VMware View (Horizon)

Contents

Introduction

This document describes steps to configure VMware View with Swivel as the authentication server. The solution is tested with VMware View 5.1. using RADIUS authentication protocol with SMS, Token, Mobile Phone Client, and Taskbar Authentication

The VMware View Client also functions on a number of mobile phone client devices including iPhone, iPad and Android.

Credits

Swivel would like to thank the following contributors to this document:

Barry Coombs (VMware vExpert) of Computerworld Systems LTD www.computerworld.co.uk

Prerequisites

VMware View 5.1 or higher

VMware View documentation

Swivel 3.x,

Baseline

VMware View 5.1

Swivel 3.8

Architecture

The VMware View makes authentication requests against the Swivel server by RADIUS.

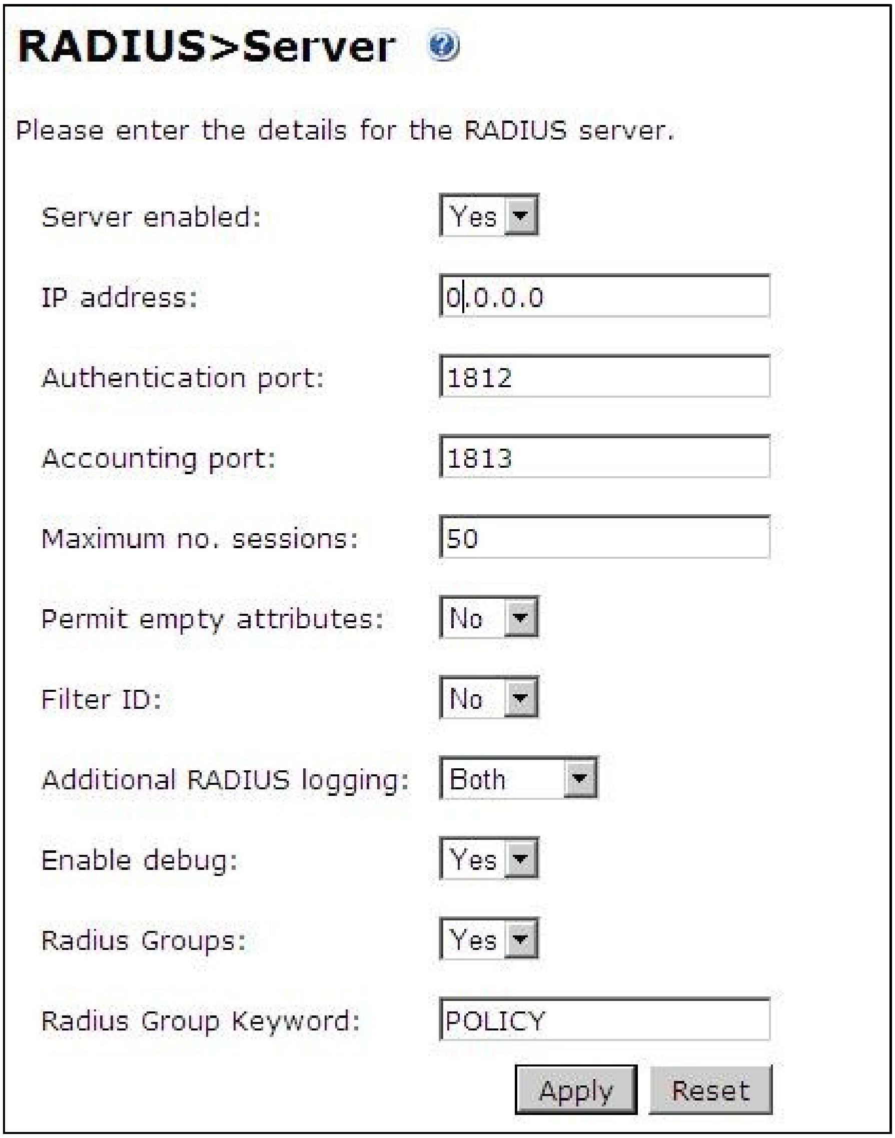
Swivel Configuration

Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console by selecting RADIUS Server. To turn on RADIUS authentication set **Server Enabled** to YES. The Host or IP address is the interface which will accept RADIUS requests, leave this blank to allow RADIUS requests on any interface. (In this example the HOST IP is set to 0.0.0.0 which is the same as leaving it blank).

For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

Note: for appliances, the Swivel VIP should NOT be used as the server IP address, see VIP on PINsafe Appliances



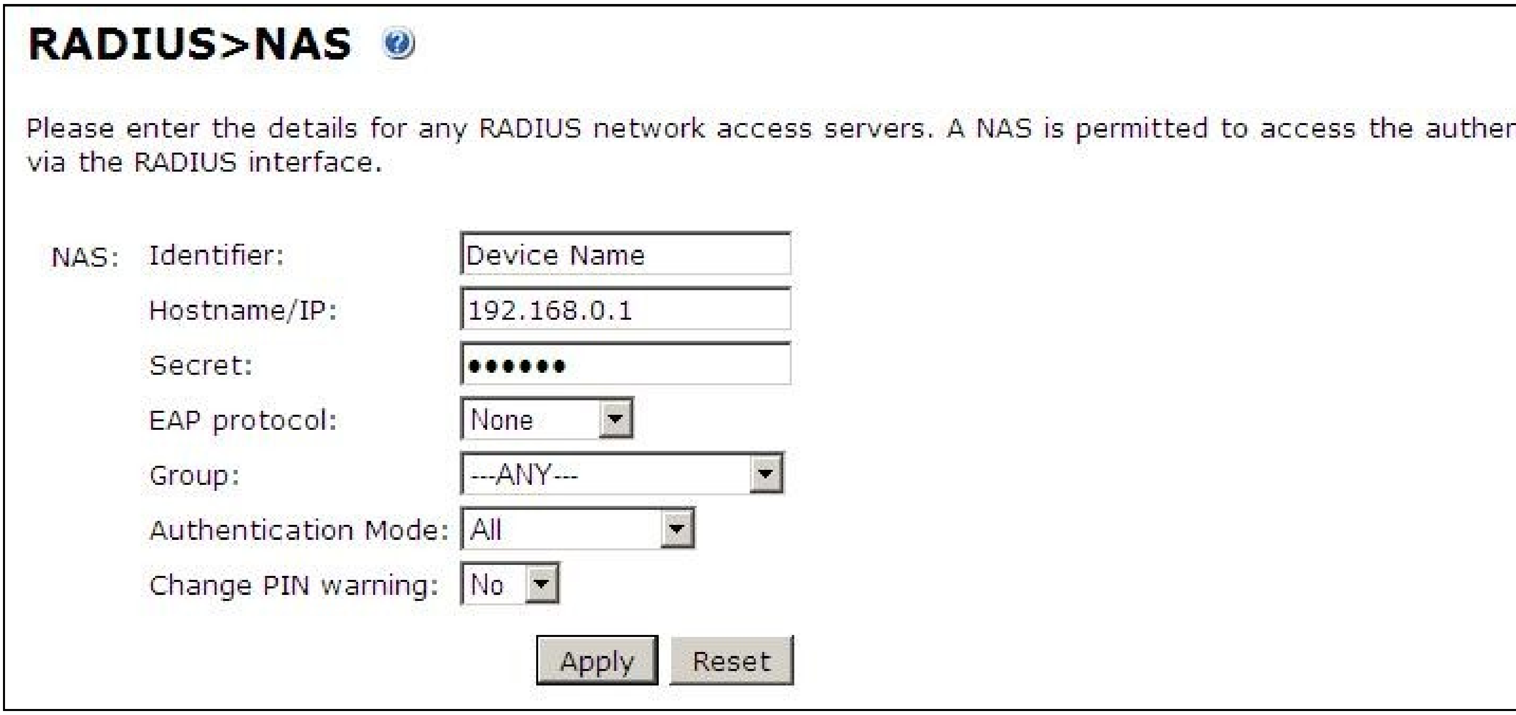
RADIUS>Server

Please enter the details for the RADIUS server.

Server enabled:	Yes
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No
Filter ID:	No
Additional RADIUS logging:	Both
Enable debug:	Yes
Radius Groups:	Yes
Radius Group Keyword:	POLICY

Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the Swivel Administration console. Enter a name for the NAS Client. The IP address has been set to the IP of the NAS Client, and the secret ?secret? assigned that will be used on both the Swivel server and the NAS Client.



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: Identifier: Device Name

Hostname/IP: 192.168.0.1

Secret: ●●●●●●

EAP protocol: None

Group: ---ANY---

Authentication Mode: All

Change PIN warning: No

You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless authentication is restricted to a specific repository group.

Enabling Session creation with username

The Swivel server can be configured to return an image stream containing a TURing image in the Taskbar

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid Swivel username:

Appliance

https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

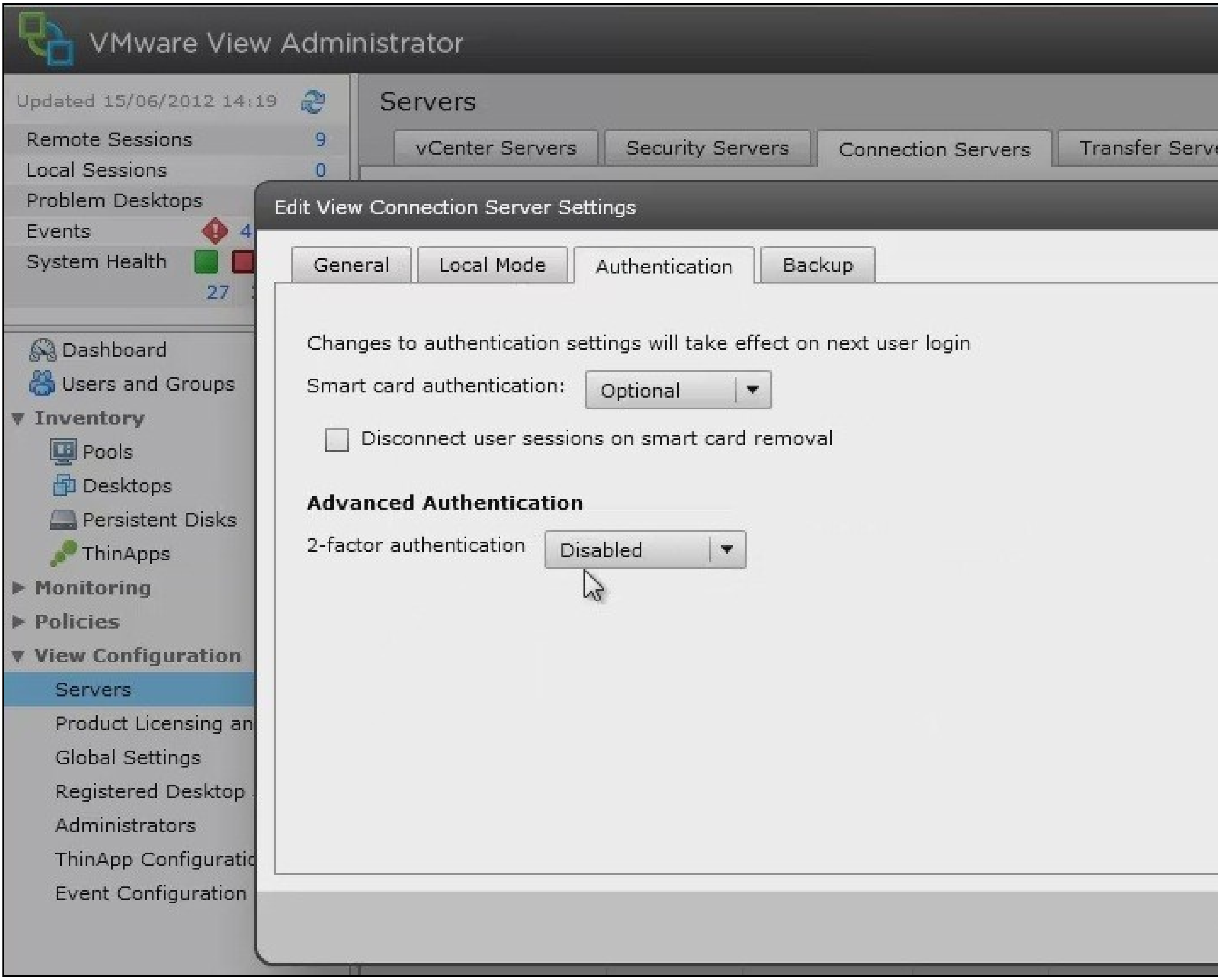
For a software only install see Software Only Installation

VMware View Configuration

Ensure that the VMware View is fully functioning using standard authentication, then start the Swivel integration configuration.

Create a Radius Authentication Server Group

On the VMware View Administrator select **View Configuration**, then **Servers**, select the **Connection Servers** tab and then **Edit** to bring up the Edit View Connection Server Settings and select the **Authentication** tab.



Edit View Connection Server Settings

Changes to authentication settings will take effect on next user login

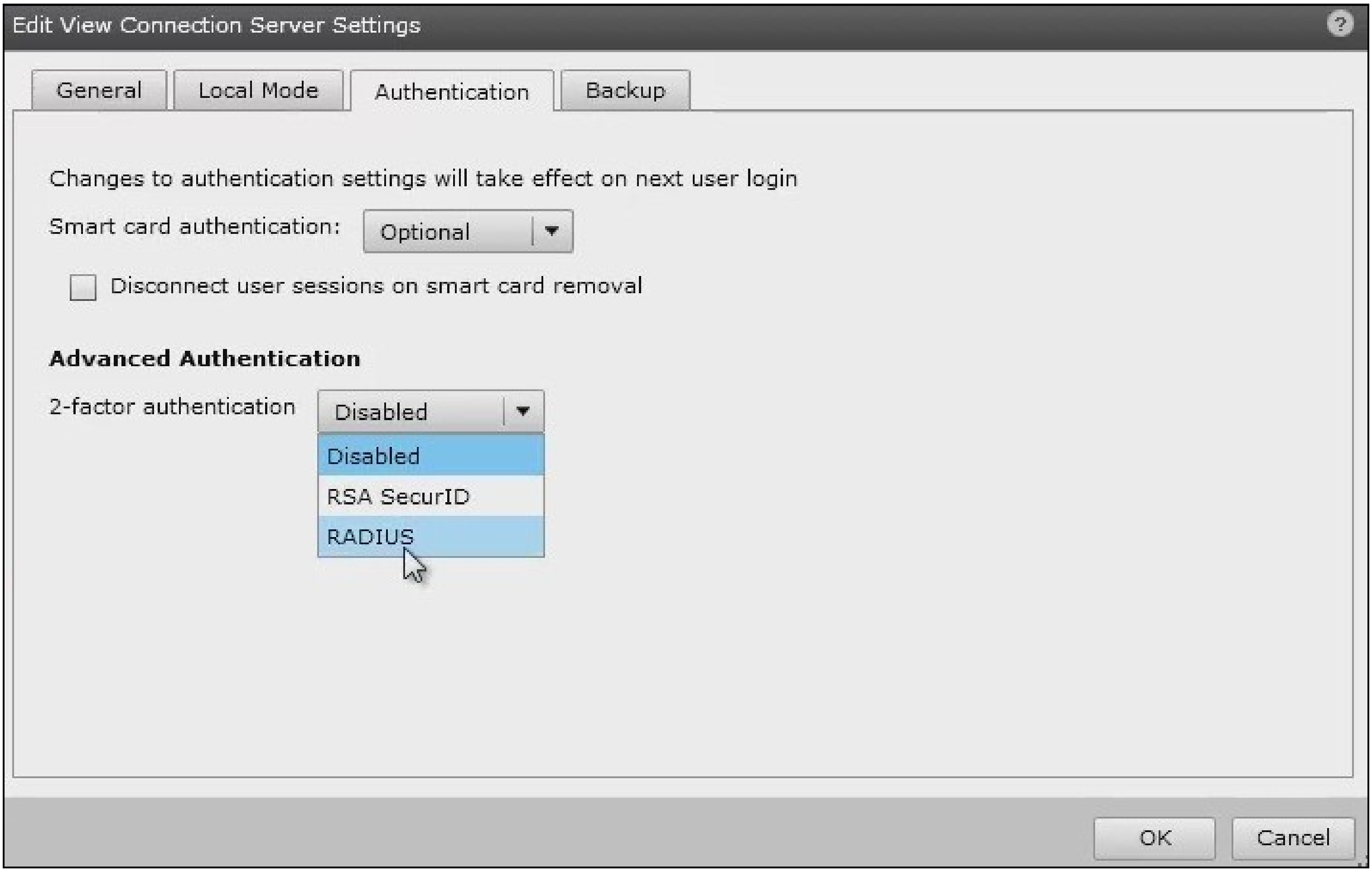
Smart card authentication: Optional

□ Disconnect user sessions on smart card removal

Advanced Authentication

2-factor authentication Disabled

Under Advanced Authentication choose, for 2-factor authentication, the **RADIUS** tab.



Edit View Connection Server Settings

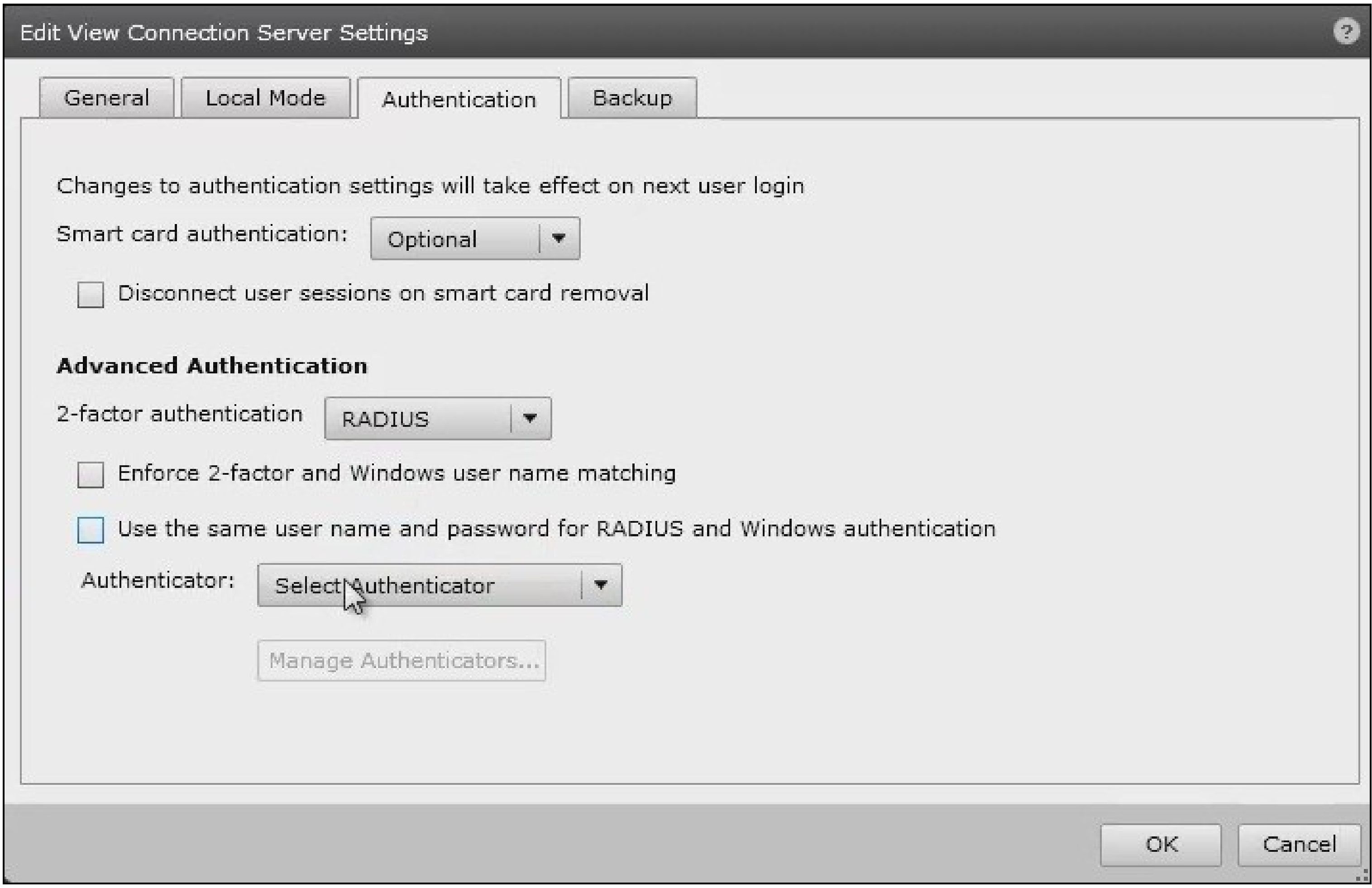
Changes to authentication settings will take effect on next user login

Smart card authentication: Optional

□ Disconnect user sessions on smart card removal

Advanced Authentication

2-factor authentication: Disabled



Changes to authentication settings will take effect on next user login

Smart card authentication: Optional

□ Disconnect user sessions on smart card removal

Advanced Authentication

2-factor authentication: RADIUS

□ Enforce 2-factor and Windows user name matching

□ Use the same user name and password for RADIUS and Windows authentication

Authenticator: Select Authenticator

Under Authenticator select Create new, this opens the Add RADIUS Authenticator screen, this allows a Primary and Secondary RADIUS authentication servers to be configured, enter the following:

Label: A label shown to clients

Primary Authentication Server

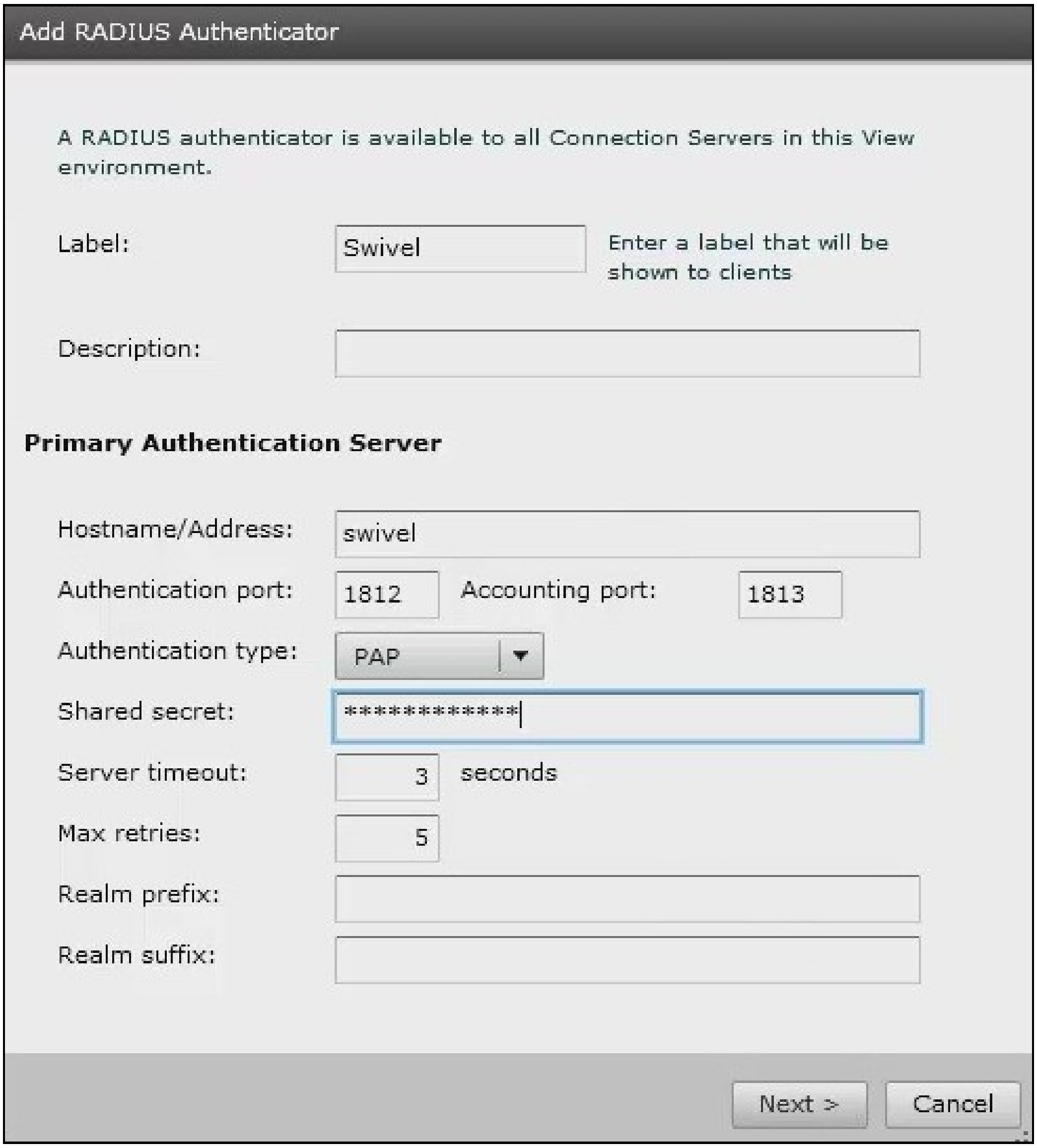
Hostname/Address: IP address of the Swivel server (This must not be a Swivel VIP for Active/Active appliances)

Authentication Type: select RADIUS authentication type, use PAP for initial setup.

Shared secret: The shared secret, the same as entered on the Swivel server

Domain Prefix: Allows a domain name to be added, and to be sent to the Swivel server in the format domain\username

Domain Suffix: Allows a domain name to be added, and to be sent to the Swivel server in the format username@domain



Add RADIUS Authenticator

A RADIUS authenticator is available to all Connection Servers in this View environment.

Label: Swivel — Enter a label that will be shown to clients

Description:

Primary Authentication Server

Hostname/Address: swivel

Authentication port: 1812 Accounting port: 1813

Authentication type: PAP

Shared secret: ************

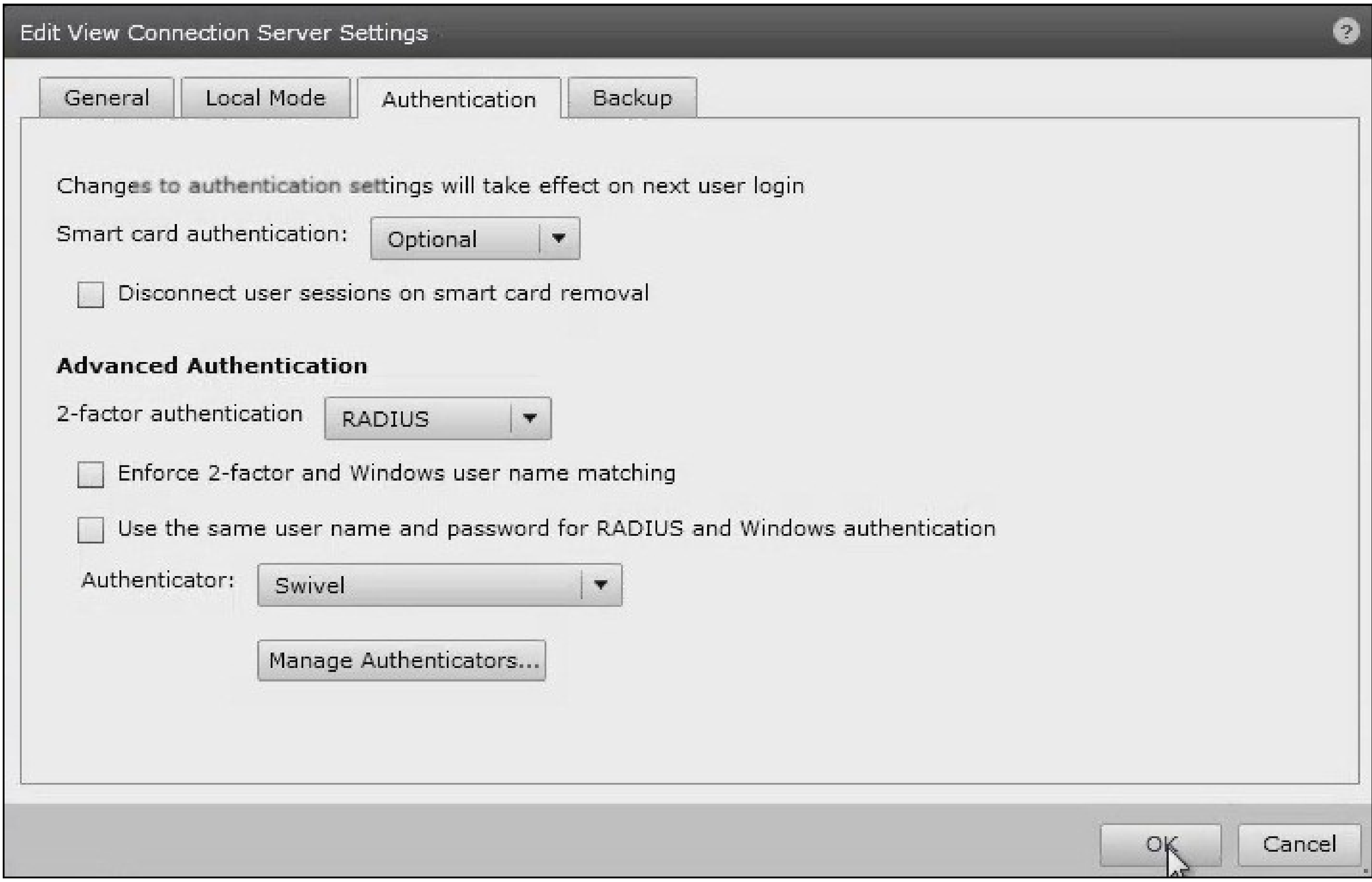
Server timeout: 3 seconds

Max retries: 5

Realm prefix:

Realm suffix:

Clicking OK returns to to the Authentication tab.



Edit View Connection Server Settings

Changes to authentication settings will take effect on next user login

Smart card authentication: Optional

□ Disconnect user sessions on smart card removal

Advanced Authentication

2-factor authentication RADIUS

□ Enforce 2-factor and Windows user name matching

□ Use the same user name and password for RADIUS and Windows authentication

Authenticator: Swivel

It is possible to specify here the option **Enforce 2-factor and Windows name matching** so that the AD username is used for the Swivel authentication.

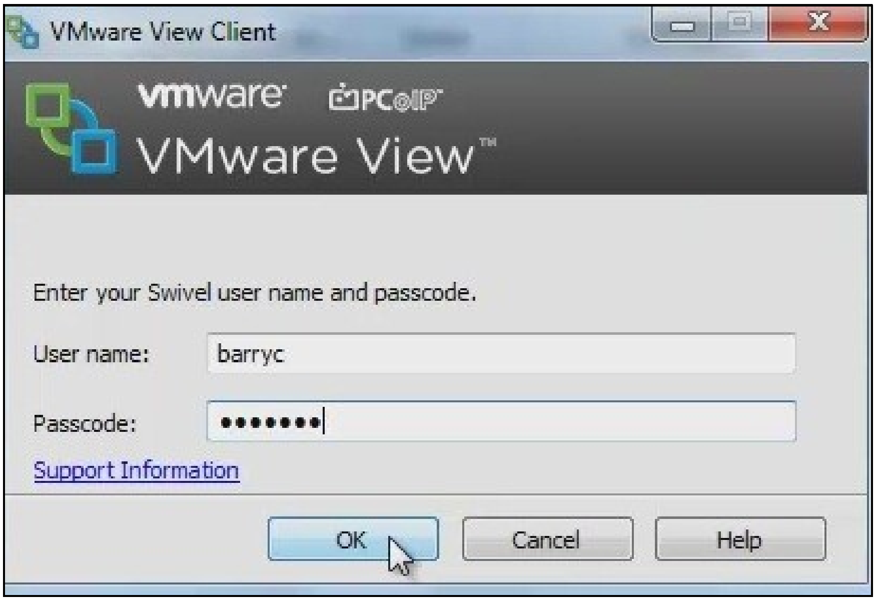
Additional Configuration Options

Challenge and Response with Two Stage Authentication

Challenge and Response is supported by using Two Stage authentication and Check Password with Repository using RADIUS PAP authentication. See Challenge and Response How to Guide. Using the option to allow the Same Username and Password for Windows and RADIUS authentication allows the AD username and password to be entered once and then challenge for a One Time Code.

Testing

The VMware View client will display fields for Username and Password. The username should be entered followed by the Swivel One Time Code in the Passcode field.

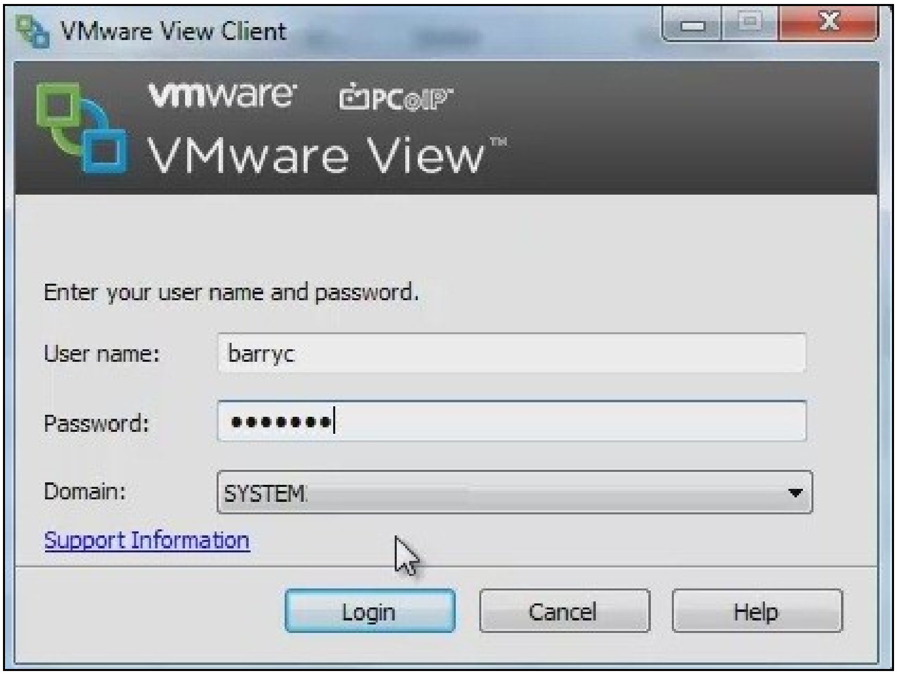


Enter your Swivel user name and passcode.

User name: barryc

Passcode: •••••••

If the OTC is correct the user will be prompted for a AD Password



Enter your user name and password.

User name: barryc

Password: •••••••

Domain: SYSTEM

Troubleshooting

Check the Swivel logs for RADIUS requests. RADIUS requests should be seen even if the OTC is incorrect.

Known Issues and Limitations

None

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