# RSA SecurID Ready Implementation Guide

Last Modified: 06/14/05

## Partner Information

| Product Information | |
|---|---|
| **Partner Name** | Digi International |
| **Web Site** | www.digi.com |
| **Product Name** | Digi CM Family |
| **Version & Platform** | Firmware 1.6 and above |
| **Product Description** | Secure, intelligent, easy-to-use console server provides remote access to data center equipment via a serial port. With Digi CM, administrators can securely monitor and control servers, routers, switches, PBX, firewalls and other network devices from anywhere on the corporate TCP/IP network, over the Internet, or through dial-up modem connections - even when the server is unavailable through the network. |
| **Product Category** | Remote Access |

## Solution Summary

Digi CM provides simple integration with RSA SecurID through RADIUS, providing a secure method for centralized control of network equipment and computer systems. Digi CM uses the RSA Authentication Manager Server to validate access to the Digi CM itself and to devices that are console-attached to its serial ports, providing a unified Access, Authorization, and Accounting (AAA) methodology that is easy to deploy, configure, maintain, and can seamlessly expand to serve future needs.

Data integrity, data privacy, and effective controls over financial and data systems are critical to modern business success. RSA SecurID solutions and Digi CM provide a complete method of ensuring that all system-level and network-level changes to existing systems are monitored and logged. This minimizes the cost and duration of system audits, and maximizes system availability. Digi CM provides the capability to log access to attached systems and changes made to those systems, while RSA Authentication Manager Server provides independent auditing and monitoring of all access to systems and to the CM itself against the authoritative corporate authentication database, eliminating directory synchronization costs.

| **Partner Integration Overview** | |
|---|---|
| **Authentication Methods Supported** | RADIUS |
| **List Library Version Used** | N/A |
| **RSA Authentication Manager Name Locking *** | N/A |
| **RSA Authentication Manager Replica Support *** | N/A |
| **Secondary RADIUS Server Support** | Yes, Primary and Secondary |
| **Location of Node Secret on Agent** | 'None stored', In Registry or Path to Node Secret File |
| **RSA Authentication Agent Host Type** | Communication Server |
| **RSA SecurID User Specification** | Designated Users |
| **RSA SecurID Protection of Administrative Users** | No (root is only authenticated locally) |
| **RSA Software Token API Integration** | No |
| **Use of Cached Domain Credentials** | No |
| | * = Mandatory Function when using Native SecurID Protocols |

# Product Requirements

| Partner Product Requirements: Digi CM Family | |
|---|---|
| **CPU** | Motorola PowerPC 855 / 40 MHz |
| **Memory** | 64 MB |
| **Storage** | -- |
| **Firmware Version** | Digi CM 1.6.0.1 and above |
| | |

| Operating System | |
|---|---|
| **Platform** | **Required Patches** |
| Linux | 2.4.2_hhl20 |
| | |

# Agent Host Configuration

To facilitate communication between Digi CM 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 the Digi CM within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret

When adding the Agent Host Record, you should configure the Digi CM as a Communications Server. This setting is used by the RSA Authentication Manager to determine how communication with the Digi CM will occur.

**Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

# Partner Authentication Agent Configuration

## *Before You Begin*

This section provides instructions for integrating the partners' product 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.

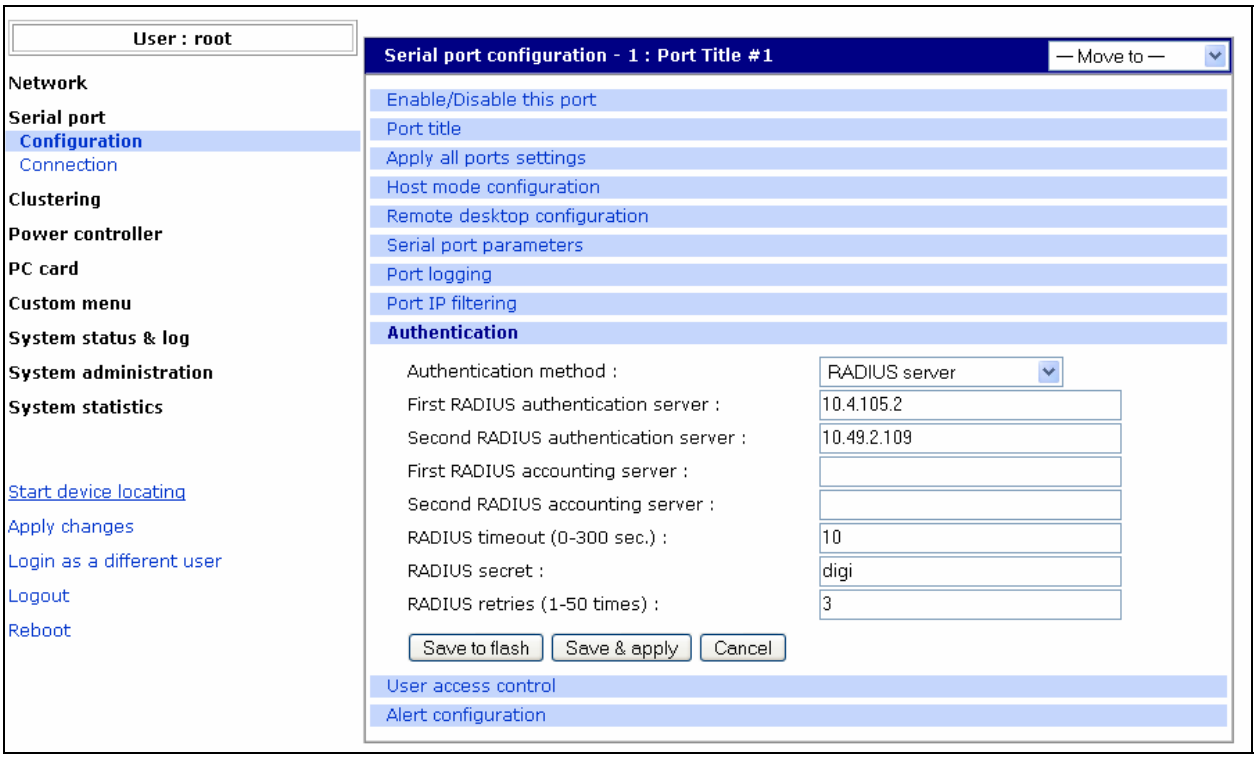
All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

## *Documenting the Solution*

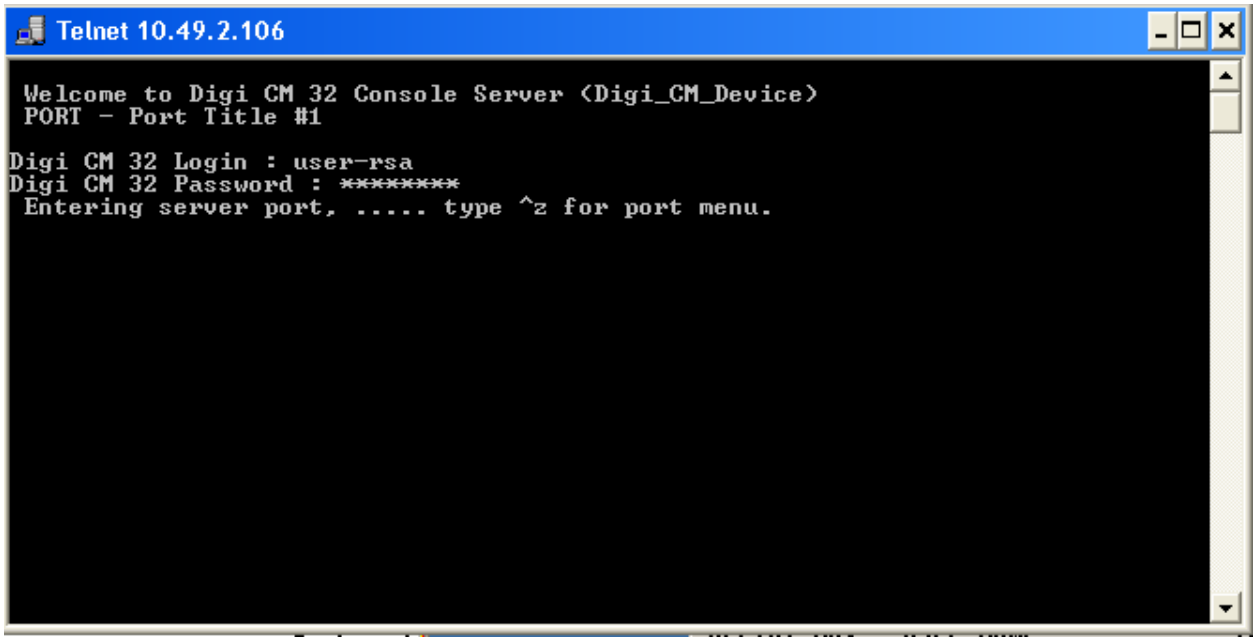
To configure the Digi CM to use RSA SecurID Authentication, perform the following steps

1. Log into the Web UI with the user **root** and password **dbps**.
2. Go into the configuration page of one of the serial ports
3. Click on the **Authentication** Tab and select **RADIUS server** as the Authentication method
4. Fill in the IP address of the RSA Server and enter the RADIUS secret.
5. Click on **Save & apply** as the final step.

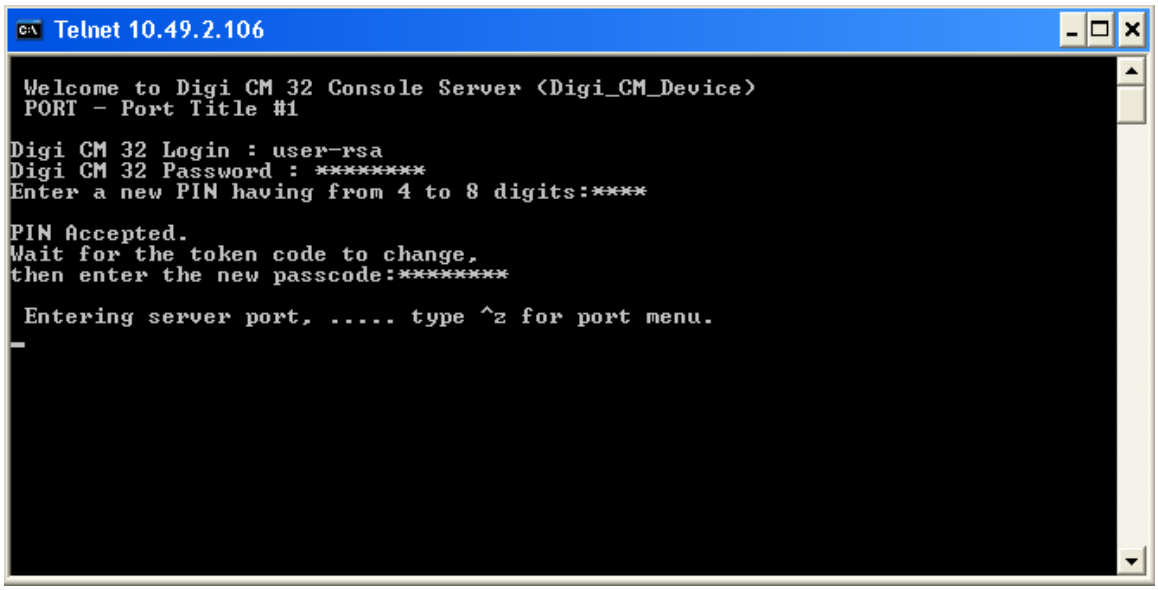
### Configuration Example:



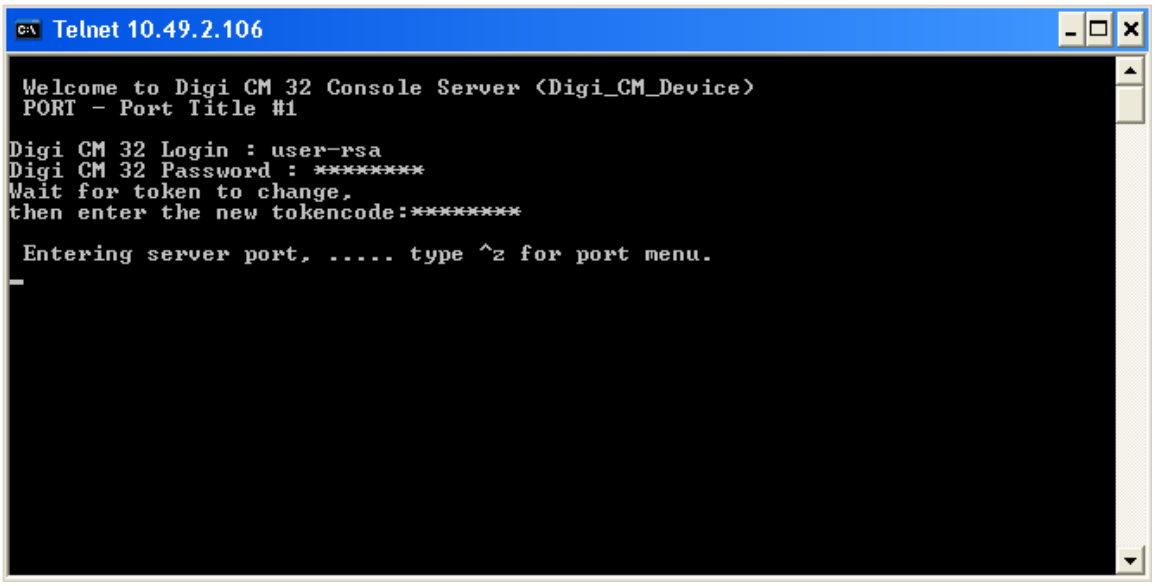
**Login Example:**




**New PIN Mode:**



**Next Tokencode Mode:**



# Certification Checklist

Date Tested: June 7th, 2005

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| **RSA Authentication Manager** | Windows 2000 | 5.2 |
| **RSA Authentication Agent** | Windows 2000 | 5.6 |
| **RSA Software Token** | Windows 2000 | 3.0.5 |
| **Digi CM Family 8,16,32 and 48** | Linux | 1.6.0.1 and above |

| Mandatory Functionality | | | |
|---|---|---|---|
| **RSA Native Protocol** | | **RADIUS Protocol** | |
| **New PIN Mode** | | | |
| Force Authentication After New PIN | N/A | Force Authentication After New PIN | ✓ |
| System Generated PIN | N/A | System Generated PIN | ✓ |
| User Defined (4-8 Alphanumeric) | N/A | User Defined (4-8 Alphanumeric) | ✓ |
| User Defined (5-7 Numeric) | N/A | User Defined (5-7 Numeric) | ✓ |
| User Selectable | N/A | User Selectable | ✓ |
| Deny 4 and 8 Digit PIN | N/A | Deny 4 and 8 Digit PIN | ✓ |
| Deny Alphanumeric PIN | N/A | Deny Alphanumeric PIN | ✓ |
| **PASSCODE** | | | |
| 16 Digit PASSCODE | N/A | 16 Digit PASSCODE | ✓ |
| 4 Digit Password | N/A | 4 Digit Password | ✓ |
| **Next Tokencode Mode** | | | |
| Next Tokencode Mode | N/A | Next Tokencode Mode | ✓ |
| **Load Balancing / Reliability Testing** | | | |
| Failover (3-10 Replicas) | N/A | Failover | ✓ |
| Name Locking Enabled | N/A | Name Locking Enabled | |
| No RSA Authentication Manager | N/A | No RSA Authentication Manager | ✓ |
| **Additional Functionality** | | | |
| **RSA Software Token API Functionality** | | | |
| System Generated PIN | N/A | System Generated PIN | N/A |
| User Defined (8 Digit Numeric) | N/A | User Defined (8 Digit Numeric) | N/A |
| User Selectable | N/A | User Selectable | N/A |
| Next Tokencode Mode | N/A | Next Tokencode Mode | N/A |
| **Domain Credential Functionality** | | | |
| Determine Cached Credential State | N/A | Determine Cached Credential State | |
| Set Domain Credential | N/A | Set Domain Credential | |
| Retrieve Domain Credential | N/A | Retrieve Domain Credential | |

JEC

✓ = Pass ✗ = Fail N/A = Non-Available Function