Swivel Authentication Version 3.9.7

Release Bulletin

Introduction

This release bulletin relates to Version 3.9.7 of the Swivel Authentication Platform.

This latest release brings with it new product enhancements to the Swivel Core, user experience and integrations. Full feature information and details are set out in this document.

We strongly recommend that all our customers upgrade to the latest version as soon as possible. Upgrades are included as part of your annual maintenance renewal and are free of charge.

Feature Overview

Introduction 1
Product Enhancements 4
Swivel Core 4
Configuration replication 4
Admin API 4
RADIUS Updates 4
Integrations 4
Outlook Web Access 4
SharePoint 5
Citrix Netscaler Gateway 10 5
Microsoft TMG 5
Microsoft Small Business Server 5
Fortinet Fortigate 5
Mobile 5
Get Server Settings from a url 5
Mobile: Users Can Provision from a URL (All Devices) 5
Support for RADIUS CHAP 6
Swivel Core – bug fixes 6
Radius Leap 6
Security strings for new users 6
Base DN for Active Directory Global Catalog 6
Helpdesk Group Rights 6
User Sync And The Repository ID 7
Bad Token Seed Issues 7
Copy Strings to Alert 7
Mobile - bugs fixed 7
Windows Phone Physical Device Forced Shutdown 7
IOS client policy 7
If the policy dictates that the user could not change the policy but the policy is set to yes for OTC extraction, the policy screen showed it as no – This is now fixed to show the correct information 7
iPhone: Forced PIN Entry 7

Third party data is escaped in AgentXML return 7

Product Enhancements

Swivel Core

Configuration replication

When using Swivel Active/Active appliances, certain configuration elements now replicate between appliances. The configuration replication has granular controls, enabling the administrator to determine which elements synchronize. For more information see:
https://kb.swivelsecure.com/wiki/index.php/Administration_Synchronisation

Admin API

The admin API now supports setting and returning user attributes, including transport destinations.

RADIUS Updates

Supports calling station ID in RADIUS.

Calling station ID is the IP address of the client computer that has made a RADIUS authentication request. This relies on the RADIUS NAS supporting the feature and passing the information to Swivel.

Optional username send as part of RADIUS challenge.

If enabled, the usual challenge string is prefixed with the username followed by a colon.

2-stage RADIUS

When re-authenticating within a specified time of the original authentication, if a user's IP address is identified as "internal", and the user enters their password correctly, Swivel returns RADIUS Accept, rather than RADIUS Challenge, removing the need to enter the one-time code the second time.

Radius Logging

Due to changes in the logging mechanism, when debugging is enabled in RADIUS, it writes to the normal log as INFO category messages as opposed to a using its own DEBUG category.

An updated RADIUS how to guide can be found at:
https://kb.swivelsecure.com/wiki/index.php/RADIUS_How_To_Guide

Integrations

Outlook Web Access

Swivel filter for Outlook Web Access 2013 is now available. See:
https://kb.swivelsecure.com/wiki/index.php/Microsoft_OWA_2013_IIS_Integration.

SharePoint

Swivel SharePoint filter now compatible with SharePoint 2013. See:
https://kb.swivelsecure.com/wiki/index.php/Microsoft_Sharepoint_2013_Integration

Citrix Netscaler Gateway 10

The Citrix Netscaler Gateway 10.1 uses a different method for custom pages and these have been incorporated into a new integration document here:
https://kb.swivelsecure.com/wiki/index.php/Citrix_Netscaler_Gateway_10.x

Microsoft TMG

Microsoft TMG filter to version 1.4.4;
https://kb.swivelsecure.com/wiki/index.php/Microsoft_TMG_2010_Integration

Microsoft Small Business Server

Swivel Microsoft SBS 2011 integration release
https://kb.swivelsecure.com/wiki/index.php/Microsoft_Windows_Small_Business_Server_2011

Fortinet Fortigate

Updated installation guide:
https://kb.swivelsecure.com/wiki/index.php/Fortinet_Fortigate_Integration

Mobile

Get Server Settings from a url

The mobile client now has the ability to be provisioned via a URL and it is also able to respond to requests to getServerSettings from id. For instance when messaged for the first time the user will receive a URL which, when clicked will load the server details onto their device.
For full user guide see:
https://kb.swivelsecure.com/wiki/index.php/Provision_URL

Mobile: Users Can Provision from a URL (All Devices)

We have enabled the following simple workflow for provisioning new mobile users on the Swivel app.

1. The user receives an SMS message from the Swivel platform
2. The user clicks the link in this SMS message
3. Where possible the user will be prompted to see if they want to load the browser to use the URL or if they want to load the Swivel App. each produces different responses:

If the URL is used with the Swivel app. the application will respond to the URL given to it, and make a provision request.

If the URL is used with the mobiles web browser, a web page will be shown containing a button. The user clicks on the button enabling them to provision their mobile. A video link is provided to show the two possible scenarios.

For more information see:
https://kb.swivelsecure.com/wiki/index.php/Mobile_Provision_Code#Mobile_Provisioning

Support for RADIUS CHAP

The Mobile client has been updated to support RADIUS CHAP. Due to how CHAP (and other non-PAP RADIUS protocols work) authentication works users have to use a specific security string to authentic. A user now has the ability to select the authentication string to be used. Strings can only be used once.

From a mobile app UI point of view the addition of a 'next and 'previous' button has been added to the authenticate screen. This will allow them to work with the challenge/response mechanism provided by Quest/VDI which is based on CHAP rather than PAP RADIUS.

Swivel Core – bug fixes

Radius Leap

Previously, if using the RADIUS LEAP protocol with dual channel authentication, a new security string was not sent out after authentication. This has been corrected.

Security strings for new users

As of 3.9.6, new users were not sent initial security strings. This was fixed in a patch for 3.9.6, and has also been fixed in this release.

Base DN for Active Directory Global Catalog

If you configured an Active Directory repository with Global Catalog, the detected base DN was previously the base DN for the domain the configured Domain Controller was in, rather than the global one. This meant that it was not possible to browse below the domain base DN, although user sync functionality was not affected. This error has now been corrected.

Helpdesk Group Rights

The Type drop down on the Group Rights screen (accessed via Repository -> Groups screen, 'Group Rights' button), did not retain the setting following an upgrade to version 3.9.6.

The effect was that helpdesk users were unable to view any users in user administration until the setting was corrected. Also, the default setting was “no rights for helpdesk users”. The default setting is now set to enable all helpdesk users to manage all users, and on upgrade, the current setting is retained.

User Sync And The Repository ID

Repository IDs were not changed when the database was changed (for example, after reset to shipping), meaning that user sync failed. This required a Tomcat restart to fix. Repository IDs are now handled correctly on database change.

Bad Token Seed Issues

If you manually entered an invalid seed, e.g. BADSEED, you got an unhandled exception. This is now fixed.

Copy Strings to Alert

Copy security strings to alert was broken as a result of transport changes in 3.9.6. This has now been fixed.

Mobile - bugs fixed

Windows Phone Physical Device Forced Shutdown

Buttons now present correctly following a forced shutdown either manually or due battery failure.

IOS client policy

If the policy dictates that the user could not change the policy but the policy is set to yes for OTC extraction, the policy screen showed it as no – This is now fixed to show the correct information

iPhone: Forced PIN Entry

The iPhone no longer turns PIN entry off when the server was setup to force the user to enter their pin and have the OTC auto extract after exiting from the authentication screen and returning.

Third party data is escaped in AgentXML return

The format of the data is now changed in version 3.9.6 when returning third party authentication data (e.g. Windows GINA)