RSA SecurID 就绪实施指南

最后修订：2004 年 5 月 27 日

1. 合作伙伴信息

合作伙伴名称	IBM
网站	http://www.ibm.com/software/cn/websphere/datapower/
产品名称	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	johnlee@cn.ibm.com	cuipeng@cn.ibm.com
电话	(86-10)63618826	(86-10)63612176
网站	http://www.ibm.com/software/cn/websphere/datapower/	http://www.ibm.com/software/cn/websphere/datapower/

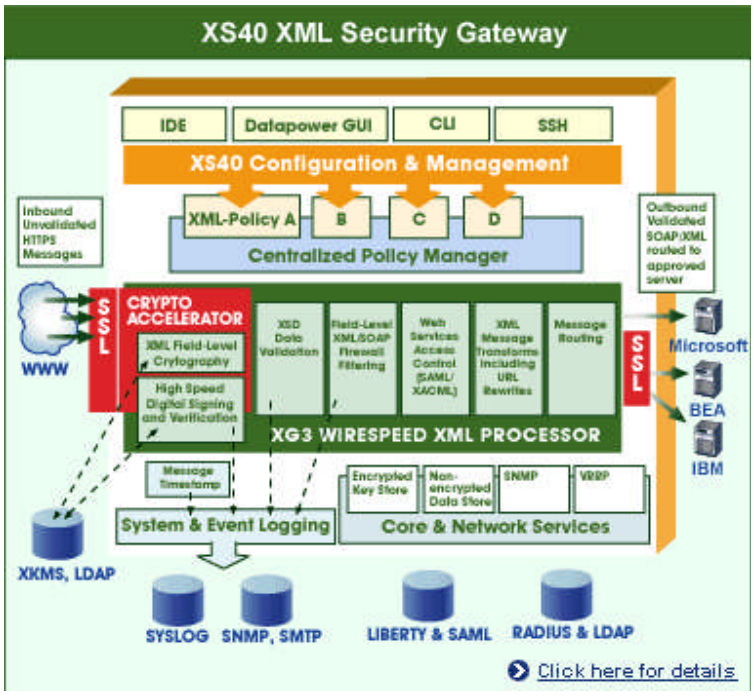
3. 解决方案摘要

特性	详细资料
支持的验证方法	RADIUS
RSA ACE/Agent 库版本	5.2
RSA ACE 5 锁定	N/A
副本 RSA ACE/Server 支持	N/A
辅助 RADIUS 服务器支持	有；不超过 5 台
客户机节点密钥位置	N/A
RSA ACE/Server 代理主机类型	Communication server
RSA SecurID 用户规范	指定用户
RSA Secu rID 合作伙伴产品保护	有
管理员	
RSA 软件令牌整合	无

4. 产品需求

硬件和软件需求

组件名称： **XS40 设备**	
DataPower 固件	Release 3（或更新版本）
OpenSSL	用于将 base64 转换为 DER（任何等效工具均适用）

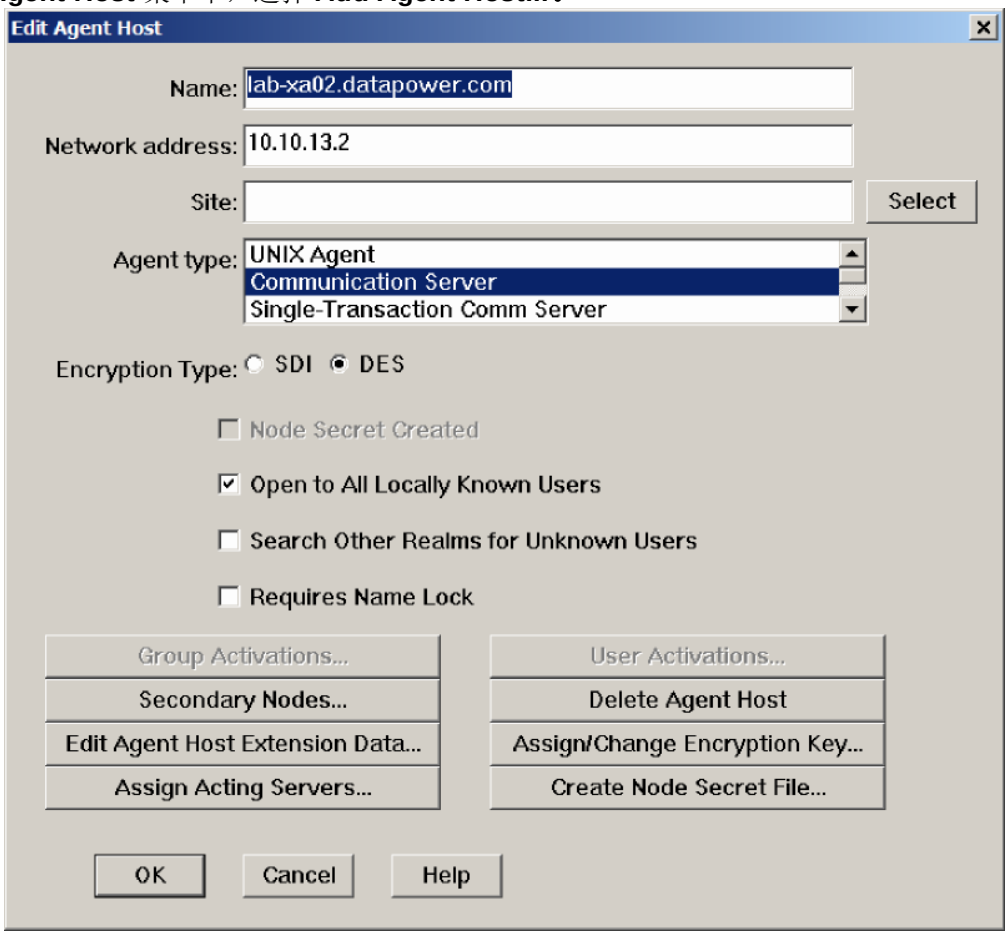


5. RSA ACE/Server 配置

执行以下步骤，将 XS40 作为 RSA ACE/Server 数据库内部的代理主机进行安装。

- 在 RSA ACE/Server 计算机上的 Windows 中，单击 **Start > Programs > RSA ACE/Server**，再单击 **Database Administration - Host Mode**。

1. 在 **Agent Host** 菜单中，选择 **Add Agent Host...**。



- o 在 **Name** 栏中，输入设备的主机名。
- o 在 **Network address** 栏中，输入 XS40 的 IP 地址。
- o 在 **Agent Type** 中，选择 Communication Server。
- o XS40 与使用 Radius 的 ACE/Server 通信。单击 **Assign/Change Encryption Key...**，输入加密密钥。此**密钥**必须与您在 XS40 上所输入的相同。

注意： 所有主机名和 IP 地址均应相互解析，这至关重要。请参考 RSA ACE/Server 文档以获得关于此窗口中这一项及其他配置参数的详细信息。其次，您还可以选择单击窗口底部的“Help”按钮。

2. 执行上述相同步骤，将您已安装了 ACE/server 的主机添加为代理主机。这将允许 Radius 服务器作为代理与 ACE/server 通信。在此您无需指定加密密钥。

疑难解答： 您可单击 **Start > Programs > RSA ACE/Server -> Log monitor，** 从而启动日志记录。如果看到“node verification failed”，请确认 Radius 服务器能与 RSA ACE/server 通信。参看 ACE/server 管理指南，以清除节点密钥从而允许通信。

如果您已为用户输入了正确的初始密码，但仍在日志中看到“bad password”，请检查确定在 ACE/server 数据库管理界面中，已为 XS40 指定的加密密钥与用于配置 XS40 的密钥相同。

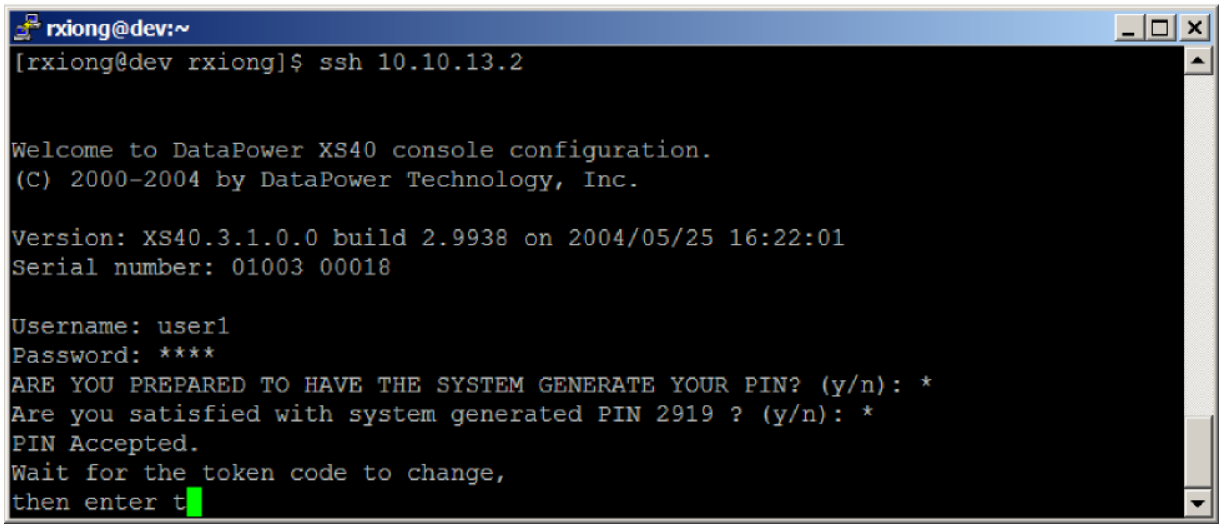
6. 合作伙伴 RSA ACE/Agent 配置

Radius 身份验证是 XS40 的标准。参看 DataPower XS40 文档，了解如何将 CE/Server 添加为 Radius 服务器。

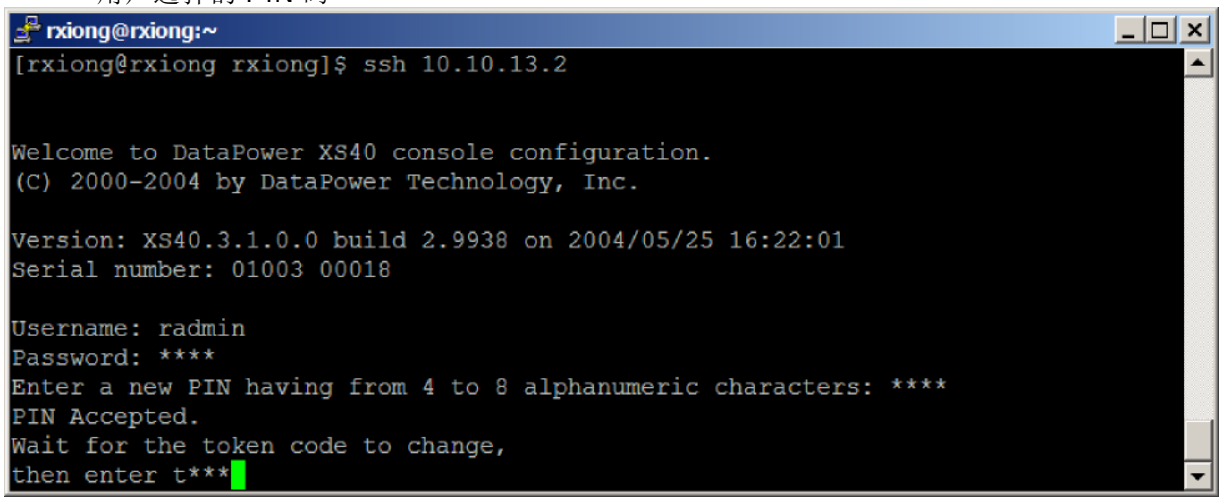
- 要为 Radius 服务器设置**密钥**字段，请输入您将 XS40 安装为 ACE/Server 上的代理主机时使用的加密密钥。

然后您就应该能够作为 ACE/Server 上已配置的用户登录了。参看下例登录窗口，了解

- 系统生成的 PIN 码



- 用户选择的 PIN 码



7. 认证清单

测试日期：2004 年 5 月 27 日

产品	已测试版本
RSA ACE/Server	5.2
RSA ACE/Agent	N/A (Radius)
DataPower XS40	Release 3.0

测试	ACE	RADIUS
第一次审计（节点密钥创建）	N/A	通过
新的 PIN 模式： 系统生成		
非 PINPAD 令牌	N/A	通过
PINPAD 令牌	N/A	通过
用户定义（4-8 个文字和数字）		
非 PINPAD 令牌	N/A	通过
密码	N/A	通过
用户定义（5-7 个数字）		
非 PINPAD 令牌	N/A	通过
PINPAD 令牌	N/A	通过
软件令牌	N/A	通过
拒绝 4 位令牌	N/A	通过
拒绝文字和数字	N/A	通过
用户可选		
非 PINPAD 令牌	N/A	通过
PINPAD 令牌	N/A	通过
PASSCODE		
16 位 PASSCODE	N/A	通过
4 位密码	N/A	通过
“无引线”令牌代码	N/A	通过
下一个令牌代码模式		
非 PINPAD 令牌	N/A	通过
PINPAD 令牌	N/A	通过
软件令牌 API 验证		
新的 PIN 模式	N/A	通过
8 位 PIN 和 8 位令牌代码	N/A	通过
故障转移	N/A	N/A
用户说定测试（RSA ACE 锁定功能）	N/A	
非 RES ACE/Server	N/A	通过

JEC 通过，失败或 N/A（N/A=不可用功能）

8. 已知问题

- 无。