Password How to Guide

Contents

Overview

Swivel can use a static password in addition to a One Time Code. The static password may be used to make shoulder surfing techniques less effective, since it will be difficult to discern password from OTC, as well as its length. When a Swivel password is set for a user, it must be used.

Passwords

There are two types of password that Swivel can use in addition to the One Time Code:

1. A Swivel password, set on the Swivel server. If a Swivel password is set, then it must be used for all Swivel authentications.

2. A Repository password, defined on the repository such as AD or LDAP. This is used with the 'Check password with repository' option on the Swivel server under Policy/Password or Authenticate non-user with just password under RADIUS NAS.

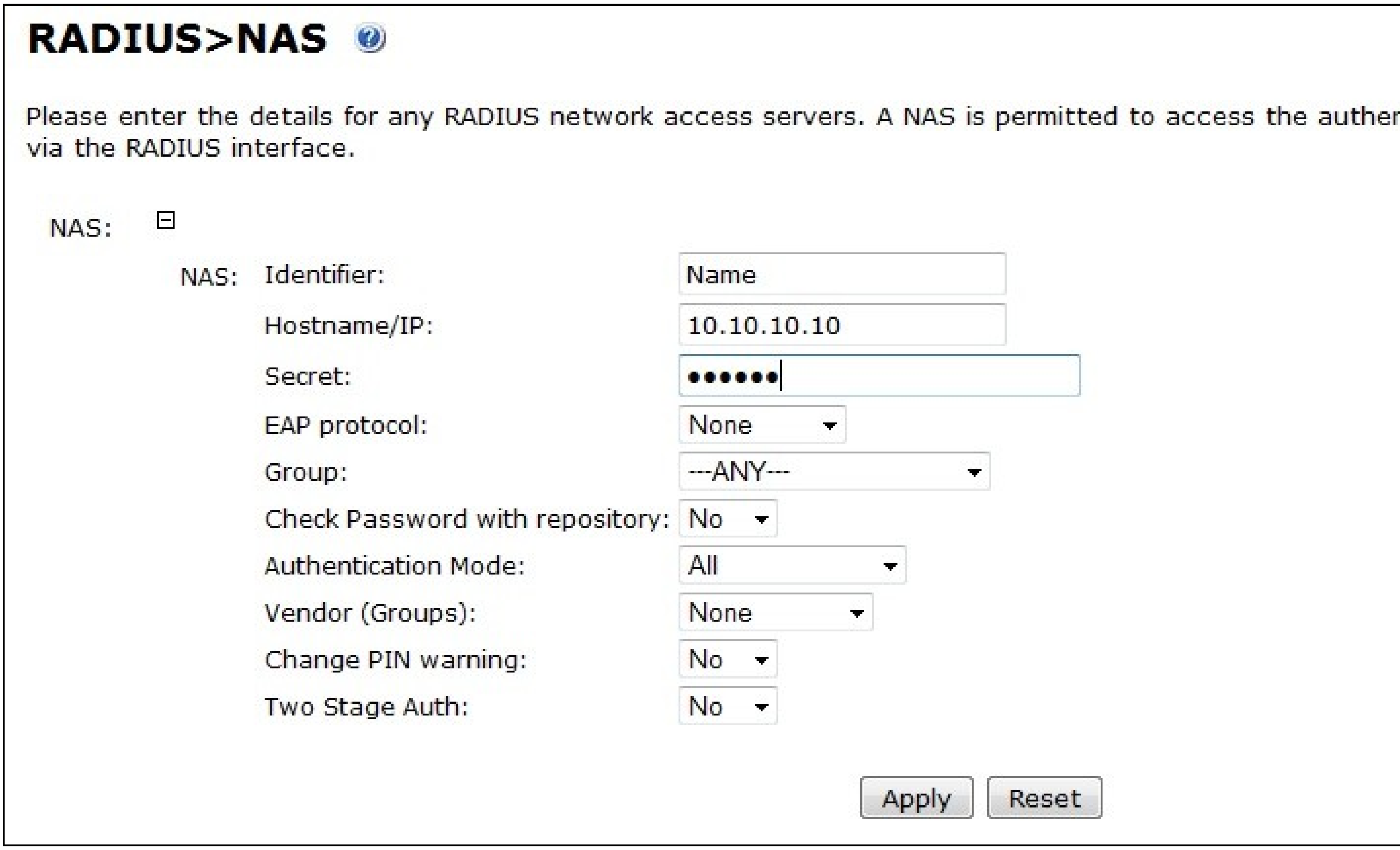
Check password with repository

From Swivel 3.8 onwards the option for Check Password with Repository is applied for an agent or RADIUS NAS entry, see RADIUS How To Guide and Agents How to Guide.

For Swivel versions prior to Swivel 3.8, the Check Password with Repository is a global option located under Policy then Password.

When this option is selected the user must enter their password with their OTC. If the password is an external repository such as AD, then they must enter their AD password. If there is a Swivel password then this must be entered. If the Swivel password is not set, then the field should be left empty, see below.

Note: For Active Directory (see AD data source configuration) and LDAP (see LDAP How to Guide) the username must be passed as username@domain in order to authenticate via LDAP. This can be specified by using the the administrator or service account username for the repository configuration as administrator@domain.name, rather than just administrator or service account username, Swivel will automatically append the domain to the username when authenticating, if one is not specified.



RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther
via the RADIUS interface.

NAS: ⊟

NAS:	Identifier:	Name
	Hostname/IP:	10.10.10.10
	Secret:	••••••
	EAP protocol:	None
	Group:	---ANY---
	Check Password with repository:	No
	Authentication Mode:	All
	Vendor (Groups):	None
	Change PIN warning:	No
	Two Stage Auth:	No

Check Password with Repository with local users

The local XML repository uses the repository.xml file as a repository, so a password cannot be set for the XML repository data source unless manually edited.

It is possible to set a password for the user in the data store and if the *Check password with repository* is set to No, it will check the password for that user.

When Check password with repository is used the Reset Password option is greyed out in some versions and not selectable, since there is no XML repository data source password.

Authenticate non-user with just password

This setting under RADIUS NAS allows a external Repository to be checked for a password when the user is not a Swivel user, See RADIUS How To Guide. The server to be used is configured under Repository/Servers with the setting **Server to use to attempt to authenticate non-users:**. See also RADIUS Static Password.

Swivel Password

The Swivel password can be set in a number of ways:

- On the Swivel administration console. See Reset Password
- Automatically generated at account creation time
- Set using Change PIN, see ChangePIN How to Guide
- Imported from the data repository source as a password attribute

Swivel Password settings

The Swivel password is configured on the Swivel Administration console under Policy/Pasword, the available settings are:

Require password: , default No, Options Yes/No. If set to Yes then the user is required to have a Swivel password, a password is created for the user if credentials are automatically created for the user.

Password mask: , default adsxxx. This is the password requirements for creation and automatic generation of a password. The following parameters are used for the creation or as a password requirement:

a alpha character a-Z,

d decimal 0-9,

s special character such as !"£$%^&*()-_=+,

x a random character also defining password length.

External Repository Password

Swivel does not know what this password is and cannot change it. However Swivel can check if a password entered by the user is correct by making an LDAP bind against the AD or LDAP server. This is used with the 'Check password with repository' option on the Swivel server under Policy/Password.

Note: When using Check Password with Repository and RADIUS is being used, then the RADIUS authentication method must be set to PAP. CHAP, MSCHAP and MSCHAP v2 will not work. See RADIUS How To Guide

Note: the local XML Repository does not have a password, passwords that are set, are entered into the Swivel Data Store.

Where do I use the Passwords

There is a large degree of flexibility in the configuration of how a password can be used, and can be adapted to suit certain environments thus the password to be used varies with each deployment. Below are the common use cases.

1. An Access device may have a single RADIUS field defined for authentication, in which case the password, is configured with the One Time Code in the format:

```
Password Field:  passwordOTC
```

2. Where Swivel is defined as a secondary authentication server, it is usual to have the LDAP or AD server defined as the Primary password field, usually to enable sign on to AD/LDAP resources, and the Swivel field used just for a One Time Code.

```
Primary Password Field 1:  AD or LDAP Password
Secondary Password Field 2:  OTC
```

3. Where the 'Check password with repository' option is used then the password is entered with the One Time Code in the format:

```
Password Field: passwordOTC
```

Swivel Administration Console Passwords

Check password with repository option is not available for the Administration console login. The Swivel Administration console uses only Swivel Passwords and not data source passwords such as that from Active Directory or LDAP.

Known Issues

Troubleshooting

Error Messages

x.x.x.x Identifier:Failed to get LDAP context for username@domain

Password has failed to be matched from a LDAP data source when using Check Password with repository. This could be due to an incorrect password being entered or not recognised. On the Swivel Administration console when using AD try setting the AD server settings username to the UPN name. Below version 3.9.1 the domain is taken from the AD configuration, if a different domain is required, use a service account with the same domain.

RADIUS: <0> Access-Request(1) LEN=64 x.x.x.x:1265 Access-Request by username Failed: AccessRejectException: Two Stage Password Fail

x.x.x.x Identifier:Failed to get LDAP context for username@domain

The check password with repository is failing for the first stage of two stage authentication. This could be due to an incorrect password being entered or not recognised. On the Swivel Administration console when using AD try setting the AD server settings username to the UPN name. If the AD domain is incorrect then authentication will fail. Below version 3.9.1 the domain is taken from the AD configuration, if a different domain is required, use a service account with the same domain.

RADIUS: Exception in thread: DATAGRAM LEN = 155 FROM 192.168.1.2:53987 java.lang.NumberFormatException: For input string: "D5368" at java.lang.NumberFormatException.forInputString(Unknown Source) at java.lang.Integer.parseInt(Unknown Source) at java.lang.Integer.parseInt(Unknown Source) at com.swiveltechnologies.pinsafe.server.utility.Utility.extractIndex(Utility.java:265) at com.swiveltechnologies.pinsafe.server.user.LocalAuth.getChannelAndSecurityString(LocalAuth.java:527) at com.swiveltechnologies.pinsafe.server.user.LocalAuth.login(LocalAuth.java:729) at com.swiveltechnologies.pinsafe.server.radius.RadiusAccess.authenticatePAP(RadiusAccess.java:1107) at com.swiveltechnologies.pinsafe.server.radius.RadiusAccess.authenticate(RadiusAccess.java:499) at com.theorem.radserver3.RADIUSSession.o(Unknown Source) at com.theorem.radserver3.RADIUSSession.e(Unknown Source) at com.theorem.radserver3.RADIUSSession.run(Unknown Source) at java.lang.Thread.run(Unknown Source)

This is caused by a - or ' in a Check Password with repository for a RADIUS authentication and Swivel interpreting the String Index. Seen in version 3.9.6. Workaround 1. Do not use ' or - in the password. Workaround 2. If the access device supports checking AD password then configure it so that Swivel is only checking the Swivel OTC.