SWIVEL®

AUTHENTICATION YOU CAN IDENTIFY WITH

CO-SIGN AND PINSAFE

BASIC INTEGRATION GUIDE

SWIVEL SECURE
VICTORIA AVENUE
HARROGATE
HG1 1EL

CO-SIGN

INTEGRATION

CONTENTS

Introduction

This report details the steps required to integrate Co-Sign with PINsafe via RADIUS. It assumes knowledge of both products and only covers the specific of the integration and not of the deployment of the two products.

It is assumed that there is a Co-Sign server deployed at IP address 192.168.0.160 and a PINsafe server at IP address 192.168.0.157. It also assumes that both servers are connected to the same Active Directory domain controller

The user experience is as follows.

1. The user authenticates to Co-Sign using their Active Directory credentials.
2. Subsequently, whenever a user wants to sign a document they then need to provide valid PINsafe credentials.

The operation requires that Co-Sign is configured to use PINsafe as a RADIUS server.

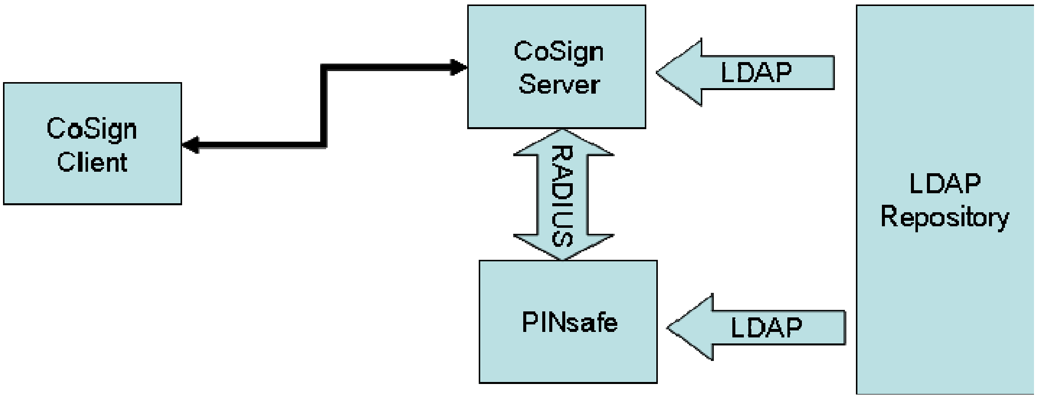
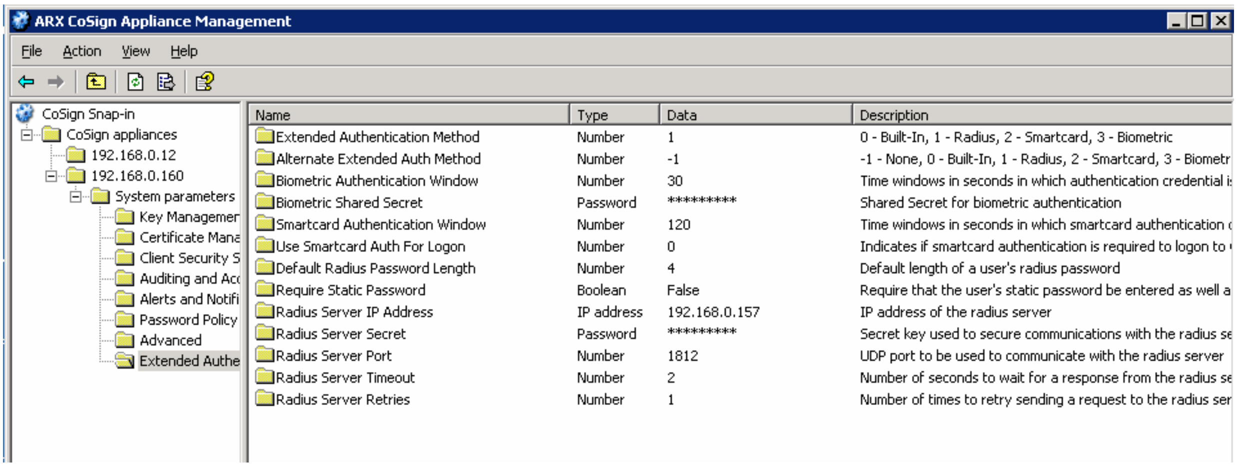


Figure 1. Basic Integration Architecture

Configuring CO-SIGN to Use RADIUS



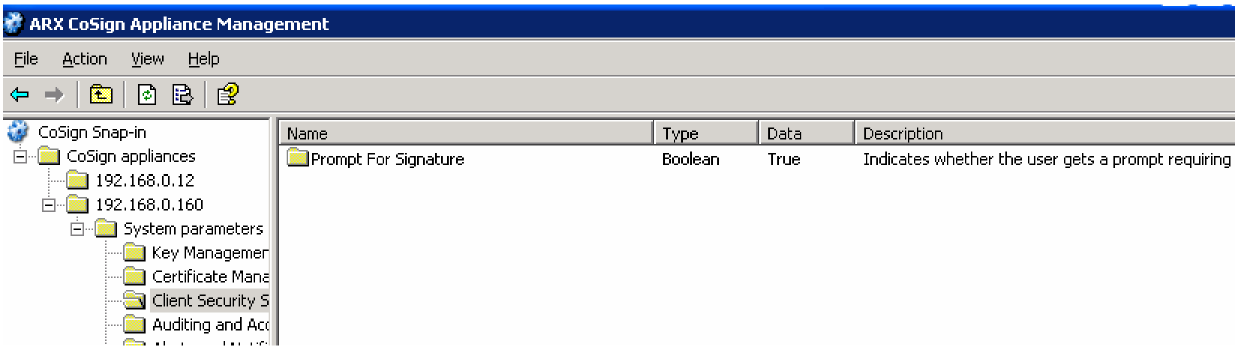
Name	Type	Data	Description
Extended Authentication Method	Number	1	0 - Built-In, 1 - Radius, 2 - Smartcard, 3 - Biometric
Alternate Extended Auth Method	Number	-1	-1 - None, 0 - Built-In, 1 - Radius, 2 - Smartcard, 3 - Biometr
Biometric Authentication Window	Number	30	Time windows in seconds in which authentication credential i
Biometric Shared Secret	Password	*********	Shared Secret for biometric authentication
Smartcard Authentication Window	Number	120	Time windows in seconds in which smartcard authentication
Use Smartcard Auth For Logon	Number	0	Indicates if smartcard authentication is required to logon to
Default Radius Password Length	Number	4	Default length of a user's radius password
Require Static Password	Boolean	False	Require that the user's static password be entered as well a
Radius Server IP Address	IP address	192.168.0.157	IP address of the radius server
Radius Server Secret	Password	*********	Secret key used to secure communications with the radius se
Radius Server Port	Number	1812	UDP port to be used to communicate with the radius server
Radius Server Timeout	Number	2	Number of seconds to wait for a response from the radius se
Radius Server Retries	Number	1	Number of times to retry sending a request to the radius ser

Figure 2. Co-Sign Extended Authentication Screen

The configuration of Co-Sign to use PINsafe as a RADIUS server is achieved within the extended authentication folder of the Co-Sign Application Management tool. The configuration requires the following settings.

Parameter	Value
Extended Authentication Method	1: This sets Co-Sign to use RADIUS
Alternate Extended Auth Method	-1: This can be used to set up an alternative if RADIUS is unavailable. Default is -1 meaning that only RADIUS is available.
Default RADIUS password length	4: This is the default length of a one-time code in PINsafe.
Require Static Password	FALSE: This would be set to TRUE if PINsafe were to check a password as well as a static password, default is false.
RADIUS Server IP address	This is the IP address of the PINsafe server, in this example, 192.168.0.157.
RADIUS shared secret	Must match the shared secret set on the PINsafe -> NAS screen.
RADIUS server port	1812: Must match port used by PINsafe, 1812 is the default port for both PINsafe and Co-Sign
RADIUS server timeout/retries	Self-explanatory, PINsafe has no special requirements in this respect, use of defaults should be fine.

The other required element is to ensure that authentication is required to sign a document. This is achieved by setting the Prompt for Signature parameter within the Client Security Settings to true.



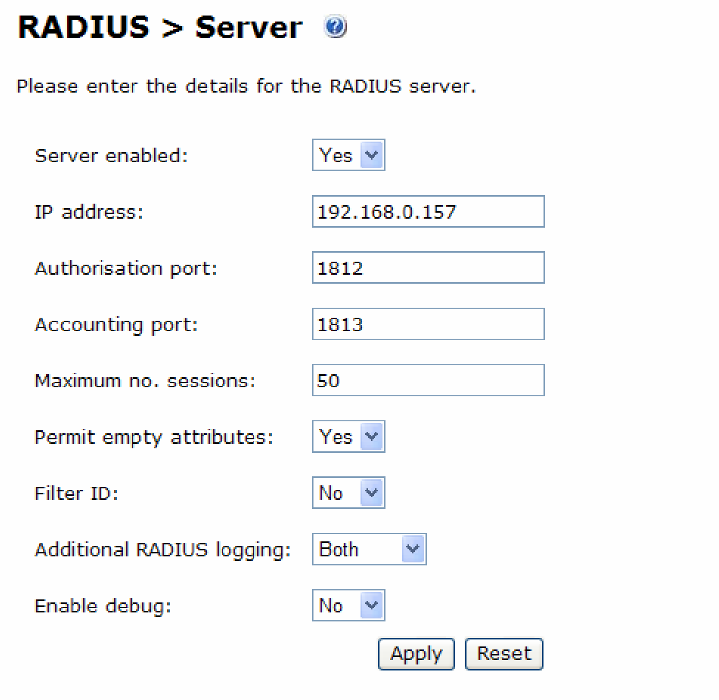
Name	Type	Data	Description
Prompt For Signature	Boolean	True	Indicates whether the user gets a prompt requiring

Figure 3. Setting Prompt for Signature

Once these changes have been made, perform a soft-restart for the changes to take affect.

Configuring PINsafe RADIUS For Co-Sign

The first stage is to ensure that the PINsafe RADIUS server is enabled and bound to the correct IP address. This is done on the RADIUS -> Server page.



RADIUS > Server

Please enter the details for the RADIUS server.

Server enabled: Yes

IP address: 192.168.0.157

Authorisation port: 1812

Accounting port: 1813

Maximum no. sessions: 50

Permit empty attributes: Yes

Filter ID: No

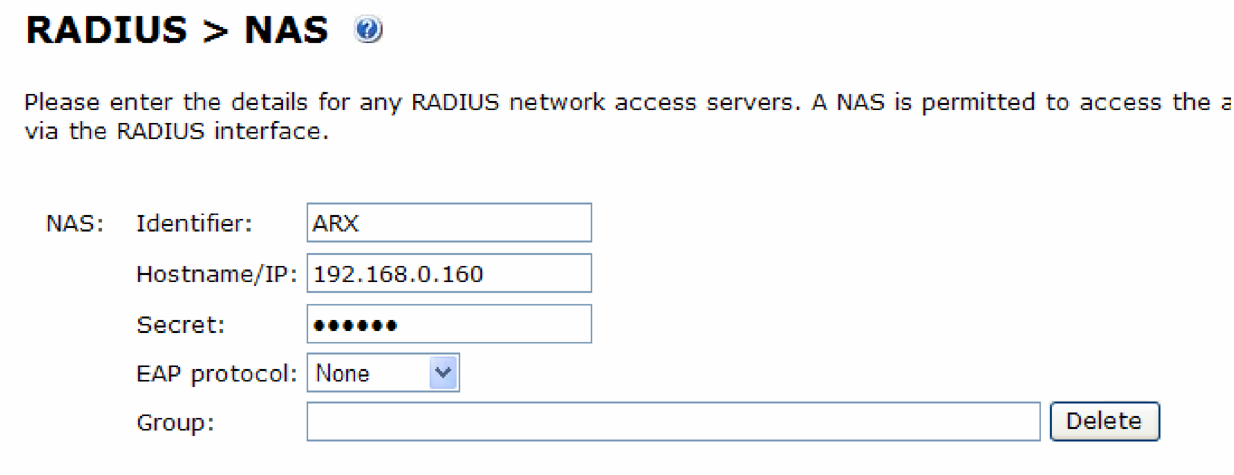
Additional RADIUS logging: Both

Enable debug: No

Figure 4. PINsafe RADIUS Configuration

Parameter	Value
Server Enabled	Yes
IP Address	The IP address needs to match the IP address of the PINsafe server; alternatively this field can be left blank and all RADIUS requests will be responded to.
Authorisation Port	The authorization port needs to match that configured on the Co-Sign server, 1812 being the default.
Accounting Port	Leave as default, 1813
Maximum Number of sessions	Leave as default, 50
Permit Empty Attributes	Set to Yes
Filter ID	Set to No
Additional RADIUS logging	Set to Both, this provides additional RADIUS log entries in PINsafe.
Enable debug	No

Once the RADIUS server has been configured you need to create a NAS entry for the Co-Sign server.



RADIUS > NAS

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

NAS: Identifier: ARX

Hostname/IP: 192.168.0.160

Secret: ●●●●●●

EAP protocol: None

Group:

Figure 5. NAS Configuration Screen.

The NAS needs a name. The IP address needs to match that of the Co-Sign server and the shared secret needs to match the setting at the Co-Sign end. PINsafe supports a range of secure RADIUS protocols, eg EAP-MD5. If this is not required leave this setting at None.

On PINsafe you can restrict the use of a NAS to a specific group within PINsafe. If you leave the Group field blank then all users can authenticate via this NAS.

PINsafe and Co-Sign work in a similar way in that they identify users from with Active Directory by their memberships of specific groups within active directory. So as part of the Co-Sign installation a group within active directory may have been created, eg

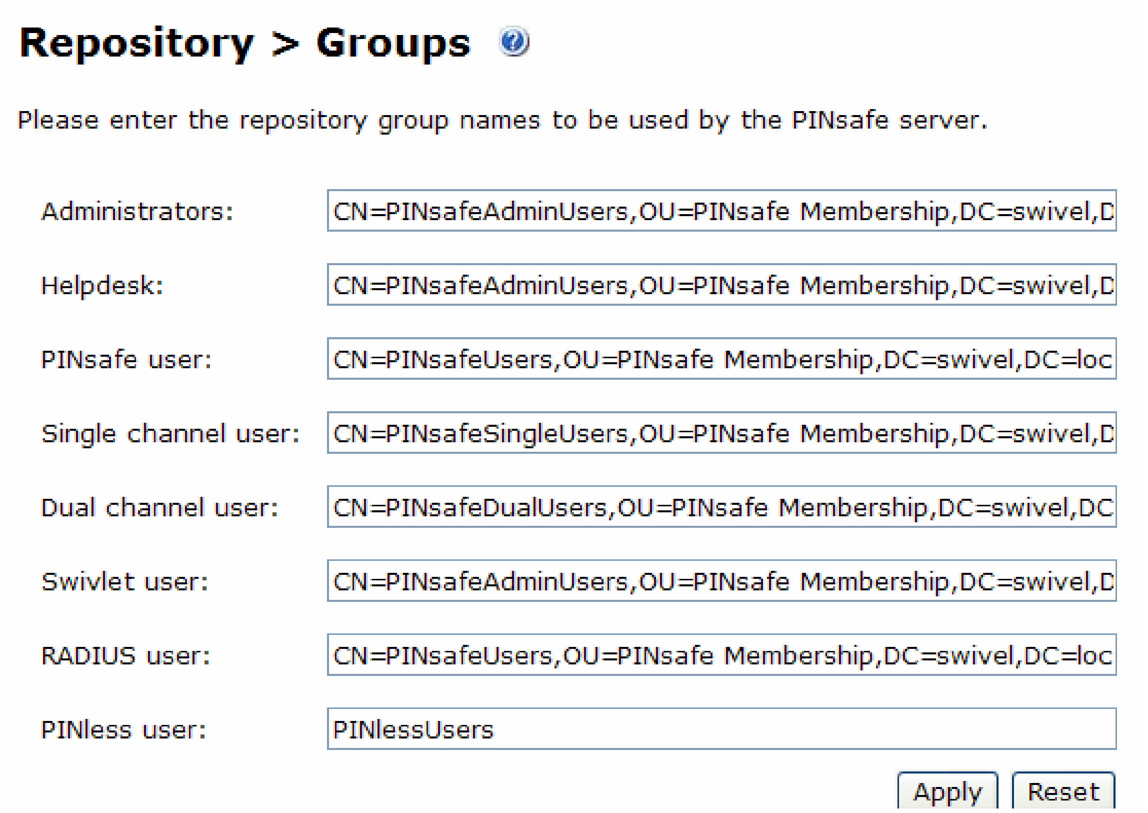
CN=CoSign Signers CN=Users, OU=Membership, DC=swivel, DC=local

In order to ensure that PINsafe can manage the same user-population you need to either,

1) Make the above group the PINsafe users group on the Repository-> Groups page

Or

2) Ensure that the above group is in turn a member of the PINsafe user group as defined of the Repository -> Groups screen.



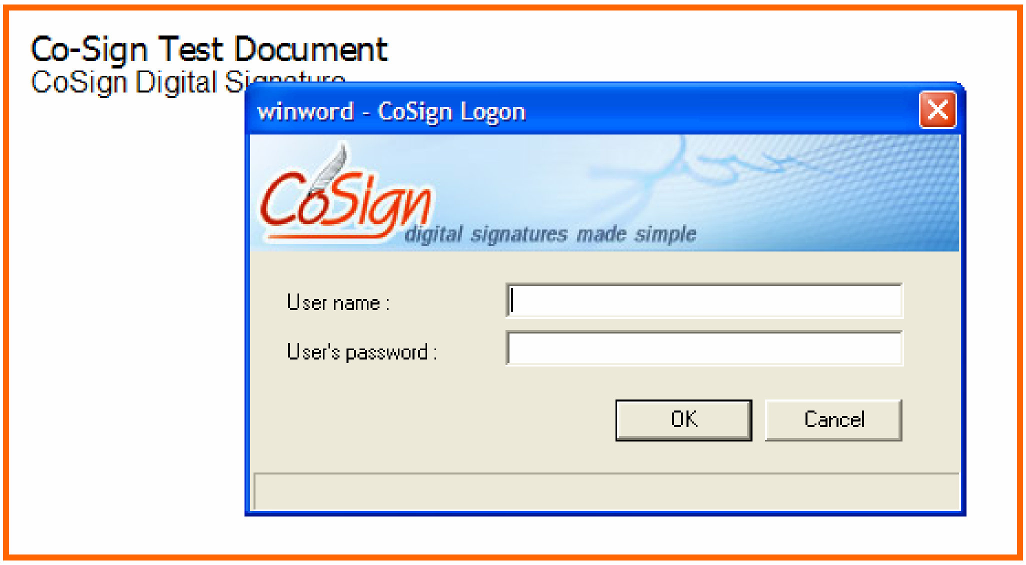
Repository > Groups

Please enter the repository group names to be used by the PINsafe server.

Administrators:	CN=PINsafeAdminUsers,OU=PINsafe Membership,DC=swivel,D
Helpdesk:	CN=PINsafeAdminUsers,OU=PINsafe Membership,DC=swivel,D
PINsafe user:	CN=PINsafeUsers,OU=PINsafe Membership,DC=swivel,DC=loc
Single channel user:	CN=PINsafeSingleUsers,OU=PINsafe Membership,DC=swivel,D
Dual channel user:	CN=PINsafeDualUsers,OU=PINsafe Membership,DC=swivel,DC
Swivlet user:	CN=PINsafeAdminUsers,OU=PINsafe Membership,DC=swivel,D
RADIUS user:	CN=PINsafeUsers,OU=PINsafe Membership,DC=swivel,DC=loc
PINless user:	PINlessUsers

Figure 6. Repository -> Groups screen

Testing



Co-Sign Test Document

CoSign Digital Signature

winword - CoSign Logon

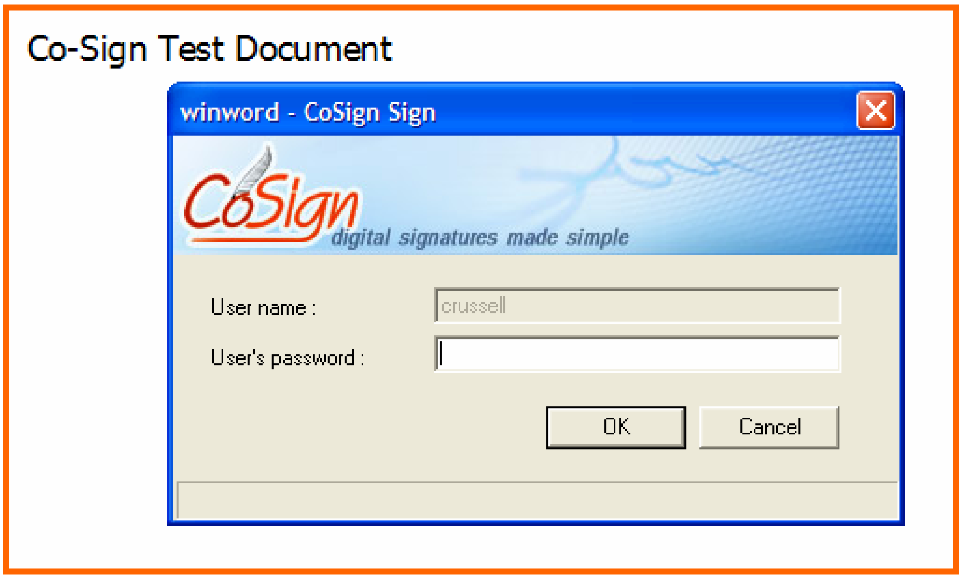
User name :

User's password :

Figure 7. Initial Sign-On Screen

If you are not currently signed into a Co-Sign server, when you first attempt to sign a document you are required to authenticate to the Co-Sign server with you Active Directory username and password.

Once you have authenticated to Co-Sign, you will then be presented with a Co-Sign authentication box with the username pre-filled. You then enters their PINsafe one-time code into this field and click on OK



Co-Sign Test Document

winword - CoSign Sign

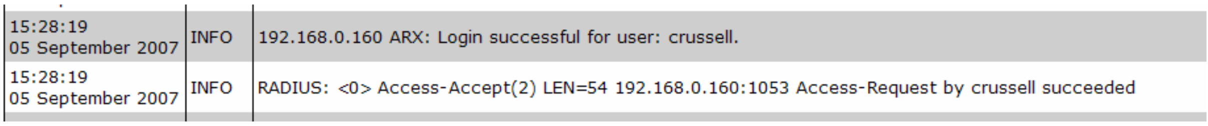
User name : crussell

User's password :

Figure 8. Signing Authentication Dialogue Box

Confirmation

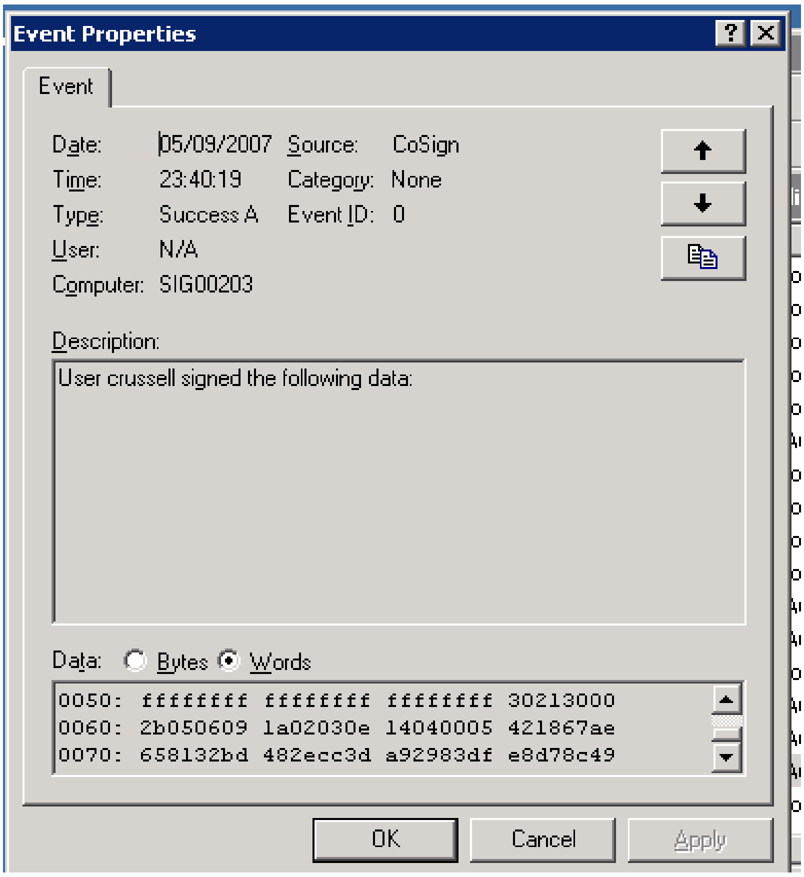
You can confirm the operation by logging at the log entries on the two servers. In the PINsafe log you will see the RADIUS authentication



```
15:28:19
05 September 2007  INFO  192.168.0.160 ARX: Login successful for user: crussell.
15:28:19
05 September 2007  INFO  RADIUS: <0> Access-Accept(2) LEN=54 192.168.0.160:1053 Access-Request by crussell succeeded
```

Figure 9. Log entry for Co-Sign signing

And on Co-Sign



Date: 05/09/2007 Source: CoSign

Time: 23:40:19 Category: None

Type: Success A Event ID: 0

User: N/A

Computer: SIG00203

Description:

User crussell signed the following data:

Data: ○ Bytes ● Words

```
0050: ffffffff ffffffff ffffffff 30213000
0060: 2b050609 1a02030e 14040005 421867ae
0070: 658132bd 482ecc3d a92983df e8d78c49
```

Figure 10. Co-Sign Event Log