var/opt/SUNWps/debug 目錄的寫入權限。
gateway.debug.dir		這是所有除錯檔案產生的目錄。 此目錄必須有足夠的權限，讓在 gateway.user 中提到的使用者寫入檔案。
gateway.logdelimiter		目前沒有使用。
gateway.external.ip		如果有多個地址的閘道機器 (一個閘道機器有多個 IP 位址) ，您需要在此指定外部的 IP 位址。此 IP 用於 Netlet 以執行 FTP。
gateway.certdir		它指定證書資料庫的位置。
gateway.allow.client.caching	true	允許或拒絕用戶端快取。 如果允許，用戶端伺服器可以快取靜態頁面和影像以取得較佳的效能 (藉由減少的網路流量)。 如果不允許，在用戶端的安全性會提高，像是沒有快取一樣，但是在較高網路負載的情況下時效能將會降低。

表 2-1 platform.conf 檔案屬性

項目	預設值	說明
gateway.userProfile.cacheSize		這是在閘道上使用者設定檔項目被快取的數目。如果項目數量超過這個值，常用的項目會清除快取。
gateway.userProfile.cacheSleepTime		以秒為單位設定休息時間，以清除快取。
gateway.userProfile.cacheCleanupTime		超過以秒為單位的最大數字的時間後，會移除設定檔項目。
gateway.bindipaddress		在多地址閘道機器上，這是閘道連接其伺服器插槽的 IP 位址。
gateway.sockretries	3	目前沒有使用。
gateway.enable.accelerator	false	如果設定為 true，則允許支持外部加速器。
gateway.enable.customurl	false	如果設定為 true，則允許管理員指定一個自訂的 URL 讓閘道重新寫入頁面。
gateway.httpurl		輸入 HTTP reverseproxy URL 以設定自訂的 URL 讓閘道重新寫入頁面。
gateway.httpsurl		輸入 HTTPS reverseproxy URL 以設定自訂的 URL 讓閘道重新寫入頁面。
gateway.favicon		它指定閘道將為 favicon.ico 檔重新導向需求的 URL。 此項目用於 Internet Explorer、Netscape 7.0 和更高的喜好設定或我的最愛中的「favorite icon」。 如果此項目保持空白，閘道會傳送一個「404 頁面找不到」的訊息給瀏覽器。
gateway.logging.password		此欄位包含使用者「amService-srapGateway」的 LDAP 密碼，閘道會使用該密碼用以建立其應用程式階段作業。 密碼可以是加密文字或一般文字。
http.proxyHost		代理伺服器主機會用於聯絡 Portal Server。
http.proxyPort		主機連接埠會用於聯絡 Portal Server。
http.proxySet		若需要代理伺服器，則屬性會設定為 true。若屬性設定為 false，則會忽略 http.proxyHost 與 http.proxyPort。

啓動和停止閘道

在預設情況下，閘道以使用者 noaccess 啓動。

➤ 啓動閘道

1. 安裝閘道並建立需要的設定檔後，執行下面的指令以啓動閘道：

   gateway-install-root/SUNWps/bin/gateway -n default start

   default 是在安裝時建立的預設閘道設定檔。您可以稍後建立自己的設定檔，並且用新的設定檔重新啓動閘道。請參閱第 36 頁的「建立閘道設定檔」。

   如果您有多閘道實例，請使用：

   gateway-install-root/SUNWps/bin/gateway start

此指令會啓動所有在該特定機器上配置的閘道實例。

備註 重新啓動伺服器 (即爲您已經配置閘道實例於其上的機器) 會重新啓動所有閘道已經配置的實例。

確定在 /etc/opt/SUNWps 目錄中沒有舊的或備份的設定檔。

2. 執行下列指令來檢查閘道是否在指定的連接埠上執行：

   netstat -a | grep *port-number*

   預設的閘道連接埠是 443。

➤ 停止閘道

使用下面的指令以停止閘道：

gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* stop

如果您有多閘道實例，請使用：

gateway-install-root/SUNWps/bin/gateway stop

此指令會停止所有在該特定機器上正在執行的閘道實例。

重新啓動閘道

一般而言，您不需要重新啓動閘道。但如果下列事件發生，您就需要重新啓動閘道：

- 您已經建立新的設定檔並且需要指定此新的設定檔給閘道。
- 您已經在現有的設定檔中修改一些屬性，並且需要變更以使其生效。

➤ 使用不同的設定檔重新啓動閘道

重新啓動「閘道」：

gateway-install-root/SUNWps/bin/gateway -n *new-gateway-profile-name* start

➤ 若要重新啓動閘道

在終端機視窗中，以根使用者身分連接並執行下列其中之一：

- 啓動監視程式程序：

  gateway-install-root/SUNWps/bin/gateway watchdog on

  會在 crontab 中建立一個項目，而現在監視程式會啓動。監視程式會監視在特定機器上閘道所有正在執行的實例和閘道連接埠，且如果閘道效能降低會重新啓動閘道。

- 手動啓動閘道：

  gateway-install-root/SUNWps/bin/rwproxd/SUNWps/bin/gateway -n *gateway-profile-name* start

  其中 *gateway-profile-name* 是對應到所需閘道實例的設定檔名稱。

➤ 配置閘道監視程式

您可以配置監視程式監視閘道狀態的時間間隔。時間間隔預設爲 60 秒。若要變更，在 crontab 中編輯下面的行：

```
0-59 * * * * gateway-install-root/SUNWps/bin/rwproxd/bin/checkgw
/var/opt/SUNWps/.gw.5 > /dev/null 2>&1
```

請參閱 crontab 的線上說明以配置 crontab 項目。

指定代理伺服器以聯絡 Identity Server

您可以指定「閘道」用以聯絡 SRA 支援 (RemoteConfigServlet) 的主機代理伺服器，該 SRA 支援部署在 Portal Server 上。「閘道」使用此代理伺服器連絡 Portal Server 與 PIdentity Server。

➤ 若要指定代理伺服器

1. 從指令行中，編輯下列檔案：

   `/etc/opt/bin/platform.conf.`*gateway-profile-name*

2. 新增下列項目：

   `http.proxyHost=`*proxy-host*

   `http.proxyPort=`*proxy-port*

   `http.proxySet=true`

3. 爲針對該伺服器所提出的請求重新啓動閘道，以使用指定的代理伺服器：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

在 chroot 環境中執行閘道

若要在 chroot 環境中提供較高安全性，chroot 目錄內容必須盡可能縮小。例如，如果有任何程式允許使用者修改在 chrooted 目錄內的檔案，在 chroot 樹下 chrooted 將不會保護伺服器不被攻擊者修改檔案。不應該在 CGI 程式中寫入解譯語言，例如 bourne shell、c-shell、korn shell 或 perl，但是應該編譯二進位以使解譯器不需要在 chroot 目錄樹下出現。

備註 監視程式功能不應該存在於 chroot 環境中。

➤ 安裝 chroot

1. 作爲根使用者，在終端視窗中複製下列檔案到外部資源，例如在網路上的電腦、備份磁帶或是磁片中。

   `cp /etc/vfstab` *external-device*

   `cp /etc/nsswitch.conf` *external-device*

   `cp /etc/hosts` *external-device*

2. 從 mkchroot script 執行：

   portal-server-install-root/SUNWps/bin/chroot

備註 在 mkchroot script 開始執行後，不能按 Ctrl-C 加以終止。

在執行 mkchroot script 後，錯誤事件請參閱第 47 頁的「mkchroot Script 執行失敗」。

會提示您另一個根使用者目錄 (new_root_directory) 。程式檔建立此新的目錄。

在下列的實例中，/safedir/chroot 是 new_root_directory。

```
mkchroot version 6.0

Enter the full path name of the directory which will be the chrooted
tree:/safedir/chroot
Using /safedir/chroot as root.
Checking available disk space...done
/safedir/chroot is on a setuid mounted partition.
Creating filesystem structure...dev etc sbin usr var proc opt bin lib tmp
etc/lib usr/platform usr/bin usr/sbin usr/lib usr/openwin/lib var/opt
var/tmp dev/fd done
Creating devices...null tcp ticots ticlts ticotsord tty udp zero conslog
done
Copying/creating etc files...group passwd shadow hosts resolv.conf netconfig
nsswitch.conf
done
Copying binaries.................................done
Copying libraries................................done
Copying zoneinfo (about 1 MB)..done
Copying locale info (about 5 MB).........done
Adding comments to /etc/nsswitch.conf ...done
Creating loopback mount for/safedir/chroot/usr/java1.2...done
Creating loopback mount for/safedir/chroot/proc...done
Creating loopback mount for/safedir/chroot/dev/random...done
Do you need /dev/fd (if you do not know what it means, press return)[n]:
Updating /etc/vfstab...done
Creating a /safedir/chroot/etc/mnttab file, based on these loopback mounts.
Copying SRAP related data ...
Using /safedir/chroot as root.
Creating filesystem structure..........done
mkchroot successfully done.
```

3. 使用下面的指令以手動裝載 `platform.conf` 檔案中提到的 Java 目錄到 chroot 目錄：

   ```
   mkdir -p /safedir/chroot/java-dir
   ```

   ```
   mount -F lofs java-dir /safedir/chroot/java-dir
   ```

   在 Solaris 9 則執行下列動作：

   ```
   mkdir -p /safedir/chroot/usr/lib/32
   ```

   ```
   mount -F lofs /usr/lib/32 /safedir/chroot/usr/lib/32
   ```

   ```
   mkdir -p /safedir/chroot/usr/lib/64
   ```

   ```
   mount -F lofs /usr/lib/64 /safedir/chroot/usr/lib/64
   ```

   若要在系統啓動時裝載此目錄，則新增對應的項目於 `/etc/vfstab` 中：

   java-dir `- /safedir/chroot/`*java-dir* `lofs - no -`

   對於 Solaris 9：

   ```
   /usr/lib/32 - /safedir/chroot/usr/lib/32 lofs - no -
   ```

   ```
   /usr/lib/64 - /safedir/chroot/usr/lib/64 lofs - no -
   ```

4. 鍵入下列的指令以重新啓動閘道：

```
chroot /safedir/chroot ./gateway-install-root/SUNWps/bin/gateway start
stopping gateway ... done.
starting gateway ...
done.
```

mkchroot Script 執行失敗

在執行 `mkchroot` script 時發生錯誤事件，script 將會把檔案復原成初始的狀態。

在下面的範例中，`/safedir/chroot` 是 chroot 目錄。

如果遇到下面的錯誤訊息：

```
Not a Clean Exit
```

1. 複製程序安裝 chroot 步驟 1 中的備分檔案到它們原來的位置，並執行下列指令：

   ```
   umount /safedir/chroot/usr/java1.2
   ```

   ```
   umount /safedir/chroot/proc
   ```

   ```
   umount /safedir/chroot/dev/random
   ```

2. 移除 /safedir/chroot 目錄。

在 chroot 環境中重新啓動閘道

每當閘道機器重新開機時，在 chroot 環境中遵循下列步驟以啓動閘道。

➤ **在 chroot 環境中重新啓動閘道**

1. 從「/」目錄停止閘道的運作。

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* stop

2. 啓動閘道以從 chroot 目錄執行：

   chroot /safedir/chroot ./*portal-server-install-root*/SUNWps/bin/gateway -n *gateway-profile-name* start

---

備註 需要管理 /safedir/chroot/etc 檔案 (例如 passwd 和 hosts)，像 /etc 檔案一樣，但僅包含在 chroot 樹中執行程式所需要的主機和帳號資訊。

例如，如果您變更了系統的識別提供者地址，您同時也變更了 /safedir/chroot/etc/hosts 檔案。

建立閘道的多個實例

使用 gwmultiinstance 程式檔以建立閘道的新實例。最好在建立閘道設定檔之後執行此程式檔。

1. 以根使用者身分登入並瀏覽至下面的目錄：

   gateway-install-root/SUNWps/bin/

2. 執行多實例程式檔：

   ./gwmultiinstance

3. 選擇下列安裝選項之一：

1) Create a new gateway instance (建立新的閘道實例)

2) Remove a gateway instance (移除一個閘道實例)

3) Remove all gateway instances (移除所有閘道實例)

4) Exit (結束)

如果您選擇 1，則請回答下列問題：

What is the name of the new gateway instance? (新閘道實例的名稱爲何 ?)

What protocol will the new gateway instance use? (此新閘道實例將會使用哪個通訊協定 ?)[https]

What port will the new gateway instance listen on? (新閘道實例將會在哪個連接埠上傾聽 ?)

What is the fully qualified hostname of the portal server? (伺服器的完全合格主機名稱爲何 ?)

What port should be used to access the portal server? (應該使用哪個連接埠以存取 Portal Server?)

What protocol should be used to access the portal server? (應該使用哪個通訊協定以存取 Portal Server?)[http]

What is the portal server deploy URI? (什麼是 Portal Server 佈置 URI?)

What is the organization DN? (組織的 DN 爲何 ?)[dc=iportal,dc=com]

What is the identity server URI? (識別伺服器 URI 爲何 ?)[/amserver]

What is the identity server password encryption key? (識別伺服器密碼加密金鑰爲何 ?)

Please provide the following information needed for creating a self-signed certificate: (請提供下列所需資訊以建立自簽證書：)

What is the name of your organization? (您的組織名稱爲何 ?)

What is the name of your division? (您的分部名稱爲何 ?)

What is the name of your city or locality? (您的城市或地區名稱爲何 ?)

What is the name of your state or province? (您的州名或省名爲何 ?)

What is the two-letter country code? (您的兩個字母國碼爲何 ?)

What is the password for the Certificate Database? Again? (證書資料庫的密碼爲何？ 再試一次 ?)

What is the password for the logging user?Again? (記錄使用者的密碼爲何？ 再試一次？)

Have you created the new gateway profile in the admin console? (您在管理主控台是否已經建立新的閘道設定檔？)[y]/n

Start the gateway after installation? (安裝後啓動閘道？)[y]/n

4. 以新的閘道設定檔名稱啓動閘道的新實例。

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

   其中 *gateway-profile-name* 是新的閘道實例。

使用網路代理伺服器

您可以使用協力廠商的網路代理伺服器，配置閘道以聯絡 HTTP 資源。網路伺服器位於客戶端與網際網路之間。

網路代理伺服器配置

不同的代理伺服器可能用於不同的網域和子網域。這些項目告訴閘道在特定的網域中，應該使用哪個代理伺服器以聯絡特定的子網域。指定在閘道中的代理伺服器配置運作方式如下：

- 在閘道服務中，建立一個清單，其中包含網域和子網域，以及「網域和子網域的代理伺服器」欄位中必要的代理伺服器。

  關於爲網域和子網域配置代理伺服器的資訊，請參閱第 238 頁的「建立網域與子網域的代理伺服器清單」。

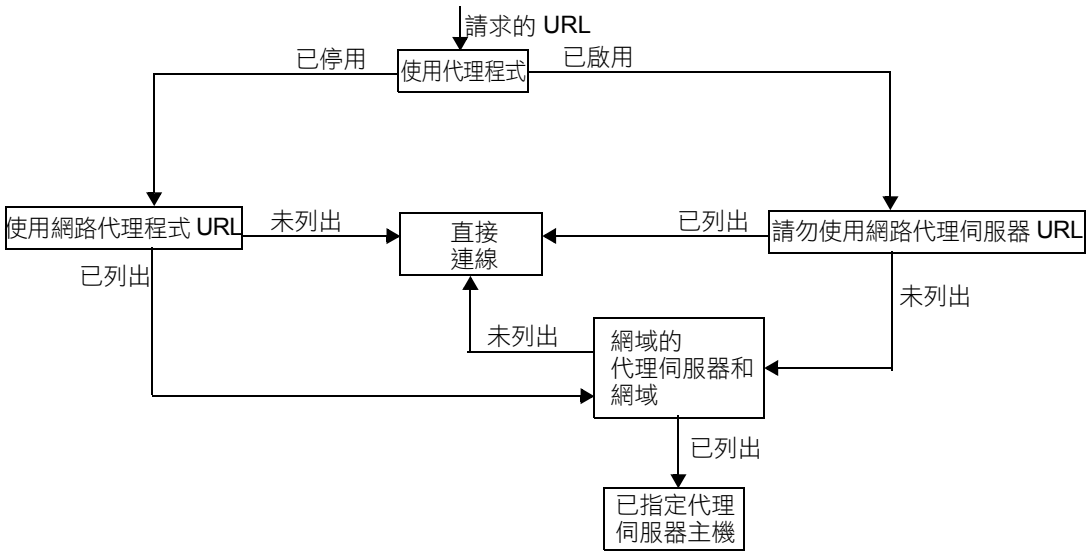
- 當「使用代理伺服器」選項啓用時：
  - 在「網域和子網域的代理伺服器」欄位所指定的代理伺服器會用於指定的主機。
  - 若要在網域和子網域 (在「網域和子網域的代理伺服器」清單中指定的) 中啓用某些 URL 的直接連線，請在「請勿使用網路代理伺服器 URL」中指定這些 URL。
- 當「使用代理伺服器」選項停用時：

- 若要確認在網域和子網域 (在「網域和子網域的代理伺服器」欄位中指定的) 中某些 URL 使用代理伺服器，請在「使用網路代理伺服器的 URL」清單中指定這些 URL。雖然停用「使用代理伺服器」功能，但仍可使用代理伺服器連接到列於「使用網路代理伺服器」清單下的 URL。這些 URL 的代理伺服器是從「網域和子網域的代理伺服器」清單中取得。

若要配置「使用代理伺服器」選項，請參閱第 236 頁的「啓用網路代理伺服器的使用」。

圖 2-1 顯示在閘道服務中，如何在代理伺服器配置的基礎下解決網路代理伺服器的訊息。

圖 2-1 網路代理伺服器管理



在圖 2-1 中，如果「使用代理伺服器」是啓用的，且要求的 URL 列於「請勿使用網路代理伺服器 URL」清單中，則閘道會直接連到目的地主機。

如果「使用代理伺服器」是啓用的，且要求的 URL 未列於「請勿使用網路代理伺服器 URL」清單中，則閘道會透過指定的代理伺服器連到目的地主機。此代理伺服器 (如果有指定) 可以從「網域和子網域的代理伺服器」清單中查看。

如果「使用代理伺服器」停用，且請求的 URL 有列於「使用網路代理伺服器」清單中，則閘道會使用列在「網域和子網域的代理伺服器」清單中的代理伺服器資訊連接目的地主機。

如果「使用代理伺服器」是停用的，且要求的 URL 未列於「請勿使用網路代理伺服器 URL」清單中，則閘道會直接連線到目的地主機。

如果您的情況不符合上述任何一項，且無法使用直接連線，閘道會顯示一個錯誤，說明連線無法使用。

備註 如果您正透過入口網站桌面的「書籤通道」存取該 URL，且您的情況不符合上述任何一項，閘道會傳送重新導向給瀏覽器。瀏覽器會使用自己的代理伺服器設定來存取該 URL。

語法

```
domainname [web_proxy1:port1]|subdomain1 [web_proxy2:port2]|......
```

範例

```
sesta.com wp1:8080|red wp2:8080|yellow|* wp3:8080
```

* 是符合所有資料的萬用字元

其中，

`sesta.com` 是網域名稱而 `wp1` 是在 8080 連接埠上連接的代理伺服器。

`red` 是子網域名稱而 `wp2` 是在 8080 連接埠上連接的代理伺服器。

`yellow` 是子網域。由於沒有指定代理伺服器，因此會使用指定給網域的代理伺服器，即爲在 8080 連接埠上的 `wp1`。

* 表示所有其他子網域 `wp3` 必須在 8080 連接埠上使用。

備註 如果您沒有指定連接埠，預設是使用連接埠 8080。

處理網路代理伺服器資訊

當客戶端嘗試存取特定的 URL 時，在 URL 中的主機名稱符合在「網域和子網域的代理伺服器」清單中的項目。符合請求主機名稱之最長後綴的項目會被考慮。例如，考慮請求的主機名稱是 `host1.sesta.com`

- 會掃描 `host1.sesta.com` 的網域和子網域的代理伺服器。如果找到符合的項目，指定給此項目的代理伺服器會用來連接此主機。
- 否則，會掃描清單中的 `*.sesta.com`。如果找到符合的項目，會使用對應的代理伺服器。

- 否則，會尋找清單中的 sesta.com。如果找到符合的項目，會使用對應的代理伺服器。
- 否則，會尋找清單中的 *.com。如果找到符合的項目，會使用對應的代理伺服器。
- 否則，會尋找清單中的 com。如果找到符合的項目，會使用對應的代理伺服器。
- 否則，會尋找清單中的 *。如果找到符合的項目，會使用對應的代理伺服器。
- 否則，會嘗試直接連線。

在「網域和子網域的代理伺服器」清單中考慮下列項目：

```
com p1| host1 p2 | host2 | * p3
sesta.com p4 | host5 p5 | * p6
florizon.com | host6
abc.sesta.com p8 | host7 p7 | host8 p8 | * p9
host6.florizon.com p10
host9.sesta.com p11
siroe.com | host12 p12 | host13 p13 | host14 | * p14
siroe.com | host15 p15 | host16 | * p16
* p17
```

閘道在內部對映的項目顯示於表 2-2 中。

表 2-2 在「網域和子網域的代理伺服器」清單中的對映項目

號碼	「網域和子網域的代理伺服器」清單中的項目	代理伺服器	說明
1	com	p1	指定於清單中。
2	host1.com	p2	指定於清單中。
3	host2.com	p1	由於沒有指定代理伺服器給 host2，會使用主機的代理伺服器。
4	*.com	p3	指定於清單中。
5	sesta.com	p4	指定於清單中。
6	host5.sesta.com	p5	指定於清單中。
7	*.sesta.com	p6	指定於清單中。
8	florizon.com	直接	詳細資料，請參閱第 14 個項目的說明。

表 2-2 在「網域和子網域的代理伺服器」清單中的對映項目

號碼	「網域和子網域的代理伺服器」清單中的項目	代理伺服器	說明
9	host6.florizon.com	–	詳細資料，請參閱第 14 個項目的說明。
10	abc.sesta.com	p8	指定於清單中。
11	host7.abc.sesta.com	p7	指定於清單中。
12	host8.abc.sesta.com	p8	指定於清單中。
13	*.abc.sesta.com	p9	指定於清單中。在 `abc.sesta.com` 網域下，除了 `host7` 和 `host8` 之外的主機，p9 會用作代理伺服器。
14	host6.florizon.com	p10	與第 9 個項目相同。第 9 個項目表示直接連線，而此項目表示應該使用代理伺服器 p10。若遇到像這樣有兩個項目的情況，含有代理伺服器資訊的項目視為是一個有效的項目。請忽略另一個項目。
15	host9.sesta.com	p11	指定於清單中。
16	siroe.com	直接	由於並沒有指定代理伺服器給 `siroe.com`，因此會嘗試直接連線。
17	host12.siroe.com	p12	指定於清單中。
18	host13.siroe.com	p13	指定於清單中。
19	host14.siroe.com	直接	由於並沒有指定代理伺服器給 `host14` 或給 `siroe.com`，因此會嘗試直接連線。
20	*.siroe.com	p14	請參閱第 23 個項目的說明。
21	host15.siroe.com	p15	指定於清單中。
22	host16.siroe.com	直接	由於並沒有指定代理伺服器給 `host16` 和給 `siroe.com`，因此會嘗試直接連線。
23	*.siroe.com	p16	與第 20 個項目類似。但是指定的代理伺服器不同。這種情形下，無法知道閘道的實際運作方式。可能會使用兩個代理伺服器。
24	*	p17	如果沒有其他的項目符合請求的 URL，就會使用 p17 作為代理伺服器。

備註 取代在「網域和子網域的代理伺服器」清單中分開代理伺服器項目，在清單中有個別的項目是比較簡單的。例如，取代如下的項目：

```
sesta.com p1 | red p2 | * p3
```

您可以將其指定爲：

```
sesta.com p1

red.sesta.com p2

*.sesta.com p3
```

如此會簡化陷入重複項目或任何其他含糊的情況。

以「網域和子網域的代理伺服器」清單爲基礎覆寫

「網域和子網域的代理伺服器」清單中的項目也會被 Rewriter 使用。網域符合列在「網域和子網域的代理伺服器」清單中網域的所有 URL，Rewriter 會重新寫入。

注意 在「網域和子網域的代理伺服器」清單中的 * 項目不會考慮重新寫入。例如，在範例表 2-2 中第 24 個項目就不被考慮。

請參閱第 3 章，「Rewriter」以取得更多關於 Rewriter 的資訊。

預設網域與子網域

當在 URL 中的目的地主機不是完整限定的主機名稱，會使用預設的網域和子網域以使其有完整合格的名稱。

假設管理主控台中「網域和子網域的代理伺服器」欄位內的項目是：

```
red.sesta.com
```

備註 在「網域和子網域的代理伺服器」清單中您必須要有對應的項目。

在上面的範例中，`sesta.com` 是預設的網域而 `red` 是預設的子網域。

如果要求的 URL 是 `host1`，則使用預設的網域和子網域以解決 `host1.red.sesta.com`。然後會在「網域和子網域的代理伺服器」清單中查詢 `host1.sesta.com`。

使用代理伺服器自動配置

若要忽略「網域和子網域的代理伺服器」清單中的資訊，請啓用「代理伺服器自動配置」(PAC) 功能。若要配置 PAC，請參閱第 240 頁的「啓用代理伺服器自動配置 (PAC) 支援」。

使用 PAC 檔案時請注意下列幾點：

- `js.jar` 必須位於閘道機器上的 `$JRE_HOME/lib/ext` 目錄中，否則閘道無法剖析 PAC 檔案。
- 在開機時，閘道從指定在閘道設定檔 PAC 檔案位置獲取 PAC 檔案。若要配置位置，請參閱第 240 頁的「指定 PAC 檔案位置」。
- 閘道使用 URLConnection API 到達此位置。如果需要配置代理伺服器以到達 PCA 檔案位置，必須以下列方式配置代理伺服器。

  a. 從指令行中，編輯下列檔案：

  `/etc/opt/bin/platform.conf.`*gateway-profile-name*

  b. 新增下列項目：

  `http.proxyHost=`*web-proxy-hostname*

  `http.proxyPort=`*web-proxy-port*

  `http.proxySet=true`

  c. 重新啓動閘道以使用指定的代理伺服器：

  gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

- 如果 PAC 檔案初始化失敗，閘道會使用「網域和子網域的代理伺服器」清單中的資訊。
- 如果從 PAC 檔案傳回 "" (空字串) 或 "null"，閘道會假設該主機不屬於此企業內部網路。這與不在「網域和子網域的代理伺服器」清單中之主機的情況類似。

  如果您想要閘道使用直接連線連到主機，請返回到「直接」。請參閱第 57 頁的「含有傳回 DIRECT 或 NULL 的範例」。
- 當指定多個代理伺服器時，閘道僅使用第一個返回的代理伺服器。閘道不會在指定給主機的多個代理伺服器之間嘗試修復錯誤或負載平衡
- 閘道忽略 SOCKS 代理伺服器並嘗試直接連線，同時假設該主機是企業內部網路的一部分。

- 若要指定一個代理伺服器用以連接不在企業內部網路的任何主機，請使用代理伺服器類型「STARPROXY」。這是 PAC 檔案格式的副檔名，與在閘道設定檔的「網域和子網域的代理伺服器」部分中的 `* proxyHost:port` 相似。請參閱第 57 頁的「含有傳回 STARPROXY 的範例」

使用範例 PAC 檔案

下列範例顯示列在「網域和子網域的代理伺服器」清單中的 URL 和對應的 PAC 檔案。

含有傳回 DIRECT 或 NULL 的範例

使用網域和子網域的這些代理伺服器：

```
intranet1.com
intranet2.com.proxy.intranet1.com:8080
```

the corresponding PAC file is:

```
// Start of the PAC File
function FindProxyForURL(url, host) {
         if (dnsDomainIs(host, ".intranet1.com")) {
             return "DIRECT";
         }
          if (dnsDomainIs(host, ".intranet2.com")) {
              return "PROXY proxy.intranet1.com:8080";
          }
          return "NULL";
}
//End of the PAC File
```

含有傳回 STARPROXY 的範例

使用網域和子網域的這些代理伺服器：

```
intranet1.com
intranet2.com.proxy.intranet1.com:8080
internetproxy.intranet1.com:80
```

the corresponding PAC file is:

```
// Start of the PAC File
function FindProxyForURL(url, host) {
          if (dnsDomainIs(host, ".intranet1.com")) {
              return "DIRECT";
          }
          if (dnsDomainIs(host, ".intranet2.com")) {
              return "PROXY proxy.intranet1.com:8080;" +
                  "PROXY proxy1.intranet1.com:8080";
          }
          return "STARPROXY internetproxy.intranet1.com:80";
}
//End of the PAC File
```

在這個情況下，如果是位於 .intranet2.com 網域，則閘道會連絡 proxy.intranet1.com:8080。如果 proxy.intranet1.com:8080 代理伺服器無法使用，請求會失敗。閘道不會修復錯誤和連絡 proxy1.intranet1.com:8080。

使用 Netlet 代理伺服器

Netlet 封包在閘道是解密的，並會傳送到目的地伺服器。然而，閘道需要透過非軍事區 (DMZ) 和企業內部網路之間的防火牆，存取所有的 Netlet 目的地主機。這需要在防火牆中開啓大量的連接埠。Netlet 代理伺服器可用以最小化在代理伺服器中開啓的連接埠。

藉由延伸用戶端的安全通道，透過閘道到存在於企業內部網路的 Netlet 代理伺服器，Netlet 強化閘道和企業內部網路之間的安全性。使用代理伺服器，Netlet 封包會由代理伺服器解密，之後會傳送至目的地伺服器。

下列原因可說明 Netlet 代理伺服器非常有用：

- 新增其他的安全性層級。
- 在非常有限的部署環境中，最小化閘道到內部防火牆之間額外 IP 地址和連接埠的使用。
- 限制閘道和 Portal Server 之間開啓的連接埠數目爲 1。您可在安裝時配置此連接埠數目。

- 延伸客戶端和閘道間的安全通道，最多到如圖 2-2 中「包含配置的 Netlet 伺服器」部分所顯示的 Portal Server。透過資料加密，Netlet 伺服器提供強化的安全益處，但可能會增加系統資源的使用。請參閱 *Sun Java Enterprise System 安裝指南* 以取得更多關於安裝 Netlet 代理伺服器的詳細資料。

您可以：

- 選擇在 Portal Server 節點上或個別節點上安裝 Netlet 代理伺服器。
- 使用管理主控台安裝多個 Netlet 代理伺服器並配置給單一閘道。這對於負載平衡很有用。請參閱第 224 頁的「啓用並建立 Netlet 代理伺服器清單」以取得詳細資料。
- 在單一機器上配置多個 Netlet 代理伺服器實例。
- 將閘道的多個實例指向 Netlet 代理伺服器的單一安裝。
- 通道 Netlet 會透過網路代理伺服器。若要配置此部分，請參閱第 241 頁的「啓用透過網路代理伺服器的通道 Netlet」。

圖 2-2 顯示在有和沒有安裝 Netlet 代理伺服器的情況下，閘道和 Portal Server 的三個範例實作。元件包含一個用戶端、兩個防火牆、位於兩個防火牆之間的閘道、Portal Server 和 Netlet 目的地伺服器。

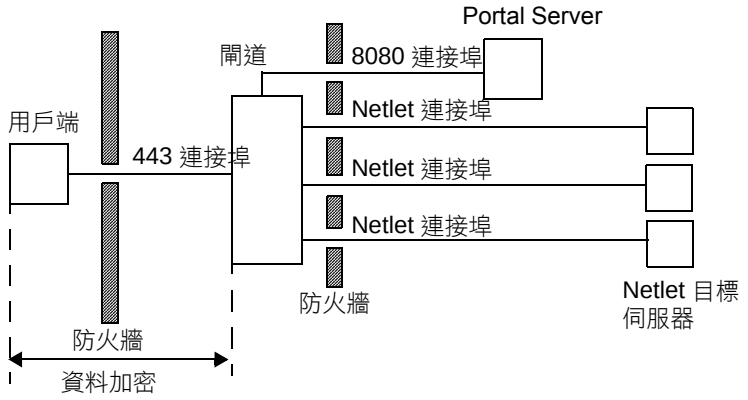
第一個方案顯示沒有安裝 Netlet 代理伺服器的閘道和 Portal Server。此處資料加密僅從用戶端延伸到閘道。在第二個防火牆中開啓一個連接埠給每個 Netlet 連線請求。

第二個方案顯示在 Portal Server 上安裝 Netlet 代理伺服器的閘道和 Portal Server。在此情況中，資料加密從用戶端一直延伸到 Portal Server。由於所有的 Netlet 連線都透過 Netlet 代理伺服器路由，僅需要在第二個防火牆中開啓一個連接埠給 Netlet 請求。

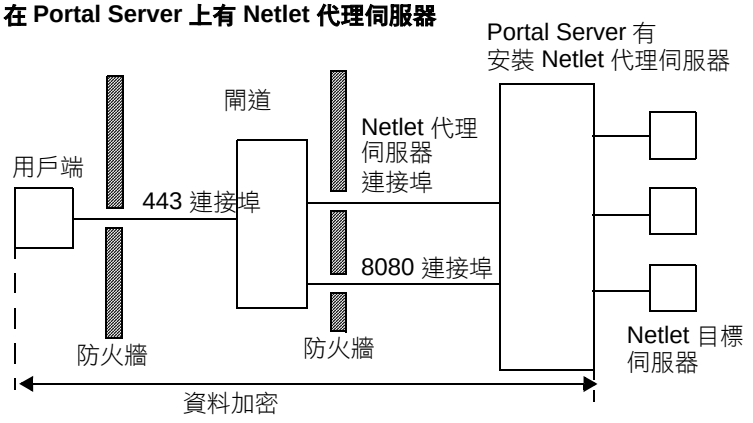
第三個方案顯示有在個別節點上安裝 Netlet 代理伺服器的閘道和 Portal Server。在個別節點上安裝 Netlet 代理伺服器會減少 Portal Server 節點上的負載。同樣的，在第二個防火牆中僅需要開啓兩個連接埠。其中一個連接埠提供給 Portal Server 使用，另一個連接埠則路由 Netlet 請求到 Netlet 代理伺服器伺服器。

圖 2-2 Netlet 代理伺服器的實作

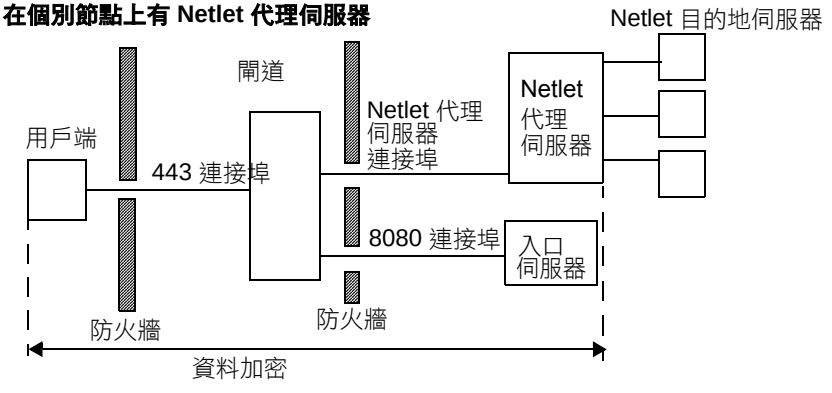
沒有配置的 Netlet 代理伺服器



在 Portal Server 上有 Netlet 代理伺服器



在個別節點上有 Netlet 代理伺服器



建立 Netlet 代理伺服器的實例

使用 `nlpmultiinstance` 程式檔以在 Portal Server 或個別節點上，建立 Netlet 代理伺服器的新實例。最好在建立閘道設定檔之後執行此程式檔：

1. 以根使用者身分登入並瀏覽至下面的目錄：

   netlet-install-dir`/SUNWps/bin`

2. 執行多實例程式檔：

   ```
   ./nlpmultiinstance
   ```

3. 回答 `nlpmultiinstance` 程式檔所問的問題：

   - What is the name of the new netlet proxy instance? (新 netlet 代理伺服器實例的名稱爲何 ?)
   - 如果您有 Rewriter 代理伺服器且是在此節點上以同樣的名稱配置，系統會問您是否要使用相同的配置給此 proxy 代理伺服器實例。
   - 如果您的回答爲是，請回答這兩個問題：
     - What port will the new netlet proxy instance listen on? (新的 Netlet 代理伺服器實例將會使用哪個連接埠傾聽 ?)
     - Start the netlet proxy after installation? (安裝後啓動 Netlet 代理伺服器 ?)
   - 如果您的回答爲否，則請回答下列問題：
     - What protocol will the new netlet proxy instance use? (新的 Netlet 代理伺服器實例會使用什麼通訊協定 ?)
     - What port will the new netlet proxy instance listen on? (新的 Netlet 代理伺服器實例將會使用哪個連接埠傾聽 ?)
     - What is the name of your organization? (您的組織名稱爲何 ?)
     - What is the name of your division? (您的分部名稱爲何 ?)
     - What is the name of your city or locality? (您的城市或地區名稱爲何 ?)
     - What is the name of your state or province? (您的州名或省名爲何 ?)
     - What is the two-letter country code? (您的兩個字母國碼爲何 ?)
     - What is the password for the certificate Database? (您證書資料庫的密碼爲何 ?)
     - What is the password for the logging user? (記錄使用者的密碼爲何 ?)

- Have you created the new netlet proxy profile in the admin console? (您是否已經在管理主控台中建立新的 Netlet 代理伺服器設定檔 ?)
- If you answered yes, start the netlet proxy after installation? (如果您的回答爲是，要在安裝後啓動 Netlet 代理伺服器 ?)

4. 以請求的閘道設定檔名稱啓動 netlet 代理伺服器的新實例：

   netlet-proxy-install-root`/SUNWps/bin/netletd -n` *gateway-profile-name* `start`

   其中 *gateway-profile-name* 是對應到所需閘道實例的設定檔名稱。

啓用 Netlet 代理伺服器

在 Identity Server 管理主控台中的 SRA 配置下，透過閘道服務啓動 Netlet 代理伺服器。請參閱第 224 頁的 「啓用並建立 Netlet 代理伺服器清單」。

重新啓動 Netlet 代理伺服器

每次代理伺服器意外結束時 您可以配置 Netlet 代理伺服器以重新啓動。您可以排程一個監視程式程序以監視 Netlet 代理伺服器，如果效能降低就重新啓動。

您也可以手動重新啓動 Netlet 代理伺服器。

➤ **重新啓動 Netlet 代理伺服器**

在終端機視窗中，以根使用者身分連接並執行下列其中之一：

- 啓動監視程式程序：

  netlet-proxy-install-root`/SUNWps/bin/netletd watchdog on`

  會在 crontab 中建立一個項目，而現在監視程式會啓動。監視程式會監視 Netlet 代理伺服器並在效能降低時開啓代理伺服器。

- 手動啓動 Netlet 代理伺服器：

  netlet-proxy-install-root`/SUNWps/bin/netletd -n` *gateway-profile-name* `start`

  其中 *gateway-profile-name* 是對應到所需閘道實例的設定檔名稱。

➤ **配置 Netlet 代理伺服器監視程式**

您可以配置監視程式監視 Netlet 代理伺服器狀態的時間間隔。時間間隔預設爲 60 秒。若要執行此步驟，在 crontab 中編輯下面的行：

```
0-59 * * * * netlet-install-dir/bin/checkgw /var/opt/SUNWps/.gw 5 > /dev/null 2>&1
```

使用 Rewriter 代理伺服器

Rewriter 代理伺服器安裝在企業內部網路中。取代嘗試直接擷取資料內容，閘道會傳送所有請求給 Rewriter 代理伺服器，而 Rewriter 代理伺服器會獲取並傳回內容給閘道。

使用 Rewriter 代理伺服器有兩個優點：

- 若在閘道與伺服器之間架設防火牆，則防火牆必須僅能開啓兩個連接埠，一個位於閘道與 Rewriter 代理伺服器之間，另一個位於閘道與 Portal Server 之間。
- 在閘道和企業內部網路間的 HTTP 流量現在很安全，即使目的地伺服器僅支援 HTTP 通訊協定 (不支援 HTTPS)。

如果您沒有指定 Rewriter 代理伺服器，當使用者嘗試存取企業內部網路的其中一台電腦，閘道元件會直接連線至企業內部網路的電腦。

要啓用 Rewriter 代理伺服器，請參閱第 221 頁的「啓用並建立 Rewriter 代理伺服器清單」。

建立 Rewriter 代理伺服器的實例

使用 `rwpmultiinstance` 程式檔以在 Portal Server 節點上建立 Rewriter 代理伺服器的新實例。最好在建立閘道設定檔之後執行此程式檔。

1. 以根使用者身分登入並瀏覽下面的目錄：

   rewriter-proxy-install-root`/SUNWps/bin`

2. 執行多實例程式檔：

   ```
   ./rwpmultiinstance
   ```

3. 回答 nlpmultiinstance 程式檔所問的問題：

   - What is the name of the new rewriter proxy instance? (新 Rewriter 代理伺服器實例的名稱爲何 ?)
   - 如果您有 Rewriter 代理伺服器且是在此節點上以同樣的名稱配置，系統會問您是否要使用相同的配置給此 Rewriter 代理伺服器實例。)
   - 如果您的回答爲是，請回答這兩個問題：

- What port will the new rewriter proxy instance listen on? (新的 rewriter 代理伺服器實例將會使用哪個連接埠傾聽 ?)
- Start the rewriter proxy after installation? (安裝後啓動 rewriter 代理伺服器 ?)

❍ 如果您的回答爲否，則請回答下列問題：

- What protocol will the new rewriter proxy instance use? (新的 rewriter 代理伺服器實例會使用什麼通訊協定 ?)
- What port will the new rewriter proxy instance listen on? (新的 rewriter 代理伺服器實例將會使用哪個連接埠傾聽 ?)
- What is the name of your organization? (您的組織名稱爲何 ?)
- What is the name of your division? (您的分部名稱爲何 ?)
- What is the name of your city or locality? (您的城市或地區名稱爲何 ?)
- What is the name of your state or province? (您的州名或省名爲何 ?)
- What is the two-letter country code? (您的兩個字母國碼爲何 ?)
- What is the password for the certificate Database? (您證書資料庫的密碼爲何 ?)
- What is the password for the logging user? (記錄使用者的密碼爲何 ?)
- Have you created the new rewriter proxy profile in the admin console? (您是否已經在管理主控台中建立新的 rewriter 代理伺服器設定檔 ?)
- If you answered yes, start the rewriter proxy after installation? (如果您的回答爲是，要在安裝後啓動 rewriter 代理伺服器 ?)

4. 以請求的閘道設定檔名稱啓動 Rewriter 代理伺服器的新實例：

rewriter-proxy-install-root`/SUNWps/bin/rwproxyd -n` *gateway-profile-name* `start`

其中 *gateway-profile-name* 是對應到所需閘道實例的設定檔名稱。

啓用 Rewriter 代理伺服器

在 Identity Server 管理主控台中，在「SRA 配置」下透過閘道服務啓用 Rewriter 代理伺服器。請參閱第 221 頁的「啓用並建立 Rewriter 代理伺服器清單」。

重新啓動 Rewriter 代理伺服器

每次代理伺服器意外結束時 您可以配置 Rewriter 代理伺服器以重新啓動。您可以排程一個 監視程式程序以監視 Rewriter 代理伺服器，如果效能降低就重新啓動。

您也可以手動重新啓動 Rewriter 代理伺服器。

➤ 重新啓動 Rewriter 代理伺服器

在終端機視窗中，以根使用者身分連接並執行下列其中之一：

- 啓動監視程式程序：

  rewriter-proxy-install-root`/SUNWps/bin/rwproxd watchdog on`

  會在 crontab 中建立一個項目，而現在監視程式會啓動。監視程式會監視 Rewriter 代理伺服器並在效能降低時開啓代理伺服器。

- 手動啓動 Rewriter 代理伺服器：

  rewriter-proxy-install-root`/SUNWps/bin/rwproxd -n` *gateway-profile-name* `start`

  其中 *gateway-profile-name* 是對應到所需閘道實例的設定檔名稱。

➤ 若要配置 Rewriter 代理伺服器監視程式

您可以配置監視程式監視 Rewriter 代理伺服器狀態的時間間隔。時間間隔預設爲 60 秒。若要執行此步驟，在 crontab 中編輯下面的行：

```
0-59 * * * * rewriter-proxy-install-root/bin/checkgw /var/opt/SUNWps/.gw 5 >
/dev/null 2>&1
```

使用含有閘道的反向代理伺服器

代理伺服器會傳送網際網路內容至企業內部網路，而反向代理伺服器則傳送企業內部網路內容至網際網路。某些反向代理伺服器的部署會配置爲傳送網際網路內容以達成載入平衡與快取的效果。

若在閘道前面部署具有協力廠商反向代理伺服器，則回應必須以反向代理伺服器的 URL (非閘道的 URL) 重新寫入。因此需要下列配置。

➤ 若要啓用反向代理伺服器

1. 以根使用者身分登入並編輯所需閘道實例的 `platform.conf` 檔：

   `/etc/opt/SUNWps/platform.conf.`*gateway-profile-name*

2. 新增下列項目：

   `gateway.virtualhost=`*fully-qualified-gateway-host gateway-ip-address fully-qualified-reverse-proxyhost*

   `gateway.enable.customurl=true`（此值的預設值設定爲 false。）

   `gateway.httpurl=`*http reverse-proxy-URL*

   `gateway.httpsurl=`*https reverse-proxy-URL*

   `gateway.httpurl` 將用於覆寫在連接埠接收的回應，其中連接埠在閘道設定檔會列示爲 HTTP 連接埠。

   `gateway.httpsurl` 將用於覆寫在連接埠接收的回應，其中連接埠在閘道設定檔會列示爲 HTTPS 連接埠。

3. 重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

如果不指定此值，則閘道會預設回一般的運作方式。

取得用戶端資訊

當閘道轉寄用戶端請求到任何內部伺服器時，閘道會新增 HTTP 標頭到 HTTP 請求。您可以使用這些標頭以取得額外的用戶端資訊並偵測閘道的出現狀態。

若要檢視 HTTP 標頭，請設定 `platform.conf` 檔案的項目爲 `gateway.error=message`，然後使用 servlet API 中的 `request.getHeader()`。

第一欄列出標頭標籤，第二欄指定標頭的語法，第三欄則是標頭標籤的說明。

表 2-3 HTTP 標頭中的訊息

標頭	語法	說明
PS-GW-PDC	PS-GW-PDC:true/false	指出閘道上的 PDC 是否啟用。

表 2-3 HTTP 標頭中的訊息

標頭	語法	說明
PS-Netlet	PS-Netlet:enabled=true/false	指出閘道上的 Netlet 是否已經啟用或停用。 如果已經啟用，則加密選項會植入，指出閘道以 HTTPS (encryption=ssl) 或以 HTTP 模式 (encryption=plain) 執行。 例如： PS-Netlet:enabled=false Netlet 是停用的。 PS-Netlet:enabled=true; encryption=ssl Netlet 使用在 SSL 模式中執行的閘道啟用。 當 Netlet 沒有啟用時，encryption=ssl/plain 並不會植入。
PS-GW-URL	PS-GW-URL:http(s)://gatewayURL(:port)	指出用戶端要連接的 URL。 如果是非標準的連接埠 (也就是說，閘道在 HTTP/HTTPS 模式中且連接埠不是 80/443)，則該 「連接埠」也會被植入。
PS-GW-Rewriting-URL	PS-GW-URL:http(s)://gatewayURL(:port)/[SessionInfo]	指出閘道重新寫入所有頁面的 URL。 1. 當瀏覽器支援 cookie 時，此標頭的值會和 PS-GW-URL 標頭的值一樣。 2. 當瀏覽器不支援 cookies： • 並且如果目的地主機在 「轉寄 Cookie URL」清單中，則值是閘道重新寫入頁面 (含有編碼 SessionID 資訊) 到 URL 的 實際 URL。 • 或，如果目的地主機不在 「轉寄 Cookie URL」清單中，而 SessionInfo 字串是 "$SessionID" 注意：在回應部分，如果使用者的 Identity Server seeionID 變更 (如來自認證頁面的回應)，則會以該值重新寫入這些頁面 (此值並非是先前所指在標頭中的值)。 例如： • 如果瀏覽器支援 cookies： PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/ • 如果瀏覽器不支援 cookies 但是終端伺服器在 「轉寄 Cookie URL」清單中。 PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/SessIDValCustomEncodedValue/ • 如果瀏覽器不支援 cookies 但是終端伺服器不在 「轉寄 Cookie URL」清單中。 PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/$SessionID

表 2-3 HTTP 標頭中的訊息

標頭	語法	說明
PS-GW-CLientIP	PS-GW-CLientIP: *IP*	這是閘道從 recievedSocket.getInetAddress().getHostAddress() 所取得的 IP 如果直接連到閘道的話，會提供用戶端的 IP。 注意：由於有 JSS/NSS 錯誤，目前這部分不提供。

使用認證鏈接

在認證的一般機制上，認證鏈接提供較高的安全性。您可以讓使用者認證一個以上的認證機制。

此處的程序說明僅適用於與在閘道上的 PDC 認證同時啓用認證鏈接。關於在閘道上沒有 PDC 認證的認證鏈結，請參考 *Sun ONE Identity Server* 管理員指南。

例如，如果您取得 PDC、Unix 和 Radius 認證模組，使用者將必須認證這三個模組以存取入口網站桌面。

備註 如果 PDC 啓用的話，它永遠都是第一個顯示在使用者面前的認證模組。

➤ **新增認證模組到現有的 PDC 實例**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選擇組織。
3. 從「檢視」功能表中選取「服務」。

   此服務會顯示於左窗格中。
4. 按一下「認證配置」旁邊的箭頭。

   顯示「服務實例清單」。
5. 按一下 gatewaypdc。

   會顯示 Gatewaypdc 屬性頁面。
6. 按一下「認證配置」前面的「編輯」。

   會顯示「新增模組」。

7. 選擇「模組名稱」並設定「旗標」爲「需要」。選項會是空白的。
8. 按一下「確定」。
9. 新增一個或多個模組後按一下「儲存」。
10. 在 gatewaypdc 屬性頁面中按一下「儲存」。
11. 若要使變更生效，重新啓動閘道：

    gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

使用萬有字元證書

萬用字元證書接受含有萬用字元的單一證書，該證書必須位於擁有完全合格 DNS 名稱的主機中。

這允許證書在相同網域中維護多個主機的安全性。例如，*.domain.com 的證書可以用於 abc.domain.com 和 abc1.domain.com。事實上，此證書對於在 domain.com 網域中的任何主機都有效。

您需要在完全合格的主機名稱中指定一個 *。例如，如果完全合格的主機名稱是 abc.florizon.com，則將之指定爲 *.florizon.com。現在，產生的證書對所有在 florizon.com 網域中的所有主機名稱都有效。

停用瀏覽器快取

當閘道元件僅使用網路瀏覽器從任何地方提供安全存取到後端公司資料時，用戶端在本機不能快取可能是必需條件。

您可以修改指定閘道在 platform.conf 中檔案的屬性，以停用透過閘道快取重新導向的頁面。

停用此選項對閘道效能有影響。每次入口桌面更新時，閘道必須擷取每個參照到頁面的東西，例如先前瀏覽器已經快取過的影像。然而，啓用這個功能後，遠端存取安全的內容將不會在用戶端留下快取過的足跡。如果企業網路是從網路咖啡館或類似的遠端位置 (不是在企業 IT 的控制下)，這個功能會比效能關係更爲重要。

➤ **停用瀏覽器快取**

1. 以根使用者身分登入並編輯所需閘道實例的 platform.conf 檔：

   /etc/opt/SUNWps/platform.conf.*gateway-profile-name*

2. 編輯下面的行：

   `gateway.allow.client.caching=true`

   此值的預設值設定爲 `true`。變更此值爲 `false` 以停止瀏覽器在用戶端快取。

3. 重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

自訂閘道服務使用者介面

本節討論可以編輯的幾個屬性檔案。您可以在管理主控台上編輯閘道服務的標籤、錯誤訊息或記錄資訊的順序。如果您嘗試爲不同的本機自訂產品，這是非常有用的。

您可以自訂下列檔案：

portal-server-install-root`/SUNWam/locale/srapGatewayAdminConsole.properties`

portal-server-installl-dir`/SUNWps/locale/srapGateway.properties`

portal-server-install-root`/SUNWps/web-src/WEB-INF/classes/srapgwadminmsg.properties`

備註 如果您有不同的本機設定，您需要分別爲這些檔案儲存備份在個別的 `locale` 目錄。

srapGatewayAdminConsole.properties 檔案

編輯這個檔案，以變更出現在管理主控台上閘道服務的欄位名稱。

srapGateway.properties 檔案

編輯這個檔案以：

- 自訂在閘道執行時可能會出現的錯誤訊息。
  - HTML-CharSets=ISO-8859-1 指定用於建立此檔案的字元集。
  - 在大括號中的數字 (例如，{0}) 表示在執行期間會顯示的值。您可以變更和此數字有關的標籤，或視需要重新整理標籤。請確定標籤和將會顯示的訊息對應，因爲數字是和訊息有關聯的。
- 自訂記錄資訊。

在預設情況下，srapGateway.properties 檔案位於 *portal-server-install-root*/SUNWps/locale 目錄中。所有出現在閘道機器上的訊息 (閘道相關的訊息) 都記錄在此檔中，無論訊息的語言爲何。

如果您需要變更出現在用戶端入口桌面上訊息的語言，請將此檔案複製到個別的本機目錄中，例如 *portal-server-install-root*/SUNWps/locale_en_US。

srapgwadminmsg.properties 檔案

編輯這個檔案以：

- 自訂出現在管理主控台上閘道服務之按鈕的標籤。
- 自訂當您配置閘道時，會出現的狀態訊息和錯誤訊息。

使用聯合管理

聯合管理允許使用者聚集他們的本機識別，以使他們有一個網路識別。聯合管理使用網路識別以允許使用者登入服務提供者的網站，並且不需要重新認證他們的識別即可存取其他服務提供者的網站。這稱爲單次登入。

可以在 Portal Server 上以開啓模式和安全模式配置聯合管理。*Sun ONE Portal Server* 管理員指南說明如何在開啓模式下配置聯合管理。於安全模式中配置聯合管理之前，請使用安全遠端存取，以確定聯合管理可在開啓模式中運作。如果您想要您的使用者同時以開啓模式和安全模式在相同的瀏覽器中使用聯合管理，他們必須從瀏覽器清除 cookie 和快取。

請參閱 *Sun ONE Identity Server Customization and API Guide* 以瞭解有關聯合管理的詳細資訊。

聯合管理方案

使用者認證到一個初始的服務提供者。服務使用者是商業用途或是提供以網路爲主之服務的非營利組織。此廣泛的種類可以包括網際網路入口網站、運輸提供者、金融機構、娛樂事業公司、圖書館、大學和政府行政機構。

服務提供者可以使用 cookie 以儲存使用者在用戶端瀏覽器的階段作業資訊。Cookie 也包含使用者的識別提供者。

識別提供者是在提供認證服務中指定的服務提供者。做爲識別的管理服務，它們同時也維持並管理認證資訊。識別提供者所完成的認證，受到隸屬於它的所有伺服器提供者所認可。

當使用者程式存取不隸屬於該識別提供者的服務時，此識別提供者會將該 cookie 轉寄給獨立的服務提供者。此服務提供者之後便可存取在 cookie 中呼叫的識別提供者。

然而，無法在不同 DNS 的網域間讀取 cookie。因此使用 「共用網域 Cookie 服務」以重新導向服務提供者到正確的識別提供者，因此使用者就可以啓用單次登入。

配置聯合管理資源

聯合資源、服務提供者、識別提供者和共同網域 Cookie 服務 (CDCS) 在其所存在的閘道中設定檔中配置。這部分說明如何配置三個方案：

1. 當所有資源位在企業內部網路時。
2. 當所有資源沒有位於企業內部網路，或識別提供者位於網際網路。
3. 當所有資源沒有位於企業網路，或當企業提供者受到閘道保護，且識別提供者是協力廠商並位於網際網路。

配置 1

在此配置中，服務提供者、識別提供者和 「共用網域 Cookie 服務」都部署在相同的企業內部網路中，而識別提供者並未發佈到網際網路網域名稱伺服器 Domain Name Server (DNS) 中。CDCS 爲選填項目。

在此配置中，閘道指向服務提供者，也就是 Portal Server。此配置對 Portal Server 的多個實例都有效。

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取管理主控台中的 「服務配置」標籤。
3. 按一下 「SRA 配置」下 「閘道」旁的箭頭。

   將顯示 「閘道」頁。
4. 按一下您想要設定其屬性之 「閘道設定檔」旁邊的 「編輯 …」。

   便會顯示 「編輯閘道設定檔」頁面。
5. 按一下 「核心」標籤。
6. 選取 「啓用 Cookie 管理」核取方塊以啓用 cookie 管理。

7. 捲動至「Portal Server 清單」欄位並輸入 Portal Server 名稱，如此您可以使用相對 URL，像是列於「未認證 URL」清單中的 /amserver 或 /portal/dt。例如：

   `http://`*idp-host*`:`*port*`/amserver/js`

   `http://`*idp-host*`:`*port*`t/amserver/UI/Login`

   `http://`*idp-host*`:`*port*`/amserver/css`

   `http://`*idp-host*`:`*port*`/amserver/SingleSignOnService`

   `http://`*idp-host*`:`*port*`/amserver/UI/blank`

   `http://`*idp-host*`:`*port*`/amserver/postLogin`

   `http://`*idp-host*`:`*port*`/amserver/login_images`

8. 捲動到「Portal Server 清單」欄位並輸入 Portal Server 名稱。例如 /amserver。
9. 按一下「儲存」。
10. 按一下「安全性」標籤。
11. 捲動到「未認證 URL」清單並新增「聯合資源」。例如：

    `/amserver/config/federation`

    `/amserver/IntersiteTransferService`

    `/amserver/AssertionConsumerservice`

    `/amserver/fed_images`

    `/amserver/preLogin`

    `/portal/dt`

12. 按一下「新增」。
13. 按一下「儲存」。
14. 如果需要網路代理伺服器以連至在「未認證 URL」清單中的 URL，按一下「代理伺服器」標籤。
15. 捲動到「網域和子網域的代理伺服器」欄位並輸入所需的網路代理伺服器。
16. 按一下「新增」。
17. 按一下「儲存」。
18. 從終端機視窗中，重新啓動閘道：

gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

配置 2

在此配置中識別提供者、識別提供者和共同網域 Cookie 提供者 (CDCP) *沒有*部署於企業內部網路，或識別提供者是位於網際網路上的協力廠商。

在此配置中，閘道指向服務提供者，也就是 Portal Server。此配置對 Portal Server 的多個實例都有效。

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取管理主控台中的「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯 …」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 選取「啓用 Cookie 管理」核取方塊以啓用 cookie 管理。
7. 捲動至「Portal Server 清單」欄位並輸入服務提供者 Portal Server 名稱，如此您可以使用相對 URL，像是列於「未認證 URL」清單中的 /amserver 或 /portal/dt。

   http://*idp-host:port*/amserver/js

   http://*idp-host:port*/amserver/UI/Login

   http://*idp-host:port*/amserver/css

   http://*idp-host:port*/amserver/SingleSignOnService

   http://*idp-host:port*/amserver/UI/blank

   http://*idp-host:port*/amserver/postLogin

   http://*idp-host:port*/amserver/login_images
8. 按一下「儲存」。
9. 按一下「安全性」標籤。

10. 捲動到「未認證 URL」清單並新增「聯合資源」。例如：

    ```
    /amserver/config/federation
    ```

    ```
    /amserver/IntersiteTransferService
    ```

    ```
    /amserver/AssertionConsumerservice
    ```

    ```
    /amserver/fed_images
    ```

    ```
    /amserver/preLogin
    ```

    ```
    /portal/dt
    ```

11. 按一下「新增」。
12. 按一下「儲存」。
13. 如果需要網路代理伺服器以連至在「未認證 URL」清單中的 URL，按一下「代理伺服器」標籤。
14. 捲動到「網域和子網域的代理伺服器」欄位並輸入所需的網路代理伺服器。
15. 按一下「新增」。
16. 按一下「儲存」。
17. 從終端機視窗中，重新啓動閘道：

    gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

配置 3

在此配置中識別提供者、識別提供者和共同網域 Cookie 提供者 (CDCP) *沒有*部署於企業內部網路，或服務提供者是位於網際網路上的協力廠商，且識別提供者受到閘道保護。

在此配置中，閘道指向識別提供者，也就是 Portal Server。

此配置對 Portal Server 的多個實例都有效。此配置在網路上是不太可能發生的，然而，一些企業網路在其企業內部網路可能會有這樣的配置，也就是說，識別提供者可能位於由防火牆保護的子網路中，而伺服器提供者可以在企業網路中直接存取。

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取管理主控台中的「服務配置」標籤。
3. 按一下「SRA 組態」下「閘道」旁的箭頭。

   將顯示「閘道」頁。

4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯 …」。

   便會顯示「編輯閘道設定檔」頁面。

5. 按一下「核心」標籤。

6. 選取「啓用 Cookie 管理」核取方塊以啓用 cookie 管理。

7. 捲動至「Portal Server 清單」欄位並輸入識別提供者 Portal Server，如此您可以使用相對 URL，像是列於「未認證 URL」清單中的 /amserver 或 /portal/dt。

   `http://`*idp-host*`:`*port*`/amserver/js`

   `http://`*idp-host*`:`*port*`/amserver/UI/Login`

   `http://`*idp-host*`:`*port*`/amserver/css`

   `http://`*idp-host*`:`*port*`/amserver/SingleSignOnService`

   `http://`*idp-host*`:`*port*`/amserver/UI/blank`

   `http://`*idp-host*`:`*port*`/amserver/postLogin`

   `http://`*idp-host*`:`*port*`/amserver/login_images`

8. 按一下「儲存」。

9. 按一下「安全性」標籤。

10. 捲動到「未認證 URL」清單並新增「聯合資源」。例如：

    `/amserver/config/federation`

    `/amserver/IntersiteTransferService`

    `/amserver/AssertionConsumerservice`

    `/amserver/fed_images`

    `/amserver/preLogin`

    `/portal/dt`

11. 按一下「新增」。

12. 按一下「儲存」。

13. 如果需要網路代理伺服器以連至在「未認證 URL」清單中的 URL，按一下「代理伺服器」標籤。

14. 捲動到「網域和子網域的代理伺服器」欄位並輸入所需的網路代理伺服器。

15. 按一下「新增」。

16. 按一下「儲存」。
17. 從終端機視窗中，重新啓動閘道：

    gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

第 3 章

Rewriter

本章說明如何定義 Rewriter 規則，以及如何在 Sun™ ONEPortal Server 管理主控台中配置 Rewriter。

其中涵蓋下列主題：

Rewriter 摘要

Secure Remote Access 的 Rewriter 元件允許一般使用者利用修改網頁上的單一資源指示碼 (Uniform Resource Identifier，URI) 參照，以指向「閘道」從而瀏覽內部網路。URI 可定義於任何已註冊名稱空間內封裝名稱的方法，並以該名稱空間爲其加標記。最常見的 URI 種類爲單一資源定址器 (URL)。URL 可具備如 http、ftp、mailto、file 及 news 等多種通訊協定。

所有的標準 URL，如 RFC-1738 所指定且及通訊協定爲 HTTP 或 HTTPS，皆由 Rewriter 識別與改寫。通訊協定不區分大小寫。例如 hTtP、HTtp 與 httP 皆爲有效的格式。以下列出一些 URL 範例：

`http://www.my.work.com/`

`http://www.w3.org:8000/imaginary/test`

`http://www.myu.edu/org/admin/people#andy`

`http://info.my.org/AboutUs/Index/Phonebook?dobbins`

`http://www.w3.org/RDB/EMP?where%20name%3Ddobbins`

`http://info.my.org/AboutUs/Phonebook`

`http://user:password@abc.com`

Rewriter 可改寫部分由 Internet Explore 與 Netscape 所支援的基本非標準 URL。將非標準 URL 轉換爲標準格式所需的資訊，會從顯示 URL 的頁面的基準 URL 擷取。此資訊可包括：

- 通訊協定
- 主機名稱
- 連接埠
- 路徑

Rewriter 僅支援相對 URL 中包含反斜線符號。

例如，

`http://abc.sesta.com\index.html` 會被改寫，

下列 URL 不會被改寫：

`http:\\abc.sesta.com`。

`http:/abc.com`

Rewriter 使用方案

使用者試圖經由「閘道」存取內部網路網頁時，即可使用 Rewriter 來順利存取網頁。下列元件會使用 Rewriter：

- URLScraper
- 閘道

URLScraper

URL Scraper 提供者會從已配置的 URI 中取得內容，並在將內容傳送至瀏覽器之前，將所有相對 URI 擴展至絕對 URI。

例如，若使用者試圖存取含有下列內容的網站：

```
<a href="../mypage.html">
```

Rewriter 會將此轉譯爲：

```
<a href="http://yahoo.com/mypage.html">
```

其中 `http://yahoo.com/test/` 是網頁的基準 URL。

有關 URLScraper 提供者的詳細資訊，請參閱 *Sun ONE Portal Server* 管理員指南。

閘道

「閘道」會從網際網路入口網站取得內容，並在將內容傳送至瀏覽器之前，將「閘道」URI 前置於現有 URI，如此來自瀏覽器的後續 URI 要求便可到達閘道。

例如，使用者試圖存取包含下列內容的網際網路機器上的 HTML 網頁：

```
<a href="http://mymachine.intranet.com/mypage.html>"
```

Rewriter 會使用參照前置這個 URL 至閘道，如下所示：

```
<a href="https://gateway.company.com/http://mymachine.intranet.com/
mypage.html>"
```

使用者點選與此控點相關的連結時，瀏覽器便會聯絡閘道。閘道會從 `mymachine.intranet.com` 取得 `mypage.html` 的內容。

閘道使用多種規則來判定是否需改寫取得網頁中的元素。

撰寫規則集

您可在「服務配置」標籤下的「Portal Server 配置」子區段定義規則集。

有關定義規則集的詳細資訊，請參閱 *Sun ONE Portal Server* 管理員指南。建立新規則集後，您必須定義所需規則。

本節涵蓋下列主題：

公開介面 (規則集 DTD)

```
<?xml version="1.0" encoding="UTF-8"?>

<!--

    The following constraints are not represented in DTD, but taken care
programatically

    1. In a Rule, All Mandatory attributes cannot be "*".

    2. Only one instance of the below elements is allowed, but in any order.

    1)HTMLRules

    2)JSRules

    3)XMLRules

    3. ID should alway be in lower case.

-->
```

```
<!ENTITY % eURL 'URL'>
<!ENTITY % eEXPRESSION 'EXPRESSION'>
<!ENTITY % eDHTML 'DHTML'>
<!ENTITY % eDJS 'DJS'>
<!ENTITY % eSYSTEM 'SYSTEM'>

<!ENTITY % ruleSetElements '(HTMLRules | JSRules | XMLRules)?'>
<!ENTITY % htmlElements '(Form | Applet | Attribute)*'>
<!ENTITY % jsElements '(Variable | Function)*'>
<!ENTITY % xmlElements '(Attribute | TagText)*'>

<!ELEMENT RuleSet (%ruleSetElements;,%ruleSetElements;,%ruleSetElements;)>
<!ATTLIST RuleSet
    id ID #REQUIRED
    extends CDATA "none"
>

<!-- Rules for identifying rules in HTML content -->
<!ELEMENT HTMLRules (%htmlElements;)>
<!ELEMENT Form EMPTY>
<!ATTLIST Form
    name CDATA #REQUIRED
    field CDATA #REQUIRED
    valuePatterns CDATA ""
    source CDATA "*"
>

<!ELEMENT Applet EMPTY>
<!ATTLIST Applet
    code CDATA #REQUIRED
```

```
    param CDATA "*"
    valuePatterns CDATA ""
    source CDATA "*"
>

<!-- Rules for identifying rules in JS content -->
<!ELEMENT JSRules (%jsElements;)>
<!ELEMENT Variable EMPTY>
<!ATTLIST Variable
    name CDATA #REQUIRED
    type (%eURL; | %eEXPRESSION; | %eDHTML; | %eDJS; | %eSYSTEM;)
"EXPRESSION"
    source CDATA "*"
>

<!ELEMENT Function EMPTY>
<!ATTLIST Function
    name CDATA #REQUIRED
    paramPatterns CDATA #REQUIRED
    type (%eURL; | %eEXPRESSION; | %eDHTML; | %eDJS;) "EXPRESSION"
    source CDATA "*"
>

<!-- Rules for identifying rules in XML content -->
<!ELEMENT XMLRules (%xmlElements;)>
<!ELEMENT TagText EMPTY>
<!ATTLIST TagText
    tag CDATA #REQUIRED
    attributePatterns CDATA ""
    source CDATA "*"
```

```
>


<!ELEMENT Attribute EMPTY>
<!ATTLIST Attribute
    name CDATA #REQUIRED
    tag CDATA "*"
    valuePatterns CDATA ""
    type (%eURL; | %eDHTML; | %eDJS; ) "URL"
    source CDATA "*"
>
```

備註 您可以使用 * 作爲規則值的一部分。但是所有強制屬性值不能僅以 * 表示。會忽略這類規則，但是訊息會記錄在 RuleSetInfo 日誌檔中。有關此日誌檔的資訊，請參閱第 122 頁「除錯檔案名稱」。

XML DTD 範例

本節包含一範例規則集。我們使用「案例研究」(第 140 頁)來說明 Rewriter 解譯這些規則的方式。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Rules for integrating a mail client with the gateway.
-->
<!DOCTYPE RuleSet SYSTEM "jar://rewriter.jar/resources/RuleSet.dtd">
<RuleSet type="GROUPED" id="owa">
<HTMLRules>
    <Attribute name="action"/>
    <Attribute name="background" />
    <Attribute name="codebase" />
    <Attribute name="href"/>
    <Attribute name="src" />
```

```
    <Attribute name="lowsrc" />
    <Attribute name="imagePath" />
    <Attribute name="viewClass" />
    <Attribute name="emptyURL" />
    <Attribute name="draftsURL" />
    <Attribute name="folderURL" />
    <Attribute name="prevMonthImage" />
    <Attribute name="nextMonthImage" />
    <Attribute name="style" />
    <Attribute name="content" tag="meta" />
</HTMLRules>
<JSRules>
<!-- Rules for Rewriting JavaScript variables in URLs -->
    <Variable name="URL"> _fr.location </Variable>
    <Variable name="URL"> g_szUserBase </Variable>
    <Variable name="URL"> g_szPublicFolderUrl </Variable>
    <Variable name="URL"> g_szExWebDir </Variable>
    <Variable name="URL"> g_szViewClassURL </Variable>
    <Variable name="URL"> g_szVirtualRoot </Variable>
    <Variable name="URL"> g_szBaseURL </Variable>
    <Variable name="URL"> g_szURL </Variable>
    <Function name="EXPRESSION" name="NavigateTo" paramPatterns="y"/>
</JSRules>
<XMLRules>
    <Attribute name="xmlns"/>
    <Attribute name="href" tag="a"/>
    <TagText tag="baseroot" />
    <TagText tag="prop2" />
    <TagText tag="prop1" />
    <TagText tag="img" />
```

```
    <TagText tag="xsl:attribute"
    attributePatterns="name=src" />
</XMLRules>
</RuleSet>
```

撰寫規則的步驟

您可遵照下列的一般步驟來撰寫規則。

- 識別出含有需改寫內容之 HTML 網頁的目錄。
- 在這些目錄中，識別出需要改寫的網頁。
- 識別出各網頁上需改寫的 URL。識別出多數 URL 的簡易方法就是搜尋 "http" 與 "/"。
- 識別出 URL 的內容類型 - HTML、JavaScript 或 XML。
- 在 Identity Server 管理主控台「Portal Server 配置」下的「Rewriter」服務中編輯需要的規則集，以撰寫改寫各個 URL 所需的規則。
- 將所有規則合併到該網域的規則集中。

規則集指導方針

請牢記下列事項：

- 規則集中的規則會依順序套用至網頁中的所有陳述式，直到有一個規則與特定陳述式匹配。

  撰寫規則時，請牢記規則的順序。規則會以出現在規則集中的順序，套用至網頁中的陳述式。若您有特定規則，及包含 "*" 的一般規則，請先定義該特定規則，然後再定義一般規則。否則，在套用特定規則之前就會先套用一般規則至所有陳述式

- 所有的規則都必須包含在 `<RuleSet> </RuleSet>` 標記內。
- 將所有需改寫 HTML 內容的規則納入規則集的 `<HTMLRules> </HTMLRules>` 區段。
- 將所有需改寫 JavaScript 內容的規則納入規則集的 `<JSRules> </JSRules>` 區段。
- 將所有需改寫 XML 內容的規則納入規則集的 `<XMLRules> </XMLRules>` 區段。

- 請在您的內部網路網頁中，識別出需改寫的 URL，然後將所需規則納入規則集的相應區段 (HTML、JSRules 或 XMLRules)。
- 將規則集指派至所需網域。有關詳細資料，請參閱第 251 頁「建立 URI 與規則集對映清單」。
- 重新啓動「閘道」以使變更產生作用：

  gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

定義規則集根元素

規則集根具有兩種屬性：

- `RuleSetName`。例如，`default_ruleset`。在「規則集至 URI 對應」中將參照此名稱。
- `Extends`。此屬性指的是規則集的繼承特性。Extends 值會指向您欲從中導出一個規則集的規則集。

  使用 extends 值 `none` 以表示此新、獨立的規則集不依附於任何其他的規則集，或將您的規則集名稱指定爲 *RuleSetName* 以表示您的規則集依附於其他規則集。

定義以語言爲基礎的規則（定義規則）

規則以下列語言爲基礎：

- HTML
- JavaScript
- XML

用於 HTML 內容的規則

可進一步將網頁上的 HTML 內容分類爲屬性、表單或 Applet。同樣地，HTML 內容的規則可分類爲：

- HTML 內容的屬性規則
- 用於 HTML 內容的表單規則
- 用於 HTML 內容的 Applet 規則

HTML 內容的屬性規則

此規則可識別需改寫值的標籤屬性。屬性值可爲簡單的 URL、JavaScript 或 DHTML 內容。例如

- "img" 標籤的 src 屬性指向影像位置 (簡單 URL)
- href 屬性的 onClick 屬性處理按一下連結時的動作 (DJS)

本節分爲下列部分：

- 屬性規則語法
- 屬性規則範例
- DJS 屬性範例

屬性規則語法

```
<Attribute name="attributeName" [tag="*" valuePatterns="" source="*"
type="URL|DHTML|DJS"]/>
```

其中，

`attributeName` 爲屬性名稱 (必須的)

`tag` 是屬性所屬的標籤 (可選、預設 * 表示任何標籤)

`valuePatterns` 請參閱第 93 頁「在規則中使用式樣匹配」。

`source` 指出定義此屬性的頁面的 URI (可選、預設 * 表示在任何網頁中)

`type` 指出值的類型 (可選)。類型可能是：

`URL` - 簡單 URL (預設值)。

`DHMTL` - DHTML 內容。此類內容可見於標準 HTML 內容。此類內容用於 Microsoft 的 HTC 格式檔案。

`DJS` - JavaScript 內容。所有 HTML 事件處理器，如 onClick 與 onMouseover，其 JavaScript 皆含有 HTML 屬性。

屬性規則範例

假設此網頁的基準 URL 是：

```
http://mymachine.intranet.com/mypage.html
```

網頁內容

```
<a href="http://mymachine.intranet.com/mypage.html>
```

規則

```
<Attribute name="href"/>
```

or

```
<Attribute name="href" tag="a"/>
```

輸出

```
<a href=gateway-URL/http://mymachine.intranet.com/myhome.html>
```

說明

因爲待改寫的 URL 已經是一個絕對 URL，因此只會將閘道 URL 前置於此 URL。

DJS 屬性範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/focus.html
```

網頁內容

```
<Form>
<input TYPE=TEXT SIZE=20 value=focus
onClick="Check('/focus.html','focus');return;">
</Form>
```

規則

```
<Attribute name=”onClick” type=”DJS”/>
<Function type="URL" name="Check" paramPatterns="y,"/>
```

輸出

```
<Form>
<INPUT TYPE=TEXT SIZE=20 value=focus
onClick="Check('gateway-URL/http://abc.sesta.com/focus.html','focus');return
;">
</Form>
```

說明

改寫特定網頁內容需要兩個規則。第一個規則可識別 onClick JavaScript 記號。第二個規則可識別需改寫的 check 函數參數。在這種情況下，僅會改寫第一個參數，因爲 paramPatterns 在第一個參數位置有值爲 y。

出現 JavaScript 記號的閘道 URL 與網頁的基準 URL 會置於所需參數之前。

用於 HTML 內容的表單規則

使用者所瀏覽的 HTML 網頁可能包含表單。某些表單元素可能會將 URL 視爲值。

本節分爲下列部分：

- 表單規則語法
- 表單規則範例

表單規則語法

```
<Form name="form1" field="visit" [valuePatterns="" source="*"]/>
```

其中

`name` 爲表單名稱 (必須的)

`field` 是表單中的欄位，其中具有需改寫的值 (必須的)

`valuePatterns` 請參閱第 93 頁 「在規則中使用式樣匹配」

`source` 是 html 網頁的 URL，即呈現此表單定義之處 (可選、預設 * 表示在任何網頁中)

表單規則範例

假設此網頁的基準 URL 是：

```
http://test.siroe.com/testcases/html/form.html
```

網頁內容

假設網頁的 URI 是 `form.html` 且位於伺服器的根目錄中。

```
<form name=form1  method=POST
action="http://test.siroe.com/testcases/html/form.html">

<input type=hidden name=abc1 value="0|1234|/test.html">

</form>
```

若要改寫出現在名爲 `abc1` (`form1` 的一部分) 隱藏欄位值中的 `/text.html`，即需要下列規則。

規則

```
<Form source="*/form.html" name="form1" field="abc1"
valuePatterns="0|1234|"/>

<Attribute name="action"/>
```

輸出

```
<FORM name=”form1” method=”POST”
action="gateway-URL/http://test.siroe.com/testcases/html/form.html">

<input type=hidden name=abc1
value="0|1234|gateway-URL/http://test.siroe.com/test.html">

</FORM>
```

說明

`action` 標籤是使用某些已定義之 HTML 屬性規則所改寫的。

輸出標籤屬性值的 `value` 的改寫方式如下列輸出中所示。已找出特定的 `valuePatterns`，然後即利用前置閘道 URL 及網頁的基準 URL 的改寫符合 `valuePatterns` 後面的所有內容。請參閱第 93 頁 「在規則中使用式樣匹配」。

用於 HTML 內容的 Applet 規則

單一網頁可以包含許多 Applet，而每個 Applet 則可以包含許多參數。Rewriter 會利用 Applet 的 HTML 定義與規則中指定的值匹配，然後修改作爲 Applet 參數定義一部分呈現的 URL 值。此取代動作會在伺服器上進行，而非在使用者瀏覽特定網頁時進行。此規則可識別並改寫 HTML 內容中的 Applet 及物件標籤的參數。

本節分爲下列部分：

- Applet 規則語法
- Applet 規則範例

Applet 規則語法

```
<Applet code="ApplicationClassName/ObjectID" param="parametername" [valuePatterns=""
source="*"] />
```

其中

`code` 是 Applet 或物件類別的名稱 (必須的)

`param` 是參數名稱，其中具有需改寫的值 (必須的)

`valuePatterns` 請參閱第 93 頁 「在規則中使用式樣匹配」。

`source` 是包含 Applet 定義的網頁的 URL (可選，預設爲 * 表示在任何網頁中)

Applet 規則範例

假設此網頁的基準 URL 是：

```
http://abc.siroe.com/casestudy/test/HTML/applet/rule1.html
```

網頁內容

```
<applet codebase=”appletcode” code=”RewriteURLinApplet.class”
archive=”/test.jar”>

<param name=Test1 value="/index.html">

</applet>
```

規則

```
<Applet source="*/rule1.html" code="RewriteURLin*.class" param="Test*"/>
```

輸出

```
<APPLET
codebase=”gateway-URL/http://abc.siroe.com/casestudy/test/HTML/applet/applet
code” code=”RewriteURLinApplet.class” archive=”/test.jar”>

<param name=”Test1” value="gateway-URL/http://abc.siroe.com/index.html">

</APPLET>
```

說明

將改寫 `codebase attribute` ，因爲 `<Attribute name="codebase"/>` 是 `default_gateway_ruleset` 中已定義的規則。

所有以 `Test` 開頭的參數都會被改寫。顯示 Applet 碼的網頁基準 URL 及閘道 URL 都會置於 `params` 標籤，`value` 屬性之前。

在規則中使用式樣匹配

您可以使用 valuePatterns 欄位來達成式樣匹配的目標，並識別需改寫之陳述式的特定部分。

若您指定 `valuePatterns` 作爲規則的一部分，則會改寫所有位於符合之樣式後的內容。

請參考下列表單規則範例。

```
<Form source="*/source.html" name="form1" field="visit" [valuePatterns="0|1234|"]/>
```

其中

`source` 是顯示表單之 Html 網頁的 URL

`name` 爲表單名稱

`field` 是表單中的欄位，其中具有需改寫的值

valuePatterns 指出需改寫的字串部分。會改寫所有出現在 valuePatterns 之後的內容（可選、預設 "" 表示需改寫 fullvalue）。請參閱第 93 頁「在規則中使用式樣匹配」。

在 valuePatterns 中使用萬用字元

您可使用 * 字元來完成用於改寫的式樣匹配。

在 valuePatterns 欄位中，您不能僅指定一個 *。因爲 * 表示與所有項目匹配，valuePattern 後將不會有任何項目，因此 Rewriter 也就沒有可改寫的項目。您可利用其他字串與 * 連用，如 *abc。在這種情況下，即會改寫所有位於 *abc 之後的內容。

備註 規則中的任何欄位皆可使用萬用字元星號 (*)。但是規則中所有的欄位不能都包含 *。若所有欄位皆包含 *，則會忽略此規則。不會顯示錯誤訊息。

您可以利用 * 或 ** 與顯示在原始陳述式中的分隔字元連用，以分隔多個欄位。一個萬用字元 (*) 會與不需改寫的所有欄位匹配，而兩個萬用字元 (**) 則會與需改寫的所有欄位匹配。

表 3-1 列出 * 萬用字元的部分範例使用方法。此表格具有三欄。第一個欄列出待改寫的範例陳述式。第二欄列出範例 valuePatterns 值。第三欄說明如何改寫。

表 3-1 * 萬用字元的使用範例

URL	valuePatterns	說明
url1, url2, url3, url4	valuePatterns = "**, *, **, *"	在這種情況下，會改寫 url1 與 url3，因為 ** 會指出待改寫的部分
XYZABChttp://host1.sesta.com/dir1.html	valuePatterns = "*ABC"	在這種情況下，僅會改寫 http://host1.sesta.com/dir1.html 部分。所有位於 *ABC 之後的項目皆需改寫。
"0|dir1|dir2|dir3|dir4|test|url1	valuePatterns = "*|*|**|*|**|*|"	在這種情況下，會改寫 dir2、dir4 與 url1。需改寫的最後一個欄位不須以 ** 表示。

用於 JavaScript 內容的規則

JavaScript 可在多個位置包含 URL。Rewriter 無法直接剖析 JavaScript 與確定 URL 部分。必須撰寫特定規則集以協助 JavaScript 處理器識別及轉譯 URL。

具有 URL 類型的 JavaScript 元素分類如下：

- 變數
- 函數引數

變數

通用語法

<Variable name="*variableName*"
[type="URL | EXPRESSION | DHTML | DJS | SYSTEM" source="*"]>

視其所持有的值類型而定，JavaScript 變數可細分爲 5 種：

- URL 變數
- EXPRESSION 變數
- DHTML (動態 HTML) 變數
- DJS (動態 JavaScript) 變數
- SYSTEM 變數

URL 變數

變數值是一個可視爲 URL 的簡單字串。

本節分爲下列部分：

- URL 變數語法
- URL 變數範例

URL 變數語法

```
<Variable name="variableName" type="URL" [source="*"]>
```

其中

`variableName` 爲變數名稱。將會改寫 `variableName` 的值 (必須的)。

`type` 爲 URL 變數 (必須的，且值必須爲 URL)

`source` 是此 JavaScript 變數所在的網頁的 URI (可選，預設爲 * 表示在任何網頁中)

URL 變數範例

假設基準 URL 是：

```
http://abc.siroe.com/tmp/page.html
```

網頁內容

```
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc1="/tmp/tmp.jpg";
var imgsrc2="http://srap.sesta.com/tmp/tmp.jpg";
var imgsrc3=imgsrc2;
//-->
</SCRIPT>
```

規則

```
<Variable name=”imgsrc*” type="URL"/>
```

輸出

```
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc="gateway-URL/http://abc.siroe.com/tmp/tmp.jpg";
var imgsrc="gateway-URL/http://srap.sesta.com/tmp/tmp.jpg";
var imgsrc2=imgsrc1;
//-->
</SCRIPT>
```

說明

所有 URL 類型的變數及名稱以 `imgsrc` 開頭的變數皆會被改寫。在輸出的第一行，會前置顯示變數的閘道 URL 與網頁 URL。第二行已包含絕對路徑，因此僅會前置閘道 URL。第三行 var imagsrc2 將不會被改寫，因爲其值並非字串，而是另一個 JavaScript 值。

EXPRESSION 變數

表示式變數的右側會有一個表示式。此表示式會產生一個 URL。Rewriter 會將 JavaScript 函數 (psSRAPRewriter_convert_expression) 附加至 HTML 網頁，因爲其無法在伺服器上計算這類表示式的值。此函數會將表示式視爲參數，並在用戶端瀏覽器中計算所需 URL 值。

若您不確定陳述式包含的是簡單 URL 或 EXPRESSION URL，我們建議您使用表示式規則，因爲其可處理兩種情況。

本節分爲下列部分：

- EXPRESSION 變數語法
- EXPRESSION 變數範例

EXPRESSION 變數語法

```
<Variable name=”variableName” [type="EXPRESSION" source=”*”]/>
```

其中

`variableName` 是 JavaScript 變數的名稱，其值爲一表示式 (必須的)

`type` 是 JavaScript 變數的類型 (可選，預設值爲 EXPRESSION)

`source` 是網頁的 URI (可選，預設爲 * 表示任何來源)

EXPRESSION 變數範例

假設此網頁的基準 URL 是：

```
http://abc.siroe.com/dir1/dir2/page.html
```

網頁內容

```
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar= getURIPreFix() + "../../images/graphics"+".gif";
document.write("<A HREF="+expvar+">Link to XYZ content</A><P>")
var expvar="../../images/graphics"+".gif";
//-->
</SCRIPT>
```

規則

```
<Variable name="expvar" type="EXPRESSION"/>
```

or

```
<Variable name="expvar"/>
```

輸出

```
var expvar=psSRAPRewriter_convert_expression(getURIPreFix() +
"../../images/graphics"+".gif");

document.write("<a href="+expvar+">>Link to XYZ content</A><P>")

var expvar="gateway-URL/http://abc.siroe.com/images/graphics"+".gif";
```

說明

psSRAPRewriter_convert_expression 函數會前置於第一行表示式變數 expvar 之前。此函數可處理表示式，並於執行時間在瀏覽器端改寫內容。在第三行中，此值將被作爲簡單 URL 改寫。

DHTML (動態 HTML) 變數

這些是含有 HTML 內容的 JavaScript 變數。

本節分爲下列部分：

- DHTML 語法
- DHTML 範例

DHTML 語法

```
<Variable name="variableName" type="DHTML" [source="*"]/>
```

其中

variableName 是含有 DHTML 內容的 JavaScript 變數的名稱 (必須的)

type 是變數的類型 (必須的，此值必須爲 DHTML)

source 是網頁的 URL (可選，預設爲 * 表示在任何網頁中)

DHTML 範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/graphics/set1/graphics/jsscript/JSVAR/page.html
```

網頁內容

```
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a href=../../images/test.html>"
var dhtmlVar="<a href=/images/test.html>"
var dhtmlVar="<a href=images/test.html>"
//-->
</SCRIPT>
```

規則

```
<Variable name=”dhtmlVar” type="DHTML"/>
<Attribute name="href"/>
or
<Attribute name="href" tag="a"/>
```

輸出

```
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a
href=gateway-URL/http://abc.sesta.com/graphics/set1/graphics/images/test.html>"
var dhtmlVar="<a href=gateway-URL/http://abc.sesta.com/images/test.html>"
var dhtmlVar="<a
href=gateway-URL/http://abc.sesta.com/graphics/set1/graphics/jscript/JSVAR/images/test.html>"
//-->
</SCRIPT>
```

說明

JavaScript 剖析器會讀取 dhtmlVar 的值，以作爲 HTML 內容，並經由 HTML 剖析器傳送內容。HTML 剖析器會套用符合 href 屬性規則的 HTML 規則，並改寫。

DJS（動態 JavaScript）變數

這些是含有 JavaScript 內容的 JavaScript 變數。

本節分爲下列部分：

- DJS 語法
- DJS 範例

DJS 語法

```
<Variable name=”variableName” type="DJS" [source=”*”]/>
```

其中

`variable` 是 JavaScript 變數，其值爲 javascript。

DJS 範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/dir1/dir2/dir3/jscript/dir4/page.html
```

網頁內容

```
//DJS Var

var dJSVar="var dJSimgsrc='/tmp/tmp.jpg';"

var dJSVar="var dJSimgsrc='../tmp/tmp.jpg';"

var dJSVar="var dJSimgsrc='http://abc.sesta.com/tmp/tmp.jpg';"
```

規則

```
<Variable name="DJS">dJSVar/>

<Variable name="URL">dJSimgsrc/>
```

輸出

```
//DJS Var - need 2 rules

var dJSVar="var dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp.jpg';"

var dJSVar="var
dJSimgsrc='gateway-URL/http://abc.sesta.com/dir1/dir2/dir3/jscript/tmp/tmp.jp
g';"

var dJSVar="var dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp.jpg';"
```

說明

此處必須使用兩個規則。第一個規則可找到動態 JavaScript 變數 dJSVar。此變數的值仍然是一種 URL 類型的 JavaScript。套用第二個規則來改寫此 JavaScript 變數的值。

SYSTEM 變數

這些是尚未告知使用者的變數，但是可作爲 JavaScript 標準的一部分獲取。例如，window.location.pathname。這些變數的支援有限。

本節分爲下列部分：

- SYSTEM 變數語法
- SYSTEM 變數範例

SYSTEM 變數語法

```
<Variable name=”variableName” type="SYSTEM" [source=”*”]/>
```

其中

variableName 是 JavaScript 系統變數 (必須的，且可能作爲匹配下列式樣的值：document.URL、document.domain、location、doument.location、location.pathname、location.href、location.protocol、location.hostname、location.host 與 location.port。此樣式皆在 generic_ruleset 中。請勿修改這些系統變數值。

type 表示這些值是系統類型 (必須的，且值爲 DJS)

source 是此網頁的 URI (可選，預設值爲 * 表示在任何網頁中)

SYSTEM 變數範例

假設此網頁的基準 URL 是：

```
http://abc.siroe.com/dir1/page.html
```

網頁內容

```
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(window.location.pathname);
//-->
</SCRIPT>
```

規則

```
<Variable name=”window.location.pathname” type="SYSTEM"/>
```

輸出

```
</SCRIPT>

<SCRIPT LANGUAGE="Javascript">

<!--

//SYSTEM Var

alert(psSRAPRewriter_convert_pathname(window.location.pathname));

//-->

</SCRIPT>
```

說明

Rewriter 會找出匹配規則的系統變數，然後前置 `psSRAPRewriter_convert_system` 函數。此函數可在執行時間中處理系統變數，然後相應改寫結果 URL。

函數引數

需改寫其值的函數參數可分爲 4 類：

- URL 參數
- EXPRESSION 參數
- DHTML 參數
- DJS 參數

通用語法

```
<Function name="functionName" paramPatterns="y,y,"
[type="URL|EXPRESSION|DHTML|DJS" source=”*”]/>
```

其中

`name` 是 JavaScript 函數的名稱 (必須的)

`paramPatterns` 指出需改寫的參數 (必須的)

y y 的位置會指出需改寫的參數。例如，在此語法中，需要改寫第一個參數，但第二個參數則不應改寫。

`type` 指出此參數所需的值種類 (可選，預設爲 EXPRESSION 類型)

source 網頁源 URI (可選，預設爲 * 表示在任何網頁中)

URL 參數

函數會將參數視爲字串，而此字串則可視爲 URL。

本節分爲下列部分：

- URL 參數語法
- URL 參數範例

URL 參數語法

```
<Function name="functionName" paramPatterns="y,," type="URL" [source=”*”]/>
```

其中

name 是含有 URL 類型參數的函數名稱 (必須的)

paramPatterns 指出需改寫的參數 (必須的)

y y 的位置會指出需改寫的參數。例如，在此語法中，需要改寫第一個參數，但第二個參數則不應改寫。

type 是函數的類型 (必須的，此值必須爲 URL)

source 是具有此函數呼叫之網頁的 URL (可選，預設爲 * 表示在任何 URL 中)

URL 參數範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/test/rewriter/test1/jscript/test2/page.html
```

網頁內容

```
<script language="JavaScript">
<!--
function test(one,two,three) {
alert(one + "##" + two + "##" +three);
}
test("/test.html","../test.html","123");
window.open("/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
```

規則

```
<Function name="URL" name="test" paramPatterns="y,y,"/>
```

```
<Function name="URL" name="window.open" paramPatterns="y,,,"/>
```

輸出

```
<SCRIPT language="JavaScript">
<!--
function test(one,two,three) {
alert(one + "##" + two + "##" +three);
}
test("gateway-URL/http://abc.sesta.com/test.html","gateway-URL/http://abc.sesta.com/test/rewriter/test1/jscript/test.html","123");
window.open("gateway-URL/http://abc.sesta.com/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
```

說明

第一個規則指出：名稱爲 test 的函數中前兩個參數需要改寫。因此，即會改寫 test 函數的前兩個參數。第二個規則指出：window.open 函數的第一個參數需要改寫。window.open 函數中的 URL 會以含有函數參數的網頁的閘道 URL 及基準 URL 前置。

EXPRESSION 參數

這些參數採用表示式值，即 URL 中的計算結果。

本節分爲下列部分：

- EXPRESSION 參數語法
- EXPRESSION 參數範例

EXPRESSION 參數語法

```
<Function name="functionName" paramPatterns="y" [type="EXPRESSION"
source=”*”]/>
```

其中

name 爲函數名稱 (必須的)。

paramPatterns 指出需改寫的參數 (必須的)

y y 的位置會指出需改寫的函數參數。上列語法中，僅會改寫第一個參數。

type 指定 EXPRESSION 值 (可選)

source 呼叫此函數的網頁 URI。

EXPRESSION 參數範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/dir1/dir2/page.html
```

網頁內容

```
<script language="JavaScript">
<!--
function jstest2(){
return ".html";
}
function jstest1(one){
return one;
}
var dir="/images/test"
var test1=jstest1(dir+"/test"+jstest2());
document.write("<a HREF="+test1+">TEST</a>");
alert(test1);
//-->
</SCRIPT>
```

規則

```
<Function type="EXPRESSION" name="jstest1" paramPatterns="y"/>
or
<Function name="jstest1" paramPatterns="y"/>
```

輸出

```
<script language="JavaScript">
<!--
```

```
function jstest2(){
return ".html";
}
function jstest1(one){
return one;
}
var dir="/images/test"
var
test1=jstest1(psSRAPRewriter_convert_expression(dir+"/test"+jstest2()));
document.write("<a HREF="+test1+">TEST</a>");
alert(test1);
//-->
</SCRIPT>
```

說明

因將之視爲 EXPRESSION 函數參數，因此這個規則指出 `jstest1` 函數的第一個參數需要改寫。在網頁內容範例中，第一個參數是僅在執行時間中計算其值的表示式。Rewriter 會將 `psSRAPRewriter_convert_expression` 函數前置於此表示式之前。從而計算此表示式，並且 `psSRAPRewriter_convert_expression` 函數在執行時間中改寫輸出。

備註 上列範例中，不需將 `test1` 變數作爲 JavaScript 變數規則的一部分。`jstest1` 的函數規則負責執行改寫。

DHTML 參數

其值爲 HTML 的函數參數

原始的 JavaScript 方法，如會以動態的方式產生 HTML 網頁的 `document.write()`，歸屬於此種類。

本節分爲下列部分：

- DHTML 參數語法
- DHTML 參數範例

DHTML 參數語法

<Function name="*functionName*" paramPatterns="y" type="DHTML" [source="*"]/>

其中

name 是函數名稱。

paramPatterns 指出需改寫的參數 (必須的)

y y 的位置會指出需改寫的函數參數。上列語法中，僅會改寫第一個參數。

DHTML 參數範例

假設此網頁的基準 URL 是：

http://xyz.siroe.com/test/rewriter/test1/jscript/JSFUNC/page.html

網頁內容

```
<script>
<!--
document.write('<a href="/index.html">write</a><BR>')
document.writeln('<a href="index.html">writeln</a><BR>')
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
//-->
</SCRIPT>
```

規則

```
<Function name="DHTML" name="document.write" paramPatterns="y"/>
<Function name="DHTML" name="document.writeln" paramPatterns="y"/>
<Attribute name="href"/>
```

輸出

```
<SCRIPT>
<!--
document.write('<a
href="gateway-URL/http://xyz.siroe.com/index.html">write</a><BR>')
document.writeln('<a
href="gateway-URL/http://xyz.siroe.com/test/rewriter/test1/jscript/JSFUNC/inde
x.html">writeln</a><BR>')
```

```
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
//-->
</SCRIPT>
```

說明

第一個規則指出 `document.write` 函數中的第一個參數需要改寫。第二個規則指出 `document.writeln` 函數中的第一個參數需要改寫。第三個規則是一個簡單 HTML 規則，指出名稱爲 `href` 的所有屬性皆需改寫。在範例中，DHTML 參數規則會識別出函數中需改寫的參數。然後便套用 HTML 屬性規則，以實際改寫識別出的參數。

DJS 參數

其值爲 JavaScript 的函數參數。

本節分爲下列部分：

- DJS 參數語法
- DJS 參數範例

DJS 參數語法

```
<Function name="functionName" paramPatterns="y" type="DJS" [source=”*”]/>
```

其中

`name` 是含有一個 DJS 參數的函數名稱 (必須的)

`paramPatterns` 指出上列函數中哪一個參數是 DJS (必須的)

`y` `y` 的位置會指出需改寫的函數參數。上列語法中，僅會改寫第一個參數。

`type` 是 DJS (必須的)

`source` 是網頁的 URI (可選，預設爲 * 表示任何 URI)

DJS 參數範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/page.html
```

網頁內容

```
<script>
menu.addItem(new NavBarMenuItem("All Available
Information","JavaScript:top.location='http://abc.sesta.com'"));
```

```
</script>
```

規則

```
<Function name="DJS" name="NavBarMenuItem" paramPatterns=",y"/>

<Variable name="URL">top.location</Variable>
```

輸出

```
<script>

menu.addItem(new NavBarMenuItem("All Available
Information","JavaScript:top.location='gateway-URL/http://abc.sesta.com'"));

</script>
```

說明

第一個規則指出包含 JavaScript 的 `NavBarMenuItem` 函數中的第二個參數需要改寫。在 JavaScript 中，`top.location` 變數亦需改寫。將使用第二個規則來改寫此變數。

用於 XML 內容的規則

網頁可能包含 XML 內容，其因此可包含 URL。需改寫的 XML 內容可分爲兩類：

- 標記文字 (與標記的 PCDATA 或 CDATA 相同)
- 屬性

標記文字

此規則是用於改寫標記元素的 PCDATA 或 CDATA。

本節分爲下列部分：

- 標記文字語法
- 標記文字範例

標記文字語法

```
<TagText tag="tagName" [attributePatterns="attribute_patterns_for_
this_tag" source="*"]/>
```

其中

`tagName` 爲標記名稱

`attributePatterns` 是此標記的屬性及值式樣 (可選，表示此標記完全不具屬性)

source 是此 xml 檔案的 URI (可選，預設爲 * 表示任何 xml 網頁)

標記文字範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/test/rewriter/test1/xml/page.html
```

網頁內容

```
<xml>
<attribute name="src">test.html</attribute>
<attribute>abc.html</attribute>
</xml>
```

規則

```
<TagText tag="attribute" attributePatterns="name=src"/>
```

輸出

```
<xml>
<attribute
name="src">gateway-URL/http://abc.sesta.com/test/rewriter/test1/xml/test.html<
/attribute>
<attribute>abc.html</attribute>
</xml>
```

說明

此網頁內容的第一行具有屬性範例；此網頁內容的第二行不包含具有屬性呼叫名稱的屬性且屬性名稱值爲 src，因此不會執行任何改寫的動作。若要進行改寫，我們亦需具有 `<TagText tag="attribute"/>`。

屬性

XML 屬性的規則與 HTML 的屬性規則類似。請參閱 「用於 HTML 內容的屬性規則」(第 118 頁)。其間的差異在於：XML 的屬性規則有大小寫之分，而 HTML 屬性規則則無。這是因爲 XML 中建立了區分大小寫的特性，而 HTML 中未建立。

Rewriter 會依據屬性名稱轉譯屬性值。

本節分爲下列部分：

- 屬性語法
- 屬性範例

屬性語法

<Attribute name="*attributeName*" [tag="*" type="URL" valuePatterns="*" source="*"]/>

其中

`attributeName` 爲屬性名稱 (必須的)

`tag` 是標記名稱，即出現此屬性的標記 (可選，預設爲 * 表示任何標記)

`valuePatterns` 請參閱第 93 頁 「在規則中使用式樣匹配」。

`source` 是此 XML 網頁的 URI (可選，預設爲 * 表示在任何 XML 網頁中)

屬性範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/test/rewriter/test1/xml/page.html
```

網頁內容

```
<xml>
<baseroot href="/root.html"/>
<img href="image.html"/>
<string href="1234|substring.html"/>
<check href="1234|string.html"/>
</xml>
```

規則

```
<Attribute name="href"tag="check" valuePatterns="1234|"/>
```

輸出

```
<xml>
<baseroot href="/root.html"/>
<img href="image.html"/>
<string href="1234|substring.html"/>
<check
href="1234|gateway-URL/http://abc.sesta.com/test/rewriter/test1/xml/string.html"/>
</xml>
```

說明

上列範例中，僅改寫第四行，因爲其符合規則中所指定的所有條件。請參閱「在規則中使用式樣匹配」(第 116 頁)。

用於 Cascading Style Sheet (串接樣式表) 的規則

HTML 網頁中的 Cascading Style Sheet (包含 CCS2) 會被轉譯。沒有任何針對此轉譯而定義的規則，因爲 URL 僅出現在 `url()` 函數與 CSS 的匯入語法中。

用於 WML 的規則

WML 與 HTML 類似，因此 HTML 規則適用於 WML 內容。請對 WML 內容使用通用規則集。請參閱第 88 頁「用於 HTML 內容的規則」。

在「閘道」服務中配置 Rewriter

藉由使用「Rewriter」標籤下的「閘道」服務，您可以執行下列兩種工作 - 基礎與進階：

- 基礎作業
  - 啓用所有 URL 的重寫
  - 建立「URI 至規則集對映」清單
  - 建立剖析器至 MIME 對映清單
  - 指定預設網域與子網域
- 進階作業
  - 建立不會重寫的 URI 清單
  - 啓用 MIME 推測
  - 建立「剖析器至 URI 對映」清單
  - 啓用混淆
  - 指定混淆器種子字串

- 建立不要混淆的 URI 清單
- 讓閘道通訊協定與原始 URI 通訊協定相同

基礎作業

啓用所有 URL 的重寫

若您啓用「閘道」服務中的「啓用所有 URI 的重寫」選項，則 Rewriter 會改寫任何 URL 而不會將其於「網域與子網域的代理伺服器」中的項目進行核對。便會忽略「網域與子網域的代理伺服器」清單中的項目。

➤ **若要使得閘道可重寫所有 URL**

1. 以管理員的身份登入 Sun™ ONE Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您要設定其屬性之閘道設定檔的「編輯 ...」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「Rewriter」標籤。
6. 選取「啓用所有 URI 的重寫」核取方塊，使得「閘道」可以重寫所有 URL。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立「URI 至規則集對映」清單

規則集會建立於 Identity Server 管理主控台中 Portal Server 配置之下的 Rewriter 服務中。有關詳細資料，請參閱 *Sun ONE Portal Server* 管理員指南 。

建立規則集後，您可使用「URI 至規則集對映」清單將網域與規則集相關聯。依預設，下列兩個項目會加入至「URI 至規則集對映」清單：

- `*://*.Sun.COM/portal/*|default_gateway_ruleset`

  其中 `sun.com` 爲入口網站的安裝網域，而 `/portal` 則是入口網站的安裝環境
- `*|generic_ruleset`

這表示，網域爲 sun.com 之入口網站目錄的所有網頁，將套用 default_gateway_ruleset。對於其他頁面，則套用常規規則集。default_gateway_ruleset 與 generic_ruleset 是預先封裝的規則集。

備註 對於所有顯示於入口網站桌面中的內容，將使用 default_gateway_ruleset 規則集，與取得內容處無關。

例如，假設入口網站桌面被配置爲從 URL yahoo.com 取得內容，但該 Portal Server 位於 sesta.com，則會套用 sesta.com 的規則集至取得的內容。

備註 您指定規則集的網域必須列於「網域與子網域的代理伺服器」清單中。

在語法中使用萬用字元

您可對映一個完全合格的 URI 或在規則集中使用星號來對映部分 URI。

例如，您可以將 java_index_page_ruleset 套用至 index.html 網頁，如下所示：

```
www.sun.com/java/index.html/java_index_page_ruleset
```

或者，您可以將 java_directory_ruleset 套用至 Java 目錄下的所有網頁，如下所示：

```
www.sun.com/java/* /java_directory_ruleset
```

➤ 若要將 URI 對映至規則集

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的「閘道」設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤。
6. 捲動至「URI 至規則集對映」欄位。

7. 在「URI 至規則集對映」欄位中鍵入需要的網域或主機名稱以及規則集並按一下「新增」。

   此項目會新增至「URI 至規則集對映」清單。

   指定網域或主機名稱以及規則集的格式如下所示：

   ```
   domain name|ruleset name
   ```

   例如：

   ```
   eng.sesta.com|default
   ```

建立剖析器至 MIME 對映清單

Rewriter 有四個不同的剖析器以根據 HTML、JAVASCRIPT、CSS 與 XML 等內容類型剖析網頁。依預設共用 MIME 類型會與這些剖析器相關。您可以在「閘道」服務中的「剖析器至 MIME 對應」欄位中將新 MIME 類型與這些剖析器相關聯。此將 Rewriter 功能延伸至其他 MIME 類型。

使用分號或逗號 (";" 或 ",") 分隔多個項目：

例如：

```
HTML=text/html;text/htm;text/x-component;text/wml; text/vnl/wap.wml
```

意味任何含有這些 MIME 的內容會被傳送到 HTML Rewriter 而 HTML 規則將被套用以重寫 URL。

提示 移除 MIME 對映清單中不需要的剖析器可以提高作業速度。例如，若您確定某些內部網站的內容將不會有任何 JavaScript，可以將 JAVASCRIPT 項目從 MIME 對映清單中移除。

➤ 若要指定 MIME 對映

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的「閘道」設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤。

6. 捲動至「剖析器至 MIME 對映」欄位，並在編輯方塊中新增需要的 MIME 類型。使用分號或逗號以分隔多個項目。

   以 `HTML=text/html;text/htm` 格式指定項目

7. 按一下「新增」以新增需要的項目至清單中。
8. 按一下頁面頂端或底部的「儲存」記錄變更。
9. 從終端機視窗重新啓動「閘道」：

   portal-server-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定預設網域與子網域

當 URL 僅包括主機名稱而沒有網域與子網域時，預設網域與子網域將特別有用。在此情況下，「閘道」將假設主機名稱位於預設網域與子網域中，並繼續執行相應的操作。

例如，若 URL 中的主機名稱爲 `host1`，且預設網域與子網域被指定爲 `red.sesta.com`，則主機名稱會被解析爲 `host1.red.sesta.com`。

➤ 若要指定預設網域與子網域

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 按一下「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的右箭頭。

   將顯示「閘道設定檔」頁面。

4. 按一下您要設定其屬性之閘道設定檔的「編輯 ...」。

   便會顯示「編輯閘道設定檔」頁面。

5. 捲動至「預設網域子網域」欄位並以 `subdomain.domain name` 格式鍵入需要的預設值。
6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   portal-server-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

進階作業

建立不會重寫的 URI 清單

➤ **若要指定預設網域與子網域**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的「閘道」設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。
6. 捲動至「不要重寫 URI 清單」欄位，並在編輯方塊中新增 URI。

   備註：將 #* 新增至此清單中，以允許重寫 URI (即使 href 規則爲規則集的一部分)。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 MIME 推測

Rewriter 會根據網頁的 MIME 類型選擇剖析器。有些網路伺服器，如 WebLogic 和 Oracle，並不會傳送 MIME 類型。若要解決這個問題，可以啓用 MIME 推測，方法是新增資料至「剖析器至 URI 對映」清單方塊。

➤ **若要啓用 MIME 推測**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的「閘道」設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。

5. 按一下「Rewriter」標籤，「進階」子區段。
6. 選取「啓用 MIME 推測」核取方塊以啓用 MIME 推測。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立「剖析器至 URI 對映」清單

若已啓用 MIME 推測核取方塊，且伺服器沒有傳送 MIME 類型，可使用這個清單方塊以對映剖析器至 URI。

由分號分隔多個 URI。

例如 HTML=*.html; *.htm;*Servlet

表示 HTML Rewriter 會用於改寫任何含有 html、htm 或 Servlet 副檔名的頁面內容。

➤ 若要剖析 URI 對映

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的「閘道」設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。
6. 捲動至「剖析器至 MIME 對映」欄位，並新增資料至編輯方塊。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用混淆

「混淆」允許 Rewriter 改寫 URI，如此即可隱藏網頁的「內部網路 URL」。

➤ 若要啓用混淆

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定屬性的「閘道設定檔」。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。
6. 選取「啓用混淆」核取方塊以啓用混淆。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定混淆器種子字串

種子字串會用於 URI 的混淆。其爲一個由混淆演算法產生的隨機字串。

備註 若此種子字串已變更或「閘道」已重新啓動，則無法將已混淆的 URI 加入書籤。

➤ 若要指定混淆種子字串

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的「閘道」設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。

6. 捲動至 「混淆器種子字串」欄位，並新增字串至編輯方塊。
7. 按一下頁面頂端或底部的 「儲存」記錄變更。
8. 從終端機視窗重新啓動 「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立不要混淆的 URI 清單

某些應用程式 (例如 applet) 需要網際網路 URI 且無法被混淆。若要指定那些應用程式，請新增 URI 至清單方塊。

例如您新增

`*/Applet/Param*`

至此清單方塊，則如果內容 URI `http://abc.com/Applet/Param1.html` 與規則集中的規則匹配，將不會混淆 URL。

➤ **若要指定 「不要混淆 URI 清單」**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取 「服務配置」標籤。
3. 按一下 「SRA 配置」下 「閘道」旁的箭頭。

   將顯示 「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的 「閘道」設定檔。

   顯示 「閘道」 - *gateway-profile-name* 頁面。
5. 按一下 「Rewriter」標籤，「進階」子區段。
6. 捲動至 「不要混淆 URI 清單」欄位，並新增 URI 至編輯方塊。
7. 按一下頁面頂端或底部的 「儲存」記錄變更。
8. 從終端機視窗重新啓動 「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

讓閘道通訊協定與原始 URI 通訊協定相同

當閘道以 http 及 https 模式執行時，可以啓用 Rewriter 以使用一致的通訊協定存取 HTML 內容中的參照資源。

例如，若原始 URL 是 `http://intranet.com/Public.html`，則會新增 http 閘道。若原始 URL 是 `https://intranet.com/Public.html`，則會新增 https 閘道。

備註 這將僅套用至靜態 URI，而非產生於 Javascript 的動態 URI。

➤ **若要讓閘道通協定與原始 URI 通訊協定相同**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的「閘道」設定檔。

   顯示「閘道」- *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。
6. 選取「讓閘道通訊協定與原始的 URI 通訊協定相同」核取方塊。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

使用除錯日誌排除故障

若要排除 Rewriter 的故障，您需啓用除錯日誌。

除錯訊息分類如下：

- `error` - 使得 Rewriter 無法復原的錯誤
- `warning` - 此檔案包含與警告訊息有關的日誌。Rewriter 可從此類型的錯誤中復原，但可能會或不會造成不當行爲。例如「Not rewriting image content」(未改寫影像內容) 被記錄爲警告訊息。這個情況並不會造成重大影響，因爲 Rewriter 並不會用於改寫影像。這個訊息僅作爲警告之用，不會對 Rewriter 的運作造成重大影響。有些出現在警告中的訊息僅是告知性的。
- `message` - 這是 Rewriter 所提供最高層級的資訊。

設定 Rewriter 除錯層級

➤ **若要設定 Rewriter 除錯層級**

1. 以超級使用者身份登入閘道機器，然後編輯下列檔案：

   gateway-install-root/SUNWam/lib/AMConfig.properties

2. 設定除錯層級：

   com.iplanet.services.debug.level=

   除錯層級爲：

   error - 僅在除錯檔案中記錄嚴重錯誤。在此種錯誤發生時，Rewriter 通常會停止運作。

   warning - 記錄警告訊息。

   message - 記錄所有除錯訊息。

   off - 不會記錄任何除錯訊息。

3. 在 AMConfig.properties 檔案的下列屬性中，指定除錯檔案目錄：

   com.iplanet.services.debug.directory=/var/opt/SUNWam/debug

   其中 /var/opt/SUNWam/debug 是預設的除錯目錄。

4. 從終端機視窗重新啓動「閘道」：

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

除錯檔案名稱

當除錯層級設定爲 message 時，除錯指令會產生一組檔案。表 3-2 列出 Rewriter 檔案，及其中所包含的資訊。第一欄爲除錯檔案的名稱，第二欄則說明檔案包含的內容。

表 3-2 Rewriter 除錯檔案

檔案名稱	資訊
RuleSetInfo	所有已用於改寫的規則集皆記錄在此檔案中。
Original Pages	包含網頁 URI、resolveURI (若其與網頁 URI 不同)、內容 MIME、套用至網頁的規則集、剖析器 MIME 與原始內容。 與剖析有關的特定錯誤 / 警告 / 訊息亦會出現在此檔案中。 在 message 模式中，會記錄完整內容；在 warning 及 error 模式下則僅會記錄改寫期間所發生的異常情況。
Rewritten Pages	包含網頁 URI、resolveURI (若其與網頁 URI 不同)、內容 MIME、套用至網頁的規則集、剖析器 MIME 與已改寫的內容。 當除錯模式設為 message 時，即會儲存這些資訊。
Unaffected Pages	包含未經修改的網頁清單。
URIInfo Pages	此檔案包含已找到及轉譯的 URL。所有其內容與原始資料相同的網頁詳細資訊將記錄至此檔案中。 已記錄的詳細資訊包括：網頁 URI、MIME 與編碼資料、用於改寫的 rulesetID 以及剖析器 MIME。

除了上述檔案之外，Rewriter 會產生一個用於未留存於上述檔案中的其他除錯訊息的檔案。檔案名稱包括兩個部分：第一部分爲 `pwRewriter` 或 `psSRARewriter`，第二部分則爲使用 `portal` 或 *gateway profile name* 的副檔名。

除錯檔案會顯示在入口網站或閘道中。這些檔案存放於 `AMConfig.properties` 檔案中指示的目錄中。

Rewriter 元件會產生下列檔案組以協助除錯作業：

*prefix*_RuleSetInfo.*extension*

*prefix*_OrginalPages.*extension*

*prefix*_RewrittenPages.*extension*

*prefix*_UnaffectedPages.*extension*

*prefix*_URIInfo.*extension*

其中

prefix 爲用於 URLScraper 用途日誌的 `psRewriter` 或用於閘道用途日誌的 `psSRAPRewriter`。

extension 則爲用於 URLScaper 用途的 `portal` 或用於閘道用途的 *`gateway-profile-name`*。

例如，若利用閘道上的 Rewriter 來轉換網頁並使用預設的閘道設定檔，則除錯作業會產生下列檔案：

`psSRAPRewriter_RuleSetInfo.default`

`psSRAPRewriter_OriginalPages.default`

`psSRAPRewriter_RewrittenPages.default`

`psSRAPRewriter_UnaffectedPages.default`

`psSRAPRewriter_URIInfo.default`

`psSRAPRewriter.default`

工作範例

本節包括：

- 含需改寫之內容的簡單 HTML
- 改寫內容所需的規則
- 已改寫的相應 HTML 網頁

這些頁面範例位於 *portal-server-URL*`/rewriter` 目錄下。您可在套用規則前瀏覽整個頁面，然後經由您的閘道檢視含已改寫之輸出的檔案，以查看規則的套用結果。在某些範例中，規則已經是 `default_gateway_ruleset` 的一部分。在某些範例中，您必須將規則納入 `default_gateway_ruleset` 中。這一點會在適當之處提及。

備註 某些以粗體顯示的陳述式表示其已被改寫。

可用的範例如下：

- HTML
  - HTML 屬性範例
  - HTML 表單範例
  - HTML Applet 範例

- JavaScript
  - 變數
    - JavaScript URL 變數的範例
    - JavaScript 內容範例
    - JavaScript DHTML 變數的範例
    - JavaScript DJS 變數的範例
    - JavaScript SYSTEM 變數的範例
  - 函數
    - JavaScript URL 函數的範例
    - JavaScript EXPRESSION 函數的範例
    - JavaScript DHTML 函數的範例
    - JavaScript DJS 函數的範例
- XML
  - XML 屬性範例

HTML 內容範例

HTML 屬性範例

➤ **若要使用 HTML 屬性範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/HTML/attrib/attribrule.html

2. 請確定您已於「閘道」服務的「網域與子網域的代理伺服器」清單中定義 `abc.sesta.com` 與 `host1.siroe.com`。

   若未定義，則會採用直接連接，且不前置閘道 URL。

您不需將此範例中指定的規則新增至 `default_gateway_ruleset` 中，因爲其已完成定義。

進行改寫前的 HTML

```
<html>
Rewriting starts
<head>
<title>TEST PAGE () </title>
</head>
ID-htmlattr.1
<br><br>
1.a href <a href="http://abc.sesta.com/images/logo.gif">http://..</a>
<br><br>
2. href <a href="https://host1.siroe.com">https://..</a>
<br><br>
3. href <a href="../images/logo.gif">../images/</a>
<br><br>
4. href <a href="images/logo.gif">images/..</a> <br><br>
5. href <a href="../../images/logo.gif">../../images/</a> <br><br>
Rewriting ends
</html>
```

規則

```
<Attribute name="href"/>
```

進行改寫後的 HTML

```
<html>
Rewriting starts
<head>
<title>TEST PAGE () </title>
</head>
ID-htmlattr.1
<br><br>
```

**1. a href http://..
**

// 改寫此 URL 是因爲 <Attrib name="href"/> 規則已於 default_gateway_ruleset 中加以定義。由於此 URL 是絕對 URL，因此僅會前置閘道 URL。請確定您已於「閘道」服務的「網域與子網域的代理伺服器」清單中定義 abc.sesta.com。否則，會認爲是直接連接，而不會前置閘道 URL。

2. href https://..

// 同樣，host1.siroe.com 需於「閘道」服務的「網域與子網域的代理伺服器」清單中定義。否則，會認爲是直接連接，而不會前置閘道 URL。

3. href ../images/

// 由於指定的是相對路徑，因此會前置閘道 URL 與 portal-server-URL (附有所需子目錄)。此連結將無法作用，因爲在所提供之範例結構的 HTML 目錄下沒有名爲 images 的目錄。

**4 href images/..

**

// 由於指定的是相對路徑，因此會前置閘道 URL 與 Portal Server URL (附有所需子目錄)。

**5. href ../../images/

**

// 由於指定的是相對路徑，因此會前置閘道 URL 與 Portal Server URL (附有所需子目錄)。此連結將無法作用，因爲在所提供之範例結構的 HTML 目錄下沒有名爲 images 的目錄。

Rewriting ends

</html>

HTML 動態 JavaScript 記號的範例

➤ **若要使用 HTML JavaScript 記號範例：**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/HTML/jstokens/JStokens.html

2. 將此範例中指定的規則新增至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。

3. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

4. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

進行改寫前的 HTML

```
<html>

<head>

Rewriting starts

<script language="javascript">

function Check(test,ind){

if (ind == 'blur')

{alert("testing onBlur")}

if (ind == 'focus')

{alert("testing onFocus")}

}

</SCRIPT>

</head>

<body>

<form>

<input TYPE=TEXT SIZE=20 value=blur
onAbort="Check('/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=blur
onBlur="Check('/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=focus
onFocus="Check('/focus.html','focus');return;">
```

```
<input TYPE=TEXT SIZE=20 value=focus
onChange="Check('/focus.html','focus');return;">

<input TYPE=TEXT SIZE=20 value=focus
onClick="Check('/focus.html','blur');return;">

<br><br>

</form>

</body>

Rewriting ends

</html>
```

規則

```
<Attribute name=”onClick” type=”DJS”/>

<Function type="URL" name="Check" paramPatterns="y"/>
```

備註 `<Function name="URL" name="Check" paramPatterns="y"/>` 爲 JavaScript 函數規則，並於 JavaScript 函數範例中詳細說明。

進行改寫後的 HTML

```
<html>

<head>

Rewriting starts

<script language="javascript">

function Check(test,ind){

if (ind == 'blur')

{alert("testing onBlur")}

if (ind == 'focus')

{alert("testing onFocus")}

}

</SCRIPT>

</head>

<body>

<form>
```

```
<input TYPE=TEXT SIZE=20 value=blur onAbort="Check('gateway
URL/portal-server-URL/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=blur onBlur="Check('gateway
URL/portal-server-URL/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=focus onFocus="Check('gateway
URL/portal-server-URL/focus.html','focus');return;">

<input TYPE=TEXT SIZE=20 value=focus onChange="Check('gateway
URL/portal-server-URL/focus.html','focus');return;">

<input TYPE=TEXT SIZE=20 value=focus onClick="Check('gateway
URL/portal-server-URL/focus.html','blur');return;">
```

// 此範例中的所有陳述式都已改寫。每次改寫都會前置 Gateway 與 Portal Server URL。這是因爲 `onAbort`、`onBlur`、`onFocus`、`onChange` 與 `onClick` 的規則都已在 `default_gateway_ruleset` 檔案中定義。Rewriter 會偵測 JavaScript 記號，並將之傳送至 JavaScript 函數規則中以便進行進一步的處理。此範例中的第二個規則會告知 Rewriter 該改寫哪一個參數。

```
</body>

<br>

Rewriting ends

</html>
```

HTML 表單範例

➤ 若要使用表單範例

1. 您可自下列路徑存取表單範例：

   portal-server-URL/rewriter/HTML/forms/formrule.html

2. 請確定您已於「閘道」服務的「網域與子網域的代理伺服器」清單中定義 `abc.sesta.com`。

   若未定義，則會採用直接連接，且不前置閘道 URL。

3. 將此範例中指定的規則新增至「改寫 HTML 屬性的規則」部分的 `default_gateway_ruleset` 中。

4. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

5. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

進行改寫前的 HTML 網頁

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head>

</head>

<body>

RW_START

<p>

<form name="form1" method="Post"
action="http://abc.sesta.com/casestudy/html/form.html">

<input type="hidden" name="name1" value="0|1234|/test.html">

<input type="hidden" name="name3" value="../../html/test.html">

<form name="form2" method="Post"
action="http://abc.sesta.com/testcases/html/form.html"><br>

<input type="hidden" name="name1"
value="0|1234|../../html/test.html"></form>

RW_END </p>

</body>

</html>
```

規則

```
<Form source="*" name="form1" field="name1" valuePatterns="0|1234|"/>
```

進行改寫後的 HTML 網頁

```
<HTML>

<HEAD>

RW_START

</HEAD>

<BODY>

<P>

<FORM name=form1  method=POST
action="gateway-URL/http://abc.sesta.com/casestudy/html/form.html">
```

// 改寫此 URL 是因爲已在 default_gateway_rulesetdefault_gateway_ruleset 中將 <Attribute name="action"/> 定義爲 HTML 規則的一部分。由於此 URL 是絕對 URL，因此僅需前置閘道 URL。請確定您已於「閘道」服務的「網域與子網域的代理伺服器」清單中定義 abc.sesta.com。否則，會認爲是直接連接，而不會前置閘道 URL。

<input type=hidden name=name1 value="0|1234|gateway URL/portal-server-URL/test.html">

// 此處的表單名稱爲 form1，而欄位名稱則爲 name1。上述名稱與規則中指定的表單名稱與欄位名稱匹配。規則指出 valuePatterns 爲 0|1234|，其符合此陳述式中的 value。因此會改寫出現在 valuePattern 之後的 URL。將前置 Portal Server URL 與閘道 URL。有關 valuePatterns 的詳細資料，請參閱 「在規則中使用式樣匹配」(第 116 頁)。

<input type=hidden name=name3 value="../../html/test.html">

// 未改寫此 URL 是因爲此 name 不符合規則中所指定的 field 名稱。

</FORM>

**<FORM name=form2 method=POST action="gateway-URL/http://abc.sesta.com/casestudy/html/form.html">
**

// 改寫此 URL 是因爲已在預設規則集中將 <Attribute name="action"/> 定義爲 HTML 規則的一部分。由於此 URL 是絕對 URL，因此僅需前置閘道 URL。

<input type=hidden name=name1 value="0|1234|../../html/test.html">

// 不改寫此 URL 是因爲此表單名稱不符合規則中所指定的名稱。

</FORM>

</BODY>

RW_END

</HTML>

HTML Applet 範例

➤ **若要使用 Applet 範例**

1. 請取得 Applet 類別檔案。`RewriteURLinApplet.class` 檔案位於下列位置：

   portal-server-URL/rewriter/HTML/applet/appletcode

   出現 Applet 代碼之網頁的基準 URL 爲：

   portal-server-URL/rewriter/HTML/applet/rule1.html

2. 將此範例中指定的規則新增至「改寫 HTML 屬性的規則」部分的 `default_gateway_ruleset` 中。

3. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

4. 重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 HTML

```
<html>

Rewriting starts

<br>

<applet codebase=appletcode code=RewriteURLinApplet.class archive=/test>

<param name=Test1 value="/index.html">

<param name=Test2 value="../index.html">

<param name=Test3 value="../../index.html">

</applet>

Rewriting ends

</html>
```

規則

```
<Applet source="*/rule1.html" code="RewriteURLinApplet.class" param="Test*"
/>
```

進行改寫後的 HTML

```
<HTML>

Rewriting starts

<BR>

<APPLET
codebase=gateway-URL/portal-server-URL/rewriter/HTML/applet/appl
etcode=RewriteURLinApplet.class archive=/test>

// 改寫此 URL 是因爲規則 <Attribute name="codebase"/> 已成爲
default_gateway_ruleset 檔案的一部分。將前置閘道與 Portal Server URL ( 附有至
appletcode 目錄的路徑。

<param name=Test1
value="gateway-URL/portal-server-URL/index.html">

// 改寫此 URL 是因爲此網頁的基準 URL 爲 rule1.html，且參數名稱符合規則中指
定的參數 Test*。由於已將 index.html 指定放置於根層級，因此將直接前置閘道與
Portal Server URL。

<param name=Test2
value="gateway-URL/portal-server-URL/rewriter/HTML/index.html">

// 改寫此 URL 是因爲此網頁的基準 URL 爲 rule1.html，且參數名稱符合規則中指
定的參數 Test*。將依需要前置路徑。

<param name=Test3
value="gateway-URL/portal-server-URL/rewriter/index.html">

// 改寫此 URL 是因爲此網頁的基準 URL 爲 rule1.html，且參數名稱符合規則中指
定的參數 Test*。將依需要前置路徑。

</APPLET>

Rewriting ends

</HTML>
```

JavaScript 內容範例

JavaScript URL 變數的範例

➤ 若要使用 JavaScript URL 變數範例

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/variables/url/js_urls.html

2. 請確定您已於「閘道」服務的「網域與子網域的代理伺服器」清單中定義 `abc.sesta.com`。

   若未定義，則會採用直接連接，且不前置閘道 URL。

3. 將此範例中指定的規則新增至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。

4. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

5. 若您新增此規則，請重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 HTML 網頁

```
<html>
Rewriting starts
<head>
<title>JavaScript Variable test page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc="/tmp/tmp.jpg";
var imgsrc="./tmp/tmp.jpg";
var imgsrc="../tmp/tmp.jpg";
var imgsrc="../../tmp/tmp.jpg";
var imgsrc="http://abc.sesta.com/tmp/tmp.jpg";
```

```
var imgsrc="../../../tmp/tmp.jpg";
var imgsrc="tmp/tmp.jpg";
//-->
</SCRIPT>
<br>
Testing JavaScript variables!
<br>
<img src="images/logo.gif">
<br>
Image
</body>
<br>
Rewriting ends
</html>
```

規則

```
<Variable name=”imgsrc” type="URL"/>
```

進行改寫後的 HTML 網頁

```
<html>
Rewriting starts
<head>
<title>JavaScript Variable test page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc="gateway-URL/portal-server-URL/tmp/tmp.jpg";
var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/variab
les/url/tmp/tmp.jpg";
```

```
var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/variab
les/tmp/tmp.jpg";

var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/tmp/tm
p.jpg";

var imgsrc="gateway-URL/http://abc.sesta.com/tmp/tmp.jpg";

var imgsrc="gateway-URL/portal-server-URL/rewriter/tmp/tmp.jpg";

var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/variab
les/url/tmp/tmp.jpg";

// 上列所有 URL 皆爲規則中所指定的 URL 類型且名稱爲 imgsrc 的 JavaScript 變
數。因此皆會前置閘道與 Portal Server URL。將依需前置位於 Portal Server URL
後的路徑。

//-->

</SCRIPT>

<br>

Testing JavaScript variables!

<br>

<img src="gateway
URL/portal-server-URL/rewriter/JavaScript/variables/url/images/logo.gif">

// 改寫此行是因爲已於 default_gateway_ruleset 中定義規則 <Attribute
name="src"/>

<br>

Image

</body>

<br>

Rewriting ends

</html>
```

JavaScript EXPRESSION 變數範例

➤ **若要使用 JavaScript 表示式變數範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/variables/expr/expr.html

2. 將此範例中指定的規則新增 (若尚不存在) 至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。

3. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

4. 若您新增此規則，請重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 HTML 網頁

```
<html>
<head>
<title>JavaScript EXPRESSION Variables Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar1="images";
var expvar2="/logo.gif";
var expvar = expvar1 + expvar2;
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
var expvar="/images/logo"+".gif";
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
//-->
</SCRIPT>
Testing JavaScript EXPRESSION variables
</body>
</html>
```

規則

```
<Variable type=”EXPRESSION” name="expvar"/>
```

進行改寫後的 HTML 網頁

```
<html>

<head>

<title>JavaScript EXPRESSION Variables Test Page</title>

</head>

<body>

<SCRIPT>

// Rewriter 會於此處附加包裝函數 psSRAPRewriter_convert_expression

</SCRIPT>

<script LANGUAGE="Javascript">

<!--

//Expression variables

var expvar1="images";

var expvar2="/logo.gif";

var expvar =psSRAPRewriter_convert_expression( expvar1 +
expvar2);
```

// Rewriter 會將此陳述式右側識別爲 JavaScript EXPRESSION 變數。Rewriter 無法在伺服器端計算出此表示式的值。因此，psSRAPRewriter_convert_expression 函數會被置於此表示式之前。此表示式將於用戶端計算，並視需要改寫。

```
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
```

// 將使用前一個陳述式之 expvar 的改寫值來計算此表示式的值。由於結果爲一有效的 URL (範例中此處出現一個圖形)，因此連結有效。

```
var expvar="gateway URL/portal-server-URL/images/logo"+".gif";
```

// Rewriter 會將 expvar 的右側識別爲字串表示式。此表示式可於伺服端計算，因此可直接改寫。

```
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
```

// 將使用前一個陳述式之 expvar 的改寫值來計算此表示式的值。由於結果不是有效的 URL (於結果位置中未出現圖形)，因此連結無效。

```
//-->
```

```
</SCRIPT>

Testing JavaScript EXPRESSION variables

</body>

</html>
```

JavaScript DHTML 變數的範例

➤ 若要使用 JavaScript DHTML 變數範例

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/variables/dhtml/dhtml.html

2. 請確定您已於「閘道」服務的「網域與子網域的代理伺服器」清單中定義 `abc.sesta.com`。若未定義，則會採用直接連接，且不前置閘道 URL。

3. 將此範例中指定的規則新增 (若尚不存在) 至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

4. 若您新增此規則，請重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 HTML 網頁

```
<html>

<head>

<title>JavaScript DHTML Variable Test Page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

//DHTML Var

var dhtmlVar="<a href=../../images/test.html>"

var dhtmlVar="<a href=/../images/test.html>"

var dhtmlVar="<a href=/images/test.html>"

var dhtmlVar="<a href=images/test.html>"

var dhtmlVar="<a href=http://abc.sesta.com/images/test.html>"
```

```
var dhtmlVar="<img src=http://abc.sesta.com/images/test.html>"
//-->
</SCRIPT>
<br><br>
Testing DHTML Variables
<br><br>
<img src="images/logo.gif">IMAGE
</body>
</html>
```

規則

```
<Variable name="DHTML">dhtmlVar</Variable>
```

進行改寫後的 HTML 網頁

```
<html>
<head>
<title>JavaScript DHTML Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//DHTML Var
```

`var dhtmlVar="<a href=gateway-URL/portal-server-URL/rewriter/JavaScript/images/test.html>"`

// JavaScript DHTML 規則會將 `dhtmlVar` 的右側識別爲動態 HTML 內容。因此會套用 `default_gateway_ruleset` 檔案中的 HTML 規則。動態 HTML 包含 `href` 屬性。`default_gateway_ruleset` 定義規則 `<Attribute name="href"/>`。因此會改寫 `href` 屬性的值。但此 URL 並不是絕對 URL。所以，網頁的基準 URL 與所需子目錄會取代相對 URL。最後會前置閘道 URL 以導出最後的改寫輸出。

`var dhtmlVar="<a href=gateway-URL/portal-server-URL/../images/test.html>"`

// 雖然已附加此網頁的基準 URL，且已前置閘道 URL，但是最後的 URL 卻無效。這是因爲初始 URL /../images/test.html 不正確。

var dhtmlVar="<a href=gateway-URL/portal-server-URL/images/test.html>"

// 同樣，JavaScript DHTML 規則會將右側識別爲動態 HTML 內容，並將之傳送至 HTML 規則。將套用 default_gateway_ruleset 中的 HTML 規則 <Attribute name="href"/>，且已如所示改寫陳述式，並已前置閘道 URL 與 Portal Server URL。

```
var dhtmlVar="<a href=gateway
URL/portal-server-URL/rewriter/JavaScript/variables/dhtml/images/test.html
>"

var dhtmlVar="<a href=gateway URL/http://abc.sesta.com/images/test.html>"
```

var dhtmlVar="<img src=gateway-URL/http://abc.sesta.com/images/test.html>"

// JavaScript DHTML 規則會識別右側的動態 HTML 內容，並將陳述式傳送至 HTML 規則。將套用 default_gateway_ruleset 中的 <Attribute name="src"/> 規則。由於此 URL 是絕對 URL，因此僅需前置閘道 URL。請確定您已於「網域與子網域的代理伺服器」清單中定義 abc.sesta.com 以便改寫此 URL。

```
//-->

</SCRIPT>

<br><br>

Testing DHTML Variables

<br><br>
```

<img src="gateway-URL/portal-server-URL/rewriter/JavaScript/variables/dhtml/images/logo.gif">

// 改寫此行是因爲已於 default_gateway_ruleset 中定義規則 <Attribute name="src"/>。

```
<br><br>

Image

</body>

</html>
```

JavaScript DJS 變數的範例

➤ **若要使用 JavaScript DJS 變數範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/variables/djs/djs.html

2. 請確定您已於「閘道」服務的「網域與子網域的代理伺服器」清單中定義 `abc.sesta.com`。若未定義，則會採用直接連接，且不前置閘道 URL。

3. 將此範例中指定的兩個規則新增 (若尚不存在) 至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

4. 重新啓動「閘道」：

   portal-server-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 HTML 網頁

```
<html>
<head>
<title>Dynamic JavaScript Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
var dJSVar="var dJSimgsrc='/tmp/tmp/jpg';"
var dJSVar="var dJSimgsrc='../../../tmp/tmp/jpg';"
var dJSVar="var dJSimgsrc='http://abc.sesta.com/tmp/tmp/jpg';"
//-->
</SCRIPT>
<br>
Testing Dynamic JavaScript Variables
<br>
<img src="images/logo.gif">
<br>
```

```
Image
</body>
</html>
```

規則

```
<Variable name=”dJSVar” type="DJS"/>
<Variable name="dJSimgsrc“ type=URL"/>
```

進行改寫後的 HTML 網頁

```
<html>
<head>
<title>Dynamic JavaScript Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
var dJSVar="var
dJSimgsrc='gateway-URL/portal-server-URL/tmp/tmp/jpg';"
var dJSVar="var
dJSimgsrc='gateway-URL/portal-server-URL/rewriter/tmp/tmp/jpg';"
var dJSVar="var
dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp/jpg';"
```

// 所有上述陳述式皆會使用閘道及 Portal Server URL 改寫。將依需要前置適當的路徑。第一個規則會將 dJSVar 右側識別爲動態 JavaScript 變數。然後傳送至第二個規則；第二個規則會將 dJSimgsrc 右側識別爲 URL 類型的 JavaScript 變數。將相應進行改寫。

```
//-->
</SCRIPT>
<br>
Testing Dynamic JavaScript Variables
<br>
<img
src="gateway-URL/portal-server-URL/rewriter/JavaScript/variables
/djs/images/logo.gif">
```

```
// 改寫此行是因爲已於 default_gateway_ruleset 中定義規則 <Attribute
name="src"/>。
<br>
Image
</body>
</html>
```

JavaScript SYSTEM 變數的範例

➤ **若要使用 JavaScript SYSTEM 變數範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/variables/system/system.html

2. 將此範例中指定的規則新增 (若尚不存在) 至「改寫 JavaScript 來源的規則」部分的 default_gateway_ruleset 中。

3. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 default_gateway_ruleset。

4. 重新啓動「閘道」：

   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start

進行改寫前的 HTML 網頁

```
<html>
<head>
<title>JavaScript SYSTEM Variables Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(window.location.pathname);
//document.write("<A HREF="+window.location.pathname+">SYSTEM</A><P>")
//-->
</SCRIPT>
```

```
Testing JavaScript SYSTEM Variables

<br>

This page displays the path where the current page is located when it is
loaded.

</body>

</html>
```

規則

```
<Variable name=”window.location.pathname” type="SYSTEM"/>
```

進行改寫後的 HTML

```
<html>

<head>

<title>JavaScript SYSTEM Variables Test Page</title>

</head>

<body>

<SCRIPT>

convertsystem function definition...

</SCRIPT>

<script LANGUAGE="Javascript">

<!--

//SYSTEM Var

alert(psSRAPRewriter_convert_system(window.location,
window.location.pathname,”window.location”));
```

// Rewriter 會將 window.location.pathname 識別爲 JavaScript SYSTEM 變數。此變數的值無法於伺服器端判定。因此 Rewriter 會在變數前前置 psSRAPRewriter_convert_pathname 函數。此包裝函數可於用戶端判定此變數的值，然後依需要改寫。

```
//-->

</SCRIPT>

Testing JavaScript SYSTEM Variables

<br>
```

```
This page displays the path where the current page is located when it is
loaded.
</body>
</html>
```

JavaScript URL 函數的範例

➤ **若要使用 JavaScript URL 函數範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/functions/url/url.html

2. 將此範例中指定的規則新增 (若尚不存在) 至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

3. 重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 HTML 網頁

```
<html>
<body>
JavaScript URL Function Test Page
<br>
<script language="JavaScript">
<!--
function test(one,two,three)
{
alert(one + "##" + two + "##" +three);
}
test("/test.html","../test.html","123");
window.open("/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
</body>
</html>
```

規則

```
<Function type="URL" name="test" paramPatterns="y,y"/>

<Function type="URL" name="window.open" paramPatterns="y"/>
```

進行改寫後的 HTML 網頁

```
<html>

<body>

JavaScript URL Function Test Page

<br>

<script language="JavaScript">

<!--

function test(one,two,three)

{

alert(one + "##" + two + "##" +three);

}

test("/test.html","../test.html","123");

window.open("gateway-URL/portal-server-URL/index.html","gen",width=500,hei
ght=500);

//-->

</SCRIPT>

</body>

</html>
```

JavaScript EXPRESSION 函數的範例

➤ **若要使用 JavaScript EXPRESSION 函數範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/functions/expr/expr.html

2. 將此範例中指定的規則新增 (若尚不存在) 至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。

3. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

4. 重新啓動「閘道」：

   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start

進行改寫前的 HTML 網頁

```
<html>
<body>
JavaScript EXPRESSION Function Test Page
<br><br><br>
<script language="JavaScript">
<!--
function jstest2()
{
return ".html";
}
function jstest1(one)
{
return one;
}
var dir="/images/test"
var test1=jstest1(dir+"/test"+jstest2());
document.write("<a HREF="+test1+">Test</a>");
alert(test1);
//-->
</SCRIPT>
</body>
</html>
```

規則

```
<Function type="EXPRESSION" name="jstest1" paramPatterns="y"/>
```

進行改寫後的 HTML 網頁

```
<html>
<body>
JavaScript EXPRESSION Function Test Page
<br><br><br>
<script>
<!--
// various functions including psSRAPRewriter_convert_expression appear
here.
//-->
</SCRIPT>
<script language="JavaScript">
<!--
function jstest2()
{
return ".html";
}
function jstest1(one)
{
return one;
}
var dir="/images/test"
var
test1=jstest1(psSRAPRewriter_convert_expression(dir+"/test"+jste
st2()));
```

// 此規則指出函數 (EXPRESSION 類型) `jstest1` 中的第一個參數需要改寫。此表示式的值爲 `/test/images/test.html`。此值會被前置 Portal Server 與閘道 URL。

```
document.write("<a HREF="+test1+">Test</a>");
alert(test1);
//-->
</SCRIPT>
```

```
</body>
</html>
```

JavaScript DHTML 函數的範例

➤ **若要使用 JavaScript DHTML 函數範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/functions/dhtml/dhtml.html

2. 將此範例中指定的規則新增 (若尚不存在) 至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。

3. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

4. 重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 HTML 網頁

```
<html>
<head>
Testing JavaScript DHTML Functions
<br>
<br>
<script>
<!--
document.write('<a href="/index.html">write</a><BR>')
document.writeln('<a href="index.html">writeln</a><BR>')
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
//-->
</SCRIPT>
</head>
<body BGCOLOR=white>
<br><br>
```

```
Testing document.write and document.writeln

</body>

</html>
```

規則

```
<Function type="DHTML" name=" document.write" paramPatterns="y"/>

<Function type="DHTML" name=" document.writeln" paramPatterns="y"/>
```

進行改寫後的 HTML 網頁

```
<html>

<head>

Testing JavaScript DHTML Functions

<br>

<br>

<script>

<!--
```

`document.write('<a href="gateway-URL/portal-server-URL/index.html">write</a><BR>')`

// 第一個規則指出 DHTML JavaScript 函數 `document.write` 的第一個參數需要改寫。Rewriter 會將第一個參數識別爲一個簡單的 HTML 陳述式。在 `default_gateway_ruleset` 中的 HTML 規則部分具有規則 `<Attribute name="href" />`，此規則指出此陳述式需改寫。

`document.writeln('<a href="gateway-URL/portal-server-URL/rewriter/JavaScript/functions/dhtml/index.html">writeln</a><BR>')`

// 第二個規則指出 DHTML JavaScript 函數 `document.writeln` 的第一個參數需要改寫。Rewriter 會將第一個參數識別爲一個簡單的 HTML 陳述式。在 `default_gateway_ruleset` 中的 HTML 規則部分具有規則 `<Attribute name="href" />`，此規則指出此陳述式需改寫。

```
document.write("http://abc.sesta.com/index.html<BR>")

document.writeln("http://abc.sesta.com/index.html<BR>")
```

// 雖然 DHTML 規則識別出函數 `document.write` 與 `document.writeln`，但上述陳述式並未改寫。這是因爲這個情況下的第一個參數並非簡單 HTML。其可能是任何字串而 Rewriter 不知如何將之改寫。

```
//-->
</SCRIPT>
</head>
<body BGCOLOR=white>
<br><br>
Testing document.write and document.writeln
</body>
</html>
```

JavaScript DJS 函數的範例

➤ **若要使用 JavaScript DJS 函數範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/JavaScript/functions/djs/djs.html

2. 請確定您已於「閘道」服務的「網域與子網域的代理伺服器」清單中定義 `abc.sesta.com`。

   若未定義，則會採用直接連接，且不前置閘道 URL。

3. 將此範例中指定的規則新增 (若尚不存在) 至「改寫 JavaScript 來源的規則」部分的 `default_gateway_ruleset` 中。在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。

4. 重新啓動「閘道」：

   portal-server-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 HTML 網頁

```
<html>
Test for JavaScript DJS Functions
<br>
<script>
menu.addItem(new NavBarMenuItem("All Available
Information","JavaScript:top.location='http://abc.sesta.com'"));
//menu.addItem(new NavBarMenuItem("All Available
Information","http://abc.sesta.com"));
</script>
```

```
</html>
```

規則

```
<Function type="DJS" name="NavBarMenuItem" paramPatterns=",y"/>

<Variable type="URL" name=”top.location”/>
```

進行改寫後的 HTML 網頁

```
<html>

Testing JavaScript DJS Functions

<br>

<script>

menu.addItem(new NavBarMenuItem("All Available
Information","javaScript:top.location='gateway-URL/http://abc.se
sta.com'"));
```

// abc.sesta.com 是「閘道」服務的「網域與子網域的代理伺服器」清單中的一項。因此 Rewriter 需要改寫此 URL。但因其爲一絕對 URL，因此不需前置 Portal Server URL。DJS 規則指出 DJS 函數 NavBarMenuItem 的第二個參數需改寫。但是該函數的第二個參數又爲 JavaScript 變數。改寫此變數的值需要第二個規則。第二個規則指出 JavaScript 變數 top.location 的值需改寫。由於符合所有條件，因此改寫 URL。

```
//menu.addItem(new NavBarMenuItem("All Available
Information","http://abc.sesta.com"));
```

// 雖然 DJS 規則指出函數 NavBarMenuItem 的第二個規則需要改寫，但此陳述式中並未進行改寫。這是因爲 Rewriter 未將第二個參數識別爲簡單 HTML。

```
</script>

</html>
```

XML 屬性範例

➤ **若要使用 XML 屬性範例**

1. 您可自下列路徑存取此範例：

   portal-server-URL/rewriter/XML/attrib.html

2. 將此範例中指定的規則新增 (若尚不存在) 至「改寫 XML 來源的規則」部分的 default_gateway_ruleset 中。

3. 在 Identity Server 管理主控台「Portal Server 配置」中的「Rewriter 服務」中編輯 `default_gateway_ruleset`。
4. 重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n gateway-profile-name start`

進行改寫前的 XML

```
<html>
RW_START
<body>
<xml>
<baseroot href="/root.html"/>
</xml>
<xml>
<img href="image.html"/>
</xml>
<xml>
<string href="1234|substring.html"/>
</xml>
<xml>
<check href="1234|string.html"/>
</xml>
</body>
RW_END
</html>
```

規則

```
<Attribute name="href" tag="check" valuePatterns="1234|"/>
```

進行改寫後的 HTML

```
<html>

Rewriting starts

<br>

<br>

<body>

<xml><baseroot href="/root.html"/></xml>

<xml><img href="image.html"/></xml>

<xml><string href="1234|substring.html"/></xml>

<xml><check
href="1234|gateway-URL/portal-server-URL/rewriter/XML/string.html"/></xml>
```

// 改寫此陳述式是因爲其符合規則中所指定的條件。attribute name 是 href，tag 是 check，valuePatterns 則是 1234。在 valuePatterns 後面的字串會被改寫。有關 valuePatterns 的詳細資料，請參閱 「在規則中使用式樣匹配」(第 116 頁)。

```
</body>

Rewriting ends

</html>
```

案例研究

本節包括某範例郵件用戶端的來源 HTML 網頁。此案例研究並未囊括所有可能的情況與規則。這只是一個範例規則集，用以幫助您爲自己的內部網路網頁收集規則。

假設狀況

針對此案例研究訂出下列假設狀態：

- 郵件用戶端的基準 URL 假設爲 abc.siroe.com
- 閘道 URL 假設爲 gateway.sesta.com
- 位於「閘道」服務的「網域與子網域的代理伺服器」清單中的相關項目

範例網頁 1

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<!-- saved from
url=(0053)http://abc.siroe.com/mailclient/destin/?Cmd=navbar -->

<HTML XMLNS:WM><HEAD>

<META http-equiv=Content-Type content="text/html; CHARSET=utf-8">

<META http-equiv=Pragma content=no-cache>

<META http-equiv=Expires content=0><!--Copyright (c) 2000 Microsoft
Corporation.All rights reserved.--><!--CURRENT FILE== "IE5" "WIN32" navbar
-->

<STYLE>WM\:DROPMENU {

BEHAVIOR:url(http://abc.siroe.com/mailweb/controls/dropmenu.htc)

}

</STYLE>

<LINK href="destin_files/navbar.css" type=text/css rel=stylesheet>

<SCRIPT language=javascript>

var g_szUserBase= "http://abc.siroe.com/mailclient/destin"+"/";

var g_szFolder= ".";

var g_szVirtualRoot= "http://abc.siroe.com/mailweb";

var g_szImagePath= g_szVirtualRoot + "/img/";

</SCRIPT>

<SCRIPT src="/destin_files/navbar.js"></SCRIPT>

<META content="MSHTML 6.00.2600.0" name=GENERATOR></HEAD>

<BODY oncontextmenu=return(event.ctrlKey); onselectstart=return(false);

id=outbar_mainbody style="BACKGROUND-COLOR:appworkspace" leftMargin=0

topMargin=0 scroll=no>

<TABLE class=nbTableMain id=nbTableMain style="HEIGHT:100%" cellSpacing=0

cols=1 cellPadding=0 rows="2">

<TBODY>

<TR>

<TD class=treeBrand>
```

```
<DIV class=treeOFLOW><IMG
style="PADDING-RIGHT:0px; PADDING-LEFT:0px; PADDING-BOTTOM:0px;
PADDING-TOP:0px"
src="/destin_files/logo-ie5.gif" border=0></DIV></TD></TR>
<TR height="100%">
<TD>
<TABLE class=nbTable cellSpacing=0 cols=1 cellPadding=0 rows="4">
<TBODY>
<TR>
<TD class=nbFlybar id=show_navbar onkeydown=flybar_keydown()
onclick=ToggleTab(this.id) tabIndex=0 noWrap>
<DIV class=treeOFLOW>Shortcuts</DIV></TD></TR>
<TR style="HEIGHT: 100%">
<TD id=idOutbarpane style="TEXT-ALIGN:center" vAlign=top><A
id=inbox
href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents
&amp;Page=1"
target=viewer alt="Go to inbox"><IMG class=nbImage alt="Go to inbox"
src="destin_files/navbar-inbox.gif"></A>
<DIV class=nbLabel>Inbox</DIV><BR><A id=calendar
href="http://abc.siroe.com/mailclient/destin/Calendar/?Cmd=contents"
target=viewer alt="Go to calendar"><IMG class=nbImage
alt="Go to calendar" src="destin_files/navbar-calendar.gif"></A>
<DIV class=nbLabel>Calendar</DIV><BR><A id=contacts

href="http://abc.siroe.com/mailclient/destin/Contacts/?Cmd=contents"
target=viewer alt="Go to contacts"><IMG class=nbImage
alt="Go to contacts" src="destin_files/navbar-contacts.gif"></A>
<DIV class=nbLabel>Contacts</DIV><BR><A id=options
href="http://abc.siroe.com/mailclient/destin/?Cmd=options"
target=viewer alt="Go to options"><IMG class=nbImage
```

```
alt="Go to options" src="destin_files/navbar-options.gif"></A>
<DIV class=nbLabel>Options</DIV></TD></TR>
<TR style="HEIGHT:1.5em">
<TD class=nbFlybar id=show_folders onkeydown=flybar_keydown()
onclick=ToggleTab(this.id) tabIndex=0 noWrap>
<DIV class=treeOFLOW>Folders</DIV></TD></TR>
<TR>
<TD class=nbTreeProgress id=treeProgress style="DISPLAY:none"
vAlign=top noWrap><SPAN id=idLoading
style="OVERFLOW:hidden">Loading...</SPAN>
</TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE>
</BODY></HTML>
```

說明

表 3-3 顯示範例規則集與案例研究之間的對應關係。第一欄列出網頁內容；第二欄列出所套用的規則；第三欄顯示 Rewriter 輸出結果；第四欄說明套用規則的方式。

表 3-3 範例規則集與案例研究之間的對映

網頁內容	套用的規則	Rewriter 輸出	說明
`var g_szVirtualRoot="http://abc.siroe.com/mailweb";`	`<Variable name="URL"> g_szVirtualRoot </Variable>`	`var g_szVirtualRoot= "http://gateway.sesta.com/http://abc.siroe.com/mailweb";`	`g_szVirtualRoot` 是一個變數，其值為簡單 URL。 此規則告知 Rewriter 搜尋 URL 類型的 `g_szVirtualRoot` 變數。若網頁中有這類變數，則 Rewriter 會將之轉換為絕對 URL，然後前置閘道 URL。
`src="/destin_files/logo-ie5.gif"`	`<Attribute name="src" />`	`src="http://gateway.sesta.com/http://abc.siroe.com/destin_files/logo-ie5.gif`	src 是屬性名稱，未附有任何標記或 valuePattern。 此規則告知 Rewriter 搜尋所有名稱為 `src` 的屬性，然後改寫該屬性的值。

表 3-3 範例規則集與案例研究之間的對映

網頁內容	套用的規則	Rewriter 輸出	說明
`href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&amp;Page=1"`	`<Attribute name="href"/>`	`href="http://gateway.sesta.com/http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&amp;Page=1"`	href 是屬性名稱，未附有任何標記或 valuePattern。 此規則告知 Rewriter 搜尋所有名稱為 `href` 的屬性，然後改寫該屬性的值。

備註 套用規則集的優先順序爲 `hostname-subdomain-domain`。

例如，假設您的以網域爲基礎規則集清單中包含下列項目：

`sesta.com|ruleset1`

`eng.sesta.com|ruleset2`

`host1.eng.sesta.com|ruleset3`

`ruleset3` 可套用於所有位於 `host1` 的網頁。

`ruleset2` 可套用於所有位於 `eng` 子網域的網頁，從 `host1` 擷取的網頁除外。

`ruleset1` 可套用於 `sesta.com` 網域中的所有頁面，除了擷取於 `eng` 子網域與 `host1` 中的頁面。

5. 按一下頁面頂端或底部的「儲存」記錄變更。
6. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Outlook Web Access 的規則集

Secure Remote Access 支援位於 Sun ONE web server 及 IBM 應用程式伺服器上的 Outlook Web Access 2000 sp3。

➤ **若要配置 OWA 規則集**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁面。
4. 按一下您想要設定其屬性的「閘道」設定檔。

   顯示「閘道」- *gateway-profile-name* 頁面。
5. 在「URI 至規則集對映」欄位中，輸入安裝 Exchange 2000 的服務器名稱，隨後輸入 Exchange 2000 Service Pack 3 OWA 規則集。

   例如：

   exchange.domain.com|exchange_2000sp3_owa_ruleset。

6.x 與 3.0 規則集對映

下表列出 Sun ONE Portal Server, Secure Remote Access Rewriter 規則與前版 Sun™ ONE Portal Server 的對映關係。

表 3-4 SP4 規則對映

Rewriter 6.0 DTD 元素	**Rewriter 3.0 清單方塊名稱**
HTML 內容的規則	
屬性 - URL	Rewrite HTML Attributes
屬性 - DJS	Rewrite HTML Attributes containing JavaScript
表單	Rewrite Form Input Tag List
Applet	Rewrite Applet/Object Parameter Values List
JavaScript 內容的規則	
變數 - URL	Rewrite JavaScript Variables in URL
變數 - EXPRESSION	Rewrite JavaScript Variables Function
變數 - DHTML	Rewrite JavaScript Variables in HTML
變數 - DJS	Rewrite JavaScript Variables in JavaScript
變數 - SYSTEM	Rewrite JavaScript System Variables

表 3-4 SP4 規則對映 *(續上頁)*

Rewriter 6.0 DTD 元素	**Rewriter 3.0 清單方塊名稱**
函數 - URL	Rewrite JavaScript Function Parameters
函數 - EXPRESSION	Rewrite JavaScript Function Parameters Function
函數 - DHTML	Rewrite JavaScript Function Parameters in HTML
函數 - DJS	Rewrite JavaScript Function Parameters In JavaScript
XML 內容的規則	
屬性 - URL	Rewrite Attribute value of XML Document
標記文字	Rewrite Text data of XMl Document
CSS 內容的規則	
不需使用規則。依預設，所有 URL 皆會被轉譯	
WML 內容的規則	
未定義任何規則。按 HTML 處理 WML，並會套用 HTML 規則。	
WMLScript 內容的規則	
不支援 WML 程序檔	

第 4 章

NetFile

本章描述 NetFile 並詳細解釋其操作方法。若要配置 NetFile，請參閱第 10 章，第 263 頁的 「配置 NetFile」。

本章涵蓋下列主題：

NetFile 概要

NetFile 是一個檔案管理應用程式，可以讓使用者存取並操作遠端檔案系統和資料夾。

Sun™ ONE Portal Server，Secure Remote Access 的 NetFile 元件可像 Java1 和 Java2 applets 使用。瀏覽器沒有安裝 Java2 plugin 的使用者可以使用 Java1 applet。Java2 applet 有比較好的介面，同時增加了存取的便利性。

NetFile 提供了下列的主要功能：

- 便於新增或移除共享或資料夾
- 檔案上傳與下載
- 搜尋檔案和資料夾

- 使用 GZIP 和 ZIP 壓縮檔案
- 在 NetFile 環境中的郵件功能
- 儲存目前 NetFile 階段作業的資訊

若要配置 NetFile，請參閱第 10 章，「配置 NetFile」。

支援檔案存取協定

NetFile 讓您可以使用 FTP、SMB (Windows) 和 NFS 協定以存取遠端系統。其中包含下列檔案存取協定功能：

- 如果使用者指定 AUTODETECT 新增系統，NetFile 會使用下列順序以自動偵測要使用的協定。
  - 檢查在 21 連接埠上的 FTP 伺服器。如果 FTP 的回應包含 「NetWare」字串，則被視爲是一個 NETWARE 主機。
  - 在 2049 埠上檢查 NFS 伺服器的主機。
  - 如果上述操作都失敗，會顯示訊息告訴您無法確定主機類型。

  第一個偵測到的檔案系統類型將用於連接所請求的主機。主機偵測順序可以在 Identity Server 管理主控台中變更。

備註 如果伺服器在非標準的連接埠上執行，連線會失敗。

- NetFile 允許使用者任意選擇檔案伺服器 / 系統協定。

  支援這些協定的平台 / 伺服器列於下表。

表 4-1 檔案系統和支援的協定

檔案系統 / 協定	平台
NFS	Solaris 2.6 和更高版本
SMB	Windows 95/98/NT/2000/ME/XP

表 4-1 檔案系統和支援的協定

檔案系統 / 協定	平台
FTP	在 Novell Netware 上的 Novell FTP 5.1 Server 在 Win NT 4.0 上的 MS FTP Server 4.0 在 Win NT 2000 上的 MS FTP Server 5.0 Solaris FTP Server WU_FTP 2.6.1 ProFTPD 1.2.8 vsFTPd 1.2.0

備註 僅能透過 FTP 支援 Novell Netware，而不能透過本地存取支援。

備註 若要使用 NetFile 上傳檔案至 ProFTPD server，必須將執行 ProFTPD server 的主機上的 `proftpd.conf` 檔案的「AllowStoreRestart」設定爲「on」。

啓用存取 NetFile

安裝 Secure Remote Access 時，僅會爲您在安裝過程中所指定的組織註冊 NetFile 服務。

➤ **爲組織和使用者啓用 NetFile**

1. 註冊 NetFile 服務至需要存取 NetFile 的組織。
2. 建立以 NetFile 服務爲基礎的 NetFile 策略，並指定 NetFile 策略給需要存取 NetFile 的組織與角色。
3. 指定 NetFile 服務給每個需要存取 NetFile 的使用者。

   更多關於建立和指定策略與服務的資訊，請參閱 *Sun ONE Identity Server 管理員指南*。

爲 NetFile 啓用記錄

使用 Identity Server 記錄服務指定記錄的位置，以啓用 NetFile 記錄。日誌檔的名稱是 srapNetFile。在預設情況下，日誌檔會在 /var/opt/SUNWam/logs 目錄中。

配置 Unix 認證

您需要在 Portal Server 上配置 Unix 認證常駐程式，以存取 NFS 系統。

➤ **若要配置 Unix 認證**

1. 在配置連接埠上遠程登入本機主機，操作如下：

   ```
   telnet localhost 58946
   ```

2. 輸入 Unix 說明程式偵聽連接埠號。

   指定預設值 57946 給偵聽連接埠。

3. 以秒爲單位輸入 Unix 說明程式階段作業逾時值。

4. 輸入 Unix 說明程式最大階段作業值。

   會顯示「amunixd 配置成功」訊息。

自訂 NetFile

您可以在 NetFile 提供者和 NetFile 服務的管理主控台中，自訂顯示於訊息視窗的文字。

- 在 NetFile 提供者中，請修改：

  portal-server-install-root/SUNWam/locale/srapNetFileProvider.properties

- 在 Identity Server 管理主控台上的 NetFile 服務，請修改：

  portal-server-install-root/SUNWam/locale/srapNetFile.properties

第 5 章

Netlet

本章會介紹如何使用 Netlet 在使用者遠端桌面以及在您的企業內部網站中執行應用程式的伺服器之間，以安全的方式執行應用程式。若要配置 Netlet，請參閱第 11 章，第 281 頁的「配置 Netlet」。

本章涵蓋下列主題：

Netlet 概要

Sun™ ONE Portal Server 軟體使用者可能希望在他們的遠端桌面上，以安全的方式執行最常使用或公司特定的應用程式。在您的平台上設定 Netlet 之後，您就可以安全存取這些應用程式。

Netlet 可以讓使用者在不安全的網路上 (例如網際網路) 安全地執行共同的 TCP/IP 服務。您可以執行 TCP/IP 應用程式 (例如 Telnet 和 SMTP)、HTTP 應用程式以及任何固定的連接埠應用程式。

在下列情況下，您可以在 Netlet 上執行應用程式：

- 它是以 TCP/IP 爲基礎的。

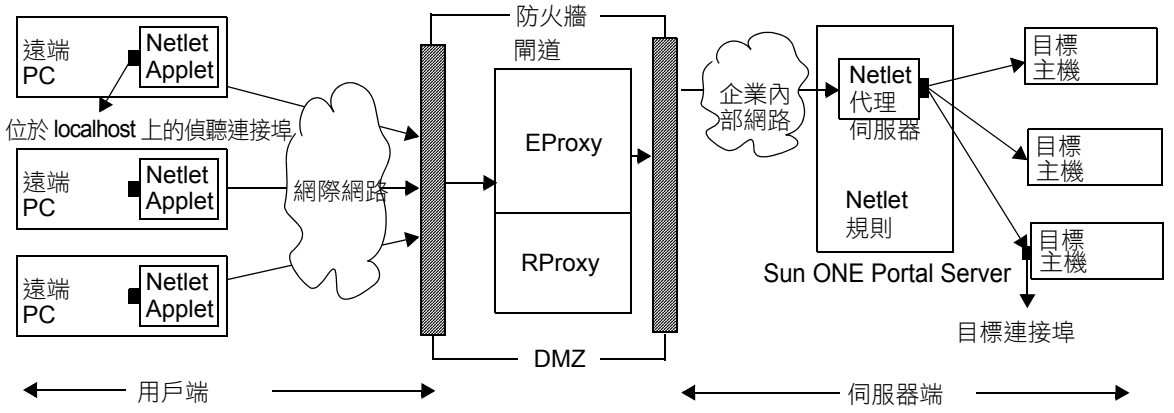
- 它使用固定連接埠。

備註 只有在使用 FTP 時才支援動態連接埠。若要使用 Microsoft Exchange，請使用 OWA (Outlook Web Access)。

Netlet 元件

Netlet 所使用的各種元件會顯示在圖 5-1 中。

圖 5-1 Netlet 元件



位於 localhost 上的偵聽連接埠

此爲用戶端機器上 Netlet applet 偵聽的連接埠。用戶端機器爲 localhost。

Netlet Applet

Netlet applet 負責在遠端用戶端機器和企業內部應用程式 (例如 Telnet、Graphon 或 Citrix) 之間設定加密的 TCP/IP 通道。Applet 會將封包加密並將它們傳送至「閘道」，並將來自 「閘道」的回應封包解密，然後將它們傳送至本機的應用程式。

對於靜態規則，當使用者登入入口網站時，會自動下載 Netlet applet。對於動態規則，會在使用者在相對應的動態規則連結上按一下時，下載 applet。有關靜態和動態規則的詳細資訊，請參閱第 173 頁的「規則類型」。

若要在 Sun Ray Environment 中執行 Netlet，請參閱第 186 頁的「在 Sun Ray Environment 中執行 Netlet」。

Netlet 規則

Netlet 規則會將需要在用戶端機器上執行的應用程式映射至相應的目標伺服器。這表示 Netlet 只會在已傳送至連接埠 (於 Netlet 規則中定義) 的封包上運作。這可確保取得較大的安全性。

作爲管理員，您需要爲 Netlet 的功能運作配置一些規則。這些規則指定了各種詳細信息，例如要使用的加密、要呼叫的 URL、要下載的 applet、目標連接埠以及目標主機。當用戶端機器上的使用者透過 Netlet 提出請求時，這些規則會協助確定如何建立連線。有關詳細資料，請參閱第 170 頁的「定義 Netlet 規則」。

Netlet 提供者

此爲 Netlet 的 UI 元件。提供者允許使用者透過 Sun ONE™ Portal Server 桌面配置必要的應用程式。會在提供者中建立連結，而使用者按一下連結以執行必要的應用程式。使用者也可以將桌面中動態規則的目標主機指定爲 Netlet 提供者。請參閱第 170 頁的「定義 Netlet 規則」。

EProxy

所有用戶端請求會透過 EProxy 傳送。EProxy 僅會處理 Netlet 請求，並會將任何其它請求傳送至 RProxy。EProxy 會剖析 Netlet 請求並將它們傳送至 Netlet 代理伺服器 (如果有啓用) 或直接傳送至目標主機。

Netlet 代理伺服器 (選擇性)

「閘道」可確保爲遠端用戶端機器以及「閘道」之間提供一條安全通道。Netlet 代理伺服器爲選用選項，您可以在安裝時選擇不安裝此代理伺服器。有關 Netlet 代理伺服器的資訊，請參閱第 50 頁的「使用網路代理伺服器」。

目標連接埠

此連接埠爲目標應用程式伺服器將用於偵聽的連接埠。

Netlet 使用方案

使用 Netlet 將會順序發生下列事件：

1. 遠端使用者登入至 Sun ONE™ Portal Server 桌面。

2. 如果已經爲使用者、角色或組織定義靜態 Netlet 規則，則將會自動下載 Netlet applet 至遠端用戶端。

   如果已經爲使用者、角色或組織定義動態規則，則使用者需要在 Netlet 提供者中配置必要的應用程式。當使用者按一下 Netlet 提供者中的應用程式連結時，將會下載 Netlet applet。有關靜態和動態規則的詳細資訊，請參閱第 170 頁的「定義 Netlet 規則」。

3. Netlet 會偵聽在 Netlet 規則中定義的用戶端連接埠。

4. Netlet 會通過 Netlet 規則中指定的連接埠，設定遠端用戶端與伺服器之間的通道。

使用 Netlet

爲了使 Netlet 在運作時能夠符合不同組織中各種使用者的需要，您必須執行下列動作：

1. 依據使用者需求確定是否需要建立靜態或動態規則。請參閱第 173 頁的「規則類型」。

2. 從 Identity Server 管理主控台上的「服務配置」標籤中，定義 Netlet 範本中的全域選項。請參閱第 11 章，第 281 頁的「配置 Netlet」。

3. 確定規則是否以組織、角色或使用者爲基礎，並視需要在每個層級中做出修改。有關組織、角色和使用者的詳細資訊，請參閱 *Sun ONE Portal Server* 管理員指南。

定義 Netlet 規則

Netlet 配置是透過 Netlet 規則定義，其中 Netlet 規則是在 Identity Server 管理主控台中「SRA 配置」區段底下進行配置。可爲組織、角色或使用者配置 Netlet 規則。如果 Netlet 規則用於角色或使用者，請在選取組織之後選取想要的角色或使用者。

Netlet 規則由下列欄位所組成：

- 規則名稱
- 加密密碼
- URL
- 下載 Applet
- 延伸階段作業

- 用戶端連接埠
- 目標主機
- 目標連接埠

注意 Netlet 規則不支援多位元組輸入。請勿在 Netlet 規則中的任何可編輯欄位中指定多位元組字元。

Netlet 規則中不能包含任何高於 64000 的連接埠號。

表 5-1 會列出 Netlet 規則中的欄位。表 5-1 有三欄。第一欄列出欄位名稱。第二欄說明欄位，及其在 Netlet 規則中的功能。第三欄則列出了該特定欄位中可能的值。

表 5-1 Netlet 規則中的欄位

參數	說明	值
規則名稱	指定此 Netlet 規則的名稱。您需要為每個規則指定唯一的名稱。如此當您在定義使用者存取特定規則時將會非常有用。有關詳細資料，請參閱第 291 頁的「定義存取 Netlet 規則」。	
加密密碼	定義加密密碼，或是指定使用者可從中選擇的密碼清單。	您選取的密碼將會在 Netlet 提供者中以清單的形式出現。使用者可以從清單中選擇需要的密碼。 預設 - 會使用 Netlet 管理主控台中指定的「預設 VM 原生密碼」和「預設 Java Plugin 密碼」。
URL	指定當使用者按一下 Netlet 提供者中的相關連結時，瀏覽器所開啟的 URL。瀏覽器會開啟應用程式的視窗，並連接至稍後在規則中指定的本機連接埠號的 `localhost`。 您需要指定一個相對的 URL。	Netlet 規則所呼叫之應用程式的 URL。例如，`telnet://localhost:30000`。 如果應用程式使用 applet 來呼叫應用程式，則指定一個 URL。 `null` – 如果應用程式不是由 URL 所啟動，或者不是被桌面所控制時，您所設定的欄位值。它一般適用於非以網路為基礎的應用程式。

表 5-1 Netlet 規則中的欄位

參數	說明	值
下載 Applet	指出是否需要為此規則下載 applet。	False - 不下載 applet。 True - 使用回送連接埠從 Portal Server 機器中下載 applet。 以 *clientport:server:serverport* 格式詳細指定 applet，其中： • *clientport* 表示用戶端上的目標連接埠。此連接埠必須與預設的回送連接埠不同。有關詳細資料，請參閱第 11 章，「配置 Netlet」。為每個規則指定唯一的 `client port`。 • *server* 是會從該處下載 applet 的伺服器名稱。 • *serverport* 代表伺服器上用來下載 applet 的連接埠。 如果要下載 applet，而且未指定伺服器，則會從 Portal Server 主機下載 applet。
延伸階段作業	此將控制 Netlet 為作用中時 Portal Server 階段作業的閒置逾時。	Enabled - 僅在 Netlet 為作用中且入口網站應用程式的其餘部分為閒置時，需要設置為這個值以保持入口網站階段作業作用中。 Disabled - 即使在 Netlet 應用程式為作用中但入口網站應用程式為閒置的情況下，階段作業閒置時間逾時則入口網站階段作業閒置時間愈時。
用戶端連接埠	Netlet 偵聽之用戶端上的連接埠。	*clientport* 的值必須唯一。您不能夠在一個以上的規則中指定某特定的連接埠號。 如果您要為多個連線指定多個主機，請指定多個用戶端連接埠。有關語法的資訊，請參閱第 178 頁的「包含多個主機連線的靜態規則」。 對於 FTP 規則，用戶端連接埠值必須為 30021。

表 5-1 Netlet 規則中的欄位

參數	說明	值
目標主機	Netlet 連線的接收者。	*host* - 接收 Netlet 連線的主機名稱。此欄位用於靜態規則。使用簡單的主機名稱 (例如 `siroe`) 或完全合格的 DNS 式主機名稱 (例如 `siroe.mycompany.com`)。您可以指定多個主機以： • 與每個指定主機建立連線。您需要為每個指定的主機指定相對應的用戶端以及目標連接埠。有關語法的資訊，請參閱第 178 頁的「包含多個主機連線的靜態規則」。 • 嘗試連接至指定主機清單中任何可用的主機。有關語法的資訊，請參閱第 179 頁的「選擇多個主機的靜態規則」。 TARGET - 在語法中指定 TARGET 的規則為動態規則。TARGET 表示一般使用者能夠在桌面的 Netlet 提供者中指定一台或多台必要的目標主機。 在單個規則中，不可以同時有靜態主機和 TARGET。
目標連接埠	目標主機上的連接埠	除了主機與目標以外，您必須指定目標連接埠。 您可以在有多個目標主機的情況下，指定多個目標連接埠。以下列格式指定多個連接埠：`port1+port2+port3-port4+port5`。 連接埠號之間的加號 (+) 指出供單一目標主機使用的替代連接埠。 連接埠號之間的減號 (-) 為不同目標主機連接埠號的分隔符號。 Netlet 在此會嘗試依序使用 `port1`、`port2` 和 `port3` 連接至指定的第一台目標主機。如果此項操作失敗，Netlet 會嘗試以 `port4` 和 `port5` 依次連接至第二台主機。 您只可以為靜態規則配置多個連接埠。

規則類型

根據規則中指定目標主機的方式，Netlet 規則類型有兩種。

靜態規則

靜態規則會將目標主機作爲規則的一部分指定。如果您建立一項靜態規則，使用者將無法指定需要的目標主機。在下列範例中，`sesta` 爲目標主機。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
ftpstatic	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30021	sesta	21

您可以爲靜態規則配置多個目標主機和連接埠。有關範例，請參閱第 178 頁的「包含多個主機連線的靜態規則」。

動態規則

在動態規則中，不會將目標主機作爲規則的一部分指定。使用者可以在 Netlet 提供者中指定必要的目標主機。在下列範例中，TARGET 爲目標主機的萬用字元。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
ftpdynamic	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30021	TARGET	21

加密密碼

根據加密密碼，可進一步將 Netlet 規則依如下分類：

- **使用者可配置加密規則** - 在本規則中，您可以指定一個密碼清單，讓使用者可以從中選擇。這些選擇性密碼會在 Netlet 提供者中以清單的形式出現。使用者可以從清單中選擇必要的密碼。在下列範例中，使用者可以從多個密碼中作出選擇。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
Telnet	SSL_RSA_WITH_RC4_128_SHA SSL_RSA_WITH_RC4_128_MD5	null	false	true	30000	TARGET	23

備註 雖然 Portal Server 主機可能已經啓用不同的密碼，但是使用者僅能從配置爲 Netlet 規則部分的清單中選擇。

有關 Netlet 支援的密碼清單以及相對應的關鍵字，請參閱第 175 頁的「支援的密碼」。

- **管理員配置的密碼規則** - 在本規則中，密碼已被定義爲 Netlet 規則的一部分。使用者無法選擇必要的密碼。在下列的範例中，已經將密碼配置爲 SSL_RSA_WITH_RC4_128_MD5。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
Telnet	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30000	TARGET	23

有關 Netlet 支援的密碼清單以及相對應的關鍵字，請參閱第 175 頁的「支援的密碼」。

支援的密碼

表 5-2 在第一欄中列出了 Netlet 支援的密碼，而在第二欄中列出用於與密碼關聯的關鍵字。使用相對應的關鍵字來指定 Netlet 規則中的密碼。

表 5-2 支援的密碼清單

密碼	關鍵字
原生 VM 密碼	
KSSL_SSL3_RSA_WITH_3DES_EDE_CBC_SHA	
KSSL_SSL3_RSA_WITH_RC4_128_MD5	
KSSL_SSL3_RSA_WITH_RC4_128_SHA	
KSSL_SSL3_RSA_EXPORT_WITH_RC4_40_MD5	
KSSL_SSL3_RSA_WITH_DES_CBC_SHA	
Java Plugin 密碼	
SSL_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_RSA_WITH_RC4_128_MD5	

表 5-2 支援的密碼清單

密碼	關鍵字
SSL_RSA_WITH_RC4_128_SHA	
SSL_RSA_EXPORT_WITH_RC4_40_MD5	
SSL_RSA_WITH_DES_CBC_SHA	
SSL_RSA_WITH_NULL_MD5	

向下相容性

先前的 Portal Server 版本並不支援將密碼作爲 Netlet 規則的一部分。爲了向下相容不含密碼的現有規則，規則會使用預設的密碼。不含密碼的現有規則如下：

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
Telnet		telnet://localhost:30000	false	true	30000	TARGET	23

將被解譯爲：

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
Telnet	預設密碼	telnet://localhost:30000	false	true	30000	TARGET	23

這類似於「加密密碼」欄位已選擇爲「預設」的「管理員配置的規則」。有關詳細資料，請參閱第 286 頁的「指定預設加密密碼」。

* loopback 在系統內部使用。

備註 Netlet 規則中不能包含任何高於 64000 的連接埠號。

Netlet 規則範例

本節包括一些 Netlet 規則的範例，以說明 Netlet 的語法。

- 基本靜態規則
- 包含多個主機連線的靜態規則
- 呼叫 URL 的動態規則
- 下載 Applet 的動態規則

基本靜態規則

本規則支援從用戶端至機器 `sesta` 的 Telnet 連線。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
myrule	SSL_RSA_WITH_RC4_128_MD5	null	false	true	1111	sesta	23

其中

`myrule` 爲規則的名稱。

SSL_RSA_WITH_RC4_128_MD5 表示要使用的密碼。

`null` 表示此應用程式不是由 URL 所啓動或透過桌面執行。

`false` 表示用戶端並不會下載 applet 以執行此應用程式。

`true` 表示當 Netlet 連線在作用中的情況下 Portal Server 不應逾時。

`1111` 爲用戶端上的連接埠，Netlet 會在此偵聽來自目標主機的連線請求。

`sesta` 是 Telnet 連線上接收者主機的名稱。

`23` 是目標主機上用於連線的連接埠號，在本例中即爲已知的 Telnet 連接埠。

桌面 Netlet 提供者並不會顯示連結，但是 Netlet 會自動在指定的連接埠 (`1111`) 上啓動與偵聽。指示使用者啓動用戶端軟體—此情形中爲連接至 `localhost` 的 Telnet 階段作業。

例如，如果要啓動 Telnet 階段作業，用戶端需要在終端機 UNIX 指令行中鍵入下列字元：

```
telnet localhost 1111
```

包含多個主機連線的靜態規則

本規則支援從用戶端至兩台機器，即 `sesta` 和 `siroe` 的 Telnet 連線。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
myrule	SSL_RSA_WITH_RC4_128_MD5	null	false	true	1111	sesta	23
					1234	siroe	23

其中

23 是目標主機上用於連線的的連接埠號 － Telnet 的保留連接埠。

1111 爲用戶端上的連接埠，Netlet 會在此偵聽來自第一個目標主機 `sesta` 的連線請求。

1234 爲用戶端上的連接埠，Netlet 會在此偵聽來自第二個目標主機 `siroe` 的連線請求。

本規則中前六個欄位與在第 177 頁的「基本靜態規則」中介紹的欄位相同。差別在於有三個欄位用於識別第二個目標主機。

當您在規則中新增額外的目標，您必須爲每個新的目標主機新增三個欄位：`client port`、`target host` 和 `target port`。

備註 您可以有多組此三個欄位，以描述與每個目標主機的連線。如果遠端用戶端是以 UNIX 爲基礎，則不可以使用低於 2048 的偵聽連接埠號，原因是數字較低的連接埠將會受到限制，並且您必須是超級使用者才能夠啓動偵聽程式。

此規則的作用與先前的規則相同。Netlet 提供者並不顯示任何連結，但是 Netlet 會自動在指定的兩個連接埠 (1234) 上啓動與偵聽。使用者需要啓動用戶端軟體，此情形中爲連接至連接埠 1111 或連接至連接埠 1234 (主機範例 2) 上 `localhost` 的 Telnet 階段作業。

選擇多個主機的靜態規則

使用此規則以指定多個替代主機。如果與規則中第一個主機的連線失敗，Netlet 會嘗試連接指定的第二個主機，以此類推。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
gojoe	SSL_RSA_WITH_RC4_128_MD5	/gojoe.html	8000:gojoeserver:8080	true	10491	siroe+sesta	35+26+491-35+491

其中

`10491` 爲用戶端上的連接埠，Netlet 會在此偵聽來自目標主機的連線請求。

Netlet 會嘗試以相同順序，在連接埠 `35`、`26` 和 `491` 上建立與 `siroe` 的連線，視何者可用而定。

如果無法建立與 `siroe` 的連線，Netlet 會嘗試以相同順序連接連接埠 `35` 和 `491` 上的 `sesta`。

主機之間的加號 (+) 表示替代的主機。

連接埠號之間的加號 (+) 指出用於單一目標主機的替代連接埠。

連接埠號之間的減號 (-) 爲不同目標主機連接埠號的分隔符號。

呼叫 URL 的動態規則

此規則可以讓使用者配置必要的目標主機，讓使用者可以通過 Netlet 遠程登入不同主機。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
myrule	SSL_RSA_WITH_RC4_128_MD5	telnet://localhost:30000	false	true	30000	TARGET	23

其中

`myrule` 爲規則的名稱。

SSL_RSA_WITH_RC4_128_MD5 表示要使用的密碼。

`telnet://localhost:30000` 爲規則所呼叫的 URL。

`false` 表示將不會下載任何 applet。

`true` 表示當 Netlet 連線在作用中的情況下 Portal Server 不應逾時。

`30000` 爲用戶端上的連接埠，Netlet 會在此偵聽此規則的連線需求。

`TARGET` 表示使用者需要使用 Netlet 提供者配置目標伺服器。

`23` 是 Netlet 開啓的目標主機上的連接埠，在本例中爲已知的 Telnet 連接埠。

➤ 若要在新增規則之後執行 Netlet

在新增規則之後，使用者必須完成某些步驟，使得 Netlet 能夠如預期般執行。使用者需要在用戶端執行下列動作：

1. 在 Portal Server 桌面的 Netlet 提供者區段中，按一下「編輯」。

   新的 Netlet 規則會列在「新增新目標」區段中的「規則名稱」底下。

2. 變更規則名稱，然後鍵入目標主機的名稱。
3. 儲存變更。

   使用者會返回桌面，此時您可以在 Netlet 提供者區段中看見此新連結。

4. 按一下新連結。

   會啓動一個新的瀏覽器，並進至 Netlet 規則中所提供的 URL。

備註 透過重複上述步驟，您可以在相同的規則中新增一個以上的目標主機。

下載 Applet 的動態規則

本規則定義從用戶端至動態配置的主機之間的 GO-Joe 連線。規則會從 applet 所在的伺服器上將 GO-Joe applet 下載至用戶端。

規則名稱	加密密碼	URL	下載 Applet	延伸階段作業	用戶端連接埠	目標主機	目標連接埠
gojoe	SSL_RSA_WITH_RC4_128_MD5	/gojoe.html	8000:gojoeserve:8080	true	3399	TARGET	58

其中

gojoe 是規則的名稱。

SSL_RSA_WITH_RC4_128_MD5 表示要使用的密碼。

例如 /gojoe.html 是包含 applet 的 HTML 頁面的路徑，路徑應與部署入口網站的網路容器的說明文件根目錄是相對的。

8000:server:8080 表示連接埠 8000 是用戶端上用來接收 applet 的目標連接埠，gojoeserve 是提供 applet 的伺服器名稱，而 8080 則是伺服器上的連接埠，applet 則從該處下載。

表示當 Netlet 連線在作用中的情況下 Portal Server 不應逾時。

3399 爲用戶端上的連接埠，Netlet 會在此偵聽此類型的連線請求。

TARGET 表示需要使用 Netlet 提供者，由使用者進行配置的目標伺服器。

58 爲 Netlet 所開啓的目標伺服器上的連接埠，在本例中爲 GoJoe 的連接埠。連接埠 58 爲目標主機偵聽其本身通訊的連接埠。Netlet 會將資訊從新的 applet 傳送至此連接埠。

Netlet 規則範例

表 5-3 列出某些共用應用程式中的範例 Netlet 規則。

表格中有 7 欄，與 Netlet 規則的下列欄位相對應。規則名稱、URL、下載 Applet、用戶端連接埠、目標主機、目標連接埠。最後一欄包含規則的說明。

備註 表 5-3 並不會列出 Netlet 規則的「密碼」和「延伸階段作業」欄位。假設提供的範例中這兩個欄位是 "SSL_RSA_WITH_RC4_128_MD5" 和 "true"。

表 5-3 Netlet 規則範例

規則	URL	下載 Applet	用戶端連接埠	目標主機	目標連接埠	說明
IMAP	null	false	10143	imapserver	143	用戶端中的 Netlet `client port` 不需要和伺服器端上的 `target port` 相同。如果您使用任何標準 IMAP 和 SMTP 連接埠以外的連接埠，請確定已將用戶端配置為可在不同於標準連接埠的連接埠上進行連接。 Solaris 用戶端使用者在連接至連接埠號低於 1024 的號碼時會遇到問題，除非他們是以超級使用者的身份來執行。
SMTP	null	false	10025	smtpserver	25	
Lotus Web Client	null	false	80	lotus-server	80	本規則會告知 Netlet 偵聽連接埠 80 上的用戶端，並連接至 lotus 伺服器－連接埠 80 上的伺服器。Lotus Web Client 的一個需求是用戶端偵聽連接埠必須與伺服器連接埠相符。
Lotus Notes 非 Web Client	null	false	1352	lotus-domino	1352	利用此規則，Lotus Notes 用戶端可以透過 Netlet 連接至 Lotus Domino 伺服器。可確保當用戶端嘗試連接至伺服器時，它一定不會指向 `localhost` 作為伺服器名稱。它必須指向 Lotus Domino 伺服器實際的伺服器名稱。伺服器名稱必須與伺服器的系統名稱相同。在使用 Netlet 時，用戶端必須將該名稱解析為 `127.0.0.1`。實現這個動作的方法有兩種： • 將伺服器名稱設定為指向用戶端主機表中的 `127.0.0.1`。 • 將指向 `127.0.0.1` 的伺服器名稱的 DNS 項目匯出。 伺服器名稱必須和在設定期間用來配置 Domino 伺服器的伺服器名稱相同。

表 5-3 Netlet 規則範例

規則	URL	下載 Applet	用戶端連接埠	目標主機	目標連接埠	說明
Microsoft Outlook 和 Exchange Server 這個無法作用於 Windows NT、2000 與 XP。在 Windows NT、2000 與 XP 中，請透過 Rewriter 使用 Outlook Web Access	null	false	135	exchange	135	此規則可告知 Netlet 偵聽用戶端上的連接埠 135，並連接至連接埠 135 上的伺服器 `exchange`。Outlook 用戶端會使用此連接埠與 Exchange 伺服器嘗試初始連絡，並決定與伺服器溝通所使用的後續連接埠。 在用戶端機器上： • 使用者必須將已經在 Outlook 用戶端中進行配置的 Exchange 伺服器的主機名稱變更為 `localhost`。此選項的位置會因為 Outlook 的版本而有所差異。 • 使用者必須使用主機檔案將 Exchange 伺服器的主機名稱 (單一和完全合格) 映射至 IP 位址 `127.0.0.1`。 • 在 Windows 95 或 98 中，檔案位於 `\Windows\Hosts` • 在 Windows NT4 中，檔案位於 `\WinNT\System32\drivers\etc\Hosts`。 項目的外觀如下： `127.0.0.1 exchange exchange.company.com` Exchange 伺服器會將它自己的名稱傳回 Outlook 用戶端。此項映射可確保 Outlook 用戶端是使用 Netlet 用戶端連接回伺服器。
FTP	null	false	30021	*your-ftp_server.your-domain*	21	您可以使用受控制的一般使用者帳戶提供 FTP 服務至單一的 FTP 伺服器。如此可確保遠端的 FTP 可從一般使用者系統安全傳輸至單一位置。如果沒有使用者名稱，FTP URL 會被解譯為匿名的 FTP 連線。 您*必須*將連接埠 30021 定義為您 Netlet FTP 規則的用戶端連接埠。 使用 Netlet 連線時並不支援動態 FTP。

表 5-3 Netlet 規則範例

規則	URL	下載 Applet	用戶端連接埠	目標主機	目標連接埠	說明
Netscape 4.7 Mail Client	null	false	30143, 30025.	TARGET TARGET	10143 10025	在 Netscape 用戶端中，使用者需要： 為 IMAP 或收到的郵件指定 `localhost:30143` 為 SMTP 或外送的郵件指定 `localhost:30025`
Graphon	third_party/xsession_start.html	true	10491	TARGET	491	此為透過 Netlet 用於存取 Graphon 的規則。`xsession_start.html` 亦包含於 Graphon 中。
Citrix	third_party/citrix_start.html	true	1494	TARGET	1494	此為透過 Netlet 用於存取 Citrix 的規則。`citrix_start.html` 亦包含於 Citrix 中。
Remote Control	third_party/pca_start.html	true	5631 5632	TARGET TARGET	5631 5632	此為透過 Netlet 用於存取 Remote Control 的規則。`pca_start.html` 亦包含於 Remote Control 中。

啓用 Netlet 記錄

您可以啓用「閘道」服務中記錄 Netlet 相關活動的選項。請參閱第 262 頁的「啓用 Netlet 記錄」。Identity Server 配置屬性記錄區段的「記錄位置」屬性中指定有目錄，系統將在其中建立日誌檔。此日誌檔名稱有下列慣例：

`srapNetlet_`*gateway hostname_gateway-profile-name*

Netlet 日誌會擷取下列資訊：

- 啓動時間
- 源位址
- 源連接埠
- 伺服器位址
- 伺服器連接埠

- 停止時間
- 狀態 (啓動或停止)

登出時終止 Netlet

若要在使用者登出時終止 Netlet，「閘道」必須要從 Portal Server 獲得階段作業通知。若要獲得通知，請執行下列動作：

1. 新增此行：

   `com.iplanet.am.jassproxy.trustAllServerCerts=true`

   至下列的屬性檔中：

   Portal Server 上的 *portal-server-install-root*`/SUNWam/lib/AMConfig.properties`。

2. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

3. 重新啓動 Portal Server (網路伺服器或應用程式伺服器)。

自訂 Netlet

您可以在 Netlet 提供者和 Netlet 服務的管理主控台中自訂顯示於訊息視窗中的文字。

- 在 Netlet 提供者中，請修改：

  portal-server-install-root`/SUNWam/locale/srapNetletProvider.properties`

- 對於 Identity Server 管理主控台中的 Netlet 服務，請修改：

  portal-server-install-root`/SUNWam/locale/srapNetlet.properties`

- 對於 Netlet servlet，請修改：

  portal-server-install-root`/SUNWam/locale/srapNetletServlet.properties`

- 對於 Netlet applet，請修改：

  portal-server-install-root`/SUNWam/locale/srapNetletApplet.properties`

在 Sun Ray Environment 中執行 Netlet

如果您希望執行的應用程式將 applet 下載至 Sun Ray 環境中的用戶端機器上，您需要變更 HTML 檔。以下是一個範例檔案，您可以透過該檔案瞭解必須執行的修改。

新的 HTML 檔

```
<!-- @(#)citrix_start.html 2.1     98/08/17 Copyright (c) 1998 i-Planet, Inc., All rights reserved.  -->

<html>

<script language="JavaScript">

var KEY_VALUES;  // KEY_VALUES['key'] = 'value';

function retrieveKeyValues() {

      KEY_VALUES = new Object();

      var queryString  = '' + this.location;

      queryString = unescape(queryString);

      queryString = queryString.substring((queryString.indexOf('?')) + 1);

      if (queryString.length < 1) {

          return false; }

      var keypairs = new Object();

      var numKP = 0;

      while (queryString.indexOf('&') > -1) {

        keypairs[numKP] = queryString.substring(0,queryString.indexOf('&'));

        queryString = queryString.substring((queryString.indexOf('&')) + 1);

        numKP++;

      }

      // Store what's left in the query string as the final keypairs[] data.

      keypairs[numKP++] = queryString;

      var keyName;

      var keyValue;

      for (var i=0; i < numKP; ++i) {
```

```
        keyName = keypairs[i].substring(0,keypairs[i].indexOf('='));
        keyValue = keypairs[i].substring((keypairs[i].indexOf('=')) + 1);
        while (keyValue.indexOf('+') > -1) {
          keyValue = keyValue.substring(0,keyValue.indexOf('+')) + ' ' +
keyValue.substring(keyValue.indexOf('+') + 1);
        }
        keyValue = unescape(keyValue);
          // Unescape non-alphanumerics
        KEY_VALUES[keyName] = keyValue;
      }
}
function getClientPort(serverPort) {
    var keyName = "clientPort['" + serverPort +"']";
    return KEY_VALUES[keyName];
}
function generateContent() {
    retrieveKeyValues();
    var newContent =
        "<html>\n"
          + "<head></head>\n"
          + "<body>\n"
          + "<applet code=\"com.citrix.JICA.class\" archive=\"JICAEngN.jar\" width=800
height=600>\n"
          + "<param name=\"cabbase\" value=\"JICAEngM.cab\">\n"
          + "<param name=\"address\" value=\"localhost\">\n"
          + "<param name=ICAPortNumber value="
          + getClientPort('1494')
          + ">\n"
          + "</applet>\n"
          + "</body>\n"
```

```
          + "</html>\n";
    document.write(newContent);
}
</script>
<body onLoad="generateContent();">
</body>
</html>
```

拒絕的 HTML 檔

```
<html>
<body>
<applet code="com.citrix.JICA.class" archive="JICAEngN.jar" width=800 height=600>
<param name="cabbase" value="JICAEngM.cab">
<param name="address" value="localhost">
<param name=ICAPortNumber value=1494>
</applet>
</body>
              </html>
```

第 6 章

PDC 與 Netlet 搭配使用

本章會介紹如何配置用戶端瀏覽器的 Java Plugin，使得 Netlet 能夠和 PDC 搭配使用。請注意：

- 只有在擁有 JSSE 支援的用戶端 VM 上才能搭配使用 Netlet 與 PDC。
- 只有包含 JSSE 的 Virtual Machine (VM) 才能搭配使用 Netlet 與 PDC。

爲 PDC 配置 Netlet

➤ **若要爲 PDC 配置 Netlet**

1. 將用戶端證書從瀏覽器中以下列格式匯出：
   - PKCS
   - JKS

   在匯出用戶端證書之後，java plugin 應該擁有下列 JVM 參數，才可以讓 VM 使用證書：

   javax.net.ssl.keyStoreType

   javax.net.ssl.keyStorePassword

   javax.netl.ssl.keyStore
2. 切換至控制台，然後啓動 Java Plugin
3. 選擇進階標籤，Java Runtime Environment

4. 指定 Java 運行時間參數。例如：

   Djavax.net.ssl.keyStoreType=pkcs

   Djavax.net.ssl.keyStorePassword=testing123

   Djavax.netl.ssl.keyStore="C:\dir\test.cert"

5. 按一下「套用」。
6. 關閉 Java plugin 並重新啓動相關的瀏覽器。

第 7 章

證書

本章會介紹證書管理並解釋如何安裝自簽的證書與來自認證機構 (CA) 的證書。

本章涵蓋下列主題：

- SSL 證書概述
- 證書檔案
- 證書信任屬性
- CA 信任屬性
- certadmin 程序檔
- 產生自簽證書
- 安裝來自認證機構的 SSL 證書
- 新增根 CA 證書
- 修改證書的信任屬性
- 列示根 CA 證書
- 列示所有證書
- 刪除證書
- 列印證書

SSL 證書概述

Sun™ ONE Portal Server, Secure Remote Access 軟體提供以證書爲基礎的遠端使用者認證。Secure Remote Access 使用安全套接層 (SSL) 可實現安全通訊。此 SSL 通訊協定可實現兩部機器之間的安全通訊。

SSL 證書使用公開金鑰與私人金鑰對提供加密與解密功能。

有兩種類型的證書：

- 自簽證書 (亦稱爲根 CA 證書)
- 由認證機構 (CA) 核發的證書

依預設，當您安裝「閘道」時，系統會產生並安裝自簽證書。

安裝之後，您可以隨時產生、獲得或取代證書。

Secure Remote Access 同時支援使用個人數位證書 (PDC) 的用戶端認證。PDC 是一種機制，可透過 SSL 用戶端認證進行使用者認證。有了 SSL 用戶端認證，SSL 訊號交換模式便會於「閘道」結束。閘道會擷取使用者的 PDC 並將它傳送到認證伺服器。而此伺服器會使用 PDC 認證使用者。若要配置 PDC 與認證鏈接，請參閱第 68 頁的「使用認證鏈接」。

Secure Remote Access 提供名爲 `certadmin` 的工具，可讓您用來管理 SSL 證書。請參閱第 198 頁的「certadmin 程序檔」。

證書檔案

與證書相關的檔案位於 `/etc/opt/SUNWps/cert/default/gateway-profile-name`。此目錄依預設包含 5 個檔案。

表 7-1 列出這些檔案及其說明。第一欄列出證書檔案名稱、第二欄指定檔案類型，而第三欄則爲檔案說明。

表 7-1 證書檔案

檔案名稱	類型	說明
`cert8.db`、`key3.db`、`secmod.db`	二進位	包含證書、密鑰和密碼編譯模組的資料。 可以使用 `certadmin` 程序檔進行操控。 與 Sun™ ONE Web Server 使用的資料庫檔案具有相同的格式，其中檔案位於 *portal-server-install-root*`/SUNWwbsvr/alias`。 如有必要，這些檔案可以在 Portal Server 主機和閘道元件或閘道代理伺服器之間共享使用。
`.jsspass`	隱藏文字檔	包含用於 SRA 密鑰資料庫的加密密碼。
`.nickname`	隱藏文字檔	以 *token-name:certificate-name* 格式儲存閘道需要使用的記號與證書的名稱。 若您正在使用預設記號 (預設內部軟體加密模組的記號)，請省略記號名稱。在大部分的情形下，`.nickname` 檔案僅會儲存證書名稱。 身為管理員，您可以修改此檔案中的證書名稱。閘道現在將會使用您所指定的證書。

證書信任屬性

證書的信任屬性表示：

- 證書 (就用戶端或伺服器證書而言) 是否由信任的 CA 所核發。
- 是否可以信任證書 (就根證書而言) 作爲伺服器與用戶端證書的核發者。

每種證書有三種可能的信任種類，表達順序爲：「SSL、電子郵件和物件簽署」。對於閘道元件而言，僅第一個種類有用。在每個種類位置，可以使用零或其他信任屬性代碼。

種類的屬性代碼由逗號隔開，而整個屬性集則是由引號環繞。例如，閘道安裝期間產生並安裝的自簽證書標記爲 "u,u,u"，表示此是伺服器證書 (使用者認證) 而不是根 CA 證書。

表 7-2 列出可能的屬性值與每個值的意義。第一欄列出屬性，第二欄則說明屬性。

表 7-2 證書信任屬性

屬性	說明
p	有效點
P	可信任點 (暗含 p)
c	有效 CA
T	可信任的 CA 核發用戶端證書 (暗含 c)
C	可信任的 CA 核發伺服器證書 (僅限 SSL) (暗含 c)
u	證書可以用於認證或簽署
w	傳送警告 (在該環境中使用證書時，與其他屬性一起使用以便包含一個警告)

CA 信任屬性

證書資料庫中包含眾所皆知的公開 CA。有關修改公開 CA 信任屬性的資訊，請參閱第 207 頁的「修改證書的信任屬性」。

表 7-3 列出眾多共用的認證機構及其信任屬性。第一欄列出認證機構，而第二欄則列出該 CA 的信任屬性。

表 7-3 公開認證機構

認證機構名稱	信任屬性
Verisign/RSA Secure Server CA	CPp,CPp,CPp
VeriSign Class 4 Primary CA	CPp,CPp,CPp
GTE CyberTrust Root CA	CPp,CPp,CPp
GTE CyberTrust Global Root	CPp,CPp,CPp
GTE CyberTrust Root 5	CPp,CPp,CPp
GTE CyberTrust Japan Root CA	CPp,CPp,CPp
GTE CyberTrust Japan Secure Server CA	CPp,CPp,CPp
Thawte Personal Basic CA	CPp,CPp,CPp

表 7-3 公開認證機構

Thawte Personal Premium CA	CPp,CPp,CPp
Thawte Personal Freemail CA	CPp,CPp,CPp
Thawte Server CA	CPp,CPp,CPp
Thawte Premium Server CA	CPp,CPp,CPp
American Express CA	CPp,CPp,CPp
American Express Global CA	CPp,CPp,CPp
Equifax Premium CA	CPp,CPp,CPp
Equifax Secure CA	CPp,CPp,CPp
BelSign Object Publishing CA	CPp,CPp,CPp
BelSign Secure Server CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 0 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 1 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 2 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 3 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 4 CA	CPp,CPp,CPp
ABAecom (sub., Am. Bankers Assn.)Root CA	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 1	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 3	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 2	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 4	CPp,CPp,CPp
Deutsche Telekom AG Root CA	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority - G2	CPp,CPp,CPp

表 7-3 公開認證機構

Verisign Class 2 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 4 Public Primary Certification Authority - G2	CPp,CPp,CPp
GlobalSign Root CA	CPp,CPp,CPp
GlobalSign Partners CA	CPp,CPp,CPp
GlobalSign Primary Class 1 CA	CPp,CPp,CPp
GlobalSign Primary Class 2 CA	CPp,CPp,CPp
GlobalSign Primary Class 3 CA	CPp,CPp,CPp
ValiCert Class 1 VA	CPp,CPp,CPp
ValiCert Class 2 VA	CPp,CPp,CPp
ValiCert Class 3 VA	CPp,CPp,CPp
Thawte Universal CA Root	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 4 Public Primary Certification Authority - G3	CPp,CPp,CPp
Entrust.net Secure Server CA	CPp,CPp,CPp
Entrust.net Secure Personal CA	CPp,CPp,CPp
Entrust.net Premium 2048 Secure Server CA	CPp,CPp,CPp
ValiCert OCSP Responder	CPp,CPp,CPp
Baltimore CyberTrust Code Signing Root	CPp,CPp,CPp
Baltimore CyberTrust Root	CPp,CPp,CPp
Baltimore CyberTrust Mobile Commerce Root	CPp,CPp,CPp
Equifax Secure Global eBusiness CA	CPp,CPp,CPp
Equifax Secure eBusiness CA 1	CPp,CPp,CPp

表 7-3 公開認證機構

Equifax Secure eBusiness CA 2	CPp,CPp,CPp
Visa International Global Root 1	CPp,CPp,CPp
Visa International Global Root 2	CPp,CPp,CPp
Visa International Global Root 3	CPp,CPp,CPp
Visa International Global Root 4	CPp,CPp,CPp
Visa International Global Root 5	CPp,CPp,CPp
beTRUSTed Root CA	CPp,CPp,CPp
Xcert Root CA	CPp,CPp,CPp
Xcert Root CA 1024	CPp,CPp,CPp
Xcert Root CA v1	CPp,CPp,CPp
Xcert Root CA v1 1024	CPp,CPp,CPp
Xcert EZ	CPp,CPp,CPp
CertEngine CA	CPp,CPp,CPp
BankEngine CA	CPp,CPp,CPp
FortEngine CA	CPp,CPp,CPp
MailEngine CA	CPp,CPp,CPp
TraderEngine CA	CPp,CPp,CPp
USPS Root	CPp,CPp,CPp
USPS Production 1	CPp,CPp,CPp
AddTrust Non-Validated Services Root	CPp,CPp,CPp
AddTrust External Root	CPp,CPp,CPp
AddTrust Public Services Root	CPp,CPp,CPp
AddTrust Qualified Certificates Root	CPp,CPp,CPp
Verisign Class 1 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Class 2 Public Primary OCSP Responder	CPp,CPp,CPp

表 7-3 公開認證機構

Verisign Class 3 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Secure Server OCSP Responder	CPp,CPp,CPp
Verisign Time Stamping Authority CA	CPp,CPp,CPp
Thawte Time Stamping CA	CPp,CPp,CPp
E-Certify CA	CPp,CPp,CPp
E-Certify RA	CPp,CPp,CPp
Entrust.net Global Secure Server CA	CPp,CPp,CPp
Entrust.net Global Secure Personal CA	CPp,CPp,CPp

certadmin 程序檔

您可以使用 `certadmin` 程序檔執行下列證書管理工作：

- 產生自簽證書
- 產生證書簽署要求 (CSR)
- 新增根 CA 證書
- 安裝來自 CA 的證書
- 刪除證書
- 修改證書的信任屬性
- 列示根 CA 證書
- 列示所有證書
- 列印證書

產生自簽證書

您需要爲每個伺服器和閘道元件之間的 SSL 通訊產生證書。

➤ **安裝之後若要產生自簽證書**

1. 以 root 身份，在您想要產生證書的閘道機器上執行 certadmin 程序檔：

   portal-server-install-root/SUNWps/bin/certadmin -n *gateway-profile-name*

   系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書

6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )

7) 列示 Root CA 證書

8) 列示所有證書

9) 列印證書內容

10) 退出

選擇： [10] 1
```

2. 在證書管理功能表上選擇選項 **1**。

   證書管理程序檔會詢問您是否想要保留現有的資料庫檔案。

3. 請輸入組織特定的資訊、記號名稱和證書名稱。

備註 關於萬用字元證書，請在主機的完全合格的 DNS 名稱中指定一個 * 號。例如，如果主機的完全合格 DNS 名稱爲 abc.sesta.com，請指定爲 *.sesta.com。產生的證書現在對於 sesta.com 網域中的所有主機名稱而言，都有效。

```
此主機的完整限定 DNS 名稱是什麼？[host_name.domain_name]

您的社團組織名稱（如：公司）是什麼？[]

您的組織單位名稱（如：部門）是什麼？[]

您所在的城市或地區的名稱是什麼？ []

您所在的州或省份名稱（請勿使用縮寫）是什麼？ []

此單位的雙字母國碼是什麼？ []

僅當您不使用預設的內部（軟體）加密模組時才需要使用記號名稱，例如，如果您想要使用
密碼卡時 ( 記號名稱可以使用 modutil -dbdir
/etc/opt/SUNWps/cert/gateway-profile-name ñlist 列示 )；否則，請按一下下
列的「傳回」鍵。

請輸入記號名稱。 []

爲此證書輸入想使用的名稱？

請輸入證書的有效期間 ( 以月計 ) [6]
A self-signed certificate is generated and the prompt returns. ( 自簽
證書將會產生並傳回提示。)
```

記號名稱 (預設空白) 和證書名稱儲存於 .nickname 檔案中，路徑是 /etc/opt/SUNWps/cert*gateway-profile-name*。

4. 重新啓動證書閘道才會生效：

gateway-install-root/SUNWps/bin/gateway -n *new gateway-profile-name* start

產生證書簽署要求 (CSR)

可以從 CA 訂制證書之前，您需要產生包含 CA 所需要資訊的證書簽署要求。

➤ **若要產生 CSR**

1. 以超級使用者身份執行 `certadmin` 程序檔：

   portal-server-install-root`/SUNWps/bin/certadmin -n` *gateway-profile-name*

   系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書

6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )

7) 列示 Root CA 證書

8) 列示所有證書

9) 列印證書內容

10) 退出

選擇： [10] 2
```

2. 在證書管理功能表上選擇選項 **2**。

   程序檔提示您輸入組織特定的資訊、記號名稱和網路管理員電子郵件及電話號碼。

   請指定主機的完整合格 DNS 名稱。

```
此主機的完整限定 DNS 名稱是什麼？[snape.sesta.com]

您的社團組織名稱（如：公司）是什麼？[]

您的組織單位名稱（如：部門）是什麼？[]

您所在的城市或地區的名稱是什麼？ []

您所在的州或省份名稱（請勿使用縮寫）是什麼？ []

此單位的雙字母國碼是什麼？ []

僅當您不使用預設的內部（軟體）加密模組時才需要使用記號名稱，例如，如果您想要使用密
碼卡時 ( 記號名稱可以使用 modutil -dbdir /etc/opt/SUNWps/cert -list 列示 )；
否則，請按一下下列的「傳回」鍵。

請輸入記號名稱 []

現在請輸入本機器（將爲其證書的機器）網站管理員的部份聯絡資訊。

此伺服器管理員 / 網站管理員的電子郵件位址是什麼？[]

此伺服器管理員 / 網站管理員的電話號碼是什麼？ []
```

3. 輸入所有需要的資訊。

備註	請務必填寫網路管理員電子郵件和電話號碼。爲了獲得有效的 CSR，必須填寫這兩項資訊。

CSR 會產生並儲存於 *portal-server-install-root/SUNWps/bin/csr.hostname.datetimestamp* 檔案中。CSR 同時會列印於螢幕上。當您從 CA 訂制證書時，可以直接複製並貼上 CSR

新增根 CA 證書

若用戶端站台提交的的證書由閘道證書資料庫中不包含的 CA 所簽署，則 SSL 訊號交換模式將會失敗。

若要避免這種情況，您需要新增根 CA 證書到證書資料庫。這項動作可以確保 CA 變成閘道所知的 CA。

瀏覽至 CA 的網站並獲得此 CA 的根證書。當您使用 `certadmin` 程序檔時，請指定根 CA 證書的檔案名稱和路徑。

➤ 若要新增根 CA 證書

1. 以超級使用者身份執行 `certadmin` 程序檔。

   portal-server-install-root`/SUNWps/bin/certadmin -n` *gateway-profile-name*

   系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書

6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )

7) 列示 Root CA 證書

8) 列示所有證書

9) 列印證書內容

10) 退出

選擇： [10] 3
```

2. 在證書管理功能表上選擇選項 **3**。
3. 輸入包含根證書的檔案名稱並輸入證書名稱。

   根 CA 證書將會新增至證書資料庫。

安裝來自認證機構的 SSL 證書

Secure Remote Access 閘道元件安裝期間，依預設系統會建立自簽證書並安裝。在安裝之後的任何時間，您都可以安裝由供應商或由您公司的 CA 提供簽署的 SSL 證書，其中這些供應商會提供正式的認證機構 (CA) 服務。

這項工作包含的三個步驟爲：

- 產生證書簽署要求 (CSR)
- 從 CA 訂制證書
- 安裝來自 CA 的證書

從 CA 訂制證書

產生證書簽署要求 (CSR) 之後，您需要使用 CSR 從 CA 訂制證書。

➤ **若要從 CA 訂制證書**

1. 請至認證機構的網站並訂制您的證書。
2. 提供 CA 所要求的 CSR。若 CA 要求請提供其他資訊。

   您將會收到 CA 簽署的證書。請將它儲存在檔案中。檔案中證書內容前後請包含 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 兩行。

   下面的範例省略了實際的證書資料。

```
-----BEGIN CERTIFICATE-----

The certificate contents ( 證書內容 )...

----END CERTIFICATE-----
```

安裝來自 CA 的證書

使用 certadmin 程序檔，將您從 CA 獲得的證書安裝在本機資料庫檔案中，路徑是 /etc/opt/SUNWps/cert*gateway-profile-name*。

➤ 若要安裝來自 CA 的證書

1. 以超級使用者身份執行 certadmin 程序檔。

   portal-server-install-root/SUNWps/bin/certadmin -n *gateway-profile-name*

   系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書

6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )

7) 列示 Root CA 證書

8) 列示所有證書

9) 列印證書內容

10) 退出

選擇： [10] 4
```

2. 在證書管理功能表上選擇選項 **4**。

   程序檔會讓您輸入證書檔案名稱、證書名稱和記號名稱。

```
含有此證書的檔案名稱（包括路徑）是什麼？
請輸入爲此證書建立 CSR 時所用的記號名稱。 []
```

3. 提供所有需要的資訊。

   證書將安裝於 /etc/opt/SUNWps/cert*gateway-profile-name*，而且系統會傳回螢幕提示。

4. 重新啓動證書閘道才會生效：

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

刪除證書

您可以使用證書管理程序檔刪除證書。

➤ **若要刪除證書**

1. 以超級使用者身份執行 certadmin 程序檔。

```
portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

   其中 *gateway-profile-name* 是閘道實例的名稱。

   系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書
```

```
6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )

7) 列示 Root CA 證書

8) 列示所有證書

9) 列印證書內容

10) 退出

選擇： [10] 5
```

2. 在證書管理功能表上選擇選項 **5**。
3. 輸入要刪除的證書名稱。

修改證書的信任屬性

若用戶端認證與閘道一起使用，證書信任屬性則需要修改。其中一個用戶端認證範例爲 PDC (個人數位證書)。核發 PDC 的 CA 必須受閘道所信任，其中 CA 證書的 SSL 標記必須爲 "T"。

若閘道元件設爲與 HTTPS 站台通訊，HTTPS 站台伺服器證書的 CA 必須受閘道所信任，而且 CA 證書的 SSL 標記 必須爲 "C"。

➤ **若要修改證書的信任屬性**

1. 以超級使用者身份執行 `certadmin` 程序檔。

```
gateway-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

其中 *gateway-profile-name* 是閘道實例的名稱。

系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書

6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )

7) 列示 Root CA 證書

8) 列示所有證書

9) 列印證書內容

10) 退出

選擇： [10] 6
```

2. 在證書管理功能表上選擇選項 **6**。
3. 輸入證書的名稱。例如：Thawte Personal Freemail C。

```
請輸入證書的名稱？
Thawte Personal Freemail CA
```

4. 輸入證書的信任屬性。

```
請輸入欲使證書具備的信任屬性 [CT,CT,CT]
```

系統將會變更證書信任屬性。

列示根 CA 證書

您可以使用證書管理程序檔檢視所有根 CA 證書。

➤ **若要檢視根 CA 清單**

1. 以超級使用者身份執行 `certadmin` 程序檔。

```
portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

其中 *gateway-profile-name* 是閘道實例的名稱。

系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書

6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )

7) 列示 Root CA 證書

8) 列示所有證書

9) 列印證書內容

10) 退出

選擇： [10] 7
```

2. 在證書管理功能表上選擇選項 **7**。

   系統會顯示所有根 CA 證書。

列示所有證書

您可以使用證書管理程序檔檢視所有證書及其對應的信任屬性。

➤ **若要列示所有證書**

1. 以超級使用者身份執行 `certadmin` 程序檔。

```
portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

   其中 *gateway-profile-name* 是閘道實例的名稱。

   系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書

6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )

7) 列示 Root CA 證書

8) 列示所有證書
```

```
9) 列印證書內容

10) 退出

選擇： [10] 8
```

2. 在證書管理功能表上選擇選項 **8**。

   系統會顯示所有 CA 證書。

列印證書

您可以使用證書管理程序檔列印證書。

➤ **若要列印證書**

1. 以超級使用者身份執行 `certadmin` 程序檔。

```
portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

   其中 *gateway-profile-name* 是閘道實例的名稱。

   系統便會顯示證書管理功能表。

```
1) 產生自簽證書

2) 產生證書簽署要求 (CSR)

3) 加入 Root CA 證書

4) 安裝來自認證機構 (CA) 的證書

5) 刪除證書

6) 修改證書的信任屬性 ( 例如 PDC 的信任屬性 )
```

```
7) 列示 Root CA 證書

8) 列示所有證書

9) 列印證書內容

10) 退出

選擇： [10] 9
```

2. 在證書管理功能表上選擇選項 **9**。
3. 輸入證書的名稱。

第 8 章

配置 URL 存取控制

本章會說明如何從 Sun™ ONE Identity Server 管理主控台允許或拒絕使用者存取。在 SRA 配置、存取清單下，透過特定 URL 的閘道。

備註 按一下 Identity Server 管理主控台右上角的「文件」，然後按一下 SRA 說明以快速取得有關所有 Secure Remote Access 屬性的參考。

若要配置 URL 存取控制，請執行下列動作：

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取管理主控台中的「服務配置」標籤。
3. 按一下「SRA 配置」下「存取清單」旁的箭頭。

   會顯示「存取清單」頁。

在此您可以執行下列任務：

- 設定 URL 拒絕清單
- 設定 URL 允許清單
- 管理單次登入
- 自訂存取清單介面

備註 當您安裝 Secure Remote Access 時，在預設情況下所有使用者無法使用「存取清單」服務。僅有在安裝時預設情況下建立的 `amadmin` 使用者才可使用此服務。其他使用者在沒有此服務的情況下，無法透過閘道存取桌面。以 `amadmin` 的身份登入，並指定此服務給所有的使用者。

設定 URL 拒絕清單

您可以指定一般使用者無法使用此欄位透過閘道存取的 URL 清單。

閘道會在檢查 URL 允許清單之前檢查 URL 拒絕清單。

➤ 若要設定 URL 拒絕清單

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「存取清單」旁的箭頭。

   會顯示「存取清單」頁。
4. 在「URL 拒絕清單」欄位中，指定您想要拒絕透過閘道存取的 URL。輸入的 URL 格式爲：

   ```
   http://abc.siroe.com
   ```
5. 按一下「新增」。

   該 URL 會新增到「URL 拒絕清單」。

   您也可以使用常規表示式，如 `http://*.siroe.com`。在這個情況下，會拒絕使用者存取 `siroe.com` 網域中的所有主機。
6. 按一下「儲存」以記錄變更。

設定 URL 允許清單

您可以指定可由一般使用者透過閘道存取的所有 URL。依預設，此清單有萬用字元項目 (*)，表示可以存取所有 URL。若您希望允許存取所有 URL，而僅對特定 URL 限制存取，請將限制的 URL 新增至 URL 拒絕清單中。如果您希望僅允許存取特定 URL，請將 URL 拒絕清單保留空白，並在 URL 允許清單中指定需要的 URL，方法與上述相同。

閘道會在檢查 URL 允許清單之前檢查 URL 拒絕清單。

➤ 若要設定 URL 允許清單

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。

3. 按一下「SRA 配置」下「存取清單」旁的箭頭。

   會顯示「存取清單」頁。

4. 在「URL 允許清單」欄位中，指定您想要允許透過閘道存取的 URL。輸入的 URL 格式爲：

   ```
   http://abc.siroe.com
   ```

5. 按一下「新增」。

   該 URL 會新增到「URL 允許清單」。

備註 「URL 允許清單」預設中有 *，表示可以透過閘道存取所有的 URL。

6. 按一下「儲存」以記錄變更。

管理單次登入

在 Secure Remote Access 中的「存取清單」服務允許您控制多個主機的單次登入功能。但爲使得單次登入功能可用，「啓用 HTTP 基本認證」選項必須於閘道服務中啓用。請參閱第 221 頁的「啓用 HTTP 與 HTTPS 連線」。

使用「存取清單」服務，您可以停用某些主機的單次登入功能。這表示一般使用者每次連接至需要 HTTP 基本認證的主機時，都會需要認證，除非您已啓用按階段作業單次登入。

若您已停用某個主機的單次登入，使用者可以在單一 Portal Server 階段作業中重新連接至該主機。例如，假設您已停用對 `abc.sesta.com` 的單次登入。在使用者第一次連接至此站台時，需要認證。使用者可以瀏覽其他網頁並在稍後返回此網頁，且如果該網頁是在相同的 Portal Server 階段作業，則不需要再次認證。

使用者也可以使用受限的管理主控台配置這些屬性。

➤ 停用主機的 SSO

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「存取清單」旁的箭頭。

   會顯示「存取清單」頁。

4. 在 SSO 是停用欄位的主機中指定您想要停用 SSO 的主機。

   以 `abc.siroe.com` 的格式指定主機名稱。

5. 按一下「新增」。

   主機名稱會新增至清單。

6. 按一下「儲存」以記錄變更。

➤ **按階段作業啓用 SSO**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「存取清單」旁的箭頭。

   會顯示「存取清單」頁。

4. 選擇「按階段作業啓用 SSO」核取方塊以啓用階段作業單次登入。
5. 按一下「儲存」以記錄變更。

➤ **若要指定授權層級**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「存取清單」旁的箭頭。

   會顯示「存取清單」頁。

4. 捲動「AllowedAuth」層級欄位。
5. 輸入允許的授權。使用星號以允許所有的層級。
6. 按一下「儲存」以記錄變更。

自訂存取清單介面

編輯存取清單屬性檔案，以變更 Identity Server 管理主控台的存取清單使用者介面上的標籤。編輯檔案：

portal-server-install-root/SUNWam/locale/SRAGatewayAccess.properties

下列範例顯示可以自訂的行：

```
sunPortalGatewayAccessServiceDescription=Access List
```

```
d02=URL Allow List
d05=Policy to Enable/Disable SSO
d04=Enable SSO per Session
d03=Hosts for Which SSO is Disabled
d01=URL Deny List
d06=Allowed Auth levels
```

您可以變更標籤文字，但不能變更和文字相關的數字。

第 9 章

配置閘道

本章會介紹如何透過 Sun™ ONE Identity Server 管理主控台來配置「閘道」屬性。

備註 按一下 Identity Server 管理主控台右上角的「文件」，然後按一下 SRA 說明以快速取得有關所有 Secure Remote Access 屬性的參考。

若要設定閘道，請參閱第 36 頁的「建立閘道設定檔」。

在建立閘道設定檔之後，您必須配置閘道屬性。若要配置閘道屬性，請執行下列動作：

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取管理主控台中的「服務配置」標籤。
3. 按一下「SRA 組態」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。

   在此處，按一下適當的標籤：

   - 「核心」標籤
   - 「代理程式」標籤
   - 「安全性」標籤
   - 「Rewriter」標籤
   - 「記錄」標籤

可以在每個標籤之下配置的標籤與屬性如下所列。

「核心」標籤

使用「閘道」服務中的「核心」標籤，您將可以執行下列工作：

- 啓用 HTTP 與 HTTPS 連線
- 啓用並建立 Rewriter 代理伺服器清單
- 啓用並建立 Netlet 代理伺服器清單
- 啓用 Netlet
- 啓用並建立 Netlet 代理伺服器清單
- 啓用 Cookie 管理
- 啓用 HTTP 基本驗證
- 啓用持續 HTTP 連線
- 指定每一持續連線的最大要求數
- 指定持續通訊端關閉後的逾時
- 指定帳戶往返時間的寬限逾時
- 建立「轉寄 Cookie URL 清單」
- 指定最長連線佇列長度
- 指定閘道逾時
- 指定執行緒儲存區大小
- 指定快取的通訊端逾時
- 建立 Portal Server 清單
- 指定伺服器重試間隔
- 啓用儲存外部伺服器 Cookie
- 啓用從 URL 取得階段作業
- 啓用將 Cookie 標示爲安全

啓用 HTTP 與 HTTPS 連線

若您在安裝期間選擇以 HTTPS 模式執行閘道，則在安裝後閘道會以 HTTPS 模式執行。在 HTTPS 模式中，閘道會接受來自瀏覽器的 SSL 連線並拒絕非 SSL 連線。

然而，您也可以配置以 HTTP 模式執行閘道。以 HTTP 模式執行的好處與效能有關，因爲管理 SSL 階段作業、加密與解密 SSL 通訊會佔用相當的時間。省略這些步驟可加快閘道運作的速度。

➤ **若要配置閘道以於 HTTP 或 HTTPS 模式中執行**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取管理主控台中的「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 在「核心」標籤之下執行下列作業。
   - 選取「啓用 HTTP 連線」、「啓用 HTTPS 連線」或依需要同時選取這兩個核取方塊。
   - 在 HTTPS 連接埠欄位中指定必要的 HTTPS 連接埠。
   - 在 HTTP 連接埠欄位中指定必要的 HTTP 連接埠。
6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用並建立 Rewriter 代理伺服器清單

Rewriter 代理伺服器會在「閘道」與內部網路電腦之間實現安全的 HTTP 通訊。如果您沒有指定 Rewriter 代理伺服器，當使用者嘗試存取企業內部網路的其中一台電腦，閘道元件會直接連線至企業內部網路的電腦。

在安裝之後不會自動執行 Rewriter 代理伺服器。您必須依下列所述啓用 Rewriter 代理伺服器。

➤ 若要啓用 Rewriter 代理伺服器並建立 Rewriter 代理伺服器清單

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

備註 請確定 Rewriter 代理伺服器與閘道使用相同的閘道設定檔。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 選取「啓用 Rewriter 代理伺服器」核取方塊以啓用 Rewriter 代理伺服器。
7. 在 Rewriter 代理伺服器清單編輯方塊中以 `hostname:port` 格式輸入想要的主機與連接埠。
8. 按一下「新增」。
9. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
10. 在伺服器上執行 *portal-server-install-root*`/SUNWps/bin/certadmin` 以建立 Rewriter 代理伺服器的認證。

    若您在安裝 Rewriter 代理伺服器時未選擇建立認證，則必須執行這個步驟。
11. 以超級使用者身份登入安裝 Rewriter 代理伺服器的機器並啓動 Rewriter 代理伺服器：

    rewriter-proxy-install-root`/SUNWps/bin/rwproxyd -n` *gateway-profile-name* `start`
12. 以超級使用者身份登入安裝閘道的機器並重新啓動閘道：

    gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 Netlet

Netlet 會讓使用者在不安全的網路上 (如網際網路) 安全執行共用 TCP/IP 服務。您可以執行 TCP/IP 應用程式 (例如 Telnet 和 SMTP)、HTTP 應用程式以及任何固定的連接埠應用程式。

若已啓用 Netlet，閘道需要確定外來的通訊是 Portal Server 通訊還是 Netlet 通訊。停用 Netlet 則會減少這種耗用時間，因爲閘道會假設所有外來的通訊是 HTTP 或 HTTPS 通訊。只有在確定不希望通過 Portal Server 使用任何應用程式時，才停用 Netlet。

➤ 若要啓用 Netlet

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 選取「啓用 Netlet」核取方塊。此核取方塊的預設爲已選。移除此選項將停用 Netlet。
7. 選取「啓用 Netlet 代理伺服器」核取方塊以啓用 Netlet 代理伺服器。
8. 在 Netlet 代理伺服器清單編輯方塊中以 `hostname:port` 格式鍵入想要的主機與連接埠。
9. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
10. 從終端機視窗重新啓動「閘道」：

    gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用並建立 Netlet 代理伺服器清單

藉由延伸用戶端透過閘道到存在於企業內部網路的 Netlet 代理伺服器的安全通道，Netlet 代理伺服器會強化閘道和企業內部網路之間 Netlet 通訊的安全性。

若已啓用 Netlet 代理伺服器，則 Netlet 封包會由代理 Netlet 伺服器解密，之後會傳送至目標伺服器。這將減少需要在防火牆中開啓的連接埠數目。

➤ 若要啓用 Netlet 代理伺服器並建立 Netlet 代理伺服器清單

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下左框架中「SRA 配置」中「閘道」旁的右箭頭。

   「閘道」頁面會顯示在右窗格中。
4. 按一下想要更改設定檔旁的「編輯」。

   「編輯閘道設定檔」頁面隨即顯示於右窗格上。
5. 選取「啓用 Netlet 代理伺服器」核取方塊以啓用 Netlet 代理伺服器。
6. 在「Netlet 代理伺服器主機」欄位中以 `host hostname:port` 格式鍵入想要的 Netlet 代理伺服器主機與連接埠。

提示 若要確定想要的連接埠是否可用或未使用，請在指令行中輸入：

`netstat -a | grep` *port-number* **`| wc -l`**

port-number 是想要使用的連接埠。

---

7. 按一下「新增」。
8. 按一下頁面底部的「儲存」以儲存變更。
9. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 Cookie 管理

許多網頁使用 Cookie 追蹤與管理使用者階段作業。閘道路由請求至在 HTTP 標題設定 Cookie 的網站時，閘道會以下列方法捨棄或傳遞那些 Cookie：

- 若未在閘道服務中選取「啓用 Cookie 管理」，則不會改寫 Cookie。如此，瀏覽器中的 Cookie 可能不會到達內部網路主機，反之亦然。
- 若在閘道服務中選取「啓用 Cookie 管理」，則會改寫 Cookie。閘道會確保瀏覽器的 Cookie 會到達想要的內部網路主機，反之亦然。

這個設定不適用於 Portal Server 追蹤 Portal Server 使用者階段作業所用的 Cookie。此由「轉送 Cookie URL」選項配置所控制。請參閱第 229 頁的「建立「轉寄 Cookie URL 清單」」。

這個設定適用於所有允許使用者存取的網站 (也就是，您不可以選擇捨棄某些站台的 Cookie，而保留其他站台的 Cookie)。

備註 請勿將 URL 從「Cookie 網域」清單中移除，即使是在沒有 Cookie 的閘道中。有關 Cookie 網域清單的更多資訊，請參閱 *Identity Server 管理員指南*。

➤ **若要啓用 Cookie 管理**

1. 以管理員的身份登入 Identity Server 管理主控台。
1. 選取「服務配置」標籤。
2. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
3. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
4. 按一下「核心」標籤。
5. 選取「啓用 Cookie 管理」核取方塊以啓用 cookie 管理。
6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 HTTP 基本驗證

HTTP 基本驗證可以設定於閘道服務中。

可以使用 HTTP 基本驗證保護網頁，造訪者需要在檢視站台前輸入使用者名稱與密碼 (HTTP 回應代碼爲 401 與 WWW-authenticate:BASIC)。Portal Server 可以儲存使用者名稱與密碼，所以使用者在重新造訪受 BASIC 保護的網站時不需要重新輸入憑證。這些憑證儲存於目錄伺服器的使用者設定檔中。

此設定不會確定使用者是否可造訪受 BASIC 保護的站台，但只會確定是否將使用者輸入的憑證儲存於使用者設定檔。

這個設定適用於所有允許使用者存取的網站 (也就是，不可以某些站台啓用 HTTP 基本授權快取而其他站台停用)。

備註	瀏覽由 Microsoft Internet Information Server (IIS) 傳送的 URL 是受 Windows NT 挑戰 / 回應 (HTTP 回應代碼爲 401, WWW-Authenticate: NTLM) 保護，而非受不支援的 BASIC 驗證保護。

您也可以使用管理主控台中的「存取清單」服務啓用單次登入。有關啓用單次登入的資訊，請參閱第 215 頁的「管理單次登入」。

➤ 若要啓用 HTTP 基本驗證

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 選取「啓用 HTTP 基本驗證」核取方塊以啓用 HTTP 基本驗證。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用持續 HTTP 連線

您可以在閘道啓用 HTTP 持續連線，避免爲網頁的每個物件 (例如影像與樣式表) 開啓插槽。

➤ **若要啓用持續 HTTP 連線**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 選取「啓用持續 HTTP 連線」核取方塊以啓用 HTTP 連線。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定每一持續連線的最大要求數

➤ **指定每一持續連線的最大要求數**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 捲動至「每一持續連線的最大要求數」欄位並輸入想要的要求數。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。

8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定持續通訊端關閉後的逾時

➤ **若要指定持續通訊端的逾時**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 捲動至「持續通訊端關閉後的逾時」並輸入想要的逾時 (以秒爲單位)。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定帳戶往返時間的寬限逾時

往返時間的寬限逾時爲以下兩項之和：

- 在瀏覽器傳送請求之後，請求到達閘道所需的時間。
- 閘道傳送回應與瀏覽器實際接收到回應之間的時間。

這將根據網路情況與用戶端連線速度等因素而有不同。

➤ **若要指定帳戶往返時間的逾時**

這是用戶端 (瀏覽器) 與閘道之間的網路通訊往返時間。

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。

3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。

4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。

5. 按一下「核心」標籤。

6. 捲動至「帳戶往返時間的寬限逾時」欄位並輸入想要的寬限逾時 (以秒爲單位)。

7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。

8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立「轉寄 Cookie URL 清單」

入口網站伺服器利用 Cookie 追蹤使用者階段作業。當閘道發出 HTTP 請求至伺服器時 (例如，當呼叫桌面 servlet 以產生使用者桌面頁面時)，將轉寄此 cookie 至伺服器。伺服器上的應用程式會使用 cookie 以認證並識別使用者。

Portal Server 的 cookie 不會轉寄至發給伺服器之外其他電腦的 HTTP 請求中，除非那些機器上的 URL 已指定於「轉寄 Cookie URL 清單」中。將 URL 新增至此清單，因此啓用 servlet 與 CGI 以接收 Portal Server 的 cookie 並使用 API 以識別此使用者。

使用隱式尾隨萬用字元可匹配 URL。例如，清單中的預設輸入值爲：

`http://server:8080`

將導致欲轉寄 Cookie 至所有以 `http://server:8080` 開頭的 URL。

新增：

`http://newmachine.eng.siroe.com/subdir`

將導致欲轉寄 Cookie 至所有以該實際字串開始的 URL。

例如，該 Cookie 不會轉寄至任何以 "`http://newmachine.eng/subdir`" 開始的 URL，因爲這個字串不是以轉寄清單中的實際字串開頭。若要使 Cookie 轉寄至以這個機器名稱開始的 URL，必須將其新增至轉寄清單。

同樣的，Cookie 也不會轉寄至以 "`https://newmachine.eng.siroe.com/subdir`" 開始的 URL，除非已將其新增至清單中。

➤ **若要新增一個轉寄 Cookie URL**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 捲動至「轉寄 Cookie URL」編輯方塊並輸入想要的 URL。
7. 按一下「新增」以新增此項目至「轉寄 Cookie URL 清單」。
8. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
9. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定最長連線佇列長度

您可以指定閘道需要接受的最大並行運作連線。閘道不會接受任何超出此數字的連線嘗試。

➤ **若要指定最長連線佇列長度**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 捲動至「最長連線佇列長度」欄位並指定想要的連線數。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

指定閘道逾時

您可以指定閘道與瀏覽器的連線逾時時間，以毫秒爲單位。

➤ **若要指定閘道逾時**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 捲動「閘道逾時 (毫秒)」欄位並以毫秒爲單位指定想要的間隔。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

指定執行緒儲存區大小

您可以指定可以在閘道執行緒儲存區內預先建立的最大執行緒數目。

➤ 若要指定執行緒儲存區大小

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。

6. 捲動至 「最大執行緒儲存區大小」欄位並指定想要的執行緒數。
7. 按一下 「編輯閘道設定檔」頁面頂端或底部的 「儲存」以記錄變更。
8. 從終端機視窗重新啓動 「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定快取的通訊端逾時

您可以指定在閘道與入口網站伺服器的連線逾時時間，以毫秒爲單位。

➤ **若要指定快取的通訊端逾時**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取 「服務配置」標籤。
3. 按一下 「SRA 配置」下 「閘道」旁的箭頭。

   將顯示 「閘道」頁。
4. 按一下您想要設定其屬性之 「閘道設定檔」旁邊的 「編輯…」。

   便會顯示 「編輯閘道設定檔」頁面。
5. 按一下 「核心」標籤。
6. 捲動至 「快取的通訊端逾時」欄位並以毫秒爲單位指定想要的時間間隔。
7. 按一下 「編輯閘道設定檔」頁面頂端或底部的 「儲存」以記錄變更。
8. 從終端機視窗重新啓動 「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立 Portal Server 清單

你可以爲閘道配置多個 Portal Server 以服務請求。安裝閘道時，您應該已經指定與閘道合作的 Portal Server。這個 Portal Server 會依預設列示在 Portal Server 清單。您可以將更多 Portal Server 以 `http://portal server name:port number` 格式新增至清單中。閘道會以循環方式嘗試聯絡每個列出的 Portal Server 以服務請求。

➤ **若要指定 Portal Server**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 捲動至「Portal Server 清單」欄位並指定 Portal Server。

   在編輯欄位以 `http://portal server name:port number` 格式指定 Portal Server，並按一下「新增」。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定伺服器重試間隔

這個屬性會指定若 Portal Server、Rewriter 代理程式或 Netlet 代理程式變得無法存取 (例如當機或關機) 時，嘗試啓動它們之請求的時間間隔。

➤ **若要指定 Portal Server 重試間隔**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 捲動至「Portal Server 重試間隔」欄位並指定秒數。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。

8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用儲存外部伺服器 Cookie

當啓用「儲存外部伺服器 Cookie」選項時，閘道會儲存與管理任何經由閘道存取的協力廠商應用程式或伺服器的 cookie。即使應用程式或伺服器無法服務非 cookie 裝置或根據狀態管理的 cookie (因爲老舊原因)，其會透明遮罩應用程式或伺服器以防了解其正在服務非 cookie 裝置。有關無 Cookie 裝置與用戶端偵測的資訊，請參閱 *Sun ONE Identity Server Customization and API Guide* 。

➤ **若要儲存外部伺服器 Cookie**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 選取「儲存外部伺服器 Cookie」核取方塊以儲存外部伺服器 Cookie。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用從 URL 取得階段作業

選取「從 URL 取得階段作業」選項時，階段作業資訊會編碼爲 URL 的部分，不論支援 Cookie 與否。這表示閘道會驗證在 URL 中找到的階段作業資訊，而非從用戶端瀏覽器傳送的階段作業 Cookie。

➤ **若要從 URL 取得階段作業**

1. 以管理員的身份登入 Identity Server 管理主控台。

2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 選取「從 URL 取得階段作業」核取方塊以從 URL 取得階段作業資訊。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用將 Cookie 標示爲安全

當 cookie 標示爲安全時，瀏覽器會以更加的安全小心處理此 cookie。安全性的實施會根據瀏覽器而有所不同。必須啓用「啓用 Cookie 管理」屬性才可實現此功能。

➤ **將 Cookie 標示爲安全**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「核心」標籤。
6. 選取「將 Cookie 標示爲安全」核取方塊以將 Cookie 標示爲安全。

   確定「啓用 Cookie 管理」屬性爲啓用。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

「代理程式」標籤

在閘道服務中，使用 「代理程式」標籤，您可以執行下列工作：

- 啓用網路代理伺服器的使用
- 建立網路代理伺服器 URL 清單
- 建立不使用的代理伺服器 URL 清單
- 建立網域與子網域的代理伺服器清單
- 建立代理伺服器密碼清單
- 啓用代理伺服器自動配置 (PAC) 支援
- 指定 PAC 檔案位置
- 啓用透過網路代理伺服器的通道 Netlet

啓用網路代理伺服器的使用

➤ **若要啓用網路代理伺服器的使用**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取 「服務配置」標籤。
3. 按一下 「SRA 配置」下 「閘道」旁的箭頭。

   將顯示 「閘道」頁。
4. 按一下您想要設定其屬性之 「閘道設定檔」旁邊的 「編輯…」。

   便會顯示 「編輯閘道設定檔」頁面。
5. 按一下 「代理程式」標籤。
6. 選取 「使用代理伺服器」核取方塊以使用網路代理伺服器。
7. 按一下 「編輯閘道設定檔」頁面頂端或底部的 「儲存」以記錄變更。
8. 從終端機視窗重新啓動 「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立網路代理伺服器 URL 清單

您可以指定閘道僅能透過列於「網域與子網域的代理伺服器清單」中的網路代理伺服器聯絡特定 URL，即使已停用「使用代理伺服器」選項。您需要在「使用網路代理伺服器 URL」欄位中指定這些 URL。有關此值如何影響代理伺服器使用情形的詳細資訊，請參閱第 50 頁的「使用網路代理伺服器」。

➤ 若要指定網路代理伺服器的 URL

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「代理程式」標籤。
6. 在「使用網路伺服器 URL」編輯方塊中以 `http://host name.subdomain.com` 格式輸入想要的 URL。按一下「新增」。

   URL 會新增至「使用網路伺服器 URL」清單。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立不使用的代理伺服器 URL 清單

閘道嘗試直接連接列於「不要使用網路代理伺服器 URL」清單的 URL。網路代理伺服器並不會用於連接這些 URL。

➤ 若要指定不使用的 URL

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。

4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。

5. 按一下「代理程式」標籤。

6. 在「不要使用網路伺服器 URL」編輯方塊中鍵入想要的 URL 並按一下「新增」。

   URL 會新增至「不要使用網路伺服器 URL」清單。

7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。

8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立網域與子網域的代理伺服器清單

➤ **若要指定網域與子網域的代理伺服器**

有關如何將代理伺服器資訊套用至不同主機的資訊，請參閱第 50 頁的「使用網路代理伺服器」。

1. 以管理員的身份登入 Identity Server 管理主控台。

2. 選取「服務配置」標籤。

3. 按一下「SRA 配置」下「閘道」旁的右箭頭。

   將顯示「閘道設定檔」頁。

4. 按一下您要設定其屬性之閘道設定檔的「編輯」。

   便會顯示「編輯閘道設定檔」頁面。

5. 按一下「代理程式」標籤。

6. 捲動至「網域與子網域的代理伺服器」編輯方塊，並鍵入想要的資訊與按一下「新增」。項目會新增至「網域與子網域的代理伺服器清單」方塊。

   輸入代理伺服器資訊的格式如下：

   ```
   domainname proxy1:port1|subdomain1 proxy2:port2|subdomain2
   proxy3:port3|* proxy4:port4
   ```

   * 表示 * 之後定義的代理伺服器會用於所有網域與子網域 (如果沒有特別說明)。

   若您沒有指定代理伺服器連接埠，將依預設使用連接埠 8080。

7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

建立代理伺服器密碼清單

如果代理伺服器需要認證以存取某些或全部網站，您必須設定需要的使用者名稱與密碼，以使閘道認證至指定的代理伺服器。

➤ **若要指定代理伺服器密碼**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「代理程式」標籤。
6. 捲動至「代理伺服器密碼清單」欄位，並鍵入每個代理伺服器的資訊與按一下「新增」。

   輸入代理伺服器資訊的格式如下：

   proxyserver|username|password

   proxyserver 對應至定義於「網域與子網域代理伺服器清單」的代理伺服器。
7. 爲所有需要認證的代理伺服器重複步驟 6。
8. 按一下頁面頂端或底部的「儲存」記錄變更。
9. 從終端機視窗重新啓動「閘道」：

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

啓用代理伺服器自動配置 (PAC) 支援

若您選取此選項以啓用 PAC，則會忽略提供於「網域與子網域代理伺服器」欄位的資訊。閘道只會使用 PAC 檔案用於內部網路配置。有關 PAC 檔案的資料，請參閱第 56 頁的「使用代理伺服器自動配置」。

➤ **若要啓用 PAC 支援**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「代理程式」標籤。
6. 選取「啓用 PAC 支援」核取方塊以啓用 PAC 支援。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定 PAC 檔案位置

➤ **若要指定 PAC 檔案位置**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「代理程式」標籤。
6. 捲動至「PAC 檔案位置」欄位並鍵入 PAC 檔案的名稱與位置。

7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用透過網路代理伺服器的通道 Netlet

➤ **若要啓用透過網路代理伺服器的通道 Netlet**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「代理程式」標籤。
6. 選取「透過網路代理伺服器的通道 Netlet」核取方塊以啓用通道。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

「安全性」標籤

使用「閘道」服務中的「安全性」標籤，您將可以執行下列工作：

- 建立未驗證的 URL 清單
- 建立啓用憑證的閘道主機清單
- 允許 40 位元的瀏覽器連線
- 啓用 SSL 2.0 版
- 啓用 SSL 加密選項
- 啓用 SSL 3.0 版

- 停用空加密
- 建立「信任的 SSL 網域清單」
- 配置個人數位證書 (PDC) 認證

建立未驗證的 URL 清單

您可以指定某些 URL 不需要任何驗證。這些一般是包括影像的目錄與資料夾。

➤ **若要指定未驗證的 URL 路徑**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 捲動至「未驗證的 URL」欄位並以 `folder/subfolder` 格式輸入想要的資料夾路徑。

   鍵入的非完全合格的 URL (例如，/images) 會視爲入口網站 URL。

   若要新增非入口網站 URL，請鍵入完全合格的 URL。
6. 按一下「新增」以新增此項目至「未驗證的 URL」清單。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立啓用憑證的閘道主機清單

➤ **若要新增閘道至啓用憑證的閘道主機清單**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。

   所有服務都會顯示在左窗格中。

3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   「閘道設定檔」頁面隨即顯示於右窗格上。

4. 按一下您要爲其啓用以憑證爲基礎驗證的設定檔旁的「編輯…」。

5. 按一下「安全性」標籤。

6. 新增閘道名稱至啓用憑證的閘道主機清單。

   以 `host1.sesta.com` 格式新增閘道。

7. 按一下「新增」。

允許 40 位元的瀏覽器連線

若想要允許 40 位元 (弱) 安全插槽層 (SSL) 連線，則選取這個選項。若沒有選取這個選項，就只支援 128 位元連線。

若您停用這個選項，則使用者必須確定瀏覽器的配置支援必要的連線類型。

備註 若爲 Netscape Navigator 4.7x 使用者必須執行下列作業：

- 在 Communicator 功能表中「工具」之下選取「安全資訊」。
- 在左窗格中按一下「助手」連結。
- 在「進階安全性 (SSL) 配置」之下按一下「配置 SSL v2」或「配置 SSL v3」。
- 啓用必要的密碼。

➤ **若要允許 40 位元的瀏覽器連線**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。

4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。

5. 選取「允許 40 位元瀏覽器」核取方塊以啓用 40 位元瀏覽器連線。

6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 SSL 2.0 版

您可以啓用或停用 SSL 2.0 版。停用 SSL 2.0 表示只支援舊版 SSL 2.0 的瀏覽器將不能得到認證至 Secure Remote Access。這可確保較大的安全層級。

➤ **若要啓用 SSL 2.0 版**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 選取「啓用 SSL 2.0 版」核取方塊以啓用 2.0 版。

   此選項的預設值爲啓用。
6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 SSL 加密選項

Secure Remote Access 支援一定數量的標準密碼。您可以選擇支援所有預先封裝的密碼，或單獨選擇想要的密碼。您可以爲每個閘道實例選擇特定的 SSL 密碼。若用戶端站台存在任何已選取的密碼，則會成功進入 SSL 訊號交換模式。

➤ **若要啓用個別加密選擇**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。

3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。

4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。

5. 捲動至「啓用 SSL 加密選項」欄位並選取此選項。

   這個選項允許您在 SSL2、SSL3 與 TLS 密碼清單中選取想要的密碼。

6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。

   您可以選取將在您的用戶端站台支援的密碼。取消選取「啓用個別 SSL 加密」選項將自動選取所有已列示的密碼。

7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 SSL 3.0 版

您可以啓用或停用 SSL 3.0 版。停用 SSL 3.0 表示只支援舊版 SSL 3.0 的瀏覽器將不能取得認證以存取 Secure Remote Access。這可確保較大的安全層級。

➤ **若要啓用 SSL 3.0 版**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。

4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。

5. 選取「啓用 SSL 3.0 版」核取方塊以啓用 3.0 版。
6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

停用空加密

➤ **若要停用空加密**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 選取「停用空加密」核取方塊以停用空加密。
6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立「信任的 SSL 網域清單」

➤ **若要建立「信任的 SSL 網域清單」**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 捲動至「信任的 SSL 網域清單」，並輸入網域名稱與按一下「新增」。
6. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

配置個人數位證書 (PDC) 認證

PDC 會由「認證機構 (CA)」核發且使用 CA 的私人金鑰簽署。CA 會在核發認證之前驗證請求者的身份。因此 PDC 的出現是一個非常具有權威的認證機制。

PDC 包含所有者的公開金鑰、所有者名稱、過期日期、核發數位證書的「認證機構」名稱、序號與一些其他資訊。

使用者可以使用 PDC 與已編碼的裝置，例如 Portal Server 中用於認證的智慧卡、與 Java 卡。已編碼裝置會包含一個等同於卡中 PDC 的電子文件。使用者使用其中一個機制登入，不會顯示登入畫面且不會顯示認證畫面。

PDC 認證會處理相關的數個步驟：

1. 從瀏覽器中，使用者可以輸入連線請求，例如 `https://my.sesta.com`。

   對這個請求的回應會視至 `my.sesta.com` 的閘道是否已配置爲接受證書而定。

備註 當閘道配置爲接受證書時，將僅接受使用證書的登入請求，不接受其他種類登入請求。

   閘道會檢查證書是否由已知的「認證機構」核發，是否已過期與是否被竄改。若證書有效，則閘道會讓使用者繼續執行驗證程序的下一步驟。

2. 閘道會將此證書傳遞到伺服器中 PDC 認證模組。

➤ 若要配置 PDC 與編碼裝置

配置 PDC 與已編碼裝置會包括下列步驟：

1. 在 Portal Server 機器上的 *portal-server-install-root*`/SUNWam/lib/AMConfig.properties` 檔案中新增以下指令行：

   ```
   com.iplanet.authentication.modules.cert.gwAuthEnable=yes
   ```

2. 將必要的證書匯入要啓用 PDC 的閘道的證書資料庫

   有關說明，請參閱第 7 章，「證書」。

3. 請執行下列子任務：

➤ 若要註冊需要的服務

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。

3. 在「檢視」下拉功能表中按一下「服務」。

   若已註冊，則「核心」服務將隨即顯示於瀏覽窗格中。若尚未註冊，則可以與「證書」服務並行完成。

4. 按一下導覽窗格中的「註冊」。

   在資料窗格中出現服務屬性清單。

5. 選取「證書」核取方塊。

   顯示於瀏覽窗格中的「證書」服務說明服務已註冊。

6. 按一下「註冊」。

➤ 若要修改必要屬性

1. 選取「識別管理」標籤。
2. 從「檢視」下拉功能表中選擇「服務」。
3. 按一下左窗格中「認證」之下「核心」旁的箭頭。

   將顯示「核心」頁。

4. 按一下「證書」旁的箭頭。

   顯示訊息「此服務目前不存在此範例。是否要建立？」

5. 按一下「建立」。

   「證書」頁隨即顯示於資料窗格中。

6. 視需要修改屬性。

   按一下頁面頂端的「儲存」記錄變更。

7. 按一下「核心」旁的箭頭。
8. 在「使用者設定檔」下拉功能表中選擇「動態建立」。
9. 按一下「儲存」。
10. 從終端機視窗重新啓動「閘道」：

    gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

➤ 若要新增信任的遠端主機

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取需要的組織。
3. 按一下「證書」旁的箭頭。

4. 按一下「建立…」以建立範本。
5. 按一下「儲存」。
6. 捲動至名爲「信任的遠端主機」的清單方塊。
7. 無任何反白顯示並按一下「移除」。
8. 在文字方塊中鍵入任何文字並按一下「新增」。

➤ **若要使得使用者可以無需設定檔即可登入 (登入時動態建立設定檔)**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選擇需要的組織。
3. 從「檢視」下拉功能表中選取「服務」。

   此服務會顯示於左窗格中。
4. 按一下「核心」旁的箭頭。
5. 在「使用者設定檔」下拉功能表中選擇「動態建立」。
6. 按一下「儲存」。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

➤ **若要建立一個包含證書模組的閘道範例**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選擇需要的組織。
3. 從「檢視」下拉功能表中選取「服務」。

   此服務會顯示於左窗格中。
4. 按一下「認證配置」核心服務旁的箭頭。

   顯示「服務實例清單」。
5. 按一下「新增…」。

   顯示「服務實例清單」。
6. 輸入服務實例名稱 gatewaypdc。

   備註：您必須使用這個名稱。

7. 按一下「提交」。

   顯示「服務實例清單」。

8. 按一下 gatewaypdc 以編輯服務。

   會顯示 gatewaypdc 屬性頁面。

9. 按一下「編輯…」

   隨即顯示組織的「模組清單」。

10. 按一下「新增…」

    顯示「新增模組」頁面。

11. 在「模組名稱」欄位選擇「證書」，並選擇一個「旗標」選項。

12. 按一下「確定」。

13. 在閘道機器中新增 CA 機構中的根 CA。

    有關資訊，請參閱 *Sun ONE Portal Server, Secure Remote Access Installation Guide* 中第四章「安裝 SSL 認證」的「在認證機構安裝認證」。

14. 從終端機視窗重新啓動「閘道」：

    gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

「Rewriter」標籤

使用「閘道」服務中的「Rewriter」標籤，您將可以執行下列工作：

- 啓用所有 URL 的重寫
- 建立 URI 與規則集對映清單
- 建立剖析器至 MIME 對映清單
- 指定預設網域與子網域
- 建立不要改寫 URI 清單
- 啓用 MIME 推測
- 建立剖析器至 URI 對映清單
- 啓用混淆
- 指定混淆器種子字串

- 建立不要混淆 URI 清單
- 讓閘道通訊協定與原始 URI 通訊協定相同

啓用所有 URL 的重寫

若您啓用閘道服務中「啓用所有 URI 的重寫」選項，則 Rewriter 會重寫所有 URL 而不會將其於「網域與子網域代理伺服器清單」中的項目進行核對。忽略網域與子網域清單的代理伺服器項目。

➤ **若要啓用閘道以改寫所有 URL**

1. 以管理員的身份登入 Sun™ ONE Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性之閘道設定檔的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「Rewriter」標籤，「基礎」子區段。
6. 選取「啓用所有 URI 的重寫」核取方塊，啓用「閘道」以重寫所有 URL。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立 URI 與規則集對映清單

規則集會建立於 Identity Server 管理主控台中 Portal Server 配置之下的 Rewriter 服務中。有關詳細資料，請參閱 *Sun ONE Portal Server* 管理員指南 。

建立規則集之後，您可以使用 URI 至規則集對映清單將網域與規則集關聯在一起。下列兩個項目會依預設新增至 URI 至規則集對映清單：

- *://*.Sun.COM/portal/*|default_gateway_ruleset

  其中 sun.com 是安裝入口網站的網域，而 /portal 是入口網站的安裝環境
- *|generic_ruleset

這表示對於預設網域的所有頁面，將套用預設閘道規則集。對於其他頁面，則套用常規規則集。預設閘道規則集與常規規則集爲預先封裝的規則集。

備註 對於所有顯示於桌面的內容，將使用預設網域的規則集，無論內容來自何處。

例如，假設桌面被配置爲移除 URL `yahoo.com` 的內容。Portal Server 位於 `sesta.com`。將套用 `sesta.com` 規則至獲取的內容。

備註 您爲其指定規則集的網域必須列於網域與子網域的代理伺服器清單中。

➤ 若要將 URI 對應至規則集

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「基礎」子區段。
6. 捲動至「URI 至規則集對映」欄位。
7. 在「URI 至規則集對映」欄位中鍵入需要的網域或主機名稱以及規則集並按一下「新增」。

   此項目會新增至「URI 至規則集對映」清單。

   指定網域或主機名稱以及規則集的格式如下所示：

   ```
   domain name|ruleset name
   ```

   例如：

   ```
   eng.sesta.com|default
   ```

備註 套用規則集的優先順序爲 hostname-subdomain-domain。

例如，假設您的以網域爲基礎規則集清單中包含下列項目：

sesta.com|ruleset1

eng.sesta.com|ruleset2

host1.eng.sesta.com|ruleset3

ruleset3 可套用於 host1 上的所有頁面。

ruleset2 可套用於 eng 子網域中的所有頁面，除了擷取於 host1 中的頁面。

ruleset1 可套用於 sesta.com 網域中的所有頁面，除了擷取於 eng 子網域與 host1 中的頁面。

8. 按一下頁面頂端或底部的「儲存」記錄變更。
9. 從終端機視窗重新啓動「閘道」：

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

Outlook Web Access 的規則集

Secure Remote Access 支援安裝 MS Exchange 2000 的 Outlook Web Access (OWA)。

➤ 若要配置 OWA 規則集

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 在「URI 至規則集對映」欄位中，輸入安裝 Exchange 2000 的服務其名稱，隨後輸入 exchange 2000 Service Pack 3 OWA 規則集。

   例如：

   exchange.domain.com|exchange_2000sp3_owa_ruleset.

建立剖析器至 MIME 對映清單

Rewriter 有四個不同的剖析器以根據內容類型 - HTML、JAVASCRIPT、XML 與 CSS - 剖析網頁。依預設共用 MIME 類型會與這些剖析器相關。您可以在「閘道」服務中的「剖析器至 MIME 對應」欄位中將新 MIME 類型與這些剖析器相關聯。此將 Rewriter 功能延伸至其他 MIME 類型。

使用分號或逗號 (";" 或 ",") 分隔多個項目：

例如：

HTML=text/html;text/htm;text/x-component;text/wml; text/vnl/wap.wml

意味任何含有這些 MIME 的內容會被傳送到 HTML Rewriter 而 HTML 規則將被套用以重寫 URL。

提示 移除 MIME 對映清單中不需要的剖析器可以提高作業速度。例如，若您確定某些內部網站的內容將不會有任何 JavaScript，可以將 JAVASCRIPT 項目從 MIME 對映清單中移除。

➤ **若要指定 MIME 對映**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 ñ*gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「基礎」子區段。
6. 捲動至「剖析器至 MIME 對映」欄位，並在編輯方塊中新增需要的 MIME 類型。使用分號或逗號以分隔多個項目。

   以 `HTML=text/html;text/htm` 格式指定項目
7. 按一下「新增」以新增需要的項目至清單中。
8. 按一下頁面頂端或底部的「儲存」記錄變更。
9. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定預設網域與子網域

當 URL 僅包括主機名稱而沒有網域與子網域時，預設網域與子網域將特別有用。在此情況下，「閘道」將假設主機名稱位於預設網域與子網域中，並繼續執行相應的操作。

例如，若 URL 中的主機名稱爲 `host1`，且預設網域與子網域被指定爲 `red.sesta.com`，則主機名稱會被解析爲 `host1.red.sesta.com`。

➤ **若要指定預設網域與子網域**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 按一下「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的右箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性之閘道設定檔的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 按一下「Rewriter」標籤，「基礎」子區段。
6. 捲動至「預設網域子網域」欄位並以 `subdomain.domain name` 格式鍵入需要的預設值。
7. 按一下「編輯閘道設定檔」頁面頂端或底部的「儲存」以記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立不要改寫 URI 清單

➤ **若要指定預設網域與子網域**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。

5. 按一下「Rewriter」標籤，「進階」子區段。
6. 捲動至「不要重寫 URI 清單」欄位，並在編輯方塊中新增 URI。

   備註：新增 #* 至這個清單以允許改寫 URI，即使 href 規則是規則集的一部分。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 MIME 推測

Rewriter 會根據網頁的 MIME 類型選擇剖析器。某些網路伺服器例如 WebLogic 與 Oracle 不會傳送 MIME 類型。若要解決這個問題，可以啓用 MIME 推測，方法是新增資料至「剖析器至 URI 對映」清單方塊。

➤ **若要啓用 MIME 推測**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。
6. 選取「啓用 MIME 推測」核取方塊以啓用 MIME 推測。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立剖析器至 URI 對映清單

若已啓用 MIME 推測核取方塊，且伺服器沒有傳送 MIME 類型，可使用這個清單方塊以對映剖析器至 URI。

由分號分隔多個 URI。

例如 HTML=*.html; *.htm;*Servlet

表示 HTML Rewriter 會用於改寫任何含有 html、htm，或 Servlet 副檔名的頁面內容。

➤ **若要剖析 MIME 對映**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。
6. 捲動至「剖析器至 MIME 對映」欄位，並新增資料至編輯方塊。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用混淆

混淆允許 Rewriter 改寫 URI，如此便看不見頁面的「內部網路 URL」。

➤ **若要啓用混淆**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。

4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。

5. 按一下「Rewriter」標籤，「進階」子區段。
6. 選取「啓用混淆」核取方塊以啓用混淆。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

指定混淆器種子字串

種子字串會用於模糊 URI。其爲一個由混淆演算法產生的隨機字串。

備註 若此種子字串已變更或「閘道」已重新啓動，則無法將已混淆的 URI 加入書籤。

➤ **若要指定混淆種子字串**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。

4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。

5. 按一下「Rewriter」標籤，「進階」子區段。
6. 捲動至「混淆器種子字串」欄位，並新增字串至編輯方塊。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

建立不要混淆 URI 清單

某些應用程式 (例如 applet) 需要網際網路 URI 且無法被混淆。若要指定那些應用程式，請新增 URI 至清單方塊。

例如您新增

```
*/Applet/Param*
```

至清單方塊，如果內容 URI `http://abc.com/Applet/Param1.html` 與規則集匹配，則 URL 不會被混淆。

➤ **若要指定「不要混淆 URI 清單」**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。
6. 捲動至「不要混淆 URI 清單」欄位，並新增 URI 至編輯方塊。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

讓閘道通訊協定與原始 URI 通訊協定相同

當閘道以 http 與 https 兩種模式執行時，可以啓用 Rewriter 以使用一致的通訊協定存取 HTML 內容的參照資源。

例如，若原始 URL 爲 `http://intranet.com/Public.html` 則會新增 http 閘道。若原始 URL 爲 `https://intranet.com/Public.html` 則會新增 https 閘道。

備註 這將僅套用至靜態 URI，而非產生於 Javascript 的動態 URI。

➤ **若要讓閘道通協定與原始 URI 通訊協定相同**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道設定檔」頁。
4. 按一下您要設定其屬性的閘道設定檔。

   顯示閘道 - *gateway-profile-name* 頁面。
5. 按一下「Rewriter」標籤，「進階」子區段。
6. 選取「讓閘道通訊協定與原始的 URI 通訊協定相同」核取方塊。
7. 按一下頁面頂端或底部的「儲存」記錄變更。
8. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

「記錄」標籤

使用「閘道」服務中的「記錄」標籤，您將可以執行下列工作：

- 啓用記錄
- 啓用 Netlet 記錄

啓用記錄

您可以指定閘道日誌檔以擷取每個階段作業的最少資訊或詳細資訊。Identity Server 配置屬性記錄區段的「記錄位置」屬性中指定有目錄，系統將在其中儲存日誌資訊。此日誌位於 Portal Server 機器上。

此日誌名稱使用下列慣例：

`srapGateway_`*gatewayhostname_gateway-profile-name*

日誌資訊可根據 Identity Server 配置中的指定值被儲存爲檔案或資料庫。日誌中的欄位爲以逗號分隔的 ASCII 值，且可匯出至其他資料分析工具。

➤ 若要啓用閘道記錄

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 選取「啓用記錄」核取方塊以啓用閘道記錄。
6. 選取「啓用按階段作業記錄」核取方塊以擷取日誌資訊，例如「用戶端位址」、「要求類型」與「目標主機」。

備註 日誌資訊僅會在已啓用「啓用記錄」欄位時才可以擷取。

7. 選取閘道的「啓用按階段作業記錄」以擷取詳細的日誌資訊，例如「用戶端」、「要求類型」、「目標主機」、「要求類型」、「用戶端要求的 URL」、「用戶端 Post Data 大小」、「階段作業 ID」、「回應結果代碼」與「完成回應大小」。

備註 詳細的日誌資訊僅會在已啓用「啓用每次階段作業記錄」核取方塊時才可以擷取。

8. 按一下頁面頂端或底部的「儲存」記錄變更。
9. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

啓用 Netlet 記錄

選取此選項之後，您就可以啓用 Netlet 相關活動的記錄。Netlet 日誌將包含下列關於 Netlet 階段作業的詳細資訊：

- 啓動時間
- 來源位址
- 源連接埠
- 伺服器位址
- 伺服器連接埠
- 停止時間
- 狀態 (啓動或停止)

➤ 若要啓用 Netlet 記錄

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「服務配置」標籤。
3. 按一下「SRA 配置」下「閘道」旁的箭頭。

   將顯示「閘道」頁。
4. 按一下您想要設定其屬性之「閘道設定檔」旁邊的「編輯…」。

   便會顯示「編輯閘道設定檔」頁面。
5. 選取「啓用 Netlet 記錄」核取方塊以啓用 Netlet 記錄。
6. 按一下頁面底部的「儲存」以記錄變更。
7. 從終端機視窗重新啓動「閘道」：

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

第 10 章

配置 NetFile

本章會介紹如何透過 Sun™ ONE Identity Server 管理主控台來配置 NetFile。

備註 按一下 Identity Server 管理主控台右上角的「文件」，然後按一下 SRA 說明以快速取得有關所有 Secure Remote Access 屬性的參考。

若要配置 NetFile 屬性，請遵循下列步驟：

1. 以管理員的身份登入 Sun™ ONEIdentity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   在此處，按一下適當的標籤。

   - 主機標籤
   - 許可權標籤
   - 「檢視」標籤
   - 「作業」標籤
   - 「一般」標籤

標籤以及可在每個標籤底下進行配置的屬性如下所列。

主機標籤

使用「主機」標籤底下的 NetFile 服務，您將可以執行下列工作：

- 指定 OS 字元集
- 指定主機偵測順序
- 配置共用主機清單
- 指定預設網域
- 指定 Windows 網域 / 工作群組
- 指定預設 WINS/DNS 伺服器
- 指定存取不同的主機類型
- 配置允許的主機清單
- 配置拒絕的主機清單

指定 OS 字元集

您可以指定在與主機通訊時用來作爲預設編碼的字元集。預設值是 UTF-8。

注意	如果字元集並未正確指定，將無法預測機器的行爲以及出現的錯誤訊息。

➤ 若要指定 OS 字元集

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「主機」標籤，子區段「配置」。
8. 捲動至「OS 字元集」欄位並選取字元集碼。

9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

指定主機偵測順序

➤ **若要指定主機偵測順序**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「主機」標籤，子區段「配置」。
8. 捲動至「主機偵測順序」欄位並選取主機類型。
9. 使用「上移」和「下移」按鈕以變更主機偵測順序。
10. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

配置共用主機清單

您可以配置一個主機清單，讓所有遠端 Netfile 使用者皆可以透過 Netfile 存取該清單中的主機。您必須爲每個要新增的主機指定下列資訊：

主機名稱 - 您可以鍵入簡單的主機名稱或完全合格的名稱。若您提供的主機名稱與使用者配置的主機名稱相匹配，則兩個資訊集將會合併且使用者指定的值會覆寫您指定的值。

例如，假設您已配置 4 個共用主機 - `sesta`, `siroe`、`florizon` 與 `abc`。使用者配置 3 個主機，其中 2 個是 `sesta` 與 `siroe`。使用者指定的值會在這類衝突狀況中覆寫管理員指定的值。`florizon` 與 `abc` 也會列示於使用者的 NetFile，且使用者可以在那些主機上執行各種不同作業。若您在「拒絕的主機清單」中列示 `florizon`，則 `florizon` 會列示於使用者的 NetFile 中，但不可以在 `florizon` 中執行任何作業。

主機類型 - 若使用者新增的主機已列示於「共用主機」清單，則會優先使用使用者設定。若在此類型中有衝突，則不會爲該使用者新增管理員新增的共用。若使用者與管理員新增相同共用，則此共用將新增，但將優先使用由使用者設定的密碼。

編碼 - 若在此處指定的值與使用者設定的值之間有衝突，則優先使用使用者設定的值。若您的設定值爲空白或無效，則會考慮用戶端 OS (使用者的機器) 的字元集。

備註	使用者可以在 NetFile 用戶端應用程式中編輯這些值。但這些編輯後的值只對目前的階段作業有效。如果使用者登出後再次登入，則不會保留編輯後的值。

➤ 若要配置共用主機清單

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「主機」標籤，子區段「配置」。
8. 捲動至「共用主機」欄位。

   若要刪除共用主機，請選中共用主機項目 (若有的話) 並按一下「刪除」。
9. 若要新增共用主機，請按一下「新增」。

   隨即顯示 NetFile > 加入 NetFile 主機頁面。

   a. 在下列的欄位中輸入需要的資訊：

      - 主機名稱
      - 主機類型
      - 編碼
      - Windows 網域 / 工作群組
      - 使用者名稱
      - 密碼

b. 對於您要新增的共用，請在下列欄位輸入需要的資訊並按一下 「新增至清單」：

- 共用清單
- 共用名稱
- 共用密碼

10. 按一下 「確定」。

11. 爲您要新增或刪除的每個共用主機重複設置這些資訊。

若您刪除 「共用主機清單」中的 「主機名稱」，請按一下 「刪除」並選取 「共用清單」中的 「主機名稱」。然後按一下 「移除」。

12. 按一下 NetFile 頁面頂端或底部的 「儲存」記錄變更。

指定預設網域

您可以指定 NetFile 聯絡允許的主機需要使用的預設網域。

僅在使用者當使用 NetFile 新增主機時未指定完全合格的主機名稱時，這個預設網域值才可用。

注意 請確定 「預設網域」欄位不是空白，且包含有效的網域名稱。

➤ **若要指定預設網域**

1. 以管理員的身份登入 Identity Server 管理主控台。

2. 選取 「識別管理」標籤。

3. 從 「檢視」下拉式清單中選取 「組織」。

4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。

5. 從 「檢視」清單方塊中選取 「服務」。

6. 按一下 「SRA 配置」下 NetFile 旁的箭頭。

將顯示 NetFile 頁。

7. 按一下 「主機」標籤，子區段 「配置」。

8. 捲動至 「預設網域」欄位並輸入預設網域名稱。

9. 按一下 NetFile 頁面頂端或底部的 「儲存」記錄變更。

指定 Windows 網域 / 工作群組

此爲使用者選擇存取 Windows 主機的預設 Windows 網域或工作群組。

使用者可以覆寫這個值，方法是在新增機器時，指定不同值。

➤ **若要指定預設 Windows 網域或工作群組**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「主機」標籤，子區段「配置」。
8. 捲動至「預設 Windows 網域 / 工作群組」欄位並輸入預設網域或工作群組名稱。
9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

指定預設 WINS/DNS 伺服器

這個是 NetFile 用於存取 windows 主機的 WINS/DNS 伺服器。

➤ **若要指定預設 WINS/DNS 伺服器**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「主機」標籤，子區段「配置」。

8. 捲動至「預設 WINS/DNS 伺服器」欄位並輸入預設 Windows 或 DNS 伺服器名稱。
9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

指定存取不同的主機類型

您可以指定使用者是否可以存取特定主機，例如 Windows、FTP、NFS 或 Netware 主機。您可以設定選項以允許或拒絕存取每個主機類型。所有這些選項依預設皆爲啓用。

➤ **若要指定存取不同的主機類型**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「主機」標籤，子區段「存取」。
8. 按一下其存取爲啓用的主機類型。您可以選擇：
   - 允許存取 Windows 主機
   - 允許存取 FTP 主機
   - 允許存取 NFS 主機
   - 允許存取 Netware 主機

   選取某選項可以讓使用者存取其對應的特定主機類型。清除選取某核取方塊以防止使用者存取該類型主機。
9. 按一下頁面頂端或底部的「儲存」記錄變更。

配置允許的主機清單

依預設，因爲這個清單中輸入的 *，允許使用者透過 NetFile 存取所有主機。若您希望變更該預設，請於清單中移除 * 並僅指定使用者需要透過 NetFile 存取的主機。否則，您可以在此處保留 * 項目，並於「拒絕的主機」清單中指定您要拒絕存取的主機。在這個情況中，允許存取所有的主機，「拒絕的主機」清單中指定的主機除外。

有關詳細資料，請參閱第 271 頁「配置拒絕的主機清單」。

備註 若「允許的主機」與「拒絕的主機」兩個清單皆爲空白，則不允取存取任何主機。

➤ 若要建立允許的主機清單

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「主機」標籤，子區段「存取」。
8. 捲動至「允許的主機」欄位。在編輯欄位中輸入您要允許存取的主機名稱，並按一下「新增」。

   主機名稱會新增至「允許的主機清單」清單方塊中。
9. 按一下頁面頂端或底部的「儲存」記錄變更。

配置拒絕的主機清單

如第 265 頁「配置共用主機清單」所述指定可用的共用主機清單之後，您也可以指定拒絕使用者透過 Netfile 存取的主機清單。

備註 若您拒絕存取某主機，並且使用者已在 NetFile 視窗中新增這個主機，已拒絕的主機將繼續顯示於使用者的 NetFile 視窗中。但使用者將無法在主機上執行任何作業。

在 NetFile Java2 中，拒絕的主機，若顯示於應用程式中，會使用紅十字標識以表示其爲不可存取。

備註 若「允許的主機」與「拒絕的主機」兩個清單皆爲空白，則不允取存取任何主機。

➤ 若要建立拒絕的主機清單

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「主機」標籤，子區段「存取」。
8. 捲動至「拒絕的主機」欄位。在編輯欄位中輸入您要拒絕存取的主機名稱。
9. 按一下「新增」。

   主機名稱會新增至「拒絕的主機」清單方塊中。
10. 按一下頁面頂端或底部的「儲存」記錄變更。

許可權標籤

使用 NetFile 服務中的「許可權」標籤，您可以允許或拒絕使用者從遠端主機的執行下列工作：

- 重新命名檔案
- 刪除檔案與資料夾
- 上傳檔案
- 下載檔案與資料夾
- 搜尋檔案
- 郵寄檔案
- 壓縮檔案
- 變更使用者 ID

  此選項可讓您指定使用者是否可以使用 NetFile，以不同的 ID 連接主機。在大型組織中，使用者可能有多個使用者 ID。您可能希望限制使用者使用單一使用者 ID。如果是這種情況，您可以停用「允許變更使用者 ID」選項。如此可以避免特定組織中的所有使用者變更他們的使用者 ID，並限制他們必須使用以單一 ID (桌面登入 ID) 透過 NetFile 連接至主機。另一種情況是使用者可能在不同機器上會有不同的登入 ID，在此情況下，您可能希望允許使用者依需要變更 ID。

- 變更 Windows 網域

  這個選項適用於 NT 網域。

  若當新增系統時，使用者在「使用者 NT 網域」名稱欄位中指定的網域名稱無效，將會顯示錯誤訊息。如果使用者在之後編輯主機資訊，指定的網域名稱無效時，則不會出現錯誤訊息。

  若使用者指定網域名稱，則需要指定網域的使用者名稱與密碼。若需要使用主機的使用者名稱與密碼，則使用者需要移除「使用者 NT 網域」名稱欄位中的網域。

這些選項依預設皆爲啓用。

➤ 若要啓用 / 停用許可權

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。

4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「許可權」標籤。
8. 捲動至需要的「允許」欄位並按一下核取方塊以允許執行相應工作。
9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

備註 若您在使用者開始使用 NetFile 之後停用這些選項，則只有在使用者登出 NetFile 並重新登入後，此項變更才會生效。

「檢視」標籤

使用 NetFile 服務中的「檢視」標籤，您將可以執行下列工作：

- 指定 NetFile 視窗大小
- 指定 NetFile 視窗位置

指定 NetFile 視窗大小

您可以在使用者桌面上以像素爲單位指定 NetFile 視窗的大小。預設值爲 `700|400` (以像素爲單位)。若您輸入的值無效，NetFile 會使用此預設值。

備註 使用者也可以在 (使用者可用的) 受限的管理主控台上編輯這個值。若使用者在桌面重新調整 NetFile 視窗的大小，您指定的值將會由新值取代。

➤ **若要指定 NetFile 的視窗大小**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。

4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「檢視」標籤。
8. 捲動至「視窗大小」欄位並以像素爲單位輸入需要的視窗大小。

   以 `700|400` 的格式鍵入值，其中不包含任何空格。座標的形式爲 `x|y`。不可使用其他字元作爲分隔符號。
9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

指定 NetFile 視窗位置

您可以指定 NetFile 視窗出現在使用者桌面上的位置。預設值爲 `100|50` (以像素爲單位)。若您輸入的值無效，NetFile 會使用此預設值。

備註	使用者也可以在 (使用者可用的) 受限的管理主控台上編輯這個值。若使用者在桌面重新定位 NetFile 視窗，您指定的值將會由新值取代。

➤ **若要指定 NetFile 視窗的位置**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「檢視」標籤

8. 捲動至「視窗位置」欄位並輸入需要的視窗位置座標。

   以 `100|50` 的格式鍵入值，其中不包含任何空格。座標的形式爲 `x|y`。不可使用其他字元作爲分隔符號。

9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

「作業」標籤

使用 NetFile 服務中的「作業」標籤，您將可以執行下列工作：

- 指定暫存檔目錄
- 設定檔案上傳大小限制
- 指定搜尋目錄限制
- 指定壓縮屬性

指定暫存檔目錄

NetFile 需要爲不同檔案作業指定暫存目錄。預設的暫存目錄爲 `/tmp`。暫存檔會在執行需要的作業之後刪除。

若伺服器中未存在指定的暫存目錄，則需要建立。

確定正在執行網路伺服器的 ID (例如 `nobody` 或 `noaccess`) 具有指定目錄的 `rwx` 許可權。也確定 ID 對於需要的暫存目錄的完整路徑擁有 `rx` 許可權。

提示 您可以爲 NetFile 建立單獨的暫存目錄。如果您爲 Portal Server 所有模組指定了共用的暫存目錄，磁碟空間可能很快就會用完。如果暫存目錄已無空間，則 NetFile 將無法運作。

➤ **若要指定暫存目錄**

1. 以管理員的身份登入 Sun™ ONE Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。

5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「作業」標籤，「流量」子區段。
8. 捲動至「暫存目錄位置」欄位並輸入需要的暫存目錄位置。
9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

設定檔案上傳大小限制

您可以在此欄位中指定檔案可以上傳的最大大小。如果上傳的檔案大小超過此處指定的限制，將出現一個錯誤訊息，且無法上傳檔案。預設值是 5 MB。若您輸入一個無效的值，NetFile 會將此值重新設定爲預設值。

您可以爲不同的使用者指定不同的檔案上傳大小限制。

備註	指定上傳檔案的最大大小 (單位爲百萬位元組)。請輸入整數值。

➤ **若要設定檔案上傳大小限制**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「作業」標籤，「流量」子區段。
8. 捲動至「檔案上傳限制 (MB)」欄位。以百萬位元組爲單位輸入需要的大小限制。
9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

指定搜尋目錄限制

您可以配置在單一搜尋作業中，搜尋目錄的最大數目。如果有很多使用者同時登入，此項限制將有助於減少網路擁塞並加快存取速度。預設值爲 100。若您輸入的值無效，NetFile 會將此值重新設定爲預設值。在此欄位中僅輸入正整數。

假設使用者有一個名爲 A 的目錄，且假設 A 有 100 個子目錄。若您指定欲搜尋目錄的最大數目爲 100，此作業將會搜尋整個 A 目錄並停止。此搜尋作業無法繼續搜尋使用者電腦中的其他目錄，因爲在 A 目錄中已經達到 100 的限制值。若要繼續搜尋作業，使用者必須在下個目錄中以手動方式重新啓動搜尋作業。

以深度優先的方式執行搜尋作業。這表示搜尋作業會執行於使用者所選目錄中的所有子目錄，之後再移動至下一個目錄。

➤ 若要指定搜尋目錄限制

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「作業」標籤，「搜尋」子區段。
8. 捲動至「搜尋目錄限制」欄位並輸入需要的數字。

備註	請輸入整數值。

9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

指定壓縮屬性

➤ **若要指定預設壓縮類型**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「作業」標籤，「壓縮」子區段。
8. 捲動至「預設壓縮類型」欄位。

   選擇 Zip 或 GZip
9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

「一般」標籤

使用 NetFile 服務中的「一般」標籤，您可以指定 MIME 類型的配置檔案位置。

指定 MIME 類型配置檔案位置

需要此資訊決定回應內容類型以傳送至用戶端瀏覽器。瀏覽器需要此資訊以決定在 NetFile 開啓或下載作業期間與檔案相關聯的應用程式。在安裝期間會配置這個選項。

若需要使用 Portal Server 網路伺服器的 MIME 類型檔案，請指定位置：

portal-server-install-root`/SUNWam/servers/`*instance-name-of-web-server-machine*`/config`

備註 「MIME 類型配置檔案位置」屬性只可以在組織層級中設定。

➤ **若要指定 MIME 類型配置檔案位置**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」清單方塊中選取「服務」。
6. 按一下「SRA 配置」下 NetFile 旁的箭頭。

   將顯示 NetFile 頁。
7. 按一下「一般」標籤。
8. 捲動至「MIME 類型配置檔案位置」欄位並輸入至 MIME 類型配置檔案位置的完整路徑。
9. 按一下 NetFile 頁面頂端或底部的「儲存」記錄變更。

啓用 NetFile 除錯

除錯資訊位置會根據 Portal Server 節點 `AmConfig.properties` 檔案中 `com.iplanet.services.debug.directory` 屬性的設定而有所不同。

例如，若 `com.iplanet.services.debug.directory` 屬性值爲：

```
/var/opt/SUNWam/debug/
```

則 Netfile 的除錯資訊將位於 `/var/opt/SUNWam/debug` 目錄的 `srapNetFile` 檔案。

有關詳細資訊，請參閱 *Sun ONE Identity Server 管理員指南*。

第 11 章

配置 Netlet

本章會介紹如何透過 Sun™ ONE Identity Server 管理主控台來配置 Netlet 屬性。

備註 按一下 Identity Server 管理主控台右上角的「文件」，然後按一下 SRA 說明以快速取得有關所有 Secure Remote Access 屬性的參考。

可以在組織層級進行配置的所有屬性也可以在使用者層級進行配置。有關組織、角色和使用者層級屬性的詳細資訊，請參閱 *Sun ONE Identity Server 管理員指南*。

在使用者層級還可以配置某些其他屬性。如果您未在管理主控台中指定這些值，當使用者透過 Netlet 初次建立連線時，系統將會詢問此資訊。在下列情況，系統將會詢問使用者此資訊：

- 使用者擁有 Internet Explorer 4.x、5.x 或 6.x 以及 Java plug-in (1.3.1._01 版或 1.3.1_02 版)，已經在 Java Plug-in 控制台的「代理程式」標籤中啓用「使用瀏覽器設定」選項，並且已經在 Internet Explorer 的「本地區域網路設定」對話方塊中的「使用自動配置程序檔」欄位中指定了附加產品或 INS 檔案。
- 使用者安裝了 Netscape 6.2 與 Java plug-in (1.3.1._01 版或 1.3.1_02 版) 並且已經在 Java Plug-in 控制台的「代理程式」標籤中啓用「使用瀏覽器設定」選項。不會考慮使用者指定的任何代理伺服器設定。

在上面兩種情況中，Netlet 無法確定瀏覽器設定，因此系統會要求使用者提供下列資訊：

- 瀏覽器代理伺服器類型

  此屬性值可以是 DIRECT 或 MANUAL。如果使用者從下拉清單中選擇 DIRECT，Netlet 將會直接與閘道主機連接。

- 瀏覽器代理伺服器主機

指定需要的代理伺服器主機，Netlet 需要透過此主機進行連接。

- 瀏覽器代理伺服器連接埠

  指定代理伺服器主機上的連接埠，Netlet 需要透過此連接埠進行連接。

- 瀏覽器代理伺服器置換清單 (逗號分隔)

  指定您不希望 Netlet 透過代理伺服器連接的主機。此清單可以包含多個以逗號分隔的主機名稱。

- Netlet 密碼

  如果您已經在管理主控台中啓用重新認證，每當使用者透過 Netlet 連接應用程式時，便會顯示「Netlet 認證」對話方塊。使用者需要提供 Netlet 密碼。如果並未在管理主控台中啓用重新認證，使用者將不會有變更密碼的選項。

備註 依預設，Netlet 認證密碼爲 `srap-netlet`。

您可以在此欄位中爲使用者變更認證密碼。使用者也可以使用 Netlet 通道中的「編輯」按鈕來變更此認證密碼。

若您未啓用重新認證，將在使用者桌面顯示一個連接埠警告對話方塊，說明正在通過 Netlet 的連接埠嘗試建立連線。「Netlet 認證」對話方塊不會出現。

備註 如果已停用 Netlet 服務中的選項，則也可能不會出現連接埠警告對話方塊。

若要配置 Netlet 屬性，請在組織層級遵循以下步驟以配置屬性：

1. 以管理員的身份登入 Sun™ ONEIdentity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   在此您可以執行下列任務：

- 加入 Netlet 規則
- 將 Netlet 服務指定給使用者
- 加入 Netlet 規則
- 修改現有的 Netlet 規則
- 刪除 Netlet 規則

除了配置使用者設定檔與建立 Netlet 規則之外，您需要根據站台需求配置下列屬性。這些屬性可以在組織或使用者層級中配置。

- 指定預設加密密碼
- 指定預設回送連接埠
- 啓用連線的重新認證
- 停用連線的警告快顯視窗
- 啓用連接埠警告對話方塊中的顯示核取方塊
- 設定保持現有的間隔
- 設定在入口網站登出時終止 Netlet 選項
- 定義存取 Netlet 規則
- 拒絕存取 Netlet 規則
- 允許存取主機拒絕存取主機

將 Netlet 服務指定給使用者

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。

   選取的組織名稱會反映在管理主控台左上角的位置。
5. 爲已選的組織在「檢視」下拉式清單中選取「使用者」。
6. 按一下左窗格中需要的使用者旁邊的箭頭。
7. 如果此使用者尚未包含 Netlet 服務，則爲此使用者在「檢視」下拉清單中選取「服務」

8. 按一下「新增」。
9. 從「可用服務」清單中選取 Netlet。
10. 按一下「儲存」。
11. 爲此使用者從「檢視」下拉式清單中選取 "Netlet" 服務，就可以修改 Netlet 屬性。

加入 Netlet 規則

您可以在 Identity Server 管理主控台的「識別管理」標籤中，新增或建立全域層級的 Netlet 規則。這些規則是繼承您所建立的任何新組織。

您也可以在組織、角色或使用者層級中建立新的規則或修改現有規則。

➤ **若要加入 Netlet 規則**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選擇「識別管理」標籤。
3. 請選擇您要爲其建立規則的組織。
4. 從「檢視」下拉式清單中選取「服務」。
5. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁隨即顯示於右窗格中。
6. 在「Netlet 規則」欄位中按一下「新增」。

   隨即顯示「加入 Netlet 規則」頁。所有規則的欄位都已填入範例值，您可根據需要改變這些值。
7. 在「規則名稱」欄位鍵入唯一的規則名稱。
8. 指定需要的密碼。選取「預設」以保留預設加密密碼。選取「其他」以在可用密碼清單中選擇。

   有關預設密碼的詳細資訊，請參閱第 286 頁的「若要指定預設密碼」。
9. 在 URL 欄位中鍵入對應於將被呼叫的應用程式的 URL。
10. 若需要下載 applet，則選取「下載 Applet」核取方塊。以 *`client port:server host:server port`* 格式在相關編輯方塊中鍵入 applet 詳細資訊。

備註 爲每個規則指定唯一的 `client port`。

只有在 applet 需要從 Portal Server 主機之外的主機下載時，才需要指定 applet 詳細資訊。若沒有選取核取方塊，則無法使用編輯方塊。

11. 選取「延伸式階段作業」核取方塊確保當與此規則相對應的 Netlet 階段作業在執行時，Portal Server 階段作業時間將會延長。
12. 在用戶端連接埠欄位中鍵入 Netlet 偵聽的用戶端連接埠。

    對於 FTP 規則，用戶端連接埠值必須爲 30021。
13. 在「目標主機」欄位中鍵入值。

    對於靜態規則，請輸入用於 Netlet 連線的目標機器之主機名稱。

    對於動態規則，請輸入 "TARGET"。
14. 在「目標連接埠」欄位中鍵入目標主機的連接埠。
15. 按一下「加入至清單」以反映「Port-Host-Port 清單」欄位的最後三個項目。
16. 按一下「儲存」。

    將儲存這個規則，且返回 Netlet 頁面。新規則名稱會顯示於「Netlet 規則」清單中。

修改現有的 Netlet 規則

您可以在組織、角色或使用者層級，從管理主控台「識別管理」標籤中修改現有規則。這些規則是繼承您所建立的任何新組織。

➤ **若要修改 Netlet 規則**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 請選擇您要爲其修改規則的組織。
4. 從「檢視」下拉式清單中選取「服務」。
5. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁隨即顯示於右窗格中。

6. 按一下您要修改規則的名稱。

   隨即顯示「編輯 Netlet 規則」頁。

7. 依需要變更並按一下「儲存」。

   將儲存已變更的規則，且返回 Netlet 頁面。

刪除 Netlet 規則

您可以在全域層級，從管理主控台的「識別管理」標籤中刪除 Netlet 規則。

➤ **若要刪除 Netlet 規則**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 請選擇您要爲其刪除規則的組織。
4. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁隨即顯示於右窗格中。

5. 選取您想要從 Netlet 規則清單中刪除的規則旁邊的核取方塊。
6. 按一下「刪除」。

   已選的規則將從「Netlet 規則」清單中移除。

備註 本節說明如何配置組織層級的所有屬性。

指定預設加密密碼

您需要爲 Netlet 規則指定預設密碼。如果現有規則未將密碼包括成爲規則一部分，當您在使用現有規則時，這個選項就非常有用。這是必要的欄位。請參閱第 176 頁的「向下相容性」。

➤ **若要指定預設密碼**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。

4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「預設原生 VM 密碼」或「預設 Java Plugin 密碼」欄位，並在下拉式清單中選取需要的密碼。請參閱第 175 頁的「支援的密碼」以查看所支援密碼的清單。
8. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

指定預設回送連接埠

當透過 Netlet 下載 applet 時，此屬性會指定用於用戶端的連接埠。將使用預設值 8000，除非屬性在 Netlet 規則中被置換。

➤ **若要指定預設回送連接埠**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「預設回送連接埠」欄位並鍵入想要的連接埠號碼。
8. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

啓用連線的重新認證

若您希望使用者每次都輸入 Netlet 密碼，則啓用此選項並建立 Netlet 連線。若您啓用此選項，則連線的警告快顯視窗將不會顯示於使用者桌面。有關詳細資料，請參閱第 288 頁的「停用連線的警告快顯視窗」。

啓用此選項可讓使用者使用 Netlet 通道編輯選項變更重新認證密碼。依預設，初始密碼爲 `srap-Netlet`。

➤ 若要啓用連線的重新認證

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「連線重新認證」欄位並選取選項。
8. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

停用連線的警告快顯視窗

此屬性會在使用者桌面顯示警告訊息，告知有人正嘗試透過偵聽連接埠連線至 Netlet。當使用者在 Netlet 執行應用程式以及當入侵者嘗試透過偵聽連接埠存取桌面時會出現此訊息。

若您不希望快顯示視窗出現於使用者桌面，則請取消選取此屬性。

➤ 若要啓用連線的警告快顯視窗

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的「位置」。

5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 選取「連線的警告快顯視窗」核取方塊以啓用警告快顯視窗。
8. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

啓用連接埠警告對話方塊中的顯示核取方塊

當 Netlet 嘗試透過本機可自由使用的連接埠連線至目標主機時，會在使用者桌面上出現警告快顯視窗。只有在管理主控台上已啓用連線的警告快顯視窗選項時，才會在使用者桌面出現警告快顯視窗。

您可以允許使用者抑制此警告快顯視窗，方法是在管理主控台上啓用「連接埠警告對話方塊中顯示核取方塊」選項。

➤ **若要允許使用者抑制連接埠警告對話方塊**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「連接埠警告對話方塊中顯示核取方塊」欄位，並核取該方塊。
8. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

設定保持現有的間隔

您可以用分鐘爲單位設定時間間隔，以供 Netlet 保持連線狀態，即使並沒有作業在執行。

若您沒有指定此屬性值，則 Netlet 閒置連線會與所有其他 Portal Server 閒置連線一起逾時，其逾時時間爲 Identity Server 配置的階段作業屬性區段中指定的「最大閒置時間 (分鐘)」。

➤ **若要設定保持現有的間隔**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「保持現有的間隔 (分鐘)」欄位，並鍵入需要的時間間隔。
8. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

設定在入口網站登出時終止 Netlet 選項

若您希望確保所有連線在使用者登出 Portal Server 時終止，請啓用此選項。這可確保取得較大的安全性。此選項的預設值爲啓用。

停用此選項以確保即使在使用者登出 Portal Server 桌面之後，Netlet 連線仍在作用中。

備註 停用這個選項不允許使用者在登出 Portal Server 後建立新 Netlet 連線。僅保留現有連線。

➤ **若要設定在入口網站登出時終止 Netlet 選項**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「在入口網站登出時終止 Netlet」欄位，並依需要選取或取消選取選項。
8. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

   請參閱登出時終止 Netlet。

定義存取 Netlet 規則

您可以定義存取特定 Netlet 規則以供某些組織、角色或使用者之用。

➤ **若要定義存取 Netlet 規則**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「存取 Netlet 規則」欄位。
8. 在「存取 Netlet 規則」欄位鍵入您要可用於已選組織的規則名稱。

   此欄位值如果爲星號 (*) 表示所有已定義的 Netlet 規則皆可用於已選的組織。

9. 按一下「新增」。

   指定的規則將新增至「存取 Netlet 規則」清單。

10. 爲每個您要使之可用的 Netlet 規則重複步驟 7、8 與 9。

11. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

拒絕存取 Netlet 規則

您可以拒絕存取特定 Netlet 規則以供某些組織、角色或使用者之用。

➤ **若要拒絕存取 Netlet 規則**

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「拒絕 Netlet 規則」欄位。
8. 在「拒絕 Netlet 規則」欄位中鍵入您要拒絕已選組織存取的規則的名稱。

   此欄位值如果爲星號 (*) 表示拒絕已選組織存取所有已定義的 Netlet 規則。
9. 按一下「新增」。

   指定的規則將新增至「拒絕 Netlet 規則」清單。
10. 爲每個您要拒絕存取的 Netlet 規則重複步驟 7、8 與 9。
11. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

允許存取主機

您可以定義存取特定主機以供某些組織、角色或使用者之用。這可讓您限制對特定主機的存取。例如，您可以設定含有五個主機的「允許」清單，使用者可遠端登入這五個主機。

➤ 若要允許存取主機

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。
3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「允許的主機」欄位。
8. 在「允許主機」欄位中輸入您要允許存取的主機的名稱。

   此欄位中的星號 (*) 表示此指定網域的所有主機皆爲可存取。例如，若您指定 `*.sesta.com`，則 `sesta.com` 網域中的所有 Netlet 目標將可由使用者執行。您也可以指定萬有字元的 IP 位址，例如 `xxx.xxx.xxx.*`。
9. 按一下「新增」。

   指定的主機會新增至「允許的主機」清單。
10. 爲每個您要使之可用的主機重複步驟 7 與 8。
11. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

拒絕存取主機

您可以拒絕對於組織中特定主機的存取。在「拒絕的主機」清單中指定您要拒絕存取的主機。

➤ 若要拒絕存取主機

1. 以管理員的身份登入 Identity Server 管理主控台。
2. 選取「識別管理」標籤。

3. 從「檢視」下拉式清單中選取「組織」。
4. 按一下需要的組織名稱。選取的組織名稱會反映在管理主控台左上角的位置。
5. 從「檢視」下拉式清單中選取「服務」。
6. 按一下「SRA 配置」下 Netlet 旁的箭頭。

   Netlet 頁面會顯示在右窗格中。
7. 捲動至「拒絕的主機」欄位。
8. 在「拒絕的主機」清單中指定您要拒絕存取的主機的名稱。

   此欄位中的星號 (*) 表示拒絕使用者存取所選組織中的所有主機。例如，若要拒絕存取組織 `sesta` 中所有主機，請在「拒絕的主機」欄位中鍵入 `*.sesta.com`。

   若要拒絕存取特定主機，請指定完全合格的名稱。例如，若要拒絕存取主機 `abc`，請鍵入 `abc.sesta.com`。
9. 按一下「新增」。

   指定的網域會新增至「存取網域」清單。
10. 爲每個您要使之可用的網域重複步驟 7 與 8。
11. 按一下 Netlet 頁面頂端或底部的「儲存」記錄變更。

配置 SSL 加速器

本章說明如何配置 Sun™ Portal Server, Secure Remote Access 的不同加速器。

本章涵蓋下列主題：

摘要

Crypto Accelerator 爲專用的輔助處理器，可完全卸載伺服器中央處理器的 SSL 運算資源，從而釋出中央處理器以執行其他工作，並提高 SSL 事務處理的處理速度。

Sun Crypto Accelerator 1000

Sun™ Crypto Accelerator 1000 (Sun CA1000) 板是小型的 PCI 板，作爲加密輔助處理器提高公開金鑰及對稱式加密的速度。本產品無外部介面。此 PCI 板會透過內部的 PCI 匯流排介面與主機進行通訊。此板的作用是加速電子商務應用程式中針對安全協定的多種計算密集加密演算過程。

許多重要的加密運算功能，如 RSA [7] 與 Triple-DES (3DES) [8] 可從應用程式完全卸載至 Sun CA1000，並以平行的方式執行。如此可釋出中央處理器以執行其他工作，提高 SSL 事務處理的處理速度。

啓用 Crypto Accelerator 1000

請確定已安裝 Sun™ ONE Portal Server, Secure Remote Access，且亦已安裝閘道伺服器認證 (自簽或由任何 CA 所核發)。下列核對清單可幫助您在安裝 SSL Accelerator 前跟蹤記錄所需資訊。

表 A-1 列出 Crypto Accelerator 1000 參數與值。第一欄列出參數；第二欄列出其值。

表 A-1 Crypto Accelerator 1000 安裝核對清單

參數	值
Secure Remote Access 安裝基底目錄	/opt
Secure Remote Access 認證資料庫路徑	/etc/opt/SUNWps/cert/default
Secure Remote Access 伺服器認證暱稱	server-cert
範圍	sra-keystore
範圍使用者	crypta

配置 Crypto Accelerator 1000

➤ **若要配置 Crypto Accelerator 1000**

1. 請遵照使用者指南中的指示安裝硬體。請參閱：

   `http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf`

2. 請從光碟安裝下列套件。

   `SUNWcrypm°BSUNWcrypu°BSUNWcrysu°BSUNWdcar°BSUNWcrypr°BSUNWcrysl°BSUNWdcamn°BSUNWdcav`

3. 安裝下列修補程式。(您可從 `http://sunsolve.sun.com` 取得這些修補程式)

   110383-01, 108528-05, 112438-01

4. 請確定您有下列工具：`pk12util` 與 `modutil`。

   若爲 SRA 6.0，這些工具會安裝在 `/opt/SUNWps/bin` 下

   若爲 SRA 6.2，這些工具會安裝在 `/usr/lib/mps/secv1/bin` 下

5. 建立插槽檔案：

   ```
   vi /etc/opt/SUNWconn/crypto/slots
   ```

   並將 "crypta@sra" 置於檔案中的首位且爲唯一的行。

6. 建立範圍與使用者。

   ```
   cd /opt/SUNWconn/bin/secadm
   secadm> create realm=sra
   系統管理員登入需要
   登入：root
   密碼：
   已成功建立範圍 sra。

   secadm> set realm=sra
   secadm{srap}> su
   系統管理員登入需要
   登入：root
   密碼：
   secadm{root@sra}>create user=crypta
   初始密碼：
   確認密碼：
   已成功建立使用者 crypta。

   secadm{root@sra}> login user=crypta
   密碼：
   secadm{crypta@sra}> show key
   此使用者無可用的金鑰。
   ```

7. 載入 Sun Crypto 模組。

   若爲 SRA 6.0，環境變數 LD_LIBRARY_PATH 必須指向 /opt/SUNWps/lib/solaris/sparc

   若爲 SRA 6.2，環境變數 LD_LIBRARY_PATH 必須指向 /usr/lib/mps/secv1/

   輸入：

   ```
   modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto Module"
   -libfile  /opt/SUNWconn/crypto/lib/libpkcs11.so
   ```

   請利用下列指令確認是否已載入此模組：

   ```
   modutil -list -dbdir /etc/opt/SUNWps/cert /default
   ```

8. 將閘道證書及金鑰匯出至 "Sun Crypto Module"。

   若爲 SRA 6.0，環境變數 LD_LIBRARY_PATH 必須指向 /opt/SUNWps/lib/solaris/sparc

   若爲 SRA 6.2，環境變數 LD_LIBRARY_PATH 必須指向 /usr/lib/mps/secv1/

   輸入：

   ```
   pk12util -o servercert.p12 -d /etc/opt/SUNWps/cert/default -n
   server-cert
   ```

   ```
   pk12util -i servercert.p12 -d /etc/opt/SUNWps/cert/default -h
   "crypta@sra"
   ```

   現在請執行顯示金鑰指令：

   secadm{crypta@sra}> show key

   您應可看到此使用者的兩個金鑰。

9. 變更 /etc/opt/SUNWps/cert/default/.nickname 檔案中的暱稱。

   ```
   vi /etc/opt/SUWNps/cert/default/.nickname
   ```

   以 crypta@sra:server-cert 取代 server-cert

10. 選取加速密碼。

SUN CA1000 會加速 RSA 的運行速度，但僅支援 DES 與 3DES 密碼加速。若要啓用其中一個密碼，請執行下列動作

若爲 SRA 6.0：

閘道 >> 啓用 SSL 加密選項：>> SSL3 加密：>>
SSL3_RSA_WITH_3DES_EDE_CBC_SHA 或
SSL3_RSA_WITH_DES_CBC_SHA

若爲 SRA 6.2：

閘道 >> 安全性 >> 啓用 SSL 加密選項：>> SSL3 加密：>>
SSL3_RSA_WITH_3DES_EDE_CBC_SHA 或
SSL3_RSA_WITH_DES_CBC_SHA

11. 修改 `/etc/opt/SUNWps/platform.conf.`*gateway-profile-name* 以啓用加速器：

```
gateway.enable.accelerator=true
```

12. 從終端機視窗重新啓動閘道：

portal-server-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

備註 閘道會於連接埠上與單線 ServerSocket (非 SSL) 連結，此連接埠爲閘道設定檔中所提及的 https 連接埠。

在外來用戶端通訊流量上不會進行任何 SSL 加密或解密。加速器會完成上述動作。

在此模式下 PDC 將無法運作。

Sun Crypto Accelerator 4000

Sun™ Crypto Accelerator 4000 板是一個以乙太網路爲基礎的十億位元網路介面卡，支援 Sun 伺服器上的 IPsec 及 SSL (對稱與非對稱) 加密硬體加速。

除了作爲處理未加密網路通訊流量的標準十億位元乙太網路介面卡之外，其亦包含加密硬體以提高加密 IPsec 通訊流量的輸送量。

Crypto Accelerator 4000 板可加速硬體及軟體上的加密演算過程。其亦支援 DES 與 3DES 加密的整批資料加密。

啓用 Crypto Accelerator 4000

請確定已安裝 Secure Remote Access，且亦已安裝閘道伺服器認證 (自簽或由任何 CA 所核發)。下列核對清單可幫助您在安裝 SSL Accelerator 前跟蹤記錄所需資訊。

表 A-2 列出 Crypto Accelerator 4000 參數與值。第一欄列出參數；第二欄列出其值。

.

表 A-2 Crypto Accelerator 4000 安裝核對清單

參數	值
Secure Remote Access 安裝基底目錄	/opt
Secure Remote Access 實例	預設
Secure Remote Access 證書資料庫路徑	/etc/opt/SUNWps/cert/default
Secure Remote Access 伺服器證書暱稱	server-cert
CA4000 金鑰庫	srap
CA4000 金鑰庫使用者	crypta

配置 Crypto Accelerator 4000

➤ **若要配置 Crypto Accelerator 4000**

1. 請遵照使用者指南中的指示安裝硬體與軟體套件。請參閱：

   `http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf`

2. 安裝下列修補程式。(您可從 http://sunsolve.sun.com 取得這些修補程式)：`114795`

3. 請確定您有下列工具：`certutil`°`Bpk12util` 與 `modutil`。

   若爲 SRA 6.0，這些工具會安裝在 `/opt/SUNWps/bin` 下

   若爲 SRA 6.2，這些工具會安裝在 `/usr/lib/mps/secv1/bin` 下

4. 初始化此板。

   執行 /opt/SUNWconn/bin/vcadm 工具以初始化 crypto 板並設定下列值。

   初始安全官員姓名：sec_officer

   金鑰庫名稱：sra-keystore

   在 FIPS 140-2 模式下執行：No

5. 建立使用者。

   vcaadm{vca0@localhost, sec_officer}> create user

   新使用者名稱：crypta

   輸入新使用者密碼：

   確認密碼：

   已成功建立使用者 crypta。

6. 將記號對映至金鑰庫。

   vi /opt/SUNWconn/cryptov2/tokens

   將 sra-keystore 附加 / 新增至檔案。

7. 啓用整批資料加密。

   touch /opt/SUNWconn/cryptov2/sslreg

8. 載入 Sun Crypto 模組。

   若爲 SRA 6.0，環境變數 LD_LIBRARY_PATH 必須指向 /opt/SUNWps/lib/solaris/sparc

   若爲 SRA 6.2，則其應指向 /usr/lib/mps/secv1/

   輸入：

   ```
   modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto Module"
   -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
   ```

   您可利用下列指令確認是否已載入此模組：

   ```
   modutil -list -dbdir /etc/opt/SUNWps/cert /default
   ```

9. 將閘道證書及金鑰匯出至 "Sun Crypto Module"。

若爲 SRA 6.0，環境變數 LD_LIBRARY_PATH 必須指向 /opt/SUNWps/lib/solaris/sparc

若爲 SRA 6.2，則其應指向 /usr/lib/mps/secv1/

```
pk12util -o servercert.p12 -d /etc/opt/SUNWps/cert/default -n
server-cert
```

```
pk12util -i servercert.p12 -d /etc/opt/SUNWps/cert/default -h
"sra-keystore"
```

您可利用下列指令確認是否已匯出此金鑰：

```
certutil -K -h "sra-keystore" -d /etc/opt/SUNWps/cert/default
```

10. 變更 /etc/opt/SUWNps/cert/default/.nickname 檔案中的暱稱：

```
vi /etc/opt/SUWNps/cert/default/.nickname
```

以 sra-keystore:server-cert 取代 server-cert

11. 選取加速密碼。

SUN CA4000 會加速 RSA 的運行速度，但僅支援 DES 與 3DES 密碼加速。若要啓用其中一個密碼，請執行下列動作

若爲 SRA 6.0：

閘道 >> 啓用 SSL 加密選項：>> SSL3 加密：>> SSL3_RSA_WITH_3DES_EDE_CBC_SHA 或 SSL3_RSA_WITH_DES_CBC_SHA

若爲 SRA 6.2：

閘道 >> 安全性 >> 啓用 SSL 加密選項：>> SSL3 加密：>> SSL3_RSA_WITH_3DES_EDE_CBC_SHA 或 SSL3_RSA_WITH_DES_CBC_SHA

12. 從終端機視窗重新啓動閘道：

portal-server-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

閘道將提示您輸入金鑰庫密碼。

輸入密碼或 "sra-keystore":crypta:crytpa-password 的個人識別碼

備註 閘道會於連接埠上與單線 ServerSocket (非 SSL) 連結，此連接埠爲閘道設定檔中所提及的 https 連接埠。

在外來用戶端通訊流量上不會進行任何 SSL 加密或解密。加速器會完成上述動作。

在此模式下 PDC 將無法運作。

外部 SSL 裝置與代理伺服器加速器

在開放模式下，外部 SSL 裝置可在 Secure Remote Access 之前執行。其提供用戶端與 Secure Remote Access 之間的 SSL 連結。

啓用外部 SSL 裝置加速器

請確定已安裝 Secure Remote Access，且已有閘道在安全模式 (HTTPS 模式) 下執行：

閘道 >> 啓用 HTTPS 連線

閘道 >> HTTP 連接埠：880

表 A-3 列出外部 SSL 裝置與代理伺服器加速器的參數與值。第一欄列出參數；第二欄列出其值。

表 A-3 外部 SSL 裝置與代理伺服器加速器核對清單

參數	值
SRA 實例	預設
閘道模式	https
閘道連接埠	880
外部裝置 / 代理伺服器連接埠	443

配置外部 SSL 裝置加速器

➤ **若要配置外部 SSL 裝置加速器**

1. 請遵照使用者指南中的指示安裝硬體與軟體套件。
2. 請安裝所需 / 建議安裝的修補程式 (若有的話)。
3. 啓用 SSL 裝置 / 代理伺服器支援：

   ```
   vi /etc/opt/SUNWps/platform.conf.default
   ```

   ```
   gateway.enable.accelerator=true
   ```

   若外部裝置 / 代理伺服器主機名稱與閘道主機名稱不同：

   ```
   gateway.enable.customurl=true
   ```

   ```
   gateway.httpsurl=external-device.domain.subdomain/proxy-URL
   ```

4. 有兩種方式可配置閘道通知：
   - 當 Identity Server 可於 880 埠聯繫閘道機器時 (階段作業通知將會以 http 的形式呈現)

     ```
     vi /etc/opt/SUNWps/platform.conf.default
     ```

     ```
     gateway.protocol=http
     ```

     ```
     gateway.port=880
     ```

   - 當 Identity Server 可於 443 埠聯繫外部裝置 / 代理伺服器時 (階段作業通知將會以 HTTPS 的形式呈現)

     ```
     vi /etc/opt/SUNWps/platform.conf.default
     ```

     ```
     gateway.host=External Device/Proxy Host Name
     ```

     ```
     gateway.protocol=https
     ```

     ```
     gateway.port=443
     ```

5. 請確定已開啓並執行 SSL 裝置 / 代理伺服器，且已配置爲將通訊流量導向閘道連接埠。
6. 從終端機視窗重新啓動閘道：

   gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

國家代碼

下列表格中列出了二字母國家代碼，在認證管理期間您需要指定這些國家代碼。第一欄列出了代碼，而第二欄則列出國家。

表 B-1 二字母國家代碼 *(第 1 頁，共 10 頁)*

ad	安道爾侯國
ae	阿拉伯聯合大公國
af	阿富汗伊斯蘭國
ag	安地卡及巴布達
ai	安圭拉
al	阿爾巴尼亞
am	亞美尼亞
an	荷屬安地列斯
ao	安哥拉
aq	南極大陸
ar	阿根廷
arpa	舊的美國官方網路
as	美屬薩摩亞
at	奧地利
au	澳大利亞
aw	阿魯巴
az	亞塞拜然

表 B-1 二字母國家代碼 *(第 2 頁，共 10 頁)*

ba	波士尼亞赫塞哥維納
bb	巴貝多
bd	孟加拉
be	比利時
bf	布基納法索
bg	保加利亞
bh	巴林
bi	蒲隆地
bj	貝南
bm	百慕達
bn	汶萊
bo	玻利維亞
br	巴西
bs	巴哈馬
bt	不丹
bv	布威島
bw	波札那
by	白俄羅斯
bz	貝里斯
ca	加拿大
cc	可可斯群島
cf	中非
cd	剛果民主共和國
cg	剛果
ch	瑞士
ci	象牙海岸
ck	柯克群島

表 B-1 二字母國家代碼 *(第 3 頁，共 10 頁)*

cl	智利
cm	喀麥隆
cn	中國
co	哥倫比亞
com	商業機構
cr	哥斯大黎加
cs	前捷克斯洛伐克
cu	古巴
cv	維德角
cx	聖誕島
cy	塞浦路斯
cz	捷克共和國
de	德國
dj	吉布地
dk	丹麥
dm	多米尼克
執行	多明尼加
dz	阿爾及利亞
ec	厄瓜多爾
edu	教育機構
ee	愛沙尼亞
eg	埃及
eh	西撒哈拉
er	厄利垂亞
es	西班牙
et	衣索比亞
fi	芬蘭

表 B-1 二字母國家代碼 *(第 4 頁，共 10 頁)*

fj	斐濟
fk	福克蘭群島
fm	密克羅尼西亞
fo	法羅群島
fr	法國
fx	法國 (歐洲領土)
ga	加彭
gb	英國
gd	格瑞那達
ge	喬治亞
gf	法屬圭亞那
gh	加納
gi	直布羅陀
gl	格陵蘭
gm	甘比亞
gn	幾內亞
gov	美國政府
gp	哥德普洛 (法屬)
gq	赤道幾內亞
gr	希臘
gs	聖喬治與聖文森群島
gt	瓜地馬拉
gu	關島 (美屬)
gw	幾內亞比索
gy	圭亞那
hk	香港
hm	赫德島及麥當勞群島

表 B-1 二字母國家代碼 *(第 5 頁，共 10 頁)*

hn	宏都拉斯
hr	克羅埃西亞
ht	海地
hu	匈牙利
id	印尼
ie	愛爾蘭
il	以色列
in	印度
int	國際機構
io	英屬印度洋領土
iq	伊拉克
ir	伊朗
is	冰島
it	義大利
jm	牙買加
jo	約旦
jp	日本
ke	肯亞
kg	吉爾吉斯共和國 (吉爾吉斯)
kh	柬埔寨王國
ki	吉里巴斯
km	葛摩
kn	聖基茨 - 尼維斯 - 安圭拉
kp	北韓
kr	南韓
kw	科威特
ky	開曼群島

表 B-1 二字母國家代碼 (*第 6 頁，共 10 頁*)

kz	哈薩克
la	寮國
lb	黎巴嫩
lc	聖露西亞
li	列支敦斯登
lk	斯里蘭卡
lr	賴比瑞亞
ls	賴索托
lt	立陶宛
lu	盧森堡
lv	拉脫維亞
ly	利比亞
ma	摩洛哥
mc	摩納哥
md	摩達維亞
mg	馬達加斯加
mh	馬紹爾群島
mil	美國軍隊
mk	馬其頓
ml	馬利
mm	緬甸
mn	蒙古
mo	澳門
mp	北馬里安納群島
mq	馬丁尼克 (法屬)
mr	茅利塔尼亞
ms	蒙特色拉特島

表 B-1 二字母國家代碼 *(第 7 頁，共 10 頁)*

mt	馬爾他
mu	模里西斯
mv	馬爾地夫
mw	馬拉威
mx	墨西哥
my	馬來西亞
mz	莫三比克
na	納米比亞
nato	NATO (本組織已在 1996 解散 - 請參閱 hq.nato.int)
nc	新喀里多尼亞群島 (法屬)
ne	尼日
net	網路
nf	諾福克島
ng	奈及利亞
ni	尼加拉瓜
nl	荷蘭
no	挪威
np	尼泊爾
nr	諾魯
nt	中立區
nu	紐威島
nz	紐西蘭
om	阿曼
org	非營利組織 (sic)
pa	巴拿馬
pe	秘魯
pf	玻里尼西亞 (法屬)

表 B-1 二字母國家代碼 *(第 8 頁，共 10 頁)*

pg	巴布亞紐幾內亞
ph	菲律賓
pk	巴基斯坦
pl	波蘭
pm	聖皮埃爾島及密克隆島
pn	皮特康群島
pr	波多黎各
pt	葡萄牙
pw	帛琉
py	巴拉圭
qa	卡達
re	留尼旺 (法屬)
ro	羅馬尼亞
ru	俄羅斯聯邦
rw	盧安達
sa	沙烏地阿拉伯
sb	索羅門群島
sc	塞席爾
sd	蘇丹
se	瑞典
sg	新加坡
sh	聖赫勒拿島
si	斯洛維尼亞
sj	冷岸及央棉群島
sk	斯洛伐克共和國
sl	獅子山
sm	聖馬利諾

表 B-1 二字母國家代碼 *(第 9 頁，共 10 頁)*

sn	塞內加爾
so	索馬利亞
sr	蘇利南
st	聖多美普林西比
su	前蘇聯
sv	薩爾瓦多
sy	敘利亞
sz	史瓦濟蘭
tc	土克斯及開科斯群島
td	查德
tf	法屬南方領土
tg	多哥
th	泰國
tj	塔吉克
tk	托克勞群島
tm	土庫曼
tn	突尼西亞
to	東加
tp	東帝汶
tr	土耳其
tt	千里達及托巴哥
tv	吐瓦魯
tw	台灣
tz	坦尚尼亞
ua	烏克蘭
ug	烏干達
uk	英國

表 B-1 二字母國家代碼 *(第10 頁，共10 頁)*

um	美國邊遠島嶼
us	美國
uy	烏拉圭
uz	烏茲別克
va	教廷 (梵蒂岡)
vc	聖文森及格瑞那丁
ve	委內瑞拉
vg	英屬維爾京群島
vi	美屬維爾京群島
vn	越南
vu	萬那杜
wf	瓦利斯及福杜納群島
ws	薩摩亞
ye	葉門
yt	馬約特島
yu	南斯拉夫
za	南非
zm	尚比亞
zr	薩伊
zw	辛巴威

附錄 C

配置屬性

本附錄描述您可以透過 Sun ONE Identity Server 管理主控台「服務配置」標籤中爲 Sun™ ONE Portal Server，Secure Remote Access 配置的屬性。

存取清單服務

表 C-1 列出了存取清單服務屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-1 存取清單服務屬性

屬性	預設值	說明
URL 拒絕清單		一般使用者無法透過閘道存取的 URL 清單。
URL 允許清單：	*	一般使用者可以透過閘道存取的 URL 清單。
已停用 SSO 的主機		停用清單中主機的單次登入功能。
按階段作業啟用 SSO		啟用階段作業的單次登入功能。
允許的驗證等級	*	表示信任認證的程度。使用星號可允許所有驗證等級。有關驗證等級的資訊，請參閱 *Sun ONE Identity Server 管理員指南*。

閘道服務

當您按一下「閘道」服務時，右邊的窗格會顯示一個可用來建立新設定檔的按鈕，以及顯示已經建立之所有閘道設定檔的清單。

如果您按一下「新增」，則下一個窗格將會要求您輸入新的閘道設定檔名稱。您可以選擇使用預設範本或是選擇先前建立的閘道設定檔作爲範本。

如果您在其中一個列出的閘道設定檔名稱上按一下，將會出現一個標籤清單。其中包括：

- 核心
- 代理伺服器
- 安全性
- Rewriter
- 記錄

核心

表 C-2 列出了閘道服務核心屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-2 閘道服務核心屬性

屬性	預設值	說明
啟用 HTTPS 連線	已核取	啟用 HTTPS 連線。
HTTPS 連接埠	443	指定 HTTPS 連接埠。
啟用 HTTP 連線	已取消核取	啟用 HTTP 連線。
HTTP 連接埠	80	指定 HTTP 連接埠。
啟用 Rewriter 代理伺服器	已取消核取	在閘道和企業內部網路之間實現安全的 HTTP 通訊。Rewriter 代理伺服器和閘道使用相同的閘道設定檔。
Rewriter 代理伺服器清單		列出 Rewriter 代理伺服器。
啟用 Netlet	已核取	啟用 TCP/IP (例如 Telnet 和 SMTP)、HTTP 應用程式和固定連接埠應用程式的安全性。

表 C-2 閘道服務核心屬性

屬性	預設值	說明
啟用 Netlet 代理伺服器	已取消核取	藉由透過閘道將安全通道從用戶端延伸到位於企業內部網路的 Netlet 代理伺服器，以強化閘道和企業內部網路之間的 Netlet 通訊的安全性。如果您不想要在 Portal Server 中使用應用程式，請停用此屬性。
Netlet 代理伺服器主機		列出 Netlet 代理伺服器主機，格式如下：host hostname:port
啟用 Cookie 管理	已取消核取	為允許使用者存取的所有網站追蹤與管理使用者階段作業。(不適用於 Portal Server 用來追蹤 Portal Server 使用者階段作業的 cookie)。
啟用 HTTP 基本驗證	已取消核取	儲存使用者名稱和密碼，如此當使用者重新造訪有 BASIC 保護的網站時，將不需要重新輸入其憑證。
啟用持續 HTTP 連線	已核取	在閘道啟用 HTTP 持續連線，可避免為網頁的每個物件 (例如影像與樣式表) 開啟插槽。
每一持續連線的最大要求數	10	指定每一持續連線的要求數。
持續通訊端關閉前的逾時	50	指定在關閉插槽前需要經過的時間量。
帳戶往返時間的寬限逾時	20	指定在瀏覽器傳送請求後，請求到閘道的寬限時間量，和閘道傳送回應以及瀏覽器實際收到之間的間隔時間。
轉寄 Cookie URL	可以透過閘道存取的 Portal Server URL 清單。	讓 servlet 和 CGI 可以收到 Portal Server 的 cookie 並使用 API 來識別使用者。
最長連線佇列長度	50	指定閘道可以接受的最大並行運作連線。
閘道逾時 (毫秒)	120000	指定 「閘道」與瀏覽器的連線逾時前的時間間隔 (單位：毫秒)。
最大執行緒儲存區大小	200	指定可以在閘道執行緒儲存區預先建立的最大執行緒數目。
快取的通訊端逾時	200000	指定 「閘道」與 Portal Server 的連線逾時前的時間間隔 (單位：毫秒)。
Portal Server 清單	可以透過閘道存取的 Portal Server URL 清單。	以下列格式指定 Portal Server：`http://`*portal-server-name:port -number*。閘道會以循環方式嘗試聯絡每個列出的 Portal Server 以服務請求。
伺服器重試間隔	2	指定當 Portal Server、Rewriter 代理伺服器或 Netlet 代理伺服器變得無法存取 (例如當機或關機) 之後，嘗試啟動它們之請求之間的時間間隔。
儲存外部伺服器 Cookie	已取消核取	允許閘道儲存與管理可透過閘道存取之任何第三方應用程式或是伺服器的 cookie。

表 C-2 閘道服務核心屬性

屬性	預設值	說明
從 URL 取得階段作業	已取消核取	將階段作業資訊編碼為 URL 的一部分，不論是否支援 cookie。閘道會使用 URL 中找到的階段作業資訊進行驗證，而不是使用用戶端瀏覽器傳送的階段作業 cookie。
將 Cookie 標示為安全	已取消核取	將 Cookie 標示為安全。必須啟用「啟用 Cookie 管理」選項。

代理伺服器

表 C-3 列出了閘道服務代理伺服器屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-3 閘道服務代理伺服器屬性

屬性	預設值	說明
使用代理伺服器	已取消核取	使得可以使用網路代理伺服器。
使用網路代理伺服器 URL		列出閘道需要聯絡的 URL，而聯絡僅能透過「網域和子網域的代理伺服器清單」中列出的網路代理伺服器進行 (即使「使用代理伺服器」選項已經停用)。
不要使用網路代理伺服器 URL		列出閘道可以直接連接的 URL。
網域與子網域的代理伺服器	Portal Server 的網域 (例如 sesta.com)	指定應該使用哪個代理伺服器以聯絡特定網域中的特定子網域。
代理伺服器密碼清單		如果代理伺服器需要認證以存取某些或全部網站，則指定閘道需要的使用者名稱與密碼，以使閘道認證至指定的代理伺服器。
啟用 PAC 支援	已取消核取	指定將忽略在「網域與子網域的代理伺服器」欄位中提供的資訊。
PAC 檔案位置		指定用於 PAC 支援的檔案位置。
透過網路代理伺服器的通道 Netlet	已取消核取	透過閘道將安全通道從用戶端延伸至存在於企業內部網路的網路代理伺服器。

安全性

表 C-4 列出了閘道服務安全性屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-4 閘道服務安全性屬性

屬性	預設值	說明
未驗證的 URL	/portal/desktop/images /amserver/login_images /portal/desktop/css /amserver/jss /amconsole/console/css /portal/searchadmin/console/js /amconsole/console/js /amserver/css	指定不需要任何認證的 URL，例如包含影像的目錄。
啟用憑證的閘道主機		列出已啟用憑證的閘道主機。
允許 40 位元瀏覽器	已核取	允許 40 位元 (弱) 安全套接層 (SSL) 連線。如果您沒有選取此選項，則系統將僅支援 128 位元的連線。
啟用 SSL 2.0 版	已核取	啟用 SSL 2.0 版本。 停用 SSL 2.0 表示只支援舊版 SSL 2.0 的瀏覽器將不能認證以存取 Secure Remote Access。
啟用 SSL 加密選項	已取消核取	啟用 SSL 加密選項。您可以選擇支援所有預先封裝的密碼，或者您可以單獨選擇需要的密碼。您可以為每個閘道實例選擇特定的 SSL 密碼。
SSL2 加密	已選取所有可用的 SSL2 加密	列出您可以選擇的 SSL 版本 2 密碼。
SSL3 加密	已選取所有可用的 SSL3 加密。	列出您可以選擇的 SSL 版本 3 密碼。
TLS 加密	已選取所有可用的 TLS 密碼	列出 TLS 密碼。
啟用 SSL 3.0 版	已核取	啟用 SSL 3.0 版本。 停用 SSL 3.0 表示只支援舊版 SSL 3.0 的瀏覽器將不能取得認證以存取 Secure Remote Access。這可確保較大的安全層級。
停用空加密	已取消核取	停用空加密。
信任的 SSL 網域清單		列出信任的 SSL 網域。

Rewriter

Rewriter 標籤有兩個子區段：

- 基本
- 進階

基本

表 C-5 列出了閘道服務 Rewriter 基本屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-5 閘道服務 Rewriter 屬性 - 基本

屬性	預設值	說明
啟用所有 URI 的重寫	已取消核取	指定將重寫所有 URL 而不會將其與 「網域與子網域的代理伺服器」清單中的項目進行核對。
URI 至規則集對映	*://*.<Portal Server Domain>*/portal/*|default_gateway_ruleset */portal/NetFileOpenFileServlet*|null_ruleset *|generic_ruleset REPLACE_WITH_IPLANET_MAIL_SERVER_NAME|iplanet_mail_ruleset REPLACE_WITH_EXCHANGE_SERVER_NAME|exchange_2000sp3_owa_ruleset *://*.<Portal Server Domain>*/amconsole/*|default_gateway_ruleset REPLACE_WITH_INOTES_SERVER_NAME|inotes_ruleset http*://*/portal/NetFileController*|null_ruleset	使用 「URI 至規則集對映」清單將網域與規則集進行關聯。規則集是在 Identity Server 管理主控台中的 Portal Server 配置底下建立的。

表 C-5 閘道服務 Rewriter 屬性 - 基本

屬性	預設值	說明
剖析器至 MIME 對映	JAVASCRIPT=application/x-java XML=text/xml HTML=text/html;text/htm;text/x-component;text/wml;text/vnd.wap.wml CSS=text/css	將新的 MIME 類型與 HTML、JAVASCRIPT、CSS 或 XML 進行關聯。使用分號或逗號分隔多個項目。
預設網域子網域	Portal Server 安裝的網域	將主機名稱解析為預設網域與子網域。

進階

表 C-6 列出了閘道服務 Rewriter 進階屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-6 閘道服務 Rewriter 屬性 - 進階

屬性	預設值	說明
不要重寫 URI 清單		列出不會重寫的 URI。備註：將 #* 新增至此清單中，以允許重寫 URI (即使 href 規則為規則集的一部分)。
啟用 MIME 推測	已取消核取	當未傳送 MIME 時，啟用 MIME 推測。您必須將資料新增至「剖析器至 URI 對映」清單方塊。
剖析器至 URI 對映	HTML=*.html;*.htm;*.htc;*.cgi; XML=*.xml CSS=*.css JAVASCRIPT=*.js	將剖析器對映至 URI。由分號分隔多個 URI。 例如 HTML=*.html; *.htm;*Servlet 表示 HTML Rewriter 會用於重寫任何含有 html、htm，或 Servlet 副檔名的頁面內容。
啟用混淆		允許 Rewriter 重寫 URI，如此即可隱藏網頁的內部網路 URL。
混淆器種子字串	SECRET_KEY	指定可用於 URI 混淆的種子字串。其為一個由混淆演算法產生的隨機字串。
不要混淆 URI 清單		指定不要混淆的網際網路 URI。當應用程式 (例如 applet) 需要網際網路 URI 時便可使用此選項。 例如您新增 */Applet/Param* 至此清單方塊，則如果內容 URI `http://abc.com/Applet/Param1.html` 與規則集中的規則匹配，將不會混淆 URL。

表 C-6 閘道服務 Rewriter 屬性 - 進階

屬性	預設值	說明
讓閘道通訊協定與原始 URI 通訊協定相同		讓 Rewriter 使用一致的通訊協定存取 HTML 內容中參照的資源。 這將僅套用至靜態 URI，而非產生於 Javascript 的動態 URI。

記錄

表 C-7 列出了閘道服務記錄屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-7 閘道服務記錄屬性

屬性	預設值	說明
啟用記錄	已取消核取	啟用記錄。
啟用按階段作業記錄	已取消核取	啟用擷取最小記錄資訊，例如 「用戶端位址」、「要求類型」與 「目標主機」。
啟用按階段作業記錄詳細資訊	已取消核取	使得可以擷取詳細的記錄資訊，例如 「用戶端」、「要求類型」、「目標主機」、「用戶端要求的 URL」、「用戶端 Post Data 大小」、「階段作業 ID」、「回應結果代碼」與 「完成回應大小」。 備註：必須啟用 「啟用按階段作業記錄」。
啟用 Netlet 記錄	已取消核取	指定是否啟用記錄。如果已啟用則擷取下列資訊：啟動時間、來源、位址、源連接埠、伺服器位址、伺服器連接埠、停止時間、狀態 (啟動或停止)

NetFile 服務

當您按一下 NetFile 服務，右邊的窗格將會顯示標籤。這些標籤包括：

- 主機
- 許可權
- 檢視
- 作業
- 一般

主機

「主機」標籤有兩個子區段：

- 配置
- 存取

配置

表 C-8 列出了 Netfile 主機配置屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-8 NetFile 服務主機配置屬性

屬性	預設值	說明
OS 字元集	Unicode(UTF-8)	指定在與主機通訊時用來作為預設編碼的字元集。
主機偵測順序	WIN,NETWARE,FTP,NFS	指定主機偵測順序。
共用主機		指定所有遠端 NetFile 使用者都可以透過 NetFile 使用的主機。
預設網域	Portal Server 的網域	指定 NetFile 用於聯絡允許主機所需要的預設網域。
預設 Windows 網域 / 工作群組		指定使用者選擇存取 Windows 主機的預設 Windows 網域或工作群組。
預設 WINS/DNS 伺服器		指定 NetFile 用於存取 Windows 主機的 WINS/DNS 伺服器。

存取

表 C-9 列出了 NetFile 服務主機存取屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-9 NetFile 服務主機存取屬性

屬性	預設值	說明
允許存取 Windows 主機	已核取	允許存取 Windows 主機。
允許存取 FTP 主機	已核取	允許存取 FTP 主機。
允許存取 NFS 主機	已核取	允許存取 NFS 主機。

表 C-9 NetFile 服務主機存取屬性

屬性	預設值	說明
允許存取 Netware 主機	已核取	允許存取 Netware 主機。
允許的主機	*	指定使用者能夠透過 NetFile 存取的主機。
拒絕的主機		指定使用者不能夠透過 NetFile 存取的主機。

許可權

若您在使用者開始使用 NetFile 之後停用這些選項，則只有在使用者登出 NetFile 並重新登入後，此項變更才會生效。

表 C-10 列出了 NetFile 服務許可權屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-10 NetFile 服務許可權屬性

屬性	預設值	說明
允許檔案重新命名	已核取	允許使用者重新更名檔案。
允許檔案 / 資料夾刪除	已核取	允許使用者刪除檔案及資料夾。
允許檔案上載	已核取	允許使用者上傳檔案。
允許檔案 / 資料夾下載	已核取	允許使用者下載檔案及資料夾。
允許檔案搜尋	已核取	允許使用者搜尋。
允許檔案郵寄	已核取	允許郵寄檔案。
允許檔案壓縮	已核取	允許壓縮檔案。
允許變更使用者 ID	已核取	允許使用者使用不同的 ID。
允許變更 Windows 網域	已核取	允許使用者變更 Windows 網域。

檢視

表 C-11 列出了 Netfile 服務檢視屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-11 NetFile 服務檢視屬性

屬性	預設值	說明
視窗大小 (像素)	700|400	以像素為單位指定 NetFile 視窗在使用者桌面上的大小。若您輸入一個無效的值，NetFile 將會使用預設值。
視窗位置	100|50	指定 NetFile 視窗顯示在使用者桌面上的位置。若您輸入一個無效的值，NetFile 將會使用預設值。

作業

「作業」標籤的子區段如下：

- 流量
- 搜尋
- 壓縮

流量

表 C-12 列出了 NetFile 服務作業流量屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-12 NetFile 服務作業 - 流量屬性

屬性	預設值	說明
暫存目錄位置	/tmp	為不同 NetFile 檔案作業指定暫存目錄。 確保正在執行網路伺服器的 ID (例如 nobody 或 noaccess) 擁有指定目錄的 rwx 許可權。也確定 ID 對於需要的暫時目錄的完整路徑擁有 rx 許可權。 您可以為 NetFile 建立單獨的暫存目錄。如果您為 Portal Server 所有模組指定了共用的暫存目錄，磁碟空間可能很快就會用完。如果暫存目錄已無空間，則 NetFile 將無法運作。

表 C-12 NetFile 服務作業 - 流量屬性

屬性	預設值	說明
檔案上載限制 (以 MB 為單位)	5	指定檔案可以上傳的最大大小。若您輸入一個無效的值，NetFile 會將此值重新設定為預設值。請輸入整數值。 您可以為不同的使用者指定不同的檔案上傳大小限制。

搜尋

表 C-13 列出了 NetFile 服務作業搜尋屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-13 NetFile 服務作業 - 搜尋屬性

屬性	預設值	說明
搜尋目錄限制：	100	指定在單一搜尋作業中，可搜尋目錄的最大數目。

壓縮

表 C-14 列出了 NetFile 服務作業壓縮屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-14 NetFile 服務作業 - 壓縮屬性

屬性	預設值	說明
預設壓縮類型	Zip	指定使用 Zip 或 Gzip 壓縮類型。
預設壓縮層級	6	指定壓縮層級，有效值從 1 到 9。

一般

表 C-15 列出了 Netfile 服務一般屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-15 NetFile 服務 - 一般屬性

屬性	預設值	說明
MIME 類型配置檔案位置	*portal-server-Install-root*/SUNWps/samples/config/netfile	指定傳送至用戶端瀏覽器的回應內容類型。

Netlet 服務

表 C-16 列出了 Netlet 服務屬性。第一欄包含屬性；第二欄包含預設值 (如果有的話)；第三欄則包含對於該屬性的描述。

表 C-16 Netlet 服務屬性

屬性	預設值	說明
Netlet 規則	IMAP、FTP、Telnet	選擇新增或刪除規則。
如果您新增一個規則，將會需要下列九個屬性：		
-- 規則名稱		為規則指定唯一的名稱。
-- 加密演算法		指定需要的密碼。
-- URL		指定要啟動之應用程式的 URL。
-- 下載 Applet		指定是否需要下載 Applet。如果已經使用 Applet，則相關編輯方塊中的語法為： *client port:server host:server port*
-- 延伸式階段作業		確保當與此規則相對應的 Netlet 階段作業在執行時，Portal Server 階段作業時間將會延長。
-- Port-Host-Port 清單		指定用戶端連接埠、目標主機以及目標連接埠。在輸入那些數值之後 (在此表中的下三行)，請按一下「新增」以便讓此規則出現在清單中。
-- 用戶端連接埠		指定 Netlet 偵聽的用戶端連接埠。對於 FTP 規則，用戶端連接埠值必須為 30021。
-- 目標主機		靜態規則包含用於 Netlet 連線的目標機器之主機名稱。 動態規則包含 "TARGET" 這個字。
-- 目標連接埠		指定目標主機上的連接埠。
預設的原生 VM 密碼	KSSL_SSL3_RSA_WITH_RC4_128_MD5	為 Netlet 規則指定預設密碼。如果現有規則未將密碼包括成為規則一部分，當您在使用現有規則時，這個選項就非常有用。.
預設 Java Plugin 密碼	SSL_RSA_WITH_RC4_128_MD5	為 Netlet 規則指定預設密碼。如果現有規則未將密碼包括成為規則一部分，當您在使用現有規則時，這個選項就非常有用。
預設回送連接埠	58000	當透過 Netlet 下載 applet 時，指定用戶端上使用的連接埠。可以在 Netlet 規則中忽略此預設值。
重新認證連線	已取消核取	確保使用者每次重新建立 Netlet 連線，都必須輸入 Netlet 密碼。

表 C-16 Netlet 服務屬性

屬性	預設值	說明
連線的警告快顯視窗	已核取	當使用者在 Netlet 執行應用程式且當入侵者嘗試透過偵聽連接埠存取桌面時會顯示一則訊息。
在連接埠警告對話方塊中顯示核取方塊	已核取	允許使用者不顯示警告快顯視窗。
保持現有的間隔 (以分鐘為單位)	0	設定時間間隔，以供 Netlet 保持連線狀態，即使並沒有執行作業。 若您沒有指定此屬性值，則 Netlet 閒置連線會與所有其他 Portal Server 閒置連線一起逾時，其逾時時間為 Identity Server 配置的階段作業屬性區段中指定的 「最大閒置時間 (分鐘)」。
在入口網站登出時終止 Netlet	已核取	確保在使用者登出 Portal Server 時，所有連線都已終止。
存取 Netlet 規則	*	定義存取某些組織、角色或使用者的特定的 Netlet 規則。
拒絕 Netlet 規則		拒絕存取某些組織、角色或使用者的特定的 Netlet 規則。
允許的主機	*	為某些組織、角色或使用者定義存取特定的主機。
拒絕的主機		拒絕存取組織中特定的主機。

索引

N

O

P

四畫

五畫

六畫

七畫

八畫

九畫

十畫

十一畫

十二畫

十三畫

十四畫

十五畫

十六畫

十七畫

十八畫

十九畫

二十一畫