Imprivata
OneSign 4.0

.

RSA SecurID Ready Implementation Guide

Last Modified: February 12, 2010

Partner Information

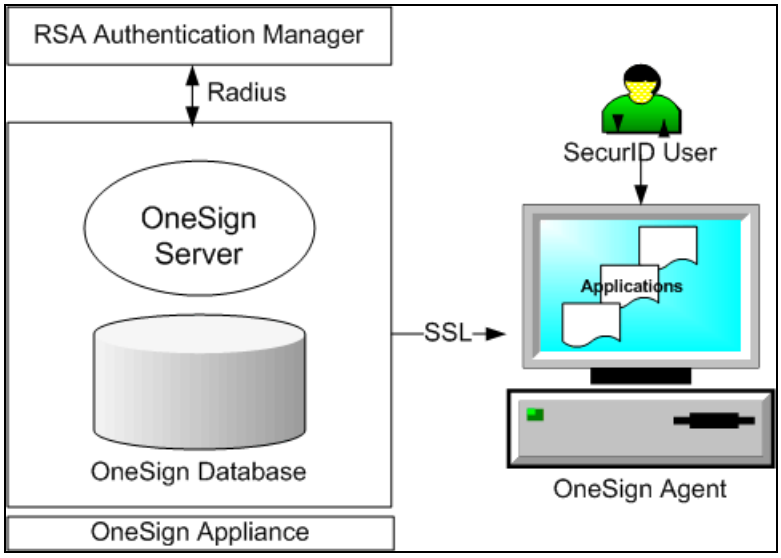
Product Information	
Partner Name	Imprivata
Web Site	www.imprivata.com
Product Name	OneSign
Version & Platform	4.0
Product Description	Imprivata OneSign is a network appliance that provides secure single sign-on service to users who have authenticated to the OneSign server. OneSign users can authenticate to the OneSign server via RSA SecurID.
Product Category	Authentication, Smart Cards, Tokens

Solution Summary

Imprivata OneSign® is an identity and access management platform that strengthens user authentication to networks, streamlines access to Web, client/server and legacy applications and simplifies the process of compliance reporting. The platform delivers its services through a secure, self-contained appliance that requires zero modifications to existing IT infrastructure and is centrally managed from a single administrative console.

OneSign can be configured to communicate with RSA Authentication Manager via the RADIUS protocol. This seamless integration allows OneSign users the strong, two-factor authentication provided by RSA SecurID.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
RSA SecurID API Version	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes (1)
RSA Authentication Agent Host Type for 7.1	N/A
RSA SecurID User Specification	Designated Users
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	No



Product Requirements

Hardware requirements

Imprivata OneSign is a network appliance and requires no external hardware. Please see the *OneSign Appliance Guide* for setup instructions including how to install the Appliance Administrator client application.

Software requirements

Partner Product Requirements: OneSign	
Required Software	**Version**
Microsoft Internet Explorer	6.0 or greater

Operating System	
Platform	**Required Patches**
Microsoft Windows	2000 Server or greater

Additional Requirements:

Each OneSign user must have an account on a domain linked to OneSign or a OneSign Directory Domain Account. Please see the *OneSign Administrator Guide* for more information. External users can be imported from the following directories:

- Active Directory
- NT Domain
- Netware NDS/eDirectory
- IBM Tivoli
- Sun ONE LDAP

Authentication Agent Configuration

Agent Host Records contain information that allows an RSA Authentication Manager server to locate its clients and establish secure communication channels with them. The server's database must contain an Agent Host Record to identify each OneSign appliance deployed in a given environment. In order to create this record, the following information is required for each instance of OneSign:

- A hostname
- An IP Address for each network interface
- A RADIUS Secret

> **Note: OneSign Agent hostnames must resolve to valid IP addresses on the local network.**

When adding the Agent Host Record, the OneSign appliance Authentication Agent Type should be set to "Standard Agent". This setting is used by the RSA Authentication Manager server to determine how it will communicate with the OneSign appliance.

> **Important: The Authentication Agent Type should be set to "Standard Agent" for all RSA Authentication Manager 7.1 Agent Host Records.**

Please refer to the appropriate RSA Security documentation for additional information about creating and managing Agent Host records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	"Not implemented'
Node Secret	"Not implemented'
sdstatus.12	"Not implemented'
sdopts.rec	"Not implemented'

Partner Product Configuration

Before You Begin

This section provides instructions for integrating OneSign 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 appropriate documentation for all products in order to install the required components.

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

Prerequisites

1. A user named "testuser" must be created in RSA Authentication Manager. OneSign will validate its RADIUS connection properties with this user, but it will never complete a successful authentication with it. Therefore, any static password may be assigned to "testuser".
2. There must be a one-to-one username mapping from OneSign to RSA Authentication Manager for each user who will authenticate with RSA SecurID. Please refer to the appropriate Imprivata OneSign and RSA Authentication Manager documents for instructions on creating users.

Configuring RSA SecurID Authentication in Imprivata OneSign

Note: The following steps can only be preformed by a OneSign user who has administrative access to OneSign Administrator. Please the OneSign Administrator Guide (version 4.0) for more information.

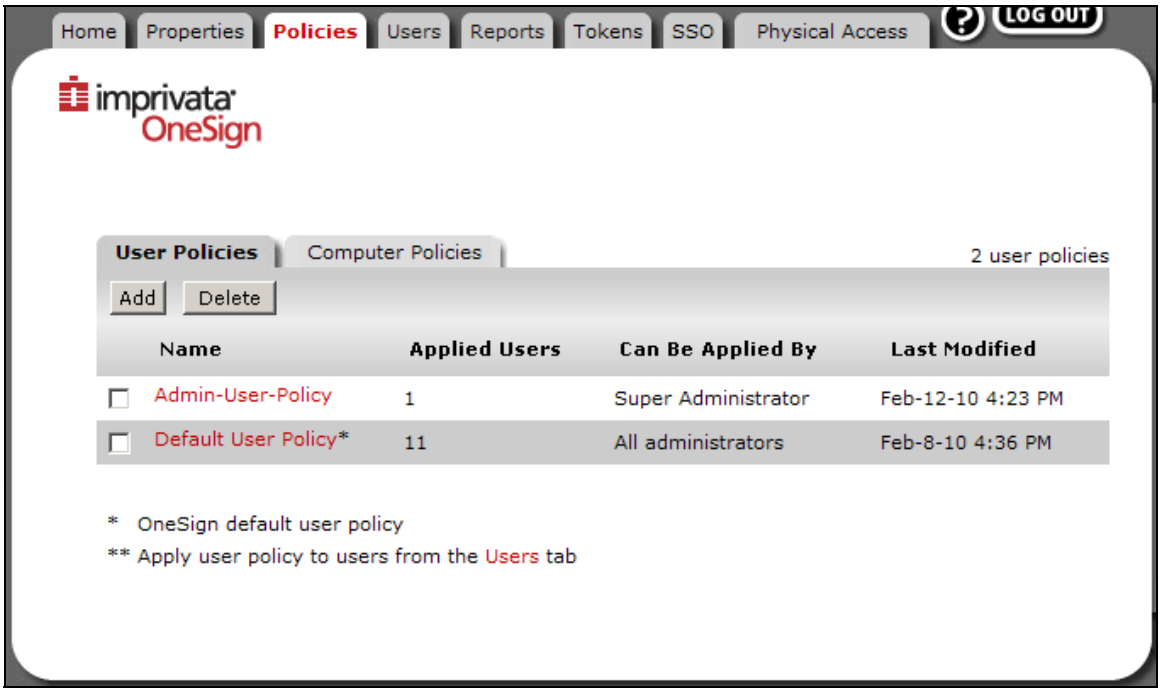
After completing the prerequisites listed above, follow the steps below to configure OneSign to use RSA SecurID two-factor authentication:

1. **Create a OneSign Authentication Policy**
2. **Assign the Authentication Policy to OneSign Users**
3. **Configure RADIUS Server Communication**

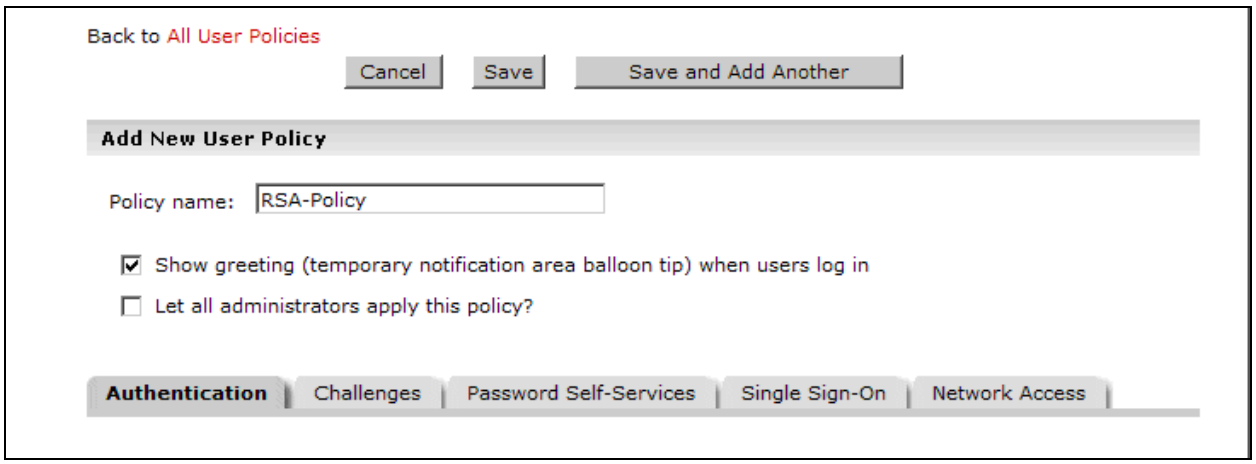
Create a OneSign Authentication Policy

Follow the steps below to create a OneSign Authentication Policy:

- Log into OneSign Administrator application and select the *Policies* tab.
- Click the *Add* button on the *User Policies* tab.

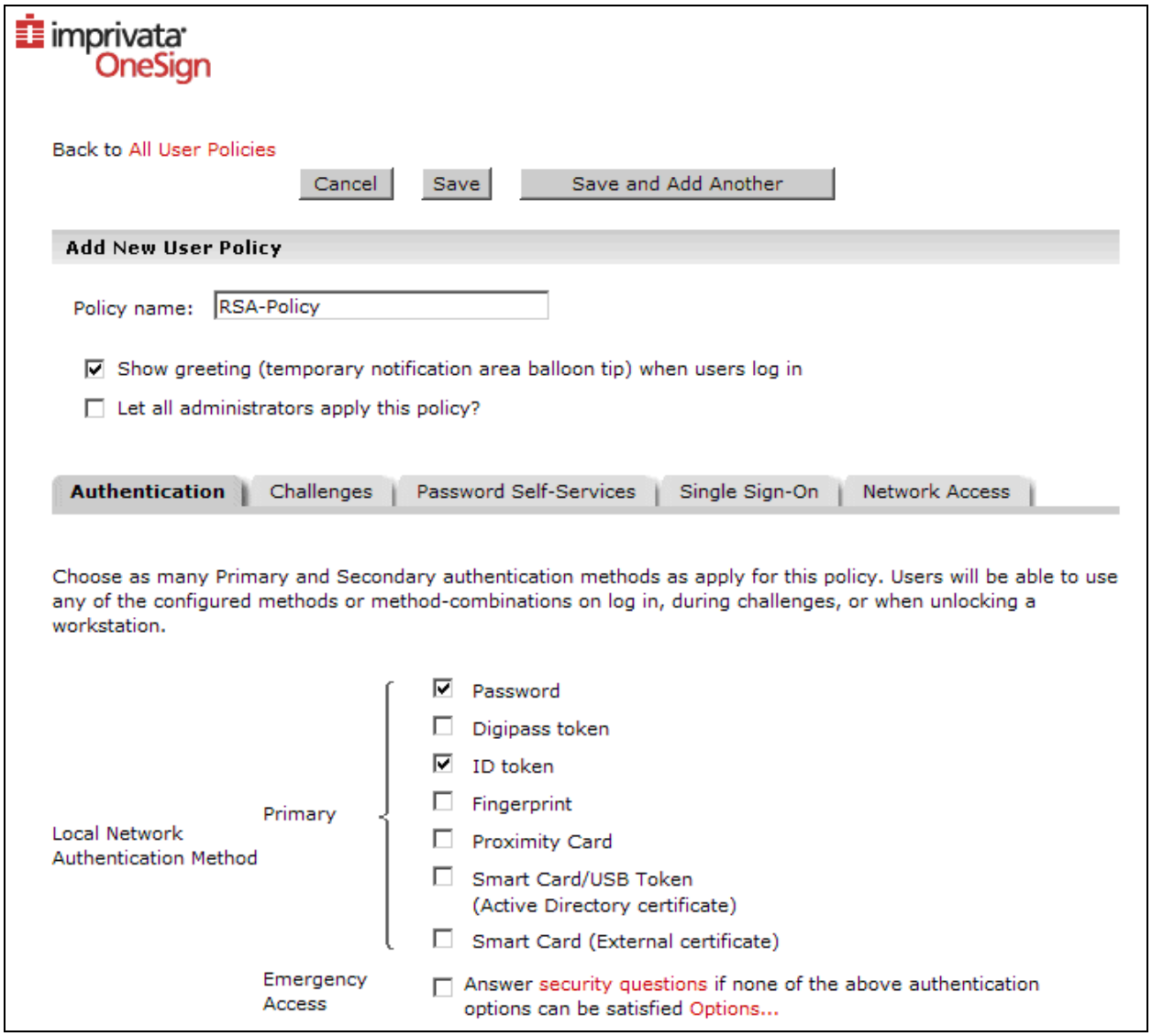


- Enter a name in the Policy name field.



Create a OneSign Authentication Policy (continued)

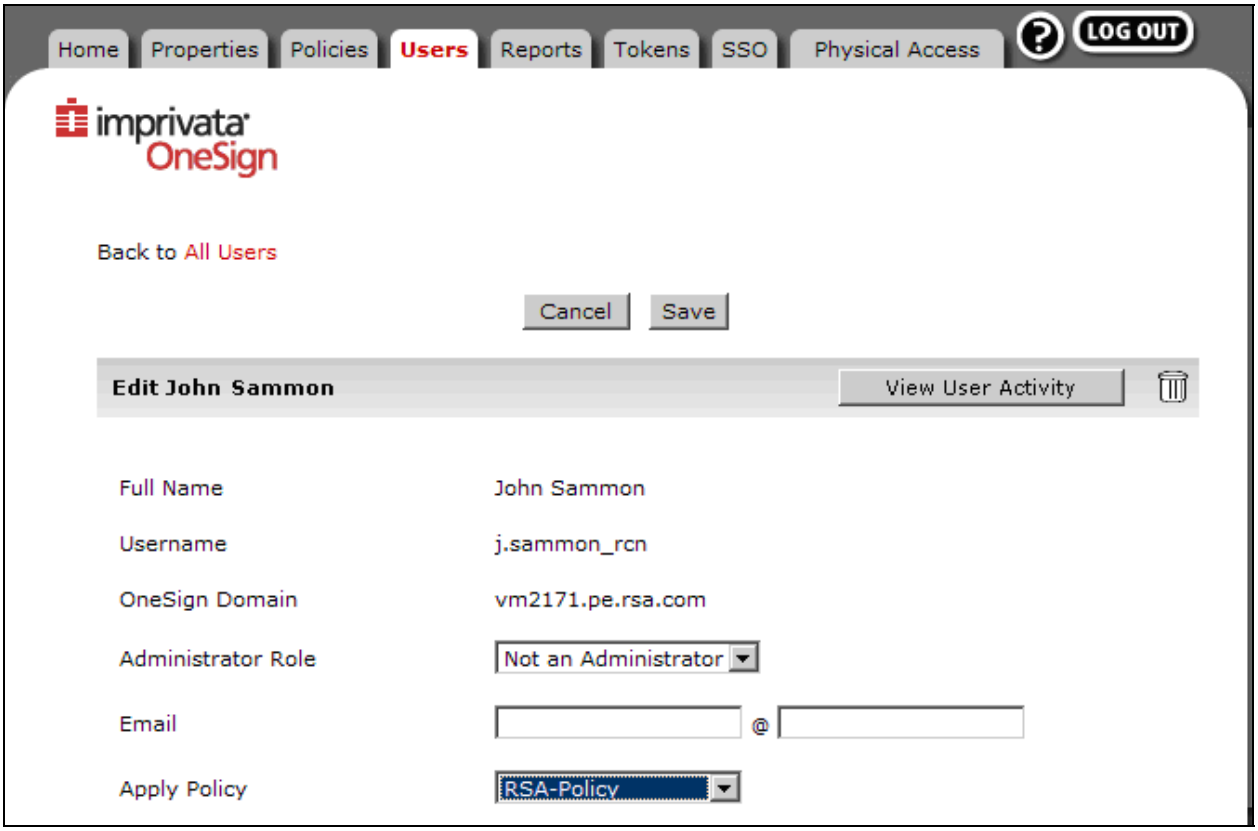
- Select the *Authentication* tab and check the *ID Token* checkbox.
- Click the *Save* button.



Assign the Authentication Policy to OneSign Users

Follow the steps below to assign the OneSign Authentication Policy for RSA SecurID to a OneSign user[1]:

- Select the *Users* tab and *Users* subtab.
- Click on the appropriate username link.
- Select the policy name from the *Apply Policy* dropdown list.
- Click the *Save* button.

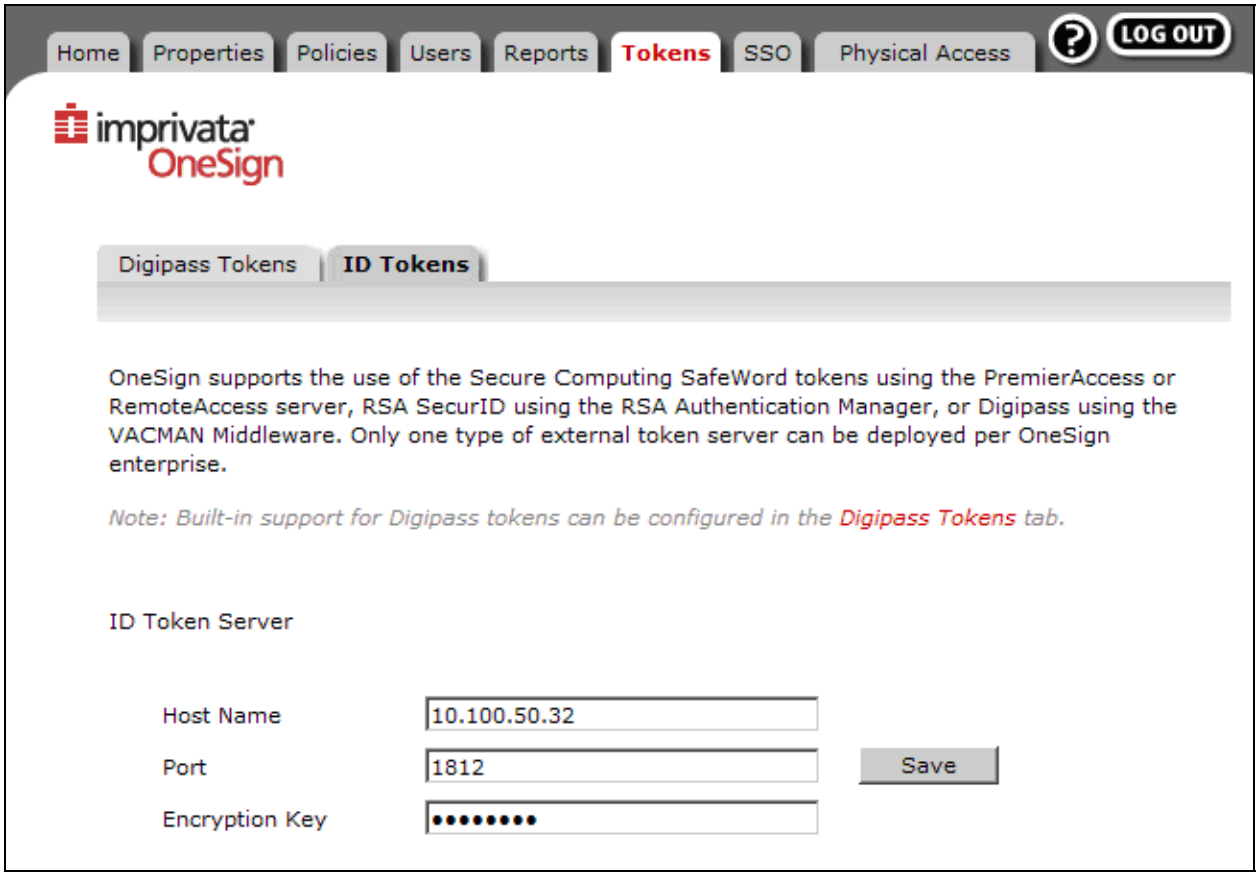


[1] See the *OneSign Administrator Guide* for instructions for assigning policies to groups of users.

Configure RADIUS Server Communication

Follow the steps below to configure communication between OneSign and the RSA Authentication Manager RADIUS server.

- Select the *Tokens* tab and the *ID Tokens* subtab.
- Enter the RSA Authentication Manager RADIUS server's hostname, port and encryption key in the appropriate fields.
- Click the Save button.



OneSign Logon

When a OneSign user attempts to access a computer that is protected by a OneSign agent, the agent displays a custom Microsoft GINA. Each RSA SecurID user must select the *ID Token* radio button and enter his or her RSA SecurID passcode in order to authenticate. Once authenticated, each user can access all OneSign-registered SSO applications for that session.

Certification Checklist for RSA Authentication Manager 7.1

Date Tested: February 11, 2010

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows 2003
Imprivata OneSign	4.0	Hardware Appliance

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)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse	N/A	PIN Reuse	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

JGS

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