

Juniper OneTouch

Contents

- 1 Overview
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Installation
 - ◆ 5.1 One Touch Demo Application Installation
 - ◆ 5.2 Swivel Integration Configuration
 - ◆ 5.3 Juniper One Touch Integration
 - ◆ 5.4 Modifying the Custom login Pages
 - ◇ 5.4.1 For Single Stage authentication
 - ◇ 5.4.2 For Two Stage Authentication
 - ◆ 5.5 Uploading the Custom Sign in pages
 - ◆ 5.6 RADIUS Authentication Server Configuration
 - ◇ 5.6.1 Authentication Realm Configuration
 - ◆ 5.7 Additional Installation Options
- 6 Verifying the Installation
- 7 Uninstalling the Swivel Integration
- 8 Troubleshooting
- 9 Known Issues and Limitations
- 10 Additional Information

Overview

This document is intended to supplement the the [OneTouch Mobile](#) guide and the [OneTouch Voice](#) guide for using the Swivel Juniper OneTouch Demo application.

Prerequisites

Swivel 3.10.4

Juniper 7.x or 8.x

Nexmo Account (or other Telephony provider) for OneTouch Voice telephone-based solution

Latest version of the Swivel Appliance Proxy available from [Downloads](#)

Swivel OneTouch Application demo available from [Downloads](#)

Juniper Custom login pages [OneStage.zip](#) or [TwoStages.zip](#)

Baseline

(The version tested with)

Swivel 3.10.4

Juniper 7.x

Architecture

See [OneTouch Voice](#) and [OneTouch Mobile](#)

Installation

One Touch Demo Application Installation

Install the Swivel [OneTouch Demo Application](#)

Swivel Integration Configuration

Configure the Swivel server and users as detailed in this guide [OneTouch Voice](#) or [OneTouch Mobile](#).

Juniper One Touch Integration

Modifying the Custom login Pages

Modify the Juniper login pages either for OneStage or TwoStage authentication.

For Single Stage authentication

Open the OneTouchOneStage.zip file

Modify the LoginPage.thtml file

edit the 2 URLs to access to your OneTouch demo app:

e.g.: <http://localhost:8081/onetouchdemo/onetouch?returnurl=>

Save the changes and create a zip. NOTE: the zip has to contain just the files and not the onetouch folder or itself a subfolder.

For Two Stage Authentication

Open the OneTouch2Stages.zip file

Modify the Defender.thtml file

edit the URLs to access to your OneTouch demo app:

e.g.: <http://localhost:8081/onetouchdemo/onetouch?returnurl=>

Save the changes and create a zip. NOTE: the zip has to contain just the files and not the onetouch folder or itself a subfolder.

Uploading the Custom Sign in pages

As with the Swivel Juniper integration, the custom pages need to be uploaded and assigned to a signing-in policy and realm.

Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.

	Sign-In Page	Typ
<input type="checkbox"/>	Default Sign-In Page	Sta
<input type="checkbox"/>	Meeting Sign-In Page	Sta

Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.

The screenshot shows the Juniper Central Manager web interface. On the left is a navigation sidebar with categories: System, Authentication, Administrators, Users, and Maintenance. The 'Authentication' section is expanded to show 'Signing In'. The main content area is titled 'Upload Custom Sign-In Pages' and includes a breadcrumb 'Signing In >'. Below the title is a descriptive paragraph: 'Custom sign-in pages allow you to provide customized templates for various pages that appear during the sign-in process. Refer to the documentation for information about creating valid templates.' The configuration form includes: 'Name:' with a text box containing 'PINsafe' and a sub-label 'Label to reference the custom sign-in pages.'; 'Page Type:' with radio buttons for 'Access' (selected) and 'Meeting'; 'Templates File:' with a text box containing 'C:\Documents and Settings' and a 'Browse...' button, with a sub-label 'Zip file containing the custom templates and assets.'; and an 'Upload' section with a checkbox 'skip validation checks during upload' and a large 'Upload Custom Pages' button.

The new signing in page should be listed.

Central Manager

- System
 - Status
 - Configuration
 - Network
 - Clustering
 - Log/Monitoring
- Authentication
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators
 - Admin Realms
 - Admin Roles
- Users
 - User Realms
 - User Roles
 - Resource Profiles
 - Resource Policies
- Maintenance
 - System
 - Import/Export
 - Push Config
 - Archiving
 - Troubleshooting

Signing In

Sign-in Policies Sign-in Pages

New Page... Upload Custom Pages... Delete

<input checked="" type="checkbox"/>	Sign-In Page	Type
<input type="checkbox"/>	PINsafe	Custo
	<u>Default Sign-In Page</u>	Stan
	<u>Meeting Sign-In Page</u>	Stan

RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.

Central Manager

- System
 - Status >
 - Configuration >
 - Network >
 - Clustering >
 - Log/Monitoring >
- Authentication
 - Signing In >
 - Endpoint Security >
 - Auth. Servers
- Administrators
 - Admin Realms >
 - Admin Roles >
- Users
 - User Realms >
 - User Roles >
 - Resource Profiles >
 - Resource Policies >
- Maintenance
 - System >
 - Import/Export >
 - Push Config
 - Archiving >
 - Troubleshooting >

Authentication Servers

New: (Select server type)

(Select server type)

IVE Authentication

LDAP Server

NIS Server

ACE Server

Radius Server

Active Directory / Windows NT

Anonymous Server

SiteMinder Server

Certificate Server

SAML Server

ervers	Type
	IVE Authentication
	IVE Authentication

The following information is required:

Name: A descriptive name for the RADIUS server

RADIUS Server: The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.

- System**
- Status
- Configuration
- Network
- Clustering
- Log/Monitoring
- Authentication**
- Signing In
- Endpoint Security
- Auth. Servers
- Administrators**
- Admin Realms
- Admin Roles
- Users**
- User Realms
- User Roles
- Resource Profiles
- Resource Policies
- Maintenance**
- System
- Import/Export
- Push Config
- Archiving
- Troubleshooting

Auth Servers >

PINsafe

Settings
Users

Name:	<input type="text" value="PINsafe"/>	Label to reference this server.
Radius Server:	<input type="text" value="82.69.194.195"/>	Name or IP address
Authentication Port:	<input type="text" value="1812"/>	
Shared Secret:	<input type="password" value="••••••"/>	
Accounting Port:	<input type="text" value="1813"/>	Port used for Radius accounting, if applicable
NAS-IP-Address:	<input type="text"/>	IP address
Timeout:	<input type="text" value="30"/> seconds	
Retries:	<input type="text" value="0"/>	
<input checked="" type="checkbox"/> Users authenticate using tokens or one-time passwords <small>Note: If you select this, IVE will send the user's authentication method as "token" if you use SAML and this credential will not be used in automatic SSO to backend applications.</small>		

Backup server

Radius Server:	<input type="text"/>	Name or IP address
Authentication Port:	<input type="text"/>	
Shared Secret:	<input type="password"/>	
Accounting Port:	<input type="text"/>	Port used for Radius accounting, if applicable

Radius accounting

NAS-Identifier:	<input type="text"/>	Name of IVE as known to Radius s
------------------------	----------------------	----------------------------------

For Two Stage Authentication Go to the auth, select the server used for one touch and add a new challenge rule. The value has to be the same as configured on Defender.html and radius_challenges.txt on the Swivel core.

Example Rule:

Name: Challenge One Touch

Response Packet Type: Access Challenge

RADIUS Attribute: Reply-Message

Operand: matches the expression

Value: One Touch

Edit Custom Radius Rule

Name: Challenge One Touch

If received Radius Response Packet ...

Response Packet Type: Access Challenge ▾

Attribute criteria:

Radius Attribute	Operand	Value	
Reply-Message (18) ▾	matches the expression ▾		Add
Reply-Message	matches the expression	One Touch	X

Then take action ...

- show **New Pin** page
- show **Next Token** page
- show **Generic Login** page
- show **user login page** with error message
 -
 - show **Reply-Message** attribute from the Radius server to the user
- send **Access Request** with additional attributes

Radius Attribute	Value	
User-Name (1) ▾		Add

Authentication Realm Configuration

Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or modify an existing realm by clicking on it.

Central Manager

System

- Status >
- Configuration >
- Network >
- Clustering >
- Log/Monitoring >

Authentication

- Signing In >
- Endpoint Security >
- Auth. Servers >

Administrators

- Admin Realms >
- Admin Roles >

Users

- User Realms >
- User Roles >
- Resource Profiles >
- Resource Policies >

Maintenance

- System >
- Import/Export >
- Push Config >
- Archiving >
- Troubleshooting >

User Authentication Realms

Authentication Realm

[Users](#)

Authentication realms specify what server to use for authentication, how policies are assigned to users,

Additional Installation Options

Verifying the Installation

Uninstalling the Swivel Integration

Troubleshooting

Known Issues and Limitations

Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com.