Perle Systems, Ltd
IOLAN Secure Device Server

RSA SecurID Ready Implementation Guide

Last Modified: February 2nd, 2015

Partner Information

Product Information	
Partner Name	Perle Systems, Ltd
Web Site	www.perle.com
Product Name	IOLAN Secure Device Server
Version & Platform	4.6
Product Description	The IOLAN Secure Device Server series of device servers are the most advanced device servers on the market for secure serial to Ethernet connectivity applications. Delivering high performance in a compact size, the IOLAN Secure Device Server series offers robust security, flexibility and next generation IPV6 technology making it ideal for applications that require secure remote device/console management, data capture or monitoring.

Solution Summary

The Perle IOLAN SDS (Secure Device Server) offers the security and convenience of secure two-factor authentication using RSA SecurID. Secure data protection is a critical business requirement and, by offering full interoperability with the RSA Authentication Manger, administrators can be sure of secure access. The IOLAN SDS is ideally suited for two primary applications - secure console access and secure remote access.

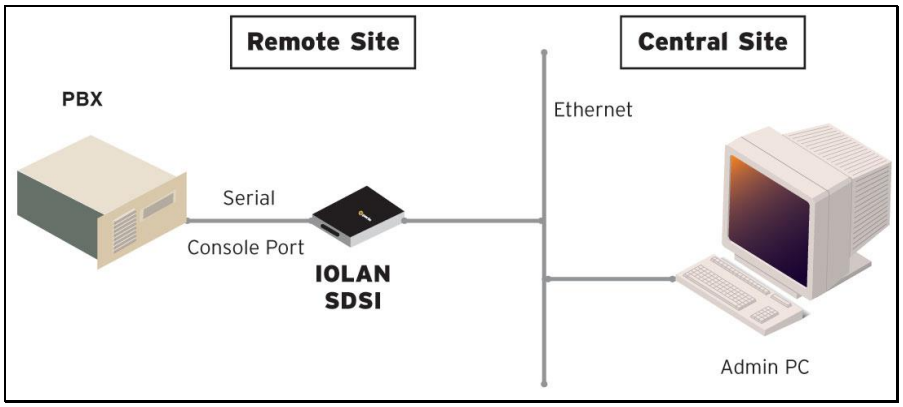
Secure Console Access

The IOLAN SDS enables administrators to securely access the serial console ports on valuable equipment such as Unix, Linux, and Windows servers, routers, switches and PBX's to name a few. Access to the IOLAN SDS will challenge the user upon connection attempts either through the LAN or over a dial-up PPP connection.

Secure Remote Access

PC and laptop users can dial-in from remote locations to access resources on a corporate LAN. SecurID authentication allows the IOLAN SDS to ensure that only authorized users can access these valuable resources.

RSA Authentication Manager supported features	
Perle IOLAN Secure Device Server	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Agent Host Configuration

To facilitate communication between Perle IOLAN and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies Perle IOLAN and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Note: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

> **Note: The RSA agent name is specified in the rsa_api.properties file.**

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Perle IOLAN will occur.

If Perle IOLAN will be communicating with RSA Authentication Manager via RADIUS, then a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

> **Note: The RADIUS client's hostname must resolve to the IP address specified.**

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Perle IOLAN with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Perle IOLAN components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

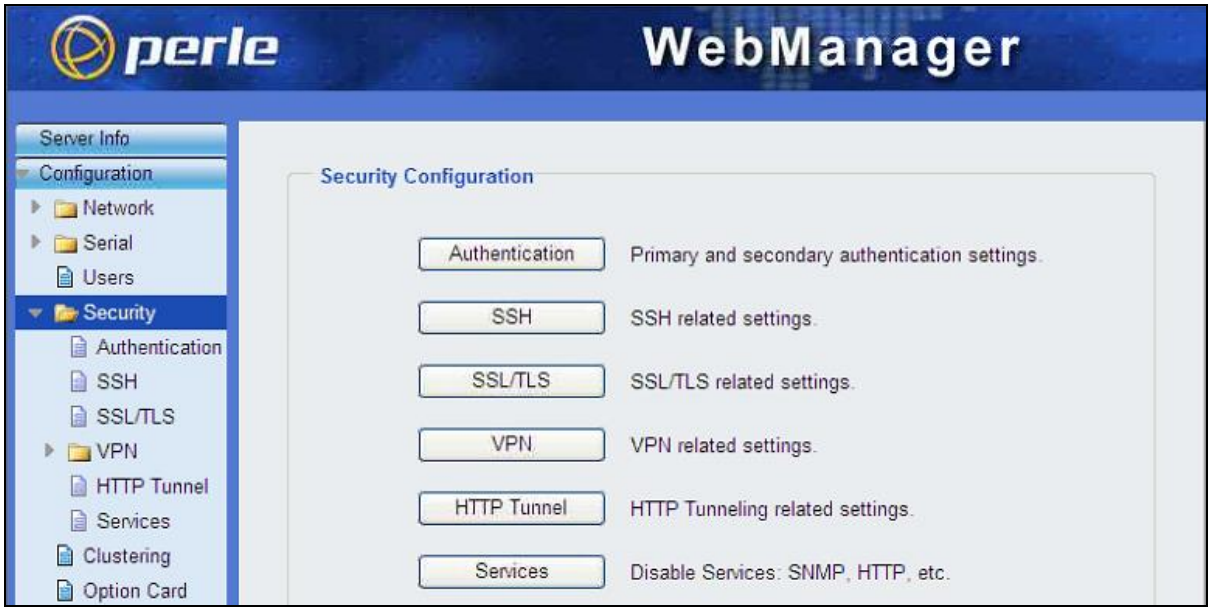
Enter RSA Authentication Manager host information

1. Logon to the IOLAN's WebManager and browse to **Configuration** > **Network** and then click **Advanced**.

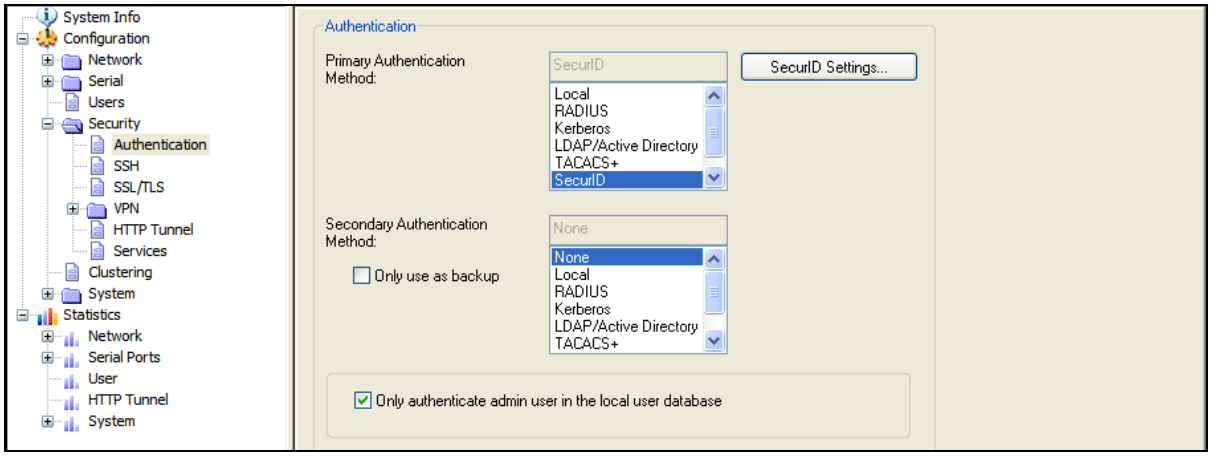
2. Click **Add** and enter the **Name** and **IP Address/FQDN** of your RSA Authentication Manager(s) to the IOLAN's **Host Table**.

Integrate IOLAN with SecurID via Native RSA Agent

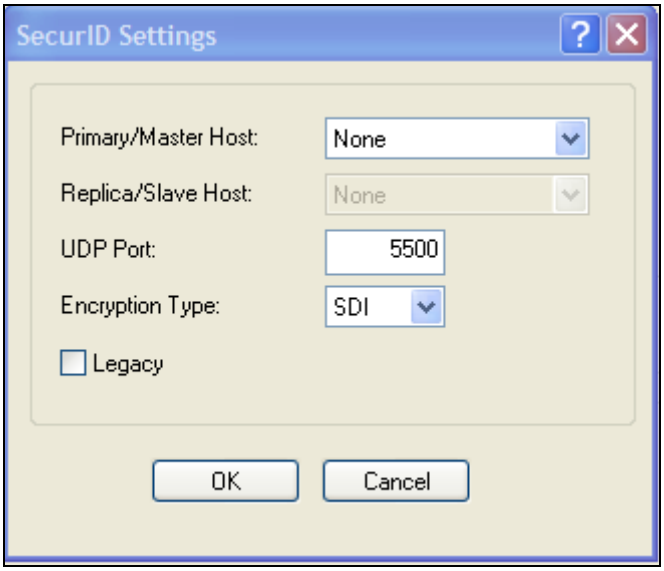
1. Browse to **Configuration** > **Security** and click **Authentication**.



2. Select **SecurID** from the **Authentication Methods** dropdown menu and click **SecurID Settings**…

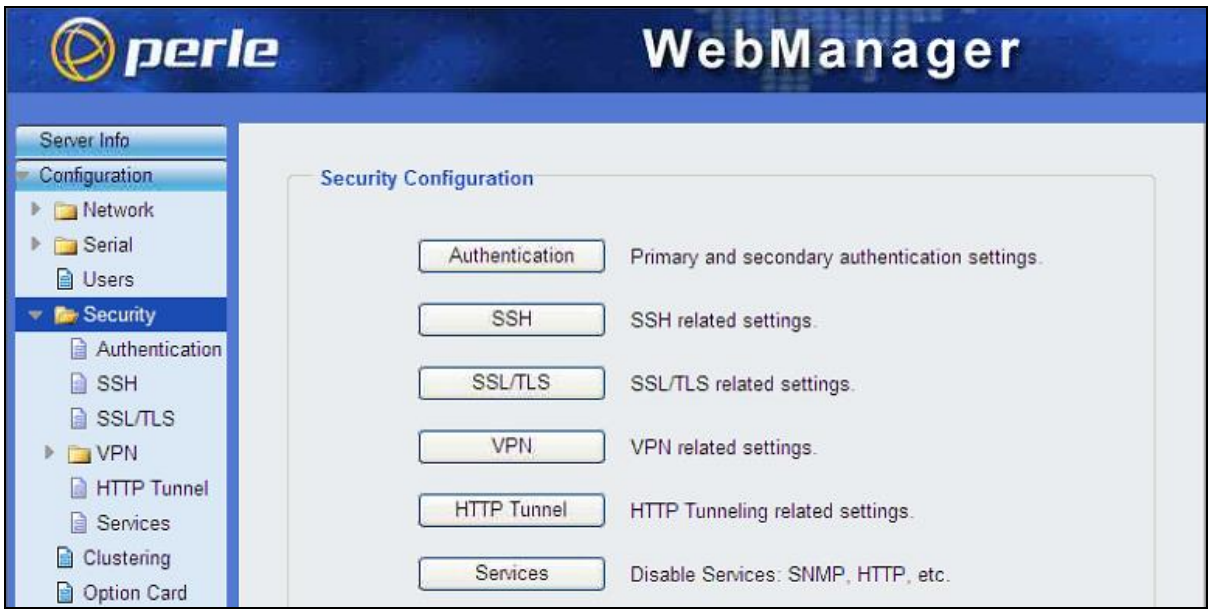


3. Select your primary Authentication Manager server from the **Primary/Master Host** dropdown menu and click **OK**.



Integrate IOLAN with SecurID via RADIUS

1. Browse to **Configuration** > **Security** and click **Authentication**.



2. Select **RADIUS** from the **Authentication Methods** dropdown menu and click **Settings**…

3. Select your primary Authentication Manager server from the **First Authentication Host** dropdown menu and click **Change Secret** to set the shared secret.
4. (if applicable) Select your replica Authentication Manager server from the **Second Authentication Host** dropdown menu and click **Change Secret** to set the shared secret.

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1 SP1	Virtual Appliance
Perle IOLAN	4.6	Proprietary

RSA SecurID Authentication

Date Tested: January 16th, 2015

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	✓	N/A	✓
System Generated PIN	✓	N/A	✓
User Defined (4-8 Alphanumeric)	✓	N/A	✓
User Defined (5-7 Numeric)	✓	N/A	✓
Deny 4 and 8 Digit PIN	✓	N/A	✓
Deny Alphanumeric PIN	✓	N/A	✓
Deny PIN Reuse	✓	N/A	✓
Passcode			
16 Digit Passcode	✓	N/A	✓
4 Digit Fixed Passcode	✓	N/A	✓
Next Tokencode Mode			
Next Tokencode Mode	✓	N/A	✓
On-Demand Authentication			
On-Demand Authentication	✓	N/A	✓
On-Demand New PIN	✓	N/A	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	N/A	✓
No RSA Authentication Manager	✓	N/A	✓

PEW / PAR

✓= Pass ✗= Fail N/A = Not Applicable to Integration

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	None stored
sdopts.rec	None stored
Node secret	In Memory
sdstatus.12 / jastatus.12	In Memory
TCP Agent Files	**Location**
rsa_api.properties	N/A
sdconf.rec	N/A
sdopts.rec	N/A
Node secret	N/A

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	Compiled from 5.0.3.1 C agent source kit
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

Click **Reset node secret** from the **Tools** drop-down menu in **DeviceManager** to reset the node secret.

sdconf.rec:

This integration features a custom compiled agent which does not require an sdconf.rec configuration file.

sdopts.rec:

This integration does not support sdopts.rec optional configuration file.

sdstatus.12:

This integration does not utilize an sdstatus.12 file.