



# 面向 Web 服务应用程序的 RSA ClearTrust 就绪实施指南

最后修订：2004 年 10 月 1 日

## 1. 合作伙伴信息

|         |   |
|---------|---|
| 合作伙伴名称  | IBM   |
| 网站      | <a href="http://www.ibm.com/software/cn/websphere/datapower/">http://www.ibm.com/software/cn/websphere/datapower/</a> |
| 产品名称    | DataPower XS40 XML Security Gateway™  |
| 版本 & 平台 | 3.0   |
| 产品说明    | 特制的 1 U 机架式网络设备，提供了全面的 XML 安全功能集合，功能包括：XML 加密、XML/SOAP 防火墙过滤、XML 数字签名、XML 架构验证、SSL、XML 访问控制。                          |
| 产品类型    | Web 服务  |



## 2. 联系人信息

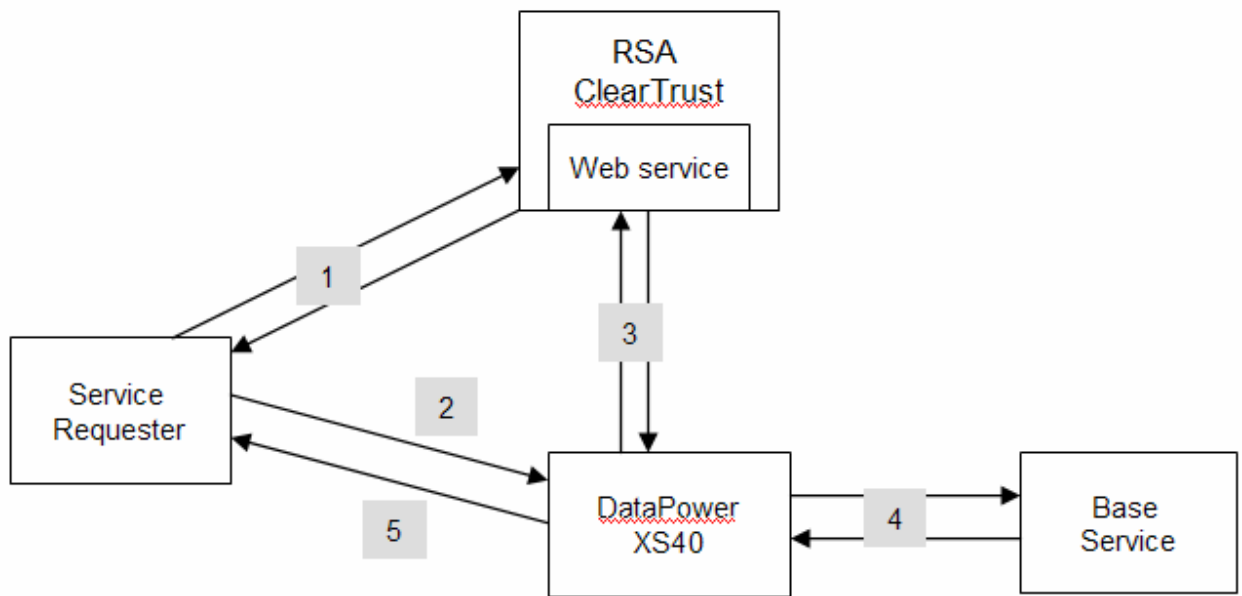
|      | 销售联系人   | 支持联系人   |
|------|---|---|
|      | 李宗灿   | 崔鹏  |
| 电子邮箱 | <a href="mailto:johnlee@cn.ibm.com">johnlee@cn.ibm.com</a>  | <a href="mailto:cuipeng@cn.ibm.com">cuipeng@cn.ibm.com</a>  |
| 电话   | (86-10)63618826   | (86-10)63612176   |
| 网站   | <a href="http://www.ibm.com/software/cn/websphere/datapower/">http://www.ibm.com/software/cn/websphere/datapower/</a> | <a href="http://www.ibm.com/software/cn/websphere/datapower/">http://www.ibm.com/software/cn/websphere/datapower/</a> |

### 3. 解决方案摘要

| 特性                         | 详细资料                              |
|----------------------------|-----------------------------------|
| 为 SSO 使用 UserID            | 可行，通过 Runtime Web Services API 实现 |
| 使用 UserID 以实现个性化           | N/A                               |
| 识别身份验证类型                   | N/A                               |
| API 级别授权支持<br>(RuntimeAPI) | 无                                 |
| 用户管理<br>(AdminAPI)         | N/A                               |

## 4. 整合概述

DataPower XS40 能够使用 RSA ClearTrust 验证 Web 服务请求。



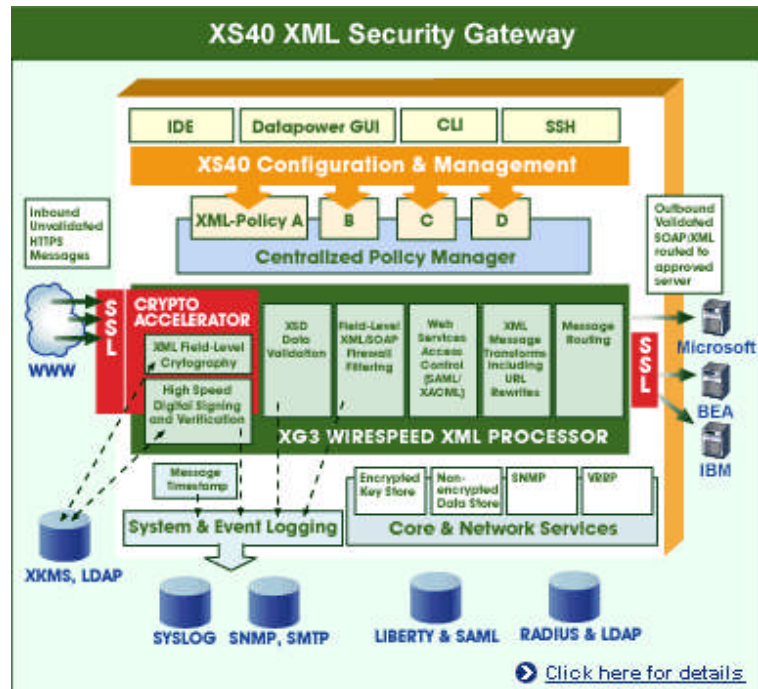
下面介绍 DataPower XS40 如何与 RSA ClearTrust 整合，从而验证 SSO 令牌：

1. Web 服务请求者首先从 ClearTrust 处获得 SSO 令牌（通常是通过标准 RSA ClearTrust Web 代理获得）。
2. 服务请求者向 XS40 发送服务请求，同时将 SSO 令牌以带 TTP 报头的 cookie 形式发送。
3. DataPower XS40 提取 SSO 令牌，并通过 Runtime Web 服务 API 联系 RSA ClearTrust 以进行身份验证。
4. 如果 SSO 令牌有效，XS40 会将服务请求传递给基本服务。
5. 然后响应被送回至服务请求者。

## 5. 产品需求

### 硬件需求

|  |                   |
|--|-------------------|
| 组件名称: <b>XS40 XML Security Gateway</b> |                   |
| DataPower 固件                           | Release 3 (或更新版本) |
|  |                   |



## 6. 产品配置


本节提供将合作伙伴产品与 RSA ClearTrust 整合的指导。本文档无意提出最佳安装或配置建议，而是假定读者拥有这两种产品的工作知识，可执行本节列出的任务，并访问两者的文档，从而安装必需的软件组件。所有产品/组件都需要在此整合前安装和应用。在进行下一步之前执行必要的测试，确保条件满足。

### 安装

确认您已根据其各自的安装说明安装了 RSA ClearTrust 和 DataPower XS40。您需要首先安装 RSA ClearTrust 服务器，然后是 Web 服务组件。

### 配置 RSA ClearTrust

使用 RSA ClearTrust 管理 UI，将 XS40 添加为服务器。参看 ClearTrust 管理文档以获取更多信息。

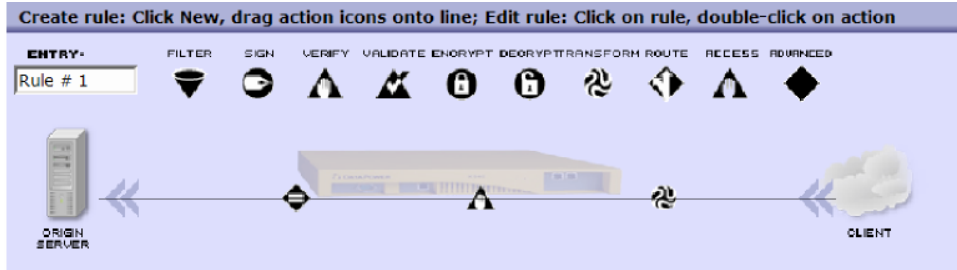


The screenshot shows the 'Add a New Server' configuration form. The form is titled 'Add a New Server' and includes a 'How To...' sidebar with links for 'Understand Servers', 'Edit Servers', and 'Add Servers'. The main form area is divided into two sections: 'Server Basics' and 'Administrative Control'. In the 'Server Basics' section, the following fields are visible: 'Server Name' (lab-xa02.datapower.com), 'Server Type' (Web Server), 'Product' (Apache), 'Hostname' (lab-xa02.datapower.com), 'Port' (8800), and 'Description' (Web service firewall on the XS40 box). In the 'Administrative Control' section, the 'Administrative Group' is set to 'Default Administrative Group' and 'Visibility' is set to 'Private (visible only to administrators of this administrative group)'. At the bottom of the form, there are three buttons: 'Save', 'Save & Add Another', and 'Cancel'.

### 配置 DataPower XS40

使用 XS40 WebGUI 为 Web 服务配置防火墙。参看 XS40 WebGUI 文档中的《创建 XML 防火墙》和《定义文档处理策略》，获得逐步指导。

步骤之一是创建 XML 防火墙策略（也被称为“文档处理策略”）。  
您可以利用 XS40 的 AAA 身份验证、授权和审计框架。



- a) 双击“=”图标以匹配规则，例如将 URL 匹配设置为 \* 以匹配所有接收的服务请求。
- b) 拖动“Access”图标到横线上。双击“Access”图表以设置 AAA 策略。

Configure an Access Control Policy
Help

Policy Name: cleartrust2

---

**Define input and optional output context**

Select input context: (auto) ▾

or enter input context: (auto)

Enter optional output context: (auto)

---

**Define how to extract a user's identity from an incoming request.**

**Identification methods**

- HTTP's Authentication header
- UserName element from WS-Security header
- BinarySecurityToken element from WS-Security header
- Subject DN from SSL client certificate
- Name from SAML attribute assertion
- Name from SAML authentication assertion
- Client IP address
- Subject DN from certificate in the message's signature
- Token extracted from the message
- Custom template

Enter a URL:

---

**Define how to map credentials.**

Method: none ▾

- c) 在标识步骤中，选择 **Custom template**。Contact DataPower for an XML 配置模板允许 XS40 提取报头中作为 cookie 发送的 SSO 令牌。在后续固件版本中，提取 cookie，它将作为单选按钮以供选择使用。
- d) 如果只进行 SSO 身份验证，您可以跳过映射凭据步骤，单击“Next”按钮。

- e) 要进行身份验证，选择 **Custom template**。Contact DataPower for an XML 配置模板允许 XS40 使用 ClearTrust Web 服务检验 SSO 令牌。您将需要修改模板以指定您安装 ClearTrust Web 服务的位置。在后续固件版本中，可以选择一个单选按钮来联系 RSA ClearTrust。
- f) 在接下来的三个窗口中，您将配置资源提取 & 映射、授权和后处理。如果您只进行身份验证，您可以使用 **URL sent by client** 来标识资源，其他选项使用默认值。然后单击 **Commit**。
- g) 单击 **Apply** 保存规则。然后您将看到“Transform”图标被插入，防火墙策略设置完成。

## 测试您的配置

现在您应该能够使用已配置的防火墙在 XS40 中直接通信了。使用主菜单中的 **Status->System Logs**，观察任何错误消息。

下例为相关日志输出，按时间逆序排列。

```

08:06:53 | aaa | info | 21131 | INPUT: Policy(cleartrust): AuthenticateClearTrustCookie.xml: Made soapcall with the result:
AAAAAgARAFBI vV3y 172xl F57mMwCaDnc6DfXh25nGKNRd7YlyVt/hVNP+4hV+oxn-DChgTR597seX721iyA19Nj74cwwCFk
TKEN VALIDATE SUCCEEDED SC TOKEN
AAAAAgARAFBI vV3y 172xl F57mMwCaDnc6DfXh25nGKNRd7YlyVt/hVNP+4hV+oxn-DChgTR597seX721iyA19Nj74cwwCFk
08:06:53 | aaa | info | 21131 | INPUT: Policy(cleartrust): AuthenticateClearTrustCookie.xml: Found cookie in
AAAAAQABAEANxH1gf6RPeJpGk1RQ8uCWQN2b_LNWCNleIpZyV172ms1GK5CnripitY3dHQjyc08DF2hJLXi03lUl/Fx7XYr/
...
08:06:53 | aaa | info | 21131 | INPUT: Policy(cleartrust): GetClearTrustCookie.xml: cookie is
AAAAAQABAEANxH1gf6RPeJpGk1RQ8uCWQN2b_LNWCNleIpZyV172ms1GK5CnripitY3dHQjyc08DF2hJLXi03hUl/Fx7XYr/

```

## 7. Web 服务应用程序的认证清单

测试日期: 2004 年 6 月 16 日

| 产品                   | 已测试版本                 |
|----------------------|-----------------------|
| RSA ClearTrust       | 5.5.2                 |
| RSA ClearTrust Agent | 4.5 for Microsoft IIS |
| DataPower XS40       | Firmware Release 3.0  |

| 测试用例  | 结果  |     |     |     |   |
|---|---|-----|-----|-----|---|
| <b>Web 服务</b><br><b>SSO</b><br>通过 RSA ClearTrust HTTP 报头实现<br>通过 SOAP 报头 (通过 Runtime API 的 BASIC 身份验证) 实现<br>通过 SOAP 报头 (通过 Runtime API 的 RSA ClearTrust 令牌验证) 实现<br>通过 Web 服务 API (通过 Web 服务 API 的 RSA ClearTrust 令牌验证) 实现 | <table border="1"> <tr><td>N/A</td></tr> <tr><td>N/A</td></tr> <tr><td>N/A</td></tr> <tr><td>P</td></tr> </table> | N/A | N/A | N/A | P |
| N/A   |   |     |     |     |   |
| N/A   |   |     |     |     |   |
| N/A   |   |     |     |     |   |
| P   |   |     |     |     |   |
| <b>授权</b><br>通过 RSA ClearTrust Runtime API 实现<br>通过 RSA ClearTrust Web 服务 API 实现  | <table border="1"> <tr><td>N/A</td></tr> <tr><td>N/A</td></tr> </table>   | N/A | N/A |     |   |
| N/A   |   |     |     |     |   |
| N/A   |   |     |     |     |   |

JEC

\*P= “通过” 或 “是” F= “失败” N/A= “不可用功能”

## 8. 已知问题

无