Authcontrol Sentry v4 Admin Guide

Swivel Secure AuthControl Sentry Version 4

- A Tutorial for Administrators

This document describes how to administer Swivel Secure?s AuthControl Sentry version 4, referred to herein simply as ?Sentry?. It assumes no previous knowledge of the product, so can be used by new users, as well as users upgrading from an earlier version.

This tutorial refers only to administration through the web consoles: it does not include administration of the Swivel Secure appliance itself, which is covered by a different document. It is therefore assumed that the appliance has been allocated an IP address and connected to the relevant network. Where instructions may be different for upgraded installations, as opposed to new ones, the upgrade instructions are preceded by the following heading:

- Upgrade

Instructions following this heading are for upgrades only, and are different from new installations. Upgrade instructions are indented.

Getting Started

- Logging In

To connect to the main Sentry web administration console, open a web browser and enter the following URL: https://<appliance_address>:8080/sentry Here, replace <appliance_address> with the IP address of the appliance, or if it has been allocated a name by DNS, the host name. Upgrade Upgrading users may need to use the old path name, /pinsafe, rather than /sentry. You will be presented with the Sentry login page.

For a brand new installation, there is one user, named admin, so enter this in the username field. Now click on the Start Session button. An image will be shown with ten random digits.

This is known as a TURing image, and is one of the possible authentication methods supported by Sentry. For a new installation, it is the only method available. To use this image, you need to apply your PIN, which will be allocated to you, to the string of digits, selecting the digits corresponding to the indexes above the string. In this particular case, the initial PIN for the admin user is 1234, so you should enter the first 4 digits shown in the OTC field: in the example above, 2476, then click Login. If this is the first time you have logged in, you will be presented with the End User Licence Agreement, which you will be required to accept in order to proceed.

This agreement will not be displayed on subsequent occasions, although you can recall it if required, as explained below.

- Status Screen

This is normally the first screen you will see when you log in. It shows a summary of the current settings. Note that it also includes a link to the EULA. Although the Status Page is the default page shown after logging in, you can also enter the full URL of a different page, or bookmark a specific page, and after logging in, you will be taken directly to that page.

- Help

Notice that on nearly every page, there is a Help link. This links to the appropriate web page on https://kb2.swivelsecure.com, and provides more detail on the options contained within the page.

- Entering the Licence

The first thing you need to do when setting up your AuthControl Sentry server for the first time is to enter the licence information. You need to enter this information on the following pages, in this order.

- Server -> Name

When referring to specific pages in the administration console, we will always use the above notation. The first part of the page name, before the -> symbol, refers to a top-level menu item on the left-hand menu, in this case Server. Click on that menu to expand it to show the sub-menu. Now click on the second part of the name, in this case Name. The appropriate page will be displayed.

Enter the site ID you have been allocated by Swivel Secure. This is unique to your installation, and is required in order to install the licence. It identifies your company both to the licence key server and to the Swivel Secure Mobile Connection server. You can also enter the name of the server, which is displayed at the top of the page. This is optional, and mainly useful if you have more than one appliance, as a quick way of identifying them. The third field on this page will be explained later. Click Apply to save these settings.

- Server -> Licensing

Use this page to enter the licence details, after you have entered your site ID. If you attempt to enter the licence details before the site ID, it will fail.

You should have been provided with a License Key. This, together with the Site ID, is enough to extract the License Information from the Swivel Secure License Server. However, if your appliance has not been configured with internet access, you will need to request this information from Swivel Secure: contact supportdesk@swivelsecure.com to request this information. In this case, you should set the Online option to No, to prevent the appliance from attempting to contact the license server. Click Apply to save the licence information. If it is correct, your current entitlements will be displayed. If it is not, an error message will be displayed. NOTE: if you later upgrade your licence, and your appliance has internet access, all you need to do is to return to this page and click Apply to retrieve the updated license information. If your appliance does not have internet access, you will need to request the updated license information from Swivel Secure once again.

- Creating A Repository

First of all a note on what a repository is: put simply, a repository is a source of users. Every user belongs to exactly one repository. Taking the user information from the repository source (server) into the application database is referred to as User Synchronisation, or ?User Sync?. Your appliance is provided with one repository. This is an internal repository (different types of repository will be described later), and contains the single admin user. You could maintain all your users in this repository, but most administrators prefer to synchronise their users from the company?s user directory. The most common directory is Microsoft??s Active Directory, and we will describe adding an Active Directory as a source of users here. If your user repository is not Active Directory, please read the more detailed notes on Repositories, later on.

- Repository -> Servers

This page is where you create your repositories.

You will see the single repository, named ?Local XML? for reasons that will be explained later. Click on New Entry and enter the name of your repository. If you will have multiple repositories, you will want to give this a meaningful name. In this case, we will simply call it ?Active Directory?. Select Active Directory as the type, and click Apply.

You will notice that the name ?Active Directory?, or whatever you have named your repository, has been added to the Repository sub-menu. Click on it.

There are a number of details you might need to enter here, but typically all you will need is the address of a domain controller, and the username and password of an Active Directory user with rights to read the directory: the username should be qualified with the domain, either as domain\username or as username@domain. Note that, since Sentry does not modify the Active Directory, this account does not have to be an administrator account. Note also that the Hostname/IP can either be the name or IP address of a specific domain controller, or simply the domain name, assuming that your DNS will resolve that correctly. You may also wish to select the port as 636 (Domain LDAP SSL), for increased security. If you do, you should also set the option Allow self-signed certificates to yes, unless you have installed a commercial certificate on your domain controller. The other setting you may wish to set now is the Synchronization schedule. This determines how often Sentry connects to your domain controller to retrieve users. If you leave it at the default setting ?NEVER?, then you can still sync users manually from the User Administration page, as explained later. We will discuss the remaining options later, but for now, leave them as default. Click Apply to save the settings. You may want to try the Browse in window button to confirm that you can connect to your domain controller ? we will discuss the repository browser later. Repository -> Groups To quote the help page: ?Groups are used within Swivel to manage user rights, messaging and other features. A Swivel group can include users from multiple repositories, and each user can be a member of multiple groups?. Put simply, the Repository -> Groups page defines two things: What rights each group is allocated The mapping between Sentry groups and Repository groups

Sentry comes with a number of groups pre-defined. You can use the groups provided, you can modify or delete them, or create your own. You do not have to use all the groups provided for all repositories (or indeed at all): any group for which you do not provide a definition for a given repository will be ignored. You will see across the top the list of rights that groups can be allocated. The first 4 and the last: Single, Dual, Push, Mobile App and OATH refer to the different authentication methods that Sentry supports. Admin indicates that the members of this group are system administrators, who are given full rights over the administration console. Helpdesk users have limited rights, mainly limited to user administration: the exact rights allocated to helpdesk users can be changed as required. The final right is PINless: members of groups with the PINless right will not be allocated PINs (but see later), and will use the PINless versions of the various authentication methods. Below the rights buttons are the mappings that associate Sentry groups with repository groups. Where Active Directory is concerned, you can use the Browse button to select the appropriate Active Directory group, rather than manually entering the full group name.

It is assumed that you have previously allocated Active Directory groups, and are sufficiently familiar with Active Directory structure to be able to locate the relevant groups.

- User Administration

You are now ready to start importing users. Click on the User Administration menu. This is probably the page that administrators, and certainly helpdesk users, will see most of.

First, a summary of the controls on this page: Max No. Users: this simply controls the maximum number of users that will be displayed. It does not relate to the number of licensed users, and can be altered as required. Users per page: this sets the number of users that will be displayed at one time. If there are more users than can fit on one page, page controls will be displayed to select different pages. Repository: this drop-down allows you to select which repository of users is displayed. State: allows you to limit the displayed users to those in a given state: user states will be discussed later. User Search: this allows you to search for users according to the value of a selected attribute, such as username, surname etc. Custom attributes will be discussed later. Members of group: allows you to restrict the display to members of a specified group. View: determines what information is displayed about the users. The categories in this drop-down will be described later. Next is a row of buttons: Search: applies the selected settings from the controls above: most drop-down selectors trigger this option automatically. Reset: resets the selected settings to the default. Purge: permanently removes all users marked as deleted. Undelete: removes the deleted mark from all users. Add User: (for editable repositories only: see later), display a screen to add a new user to the repository. Import: (for editable repositories only: see later), display a screen to import a list of users to the repository. User Sync: executes a manual user sync, to import or update users from the selected repository. Sync Count: executes a ?dummy? user sync, to determine how many users would be added, modified or deleted. All the above controls act on the entire user set. To administer a single user, click on that user

Edit allows you to change attributes for an editable user. We will talk about editable repositories in the next section. Policy allows you to modify certain policies regarding the user.

Reset PIN allows you to set the user?s PIN directly. When set from here, policies regarding PIN composition are ignored, so for example, you can set a PIN of 1234 even if sequences are not allowed. View Strings allows you to view a user?s current security strings. You can also request a new single channel string for a user. Possible uses for this are described later.

Send String will send a user a new dual channel string. The user must have the Dual right for this to show. Resend sends the user a randomly generated new PIN. It does not, despite the name, resend their existing PIN. App Provision sends the user a mobile app provision message. The user must have the Mobile App right for this to show. Lock locks the user?s account. If the account is already locked, this button shows as Unlock. Remove for editable users only, removes the user from the repository. History shows the recent activity for a user. You can select from a list of activity types.

- Managing Repositories

We will now look in more depth at how repositories work and the different types of repository.

- Repository Types

There are several different types of repository: the two most common are XML and Active Directory.

- XML Repository

An XML repository is, behind the scenes, simply an XML file. The main advantage of an XML repository is that the users can be entered directly into the User Administration page. This is an example of a writeable repository, of which more later.

- Active Directory Repository

An Active Directory repository defines a connection between the application database and a Windows Active Directory (AD) Domain Controller (DC). Note that it is a defined Domain Controller: we are often asked if we can define multiple DCs, to which the answer is no. However, you can specify the domain name as the host, which can be resolved by DNS dynamically. The online help page goes into more detail on configuring AD repositories, but 2 features should be mentioned, which will be expanded on below: it is a read-only repository, as opposed to the XML repository being writeable, and it uses LDAP, in common with other repository types.

- Writeable and Read-Only Repositories

Repository types can be split into writeable and read-only repositories. ?Writeable?, means that the users can be created, edited and deleted directly within the user administration page. When you do this, the users are automatically synchronised with the database. Another feature is that you can import text files containing user details into writeable repositories, using either CSV or XML ? the XML import uses the same schema as the XML repository, which is defined in the online help page. XML, ADAM and LDAP Writeable are the writeable repositories, the others being read-only.

- LDAP

Lightweight Directory Access Protocol (LDAP) is a standard protocol used by Active Directory, and by a number of non-Microsoft operating systems, for managing users. When defining LDAP repositories, you need to be aware of the directory structure of the LDAP server. Users are defined within LDAP as being members of a group, and we use the group membership to define how users are imported. All the repositories types supported by Sentry use LDAP to communicate with the server, except for XML and Database.

- Database

A database repository is simply that: the users are imported directly from a database. It is flexible about the database structure, but it expects a single table (or view) for users, and another for user group membership. More information on defining a database repository can be found in the online help.

- ADAM

The name ADAM is now obsolete: the name that Microsoft now use is Active Directory Lightweight Directory Services, or AD-LDS, but we use the old name ADAM for convenience. It is, as the name implies, a lightweight version of Active Directory that can be installed on any Windows PC. It works in more or less the same way as AD, but has the advantage, in our implementation, of being writeable.

- Agents as Repositories

There is a final type of repository: Agent repositories. These are managed by Agents (of which more later), using the AgentXML API (again, of which more later). They are not defined within the repository configuration.

- Repository Definitions

You define repositories by adding them to the Repository -> Servers page. All you need to add here is the name and the type. This creates a new entry in the Repository menu, where you can define the repository details. Configuring repositories is covered in more detail in the online help.

- Repository Group Management

We have already discussed the uses of repository groups, and described how to set the group mapping for Active Directory. The same Browse feature is available for other LDAP repositories as well. For XML repositories, typically the repository group name is the same as the Sentry group name. For LDAP repositories, it is the fully-qualified domain name (FQDN) of the group. All members of the group, including members of contained groups, are imported into the Sentry group. For database repositories, the group mapping should contain the value in the Group column of the User Membership table or view. A quick note on non-standard features of Active Directory: AD allows inter-domain group membership, so members of groups in other domains within a forest can be members of a group. Unfortunately, the way it does this is not part of the LDAP standard, so this behaviour is not supported by Sentry. If you need to support inter-domain membership, you must use the AD Global Catalog, which is like a single-domain view of the entire forest. It uses different ports from single-domain LDAP.

- Helpdesk Group Rights

This menu can only be found from the Repository -> Groups menu. It offers a more fine-grained way of managing which helpdesk users are allowed to manage which users, for large companies with complicated structures. The online help page describes how it works.

- Custom Attributes

Custom attributes are miscellaneous additional information imported from the repository. They are used to define email addresses and phone numbers for messaging, can be used to search in the user administration page, and as alternative usernames in authentication ? of which more later.

As with groups, you need to define which attributes from the repository map to the Sentry attributes. A default set of attributes are provided, with default mappings dependent on the repository type. You can change or remove the mappings ? if there is no mapping, then no value will be stored for the attribute. You can also add your own custom attributes. Note the other settings for each attribute: Phone Number?: this is a Yes/No flag. The repository settings allow you to specify that phone numbers can be reformatted, removing or adding country prefixes, additional notation etc. Therefore, the phone numbers need to be indicated. Sync Rule: this indicates how a user sync treats a given attribute. The default, Synchronised, means that the attribute is always read on user sync. Initialised means that it is read for new users, but not updated for existing users. Local means that it is never read from the repository. The reason for this setting is that it is possible for external applications to modify attributes, using an API described later. This prevents user sync from overwriting the effects of the API changes. Add repository qualifier?: this option allows a prefix or suffix to be added to the attribute value. The qualifier is defined in the repository settings, and can be applied to the primary username as well, in the repository settings. This is typically used to create the Windows account name form domain\username, since there is no single attribute that returns that value.

- Messaging

This section defines how Sentry communicates with users, which essentially means by email or by mobile phone. As mentioned above, Sentry uses custom attributes to control messaging, and the Messaging -> General page defines how. It contains a list of available transports, which is how we refer to the different messaging mechanisms. You will not need the majority of these, but you may need to add transports that are not shown in the default list. Swivel Secure support can provide advice on which additional transports are available, and we can develop custom transports if you wish to use an SMS portal that is not currently supported. If you need to add a new transport class, be aware that the name must be different from all other classes, but otherwise is not significant. The class name must be entered in full and is case-sensitive. All class names start with the prefix com.swiveltechnologies.pinsafe.server.transport. For brevity, we will omit this prefix when referring to specific classes, and just give the unqualified class name. The online help page defines what information you need to enter into this page. You just need to be aware that messaging is used for 3 different things: Alerts ? basically any message to the user that doesn?t come under the other categories Strings ? dual channel security strings, which will be discussed later Push notifications ? for Push / One Touch authentication, which will be discussed later The definitions require a single group for each transport. If you want to define multiple groups to use the same transport, you must create a new transport using the same transport class. Make sure the transport name is different from the original. You can define multiple transports for different alert groups (and strings groups), but if users are members of multiple transport groups, only the first one will be used. The Push repository group should only be set on the PNA transport. Once you have activated a transport by selecting an attribute and either a Strings or Alert group, a new menu item appears for you to enter the details of the transport. Most of the details are the contents of the various messages, but specific transports require specific additional information, such as gateway URLs for SMS gateways. A note on SMTP: SmtpTransport does not support secure SMTP, but there is an additional class, SecureSmtpTransport, that does. The default SmtpTransport uses the SMTP server defined by the system, but the secure SMTP transport defines its own SMTP server. It supports the StartTLS protocol, as used by mail servers like Gmail.

- Agents

Sentry uses a proprietary API called AgentXML as one protocol for user authentication. See the Agent-XML article for full details. For an external device to communicate with Sentry using the AgentXML protocol, it must be defined as an Agent, using the Server -> Agents page.

Note that one Agent, named ?local? is pre-defined. This is required, as it is used by all the other applications on the applications to communicate with the Core. Do not modify this Agent. The essential values for an Agent are the hostname or IP address and the Shared secret. Note that IP addresses can be specified as sub-nets: for example, 192.168.0.0/24 includes all IP addresses in the 192.168.0.x range. Also, multiple Agents can be defined for the same address, provided that the secret is different. The Agent device itself must send the secret as part of the AgentXML request for it to succeed. Agents can be used as repositories as well as for authentication. For this to happen, the Agent must have the option ?Can act as Repository? enabled. Once this is set, the Agent will appear in the list of repositories on the User Administration page. Note that an Agent can have the same name as a Repository. If they do, then the Agent acts on members of that repository. This can be useful, but can also have unexpected side effects. Also note that a User Sync potentially can wipe out the effects of API calls, hence the Sync Rule setting on attributes. This enables attributes to be set by API calls that

are not overwritten by user sync. We will discuss the other Agent settings when we discuss authentication methods later.

- RADIUS

We will be discussing Remote Authentication Dial-In User Service in more detail later, but in brief is it a standard authentication protocol used by many VPNs and Gateways.

- RADIUS -> Server

The RADIUS server is enabled by default, but if you are not using Sentry to authenticate any RADIUS devices, you can disable it. Typically, you do not need to set an IP address: it will use any IP address available to the appliance. The authentication port is 1812 and accounting is 1813, although Sentry does not make use of the accounting information. You may need to change these if your device uses non-standard ports. The other options will be discussed in the section on authentication, later.

- RADIUS -> NAS

This page is used to configure the Network Authentication Server (NAS) devices that will use Sentry to authenticate. Typically, you will need the IP address or host name and the shared secret: the latter will need to be configured on the device as well. Unlike Agents, you cannot specify a NAS for a sub-net, only for single devices. The other settings will be discussed later.

- Authentication

Sentry provides several different ways for users to authenticate: Single Channel Methods The following methods are all categorised as Single Channel, and can be used by users with the Single right. Single channel methods always require some form of customisation to the authentication page of the integrated device or application. Swivel Secure have developed such customisations for a large range of products: see our KnowledgeBase or contact supportdesk@swivelsecure.com for more information. Single channel authentication is always Session-Based. That is to say, requesting a single channel image starts an authentication session on the Sentry appliance. This session is both exclusive and time-limited: when a user has an active session, they cannot authenticate using any other method, and the session is only valid for a limited time. By default, the time limit is 2 minutes, but methods to change the time limit will be described later.

- TURing

A ?Captcha? image containing 10 random digits or characters is displayed on screen, and the user selects the ones corresponding to their PIN. In the above example, if the user?s PIN was 3974, then they would enter as their one-time code the digits corresponding to the indexes 3, 9, 7 and 4, i.e. 8317. The single-line TURing image is by far the most commonly used, but we do offer other formations, by selecting the Image file in Server -> Single Channel.

- Button

The indexes are not shown in this pattern, but they are the same as on a phone keypad, so for the PIN 3974, the OTC here is 6751.

- Pattern

Here the indexes go from top to bottom, left to right, so the OTC for 3974 is 2708. Pattern2

Again, the indexes go top to bottom, left to right, so the OTC for a PIN of 3974 is 8206. The image type selection is a global setting: it is not possible to choose different patterns for different users or different integrations.

- PINpad

PINpad provides an alternative input method for certain integrations:

The format may vary: some integrations display the numeric keys as rows of 3, 4 and 3 buttons, and the C and R buttons (for Clear and Refresh) are not always shown. The idea here is that you always click on the buttons corresponding to your PIN: the positions of the buttons vary at random. Clicking on the button enters the value corresponding to the position of the button, rather than the number on it.

- Dual Channel

An email or SMS is sent to the user containing 10 random digits or characters, as with TURing, except that the string is text, rather than an image. By default, the strings are sent in advance, so any user with the Dual right is sent a string as soon as their account is created, and when they use that one, a new one is sent ready for the next time. An alternative configuration is to enable On Demand Authentication on the Server -> Dual Channel menu. This means that strings are not sent out in advance, but only when requested. This means that the integration must be customised to allow a string to be sent out. The advantage here is that the user only receives the string when it?s needed, reducing the probability of losing it. The disadvantage is that the user must always be able to receive their strings, whether by email or by SMS. On Demand Authentication is also session-based: see the discussion on Single Channel to understand what that means. By contrast, dual channel strings sent in advance have an indefinite lifespan, although they can only be used once. There is a compromise solution: enable On Demand Delivery, rather than On Demand Authentication. With this option enabled, users receive security strings in advance, but if they have lost their latest one, they can request a new one by the same method as On Demand Authentication. Strings requested using On Demand Delivery, however, are not session-based.

- OATH Tokens

These are physical tokens, which display random codes using the OATH standard. Swivel Secure can provide branded OATH-compliant tokens, but any such tokens can be used with Sentry authentication, provided that the token seeds are available. Sentry supports both event-based (HOTP) and time-based (TOTP) tokens. There are also applications that can act as ?virtual? tokens: Google Authenticator is probably the best-known example of this. In fact, with the release of version 4, Swivel Secure provides OATH authentication on its Mobile App.

- AuthControl Mobile App

Swivel Secure?s AuthControl Mobile app is available for Android, iOS, Windows and Blackberry. Once a user has installed the Mobile App on their phone, it must be provisioned against the Sentry instance: instructions for this are provided elsewhere. 99 random strings are then downloaded to the phone, and displayed to the customer in order. When the strings run out, the user must request more. Alternatively, the app can be configured to use OATH, in which case there is no need to renew the strings. There is also a PC app that provides the same functionality on a Windows desktop. Push Push authentication uses the mobile app. When the user wishes to log in, a push notification is sent to the phone. The user must respond on the phone, either with a simple Yes/No, or a known code. This sends back a message, which results in a unique session ID being sent to the Agent. This also requires customisation to the authentication page.

- Authentication Protocols

We support 3 different protocols for authentication:

Agent XML ? our Proprietary API. This is used in many in-house apps, such as the IIS filter and Credential Provider. This has been mentioned previously, mainly in respect of using an Agent to modify user details, but the primary purpose of the Agent XML is to provide a means of authentication.

RADIUS ? used by many VPNs and Gateways. Sentry supports a limited range of RADIUS protocols. Only the PAP protocol is available for all authentication methods, but that is the most widely supported protocol. We also support CHAP, including MS-CHAP versions 1 and 2, but not EAP-MSCHAP. The only EAP-based protocols that we support are LEAP and EAP-MD5.

SAML ? this protocol is the basis of the Adaptive Authentication methodology. It is an industry standard, used by ADFS among others. The Adaptive Authentication solution also supports SAML over RADIUS, increasing the range of support for SAML to devices that do not support SAML natively. There is a separate tutorial on Adaptive Authentication that covers this in more detail.

- Other Configuration Settings

The online help provides details of every option on the administration menus. However, there are some features which warrant special mention. These are listed below.

- Changing the Session Validity

As mentioned previously, session-based authentication is time-limited, with a default timeout of 2 minutes. The setting that changes this timeout is on the Server -> Jobs menu. The setting is Session cleanup: the value is in seconds.

- Authenticating to Active Directory and Other Repositories

Swivel Secure?s authentication solutions are targeted primarily as additional authentication: frequently they are used alongside Active Directory authentication or other username and password solutions, which we will refer to as ?Primary? authentication. However, in some cases, it is useful for Sentry to perform the authentication to the primary server as well as the Swivel Secure ?Secondary? authentication. We support this for both AgentXML and RADIUS: in both Server -> Agents and RADIUS -> NAS, there is an option ?Check Password with Repository?. When enabled, this will expect to receive the AD or other repository password in addition to the one-time code. In the case of AgentXML, it is received as a separate field; for RADIUS, since it only supports one passcode field, the password and one-time code should be sent as a single value, the password first and no space between the values. As the one-time code has a known length, the split can be determined. This is the secondary use for repository servers, in addition to synchronizing users. In the case of LDAP (including Active Directory), a simple bind is performed. This may require the use of an alternative username to work: see the next section.

Use of this option can cause confusion in some cases, particularly in integrations which already require Active Directory authentication. You should pay close attention to whether the application you are integrating with connects directly to AD, or whether it passes the password through Sentry. For example, the Swivel Secure Credential Provider (the previous versions as well as the current), pass the password directly to Active Directory, so if the Agent is set up to handle a Credential Provider, ?Check Password with Repository? should be set to No. Likewise, when using RADIUS as an additional authentication, alongside Active Directory, typically you will not use this option. The most common use for this option is with two-stage RADIUS authentication, which is covered in a later section.

- Support for Alternative Usernames

There are occasions when users need to be referenced by identifiers other than the primary username in Sentry. An example of this is mentioned above: when authenticating to Active Directory, the unqualified username (sAMAccountName) will not usually work: you need either domain\accountName, or userPrincipalName (name@domain). Alternative username support needs to work two ways: Sentry should recognise alternative usernames where appropriate, and it should also provide alternative usernames when authenticating to repositories, as in the previous section on authenticating to Active Directory. Recognising alternative usernames is useful when integrating with products that use Sentry as a secondary authentication solution. In this case, the primary authentication method may require the username in a specific format, such as userPrincipalName. It is inconvenient if the user has to enter two different usernames for the two authentication methods, so the ability for Sentry to recognise alternative usernames is useful here.

This is supported in both Server -> Agents and RADIUS -> NAS by the option ?Allow alternative usernames?. If this option is enabled, you should also set ?Alternative username attributes?. This is a comma-separated list of Sentry attributes that should be recognised as usernames for this Agent or NAS. Note that this is the Sentry attribute name, not the repository attribute name. The most common attribute used here is ?altusername?, which maps by default to userPrincipalName in Active Directory. When checking the repository password is enabled, you will probably also want to set the ?Username attribute for repository? field. This determines which Sentry attribute to send to the repository with the password. Again, ?altusername? is the most common value. If left blank, the primary username is sent. When requesting a single-channel image or dual-channel security string, you can also use alternative usernames. This is often necessary, since the same username is used to request the image/string as to authenticate. The settings to enable this are on Server -> Single Channel and Server -> Dual Channel respectively, and as before are labelled ?Allow alternative usernames? and ?Alternative username attributes?.

- RADIUS Two-Stage Authentication

Sentry supports authentication to RADIUS in two stages, usually referred to in RADIUS devices as ?Challenge-Response?. Note that two-stage authentication is ONLY supported with the PAP protocol. It is enabled by the ?Two Stage Auth? option on the NAS settings. In this case, the first stage expects only the password. The one-time code is sent at the second stage. Several other NAS settings also relate to two-stage authentication: Check password with repository ? we have already discussed this above, but typically, when using two-stage authentication, the repository password is sent at stage 1. Allow blank password at Stage One ? if the repository password is NOT used at stage 1, then the Sentry password is checked. Frequently, Sentry passwords are not used, so this option allows stage 1 to pass in just the username and no other information Send Security String after Stage One ? a typical scenario for two-stage authentication is with dual-channel on-demand authentication. In this case, the user enters the username and password at stage 1. Only if the password is correct is the user sent a security string from which to extract the one-time code for stage 2. Even if User has Valid String ? if this option is set to No, and the user already has a valid security string, then a new string is not sent, even if the previous option is set to Yes. Send username in challenge ? this option is typically only used where stage 2 displays a single channel image on the login page. Since the image requires the username in order to display, if there is no way to determine it from other information on the page, the username is sent as part of the challenge string sent back to the NAS, in the form username:challenge. Another use of challenge-response is when a user is required to change their PIN. The option ?Change PIN warning?, when enabled, returns a challenge message ?changepin? if the user?s PIN is due to be changed. In this case, the response needs to be in the form cp1=<oldotc>cp2=<newotc>. Here, <oldotc> and <newotc> need to be replaced by the one-time code for the old PIN and the one-time code for the new PIN, both using the same security string.

- Using Security Strings Multiple Times

Both Server -> Single Channel and Server -> Dual Channel have the option ?Multiple Authentications per String?. This is mainly needed for certain badly-behaved RADIUS NAS?s that make multiple requests for the same user. However, it has also been used to provide temporary passwords: a sort of ?Multiple-Times Code?. To make this useful, you typically should increase the session cleanup time to a much larger value ? typically a day. A user can then be issued a security string, and from it extract a code that can be used repeatedly over a short period. Note that the View Strings option on User Administration has an Invalidate button to terminate this code before it expires, if required.

- Logging

Sentry logs most of the activity that occurs in the Sentry application. There is a Log Viewer that allows you to view those logs. However, we are aware that searching through these logs can be extremely slow, and occasionally fails to give the correct result. We therefore have alternative solutions. Logger messages can also be sent to Syslog devices, as controlled by the Logging -> Syslog menu. Certain messages can also be sent to a specific email address as well, as controlled by the Logging -> SMTP menu. You can decide what level of messages are sent by email, how many messages to accumulate before sending them, and whether to trigger an email on the occurrence of a higher-level log message. There is also a new, much faster log viewer. For technical reasons, this is a separate application, accessible using the URL path ?/logviewer?, rather than ?/sentry?. You need to log into that

separately from the main administration console. The new log viewer copies the logs to a database, which makes it much faster and more reliable. The down side of that is that it isn?t always up to date, as it only reads completed log files: the logs are split into separate files, which are closed when they reach a certain size. You can control the size of the log files on the Logging -> XML menu.

PIN Policies and Locking

- Locking

You can control policies for locking user accounts on the Policy -> General menu. In particular: Maximum login tries determines how many successive failures a user can make before the account is locked Account lockout time determines whether accounts are locked for a limited time, and if so, how long. Setting this value to 0 means that helpdesk intervention is required to unlock a user account. One thing to be aware of here is that the timed lockout only begins when the user attempts to log in one time too many. So, if the Maximum login tries is 3, and a user fails to login 3 times in succession, the timed lockout only starts when they attempt to login for a 4th time, or at least request an image or string for the 4th time. Inactive account expiry determines how long a user account must remain inactive, with no successful login attempts, before the account is deemed to be inactive, and locked out. Setting a value of 0 means that accounts are never locked due to inactivity.

- PIN Expiry

You can control requirements for users? PINs using options on the Policy -> PIN and OTC menu: PIN expiry indicates how long a user can keep the same PIN before they must change it. A value of 0 indicates that PINs never expire. You can also set a policy for individual accounts to override this option. PIN expiry after auto/admin reset is similar to the previous one, but applies to PINs that are reset by helpdesk, rather than by the user. PIN expiry warning sets a period during which the user is warned that their PIN is about to expire. Note that this is an interval before the actual expiry, so for example, if this value is set to 7, the first warning will occur 7 days before the PIN actually expires, and will recur daily until the user actually changes their PIN, or the PIN expires. PIN change grace period this setting applies for one specific scenario only: a user?s PIN expires and their account is locked. The helpdesk then unlocks the PIN, but does not reset the PIN. In this case, this setting determines how long the user now has to reset their PIN. Require PIN change after auto setting means that the user must change their PIN immediately after first logging in, if they have been allocated a random PIN, either on account creation, or using the Resend button from User Administration. Require PIN change after admin reset is similar to the previous option, but applies after a user has had their PIN manually reset by the helpdesk. Only warn user, do not lock account if enabled, accounts are never expired because the PIN has expired: users are only warned that they have not changed their PIN. Auto-reset PIN on expiry when enabled, accounts are not locked when the PIN expires: instead, their PIN is automatically reset to a random value. The behaviour of this option in combination with the PIN expiry warning setting is noteworthy: if PIN expiry warning is greater than 0, the PIN is changed instead of sending the first warning, so before the PIN actually expires.

- PIN Composition

The following settings apply to PIN composition: Minimum PIN size is the minimum number of digits a PIN can have Maximum repeated PIN digits is the number of times the same digit can occur in a PIN. So if 0, all digits must be different, etc. Allow numeric sequences for PIN if disabled, sequences such as 1234, 2468, 9753 are disallowed. Banned Credentials the Policy -> Banned Credentials menu allows you to specify PINs that are not permitted. You can use ??? to indicate any PIN, so for example, ?19??? prohibits any 4-digit PIN starting with 19.

- PINless

As mentioned previously, users can be designated as PINless. In this case, rather than extracting a one-time code from the security string using a PIN, they enter the entire security string as the one-time code. The following policies from Policy -> PIN and OTC affect PINless users: PINless OTC length determines the number of characters in a PINless security string (PINNed security strings are always 10 digits). Always use PIN for single channel overrides the PINless flag when authenticating as single channel. In this case, users are actually allocated a PIN, but they only need to authenticate as PINned when authenticating using a single-channel authentication method. For all other methods, they are PINless.

- Mobile App Policies

This section describes settings relating to the AuthControl Mobile app. There is one setting on Policy -> General that relates to the Mobile app: Auto send provision code when enabled, provision codes are automatically sent to users with the Mobile App right, on account creation. Some Mobile App policies are actually on the Policy -> Self-Reset menu: Allow user self-provision of mobile app if enabled, allows the user to provision their mobile app using the user portal. If disabled, the helpdesk must initiate mobile app provisioning, unless auto-send is enabled.

Send provision code as security string if enabled, the provision code is sent as a security string. Otherwise, it is sent as an alert. Mobile App Local Mode if enabled provisions the mobile app with security strings that are generated using the OATH algorithm. This means that the mobile app does not need to connect to the Sentry server to provision. However, it also means that when the 99 strings are exhausted, the app must reprovision, rather than simply requesting more strings. Mobile App OATH Mode if enabled provisions the mobile app as a virtual OATH token. Provision Code Validity period determines how long a provision code is valid. The default is 1 day. URLs the last 4 options on this menu are URLs that are used for provisioning. You should not typically change these unless told to do so by Swivel Secure. There are also policies on the Policy -> Mobile App menu that determine what control the user has over the Mobile App.

- Custom Images

The default email messages include a number of images. You can use these default images, or you can provide your own. If you want to use your own, you must first change the Base URL setting on the Server -> Name menu. This should be the public URL for your Sentry appliance, and will typically be the same as that provided for your mobile apps. If you leave the default, https://demo.swivelcloud.com, you can continue to use the default images, but the custom images you upload will not be available. If you change the base URL to your own, all the default images will still be available, as they are installed on your appliance. You can upload your own images, or remove the default ones, using the menu Upload Email Images.

- Reporting

Reports can be generated on demand, or can be scheduled, as shown by the following menus: Reporting -> Instant

Reporting -> Schedule

We provide a small list of built-in reports, but if you want a report that is not there, please contact supportdesk@swivelsecure.com. New reports can be added without having to restart Sentry.

- Managing OATH Tokens

The OATH menus are provided for administrators to import lists of OATH token seeds, and to assign tokens to users.

Note that tokens come as HOTP and TOTP ? event-based and time-based. If you import a batch of tokens as the wrong type, the only option is to remove them and try again: however, the Import menu allows you to delete all users in a list, so removing an entire set is simple. TOTP tokens cannot be synchronised, but rely on the appliance clock being correct to within a minute.

This menu allows you to import tokens: make sure you have set the correct token type on the Policies page first. You can also allocate tokens to users. Only users with the OATH right can be allocated tokens.

This menu shows all users that have been or can be allocated tokens

- High Availability

High availability settings are largely configured on the appliance CMI, but there are two menus on the web administration that are used with high availability environments. These menus have no meaning for stand-alone appliances.

- Session Synchronisation

Session synchronisation is the process by which an authentication session generated on one appliance is also available on the other. This is managed by the Appliance -> Appliance Synchronisation menu

Here, you should enter the IP address or host name of the partner appliance in the first field. Typically, the context will be ?sentry?, port is ?8080? and Use SSL should be ?Yes?. ?Ignore SSL Cert Errors? will normally be ?Yes? as well. The Shared Secret should be the same on both appliances and Synchronise Sessions will be set to ?Yes?. Now every time an authentication session is generated on one appliance, it will be duplicated to the other. This ensures that it is possible to generate sessions on one appliance, but authenticate on the other. If you are not using session-based authentication, there is no need to configure this menu. Configuration Synchronisation

Config Sync controls which settings are replicated between appliances. Not all settings can be replicated, and certain ones, in particular scheduled tasks, should not be the same on both appliances. We always recommend that either customers disable scheduled syncs on the standby, or they offset them by at least half an hour. The settings here are slightly different from session synchronisation. Here you should set the broker IP to be the primary appliance IP or host address on BOTH appliances. On the primary ONLY, set ?Act as Broker? to yes: on the standby, leave it as No. The shared secret should again be the same on both. Enable ?Synchronise configuration? on both.