This technical document is provided for historical purposes only. The Microsoft Exchange ActiveSync integration is now supported within the RSA ACE/Agent 5.3 for IIS. For more information on the integration, please refer to the RSA ACE/Agent 5.3 for IIS product documentation.

RSA SecurID Ready Implementation Guide

Last Modified: Thursday, September 09, 2004

1. Partner Information

Partner Name	Microsoft
Web Site	www.microsoft.com
Product Name	Exchange Server ActiveSync
Version & Platform	Exchange 2003
Product Description	Exchange Server ActiveSync, formerly found in Microsoft Mobile Information Server 2002, is now built-in with all Exchange Server 2003 Standard installations. Exchange Server ActiveSync allows you to synch directly and with high levels of security to your Exchange mailboxes from Microsoft Windows-powered devices such as Pocket PC 2003 and Windows Powered SmartPhone.
Product Category	Wireless Communications

2. Contact Information

	Sales Contact	Support Contact
Web	www.microsoft.com/worldwide	http://support.microsoft.com

3. Solution Summary

Feature	Details
Authentication Methods Supported	Native RSA SecurID
RSA ACE/Agent Library Version	5.03
RSA ACE 5 Locking	Yes
Replica RSA ACE/Server Support	Full Replica Support
Secondary RADIUS/TACACS+ Server Support	N/A
Location of Node Secret on Client	In Registry
RSA ACE/Server Agent Host Type	Communication server
RSA SecurID User Specification	Designated users, all users, RSA
RSA SecurID Protection of Administrators	Yes

4. Product Requirements

- ***Hardware requirements***

Component Name: Exchange 2003 Server	
CPU make/speed required	Pentium 133 MHz or higher
Memory	256 MB
HD space	500 MB free space on the drive where Exchange 2003 is installed. 200 MB free space on the system drive
Disk Partition	Disk partitions must be formatted for the NTFS file system

Component Name: Mobile Device	
	Hand held device compatible with Windows Mobile 2003 software for Pocket PC.

- ***Software requirements***

Component Name: Exchange 2003 (As Tested)	
Operating System	**Version (Patch-level)**
Windows 2000 Server, Advanced Server, or Datacenter Server	Service Pack 3 or later

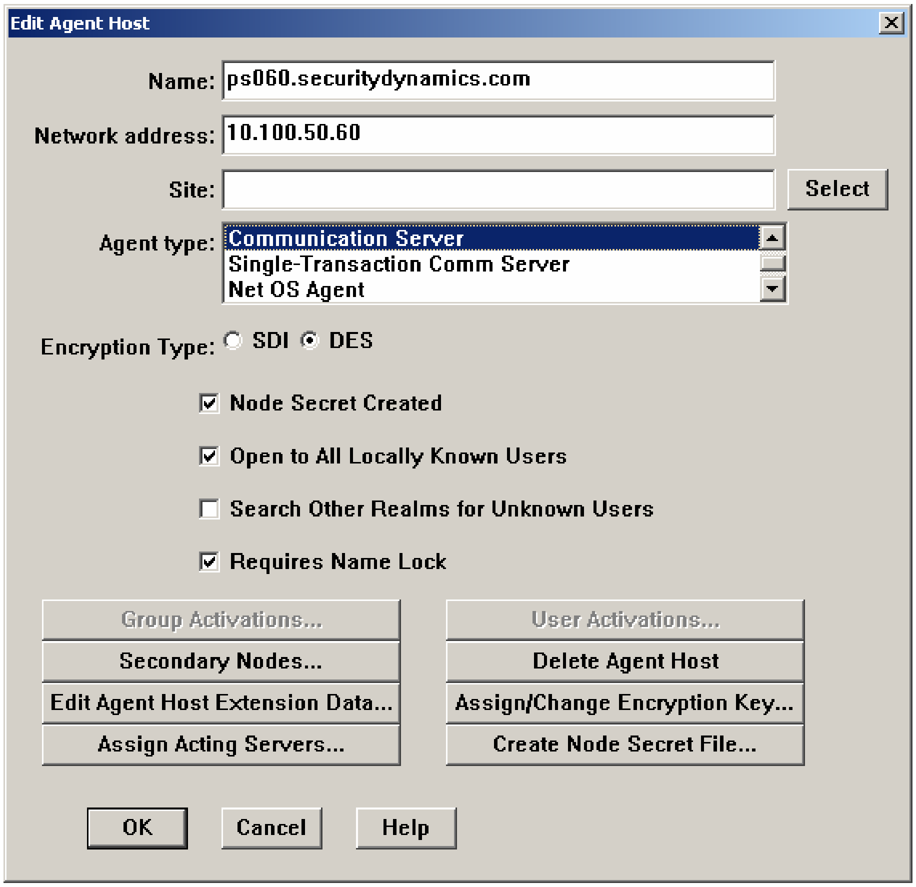
Component Name: Mobile Device	
Operating System	**Version (Patch-level)**
MS Pocket PC 2003	
Windows Mobile 2003 Pocket PC phone edition	
MS ActiveSync	3.7

5. RSA ACE/Server configuration

Perform the following steps to set up the Exchange 2003 Server as an Agent Host within the RSA ACE/Server's database.

1. On the RSA ACE/Server computer, go to **Start > Programs > RSA ACE/Server**, and then **Database Administration - Host Mode**.

2. On the **Agent Host** menu, choose **Add Agent Host...**.



Edit Agent Host

Name: ps060.securitydynamics.com

Network address: 10.100.50.60

Site:

Agent type: Communication Server (selected)
Single-Transaction Comm Server
Net OS Agent

Encryption Type: ○ SDI ● DES

☑ Node Secret Created

☑ Open to All Locally Known Users

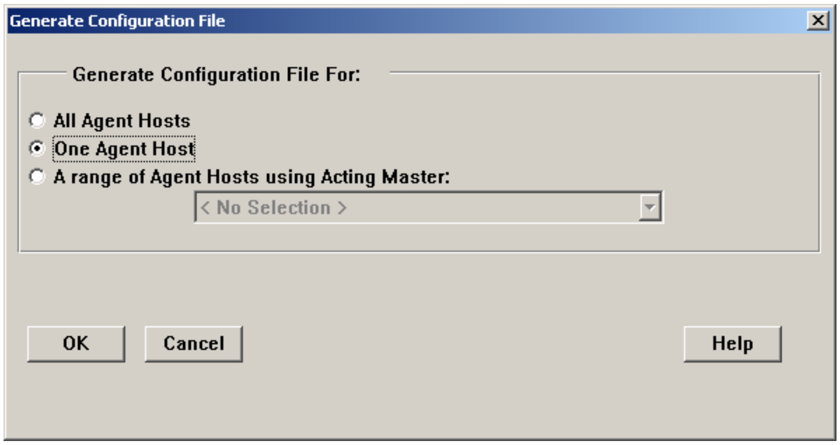
□ Search Other Realms for Unknown Users

☑ Requires Name Lock

3. In **Name**, type the hostname of the Exchange 2003 server.
4. In **Network address**, type the IP address of the Exchange 2003 server.

Note: It is important that all hostname and IP addresses resolve to each other. Please reference the RSA ACE/Server documentation for detailed information on this and other configuration parameters within this screen. Subsequently, you can also select the 'Help' button at the bottom of the screen.

5. On the **Agent Host menu** choose **Generate Configuration Files.**
6. Select **One agent host** and click OK.



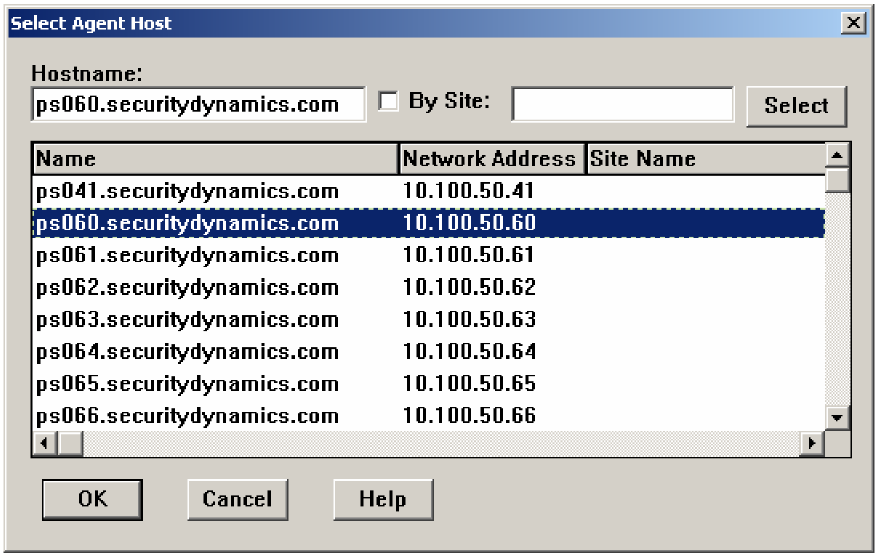
Generate Configuration File

Generate Configuration File For:

○ All Agent Hosts
● One Agent Host
○ A range of Agent Hosts using Acting Master:

< No Selection >

7. Select the appropriate agent host from the list and click OK.



Select Agent Host

Hostname: ps060.securitydynamics.com

□ By Site:

Name	Network Address	Site Name
ps041.securitydynamics.com	10.100.50.41	
ps060.securitydynamics.com	10.100.50.60	
ps061.securitydynamics.com	10.100.50.61	
ps062.securitydynamics.com	10.100.50.62	
ps063.securitydynamics.com	10.100.50.63	
ps064.securitydynamics.com	10.100.50.64	
ps065.securitydynamics.com	10.100.50.65	
ps066.securitydynamics.com	10.100.50.66	

8. Save the sd.conf file and copy it to the agent host (Exchange 2003 server).

Install the RSA ACE/Agent as described in the *RSA ACE/Agent for Windows Installation and Administration Guide.*

6. Partner RSA ACE/Agent configuration

A. Configure Internet Information Service (IIS)

Protecting the Exchange ActiveSync Virtual Directories

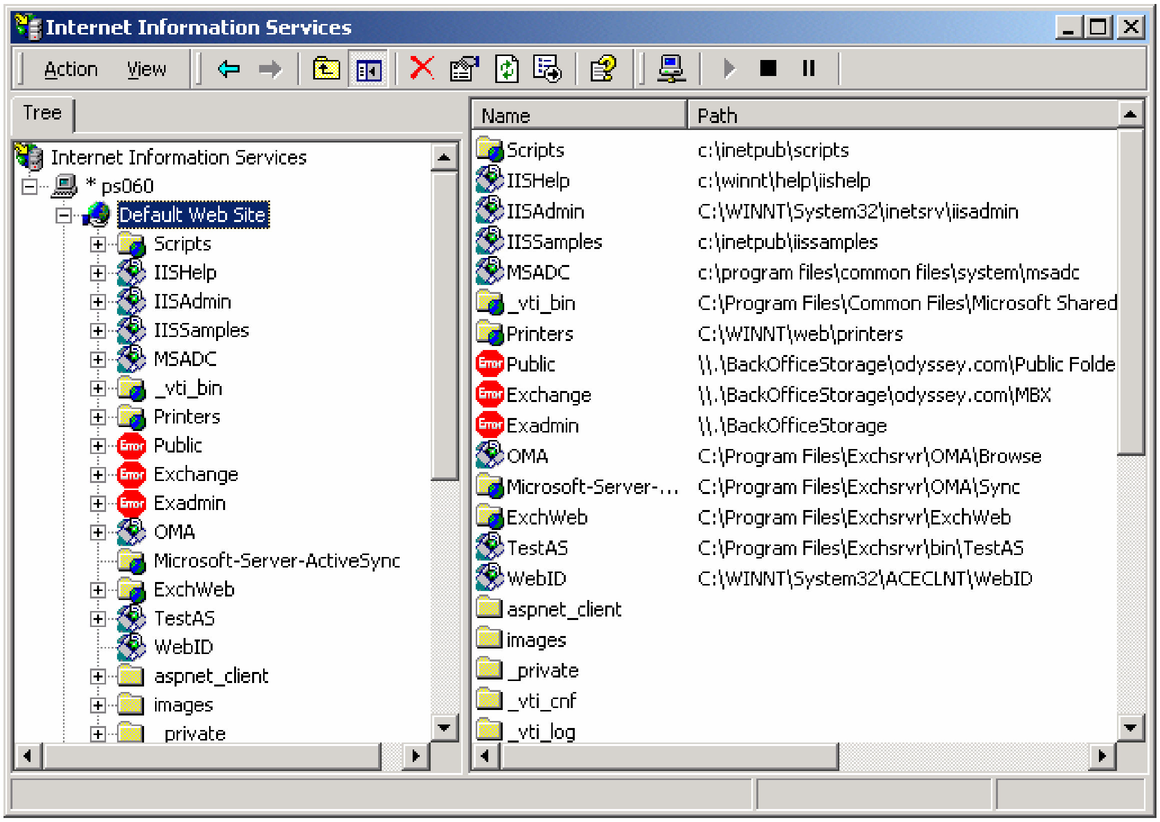
Protect the virtual directories that users access when they use Exchange ActiveSync. Exchange Server 2003 uses the \Microsoft-Server-ActiveSync virtual directory. You can protect this virtual directory in one of the following two ways:

- **Protect the entire Web server (recommended).** In this option you protect all virtual roots on the IIS server with RSA ACE/Agent, including any other services implemented by the front-end server. For example, you may have configured your front-end Exchange server as an access point for Outlook Mobile Access or for Outlook Web Access.

- **Protect only the Exchange ActiveSync virtual directories.** In this option, you configure the RSA ACE/Agent so that only Exchange ActiveSync is protected by SecurID. Use this option if you intend to enable additional service, such as Outlook Web Access and Outlook Mobile Access, on the same server without protecting those services with SecurID.

By default, the ACE/Agent is configured to protect the entire Web server. You can use the following procedure to verify this configuration.

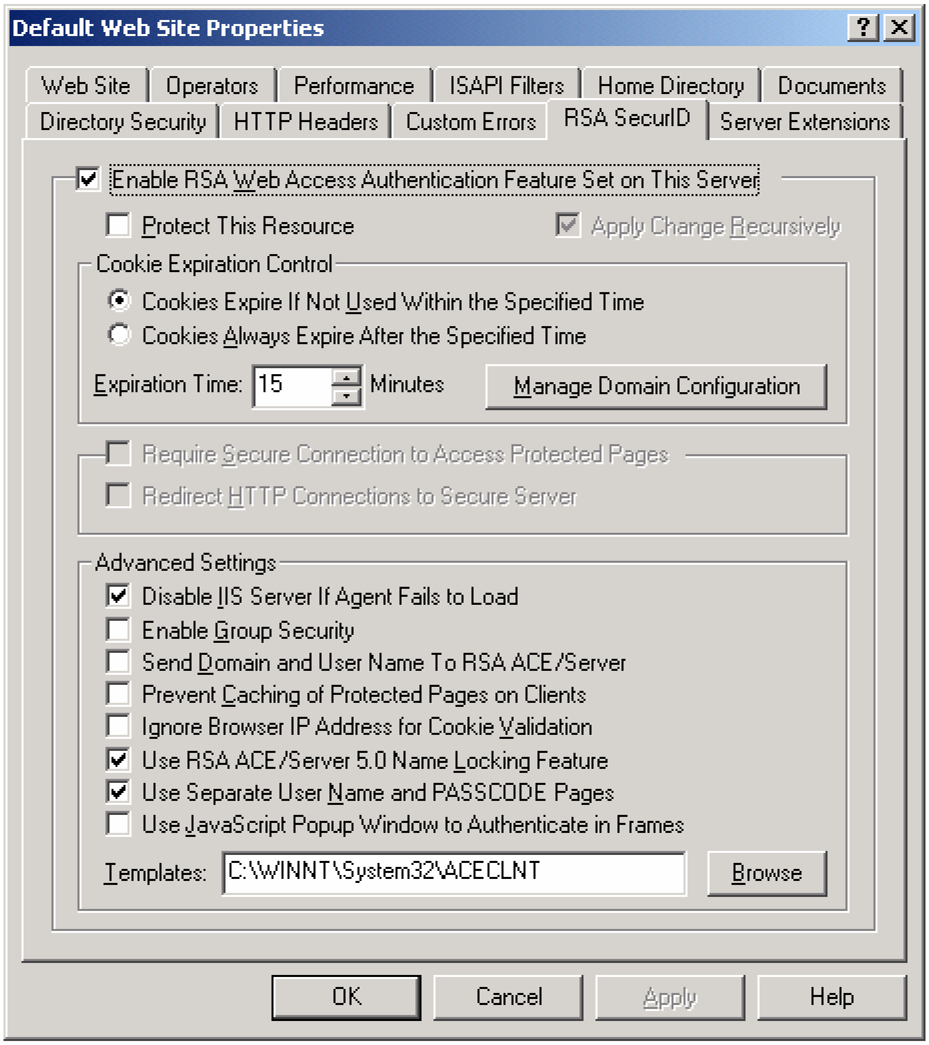
1. In the Internet Information Services snap-in for MMC, right-click the default Web server and select **Properties.**



Internet Information Services
- * ps060
  - Default Web Site
    - Scripts
    - IISHelp
    - IISAdmin
    - IISSamples
    - MSADC
    - _vti_bin
    - Printers
    - Public
    - Exchange
    - Exadmin
    - OMA
    - Microsoft-Server-ActiveSync
    - ExchWeb
    - TestAS
    - WebID
    - aspnet_client
    - images
    - _private

Name	Path
Scripts	c:\inetpub\scripts
IISHelp	c:\winnt\help\iishelp
IISAdmin	C:\WINNT\System32\inetsrv\iisadmin
IISSamples	c:\inetpub\iissamples
MSADC	c:\program files\common files\system\msadc
_vti_bin	C:\Program Files\Common Files\Microsoft Shared
Printers	C:\WINNT\web\printers
Public	\\.\BackOfficeStorage\odyssey.com\Public Folde
Exchange	\\.\BackOfficeStorage\odyssey.com\MBX
Exadmin	\\.\BackOfficeStorage
OMA	C:\Program Files\Exchsrvr\OMA\Browse
Microsoft-Server-...	C:\Program Files\Exchsrvr\OMA\Sync
ExchWeb	C:\Program Files\Exchsrvr\ExchWeb
TestAS	C:\Program Files\Exchsrvr\bin\TestAS
WebID	C:\WINNT\System32\ACECLNT\WebID
aspnet_client	
images	
_private	
_vti_cnf	
_vti_log	

2. Click the **RSA SecurID** tab and verify that the **Protect This Resource** box is selected.



☑ Enable RSA Web Access Authentication Feature Set on This Server

□ Protect This Resource ☑ Apply Change Recursively

Cookie Expiration Control

● Cookies Expire If Not Used Within the Specified Time

○ Cookies Always Expire After the Specified Time

Expiration Time: 15 Minutes

□ Require Secure Connection to Access Protected Pages

□ Redirect HTTP Connections to Secure Server

Advanced Settings

☑ Disable IIS Server If Agent Fails to Load

□ Enable Group Security

□ Send Domain and User Name To RSA ACE/Server

□ Prevent Caching of Protected Pages on Clients

□ Ignore Browser IP Address for Cookie Validation

☑ Use RSA ACE/Server 5.0 Name Locking Feature

☑ Use Separate User Name and PASSCODE Pages

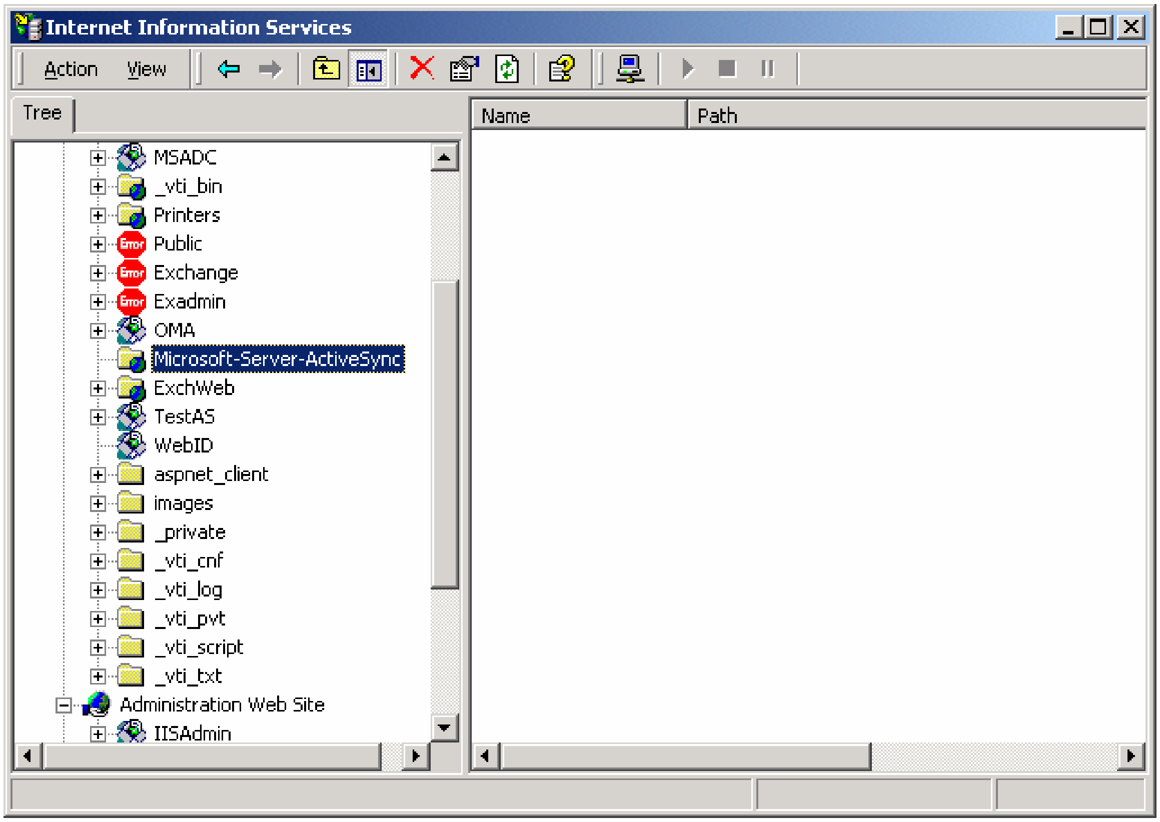
□ Use JavaScript Popup Window to Authenticate in Frames

Templates: C:\WINNT\System32\ACECLNT

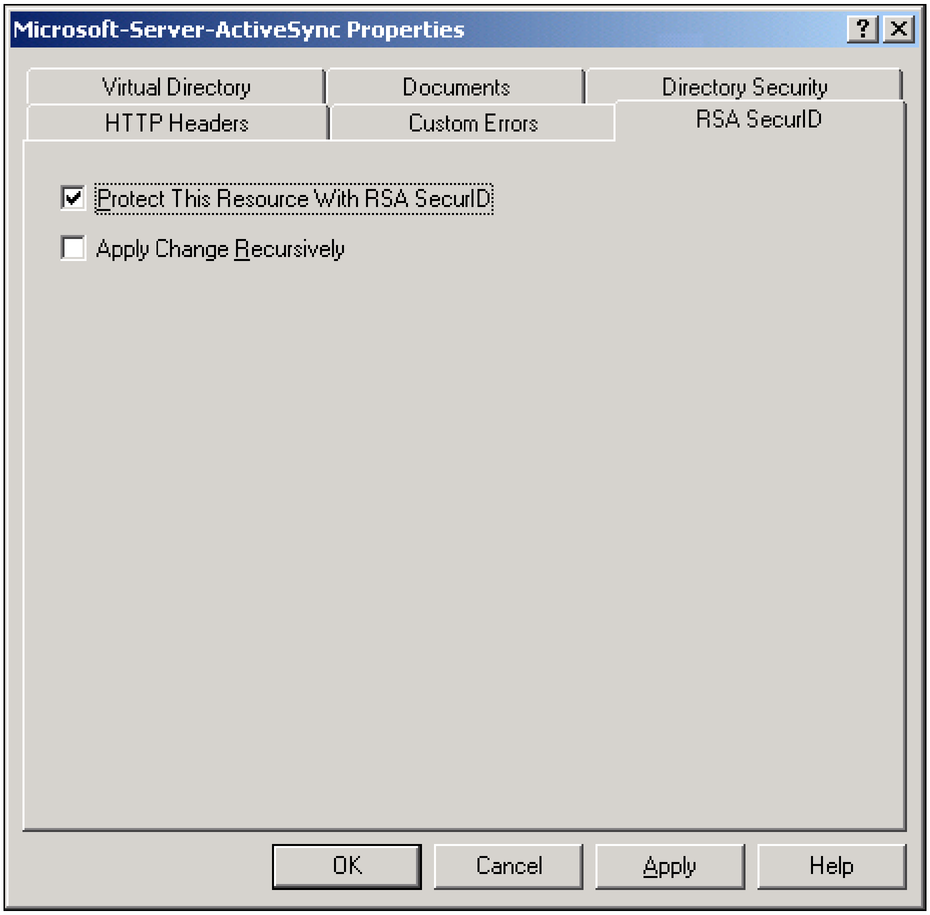
To limit SecurID Authentication to the Microsoft-Exchange-ActiveSync virtual directory:

1. To disable server-wide protection, in the IIS snap-in, right-click the default Web server, and then click **Properties.**
2. Click the **RSA SecurID** tab and then clear the **Protect This Resource** check box. (This step endures that RSA SecurID is not enabled for the entire server, but rather only for the virtual roots that you specify.)

3. To enable protection for the virtual directories, in the IIS snap-in, right-click the Microsoft-Server-ActiveSync virtual directory and then click **Properties**.



4. Select the **RSA SecurID** tab and then select the **Protect This Resource** check box.


Microsoft-Server-ActiveSync Properties

☑ Protect This Resource With RSA SecurID

□ Apply Change Recursively

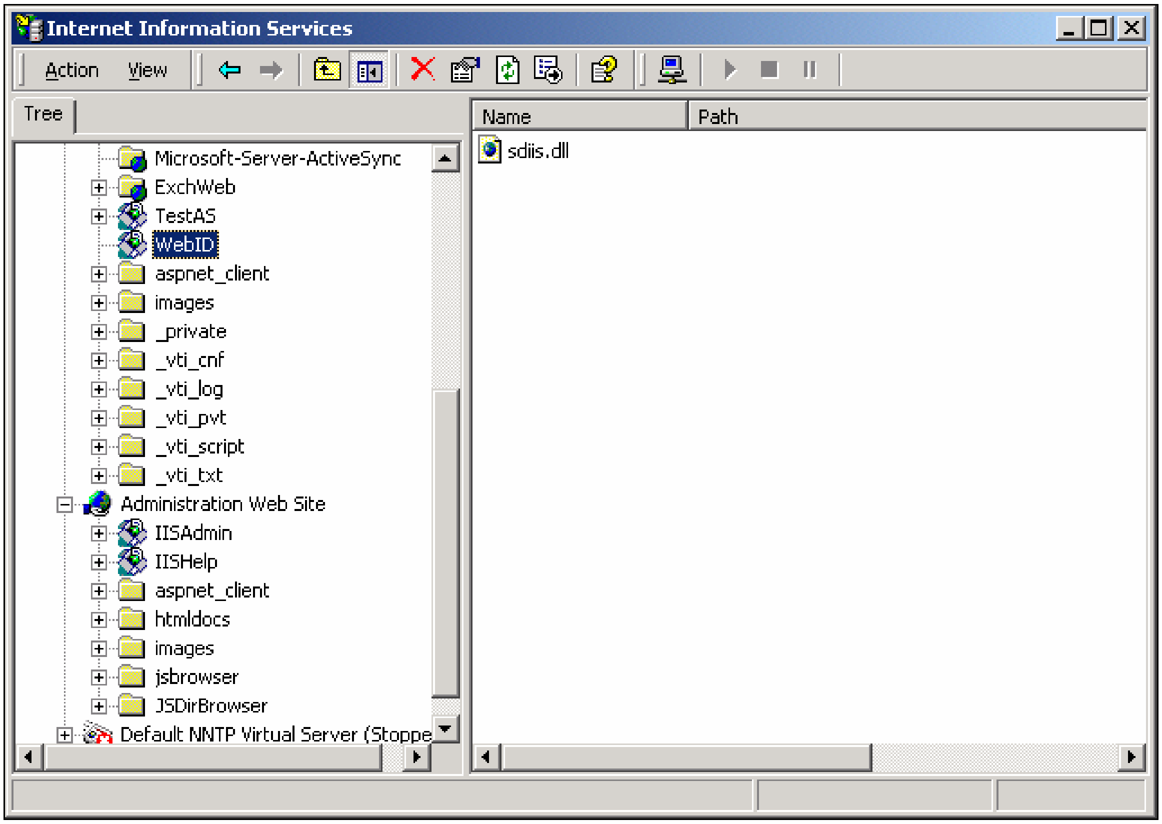
-Note- If the check box is selected and shaded, this means that the virtual directory is inheriting its setting from the parent directory. Inspect the properties for the parent directory and clear the **Protect This Resource** check box if you do not want the parent directory to be protected. Then, return to the child directory and make sure the check box is selected.

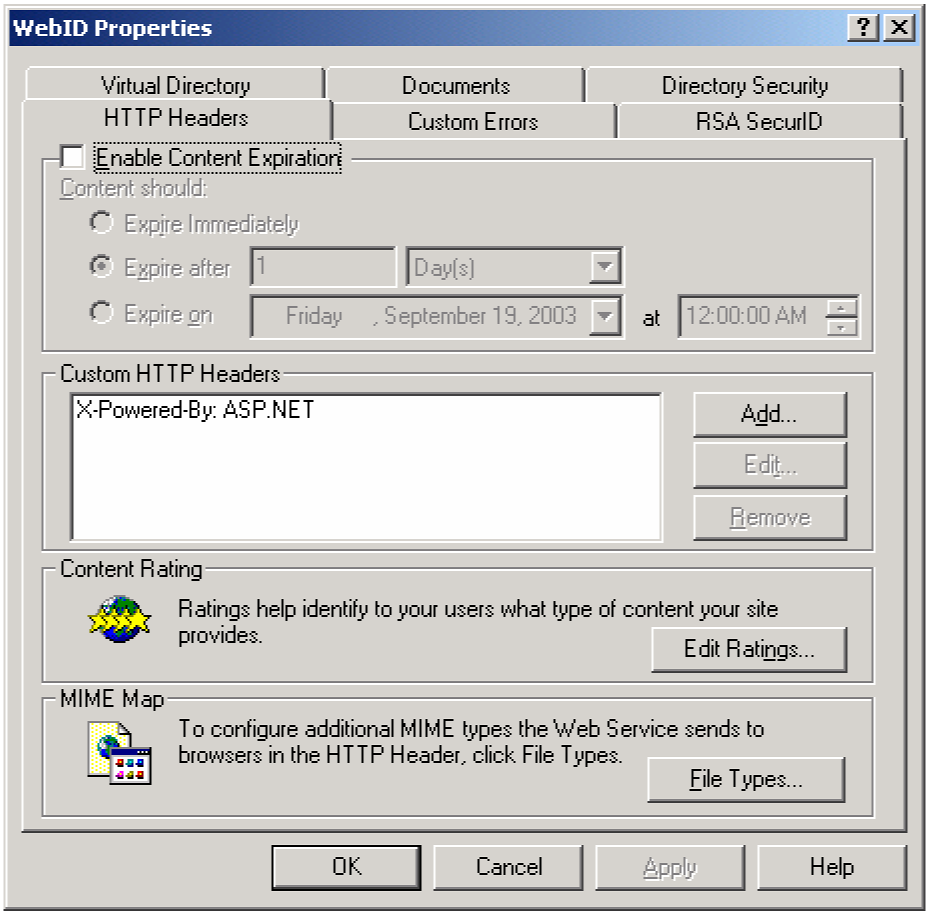
B. Customizing the HTTP Response Header for Devices

The ActiveSync client on the Microsoft Windows Mobile device must be able to distinguish between RSA SecurID authentication and Exchange ActiveSync responses. To enable this capability, you need to configure custom HTTP response headers on the WebID virtual root that contains the HTML forms configured by RSA ACE/Agent.

To configure custom HTTP responses for devices:

1. Using the IIS snap-in for MMC, locate the **WebID** virtual directory on the Exchange server. This is the virtual directory created by SecurID that contains all of the SecurID authentication forms and responses. Right click the icon and choose **Properties** to open the properties for this virtual directory.





□ Enable Content Expiration

Content should:

○ Expire Immediately

● Expire after 1 Day(s)

○ Expire on Friday , September 19, 2003 at 12:00:00 AM

Custom HTTP Headers

X-Powered-By: ASP.NET

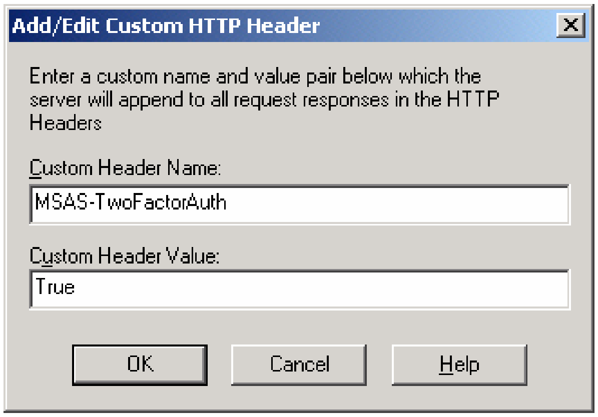
Content Rating

Ratings help identify to your users what type of content your site provides.

MIME Map

To configure additional MIME types the Web Service sends to browsers in the HTTP Header, click File Types.

2. Click the HTTP Headers tab, click the Add button and then enter the following header information. Click OK to save each addition.

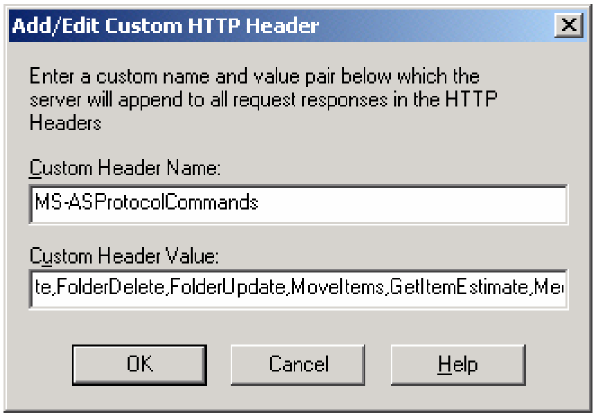


Add/Edit Custom HTTP Header

Enter a custom name and value pair below which the server will append to all request responses in the HTTP Headers

Custom Header Name: MSAS-TwoFactorAuth

Custom Header Value: True



Add/Edit Custom HTTP Header

Enter a custom name and value pair below which the server will append to all request responses in the HTTP Headers

Custom Header Name: MS-ASProtocolCommands

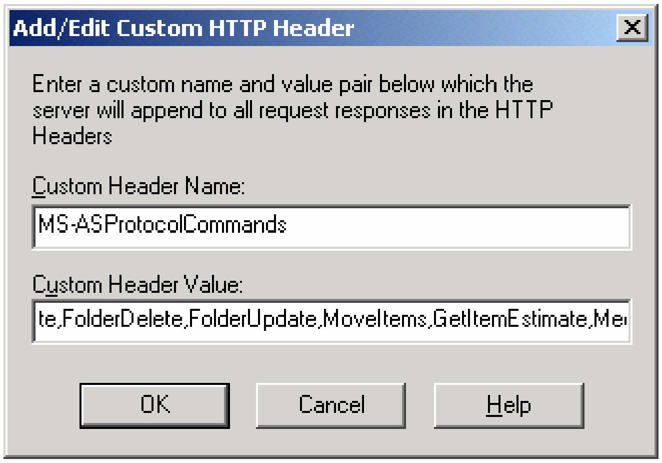
Custom Header Value: te,FolderDelete,FolderUpdate,MoveItems,GetItemEstimate,Me

-Note- The following values are case-sensitive and should be entered on one line.

Custom Header Name: MSAS-TwoFactorAuth
Custom Header Value: True

Custom Header Name: MS-ASProtocolVersions
Custom Header Value: 1.0,2.0

Custom Header Name: MS-ASProtocolCommands
Custom Header Value:
Sync,SendMail,SmartForward,SmartReply,GetAttachment,GetHierarchy,CreateCollection,DeleteCollection,MoveCollection,FolderSync,FolderCreate,FolderDelete,FolderUpdate,MoveItems,GetItemEstimate,MeetingResponse

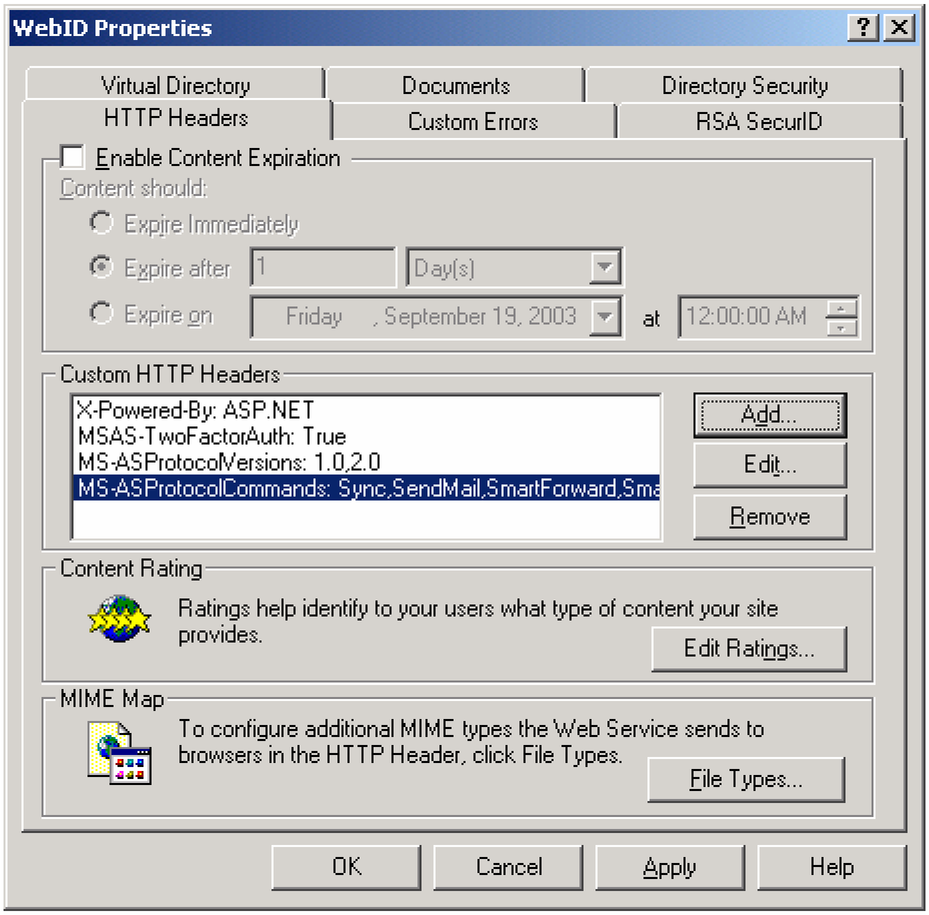


Add/Edit Custom HTTP Header

Enter a custom name and value pair below which the server will append to all request responses in the HTTP Headers

Custom Header Name: MS-ASProtocolCommands

Custom Header Value: te,FolderDelete,FolderUpdate,MoveItems,GetItemEstimate,Me



☐ Enable Content Expiration

Content should:

○ Expire Immediately

● Expire after 1 Day(s)

○ Expire on Friday , September 19, 2003 at 12:00:00 AM

Custom HTTP Headers

X-Powered-By: ASP.NET
MSAS-TwoFactorAuth: True
MS-ASProtocolVersions: 1.0,2.0
MS-ASProtocolCommands: Sync,SendMail,SmartForward,Sma

Content Rating

Ratings help identify to your users what type of content your site provides.

MIME Map

To configure additional MIME types the Web Service sends to browsers in the HTTP Header, click File Types.

3. Click OK to save your changes.

C. Install SecurID screens (Optional)

There are specially formatted SecurID HTML forms designed to deliver a better user experience on Pocket PC and SmartPhones. To use the alternative screens you simply need to copy the .HTM files to the ACECLNT folder installed with the ACE/Server.

1. Download the MS_activsync_Template.zip file from ftp.rsasecurity.com/pub/partner_engineering/SecurID/Microsoft/MS_activsync_Template.zip.
2. In Windows Explorer, navigate to the ACECLNT folder. This is located in the SYSTEM32 folder in your Windows folder. (Note that SecurID can be customized to change the location of the templates folder. Verify the location of your templates folder, as follows: In the IIS snap-in, locate the icon that represents the top-level IIS server on which Nexus is installed. Right-click the icon, then choose Properties. Choose the RSA SecurID tab, and then inspect the value contained in the text box labeled "Templates". This is the path where the custom templates should be installed.)
3. Create a backup of all HTM files. For instance, create a new folder in ACECLNT called “Original HTML” and copy all files of type “HTML document” into this folder.
4. Copy the new HTM files into the ACECLNT folder (this will over-write the original files).

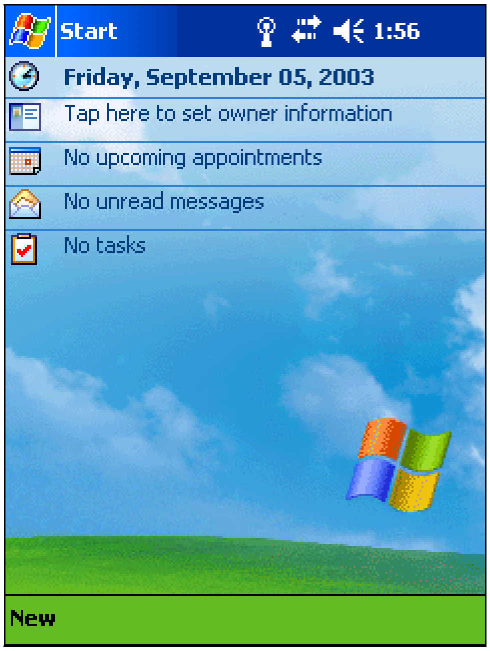
D. Set up User Accounts

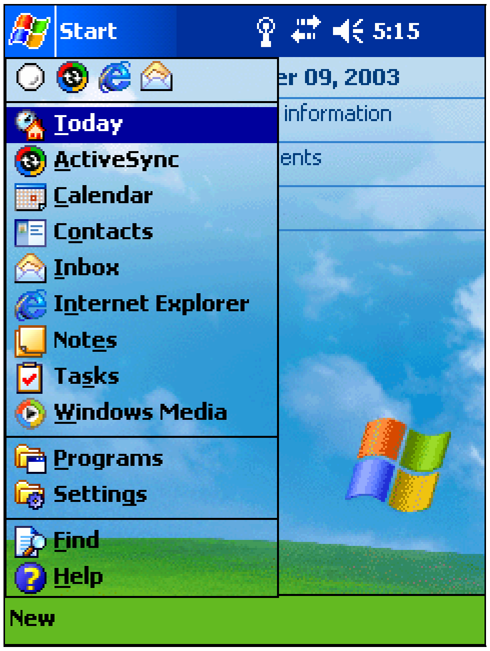
User accounts for SecurID should be set up by the Administrator as recommended by the RSA SecurID product documentation, with the following restriction:

For all users, SecurID user IDs must be selected to match the Windows account name. Exchange ActiveSync with SecurID does not function for users who have a distinct RSA user ID that does not match their Windows account name.

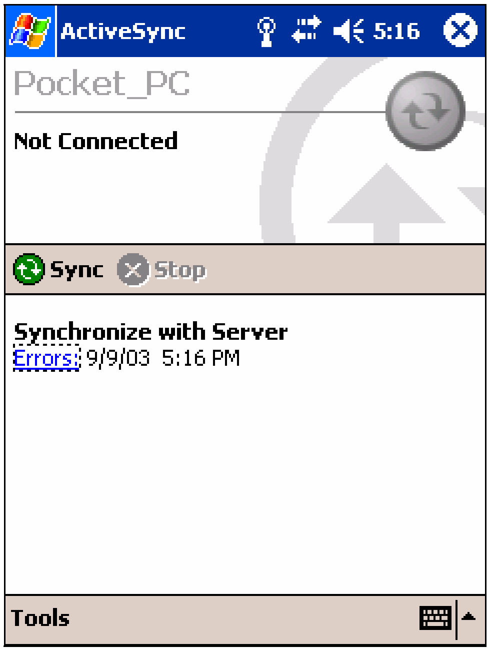
E. Device Configuration

1. From the **Today** screen on a Pocket PC 2003 device, the user taps **Start > ActiveSync**





2. Tap **Tools > Options > Server**



ActiveSync 5:16

Pocket_PC

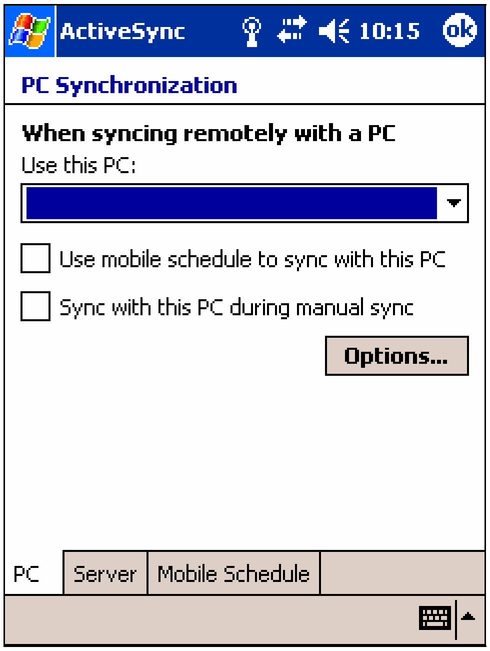
Not Connected

Sync Stop

Synchronize with Server

Errors: 9/9/03 5:16 PM

Tools



ActiveSync 10:15 ok

PC Synchronization

When syncing remotely with a PC

Use this PC:

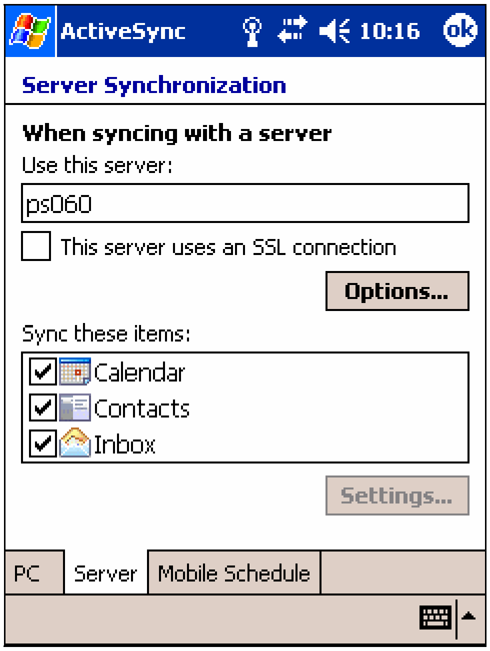
□ Use mobile schedule to sync with this PC

□ Sync with this PC during manual sync

Options...

PC | Server | Mobile Schedule

3. In the “Use this server” box enter the hostname or IP address of the Exchange 2003 server.
4. Click **Options**



ActiveSync 10:16 ok

Server Synchronization

When syncing with a server

Use this server: ps060

□ This server uses an SSL connection

Options...

Sync these items:

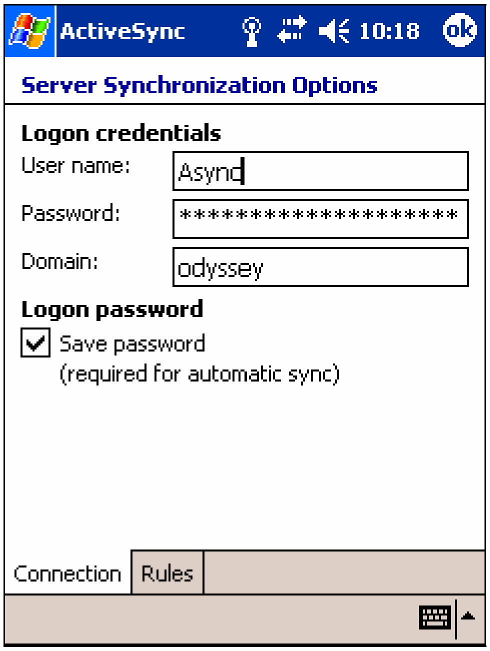
☑ Calendar

☑ Contacts

☑ Inbox

Settings...

PC | Server | Mobile Schedule



ActiveSync 10:18 ok

Server Synchronization Options

Logon credentials

User name: Async

Password: *******************

Domain: odyssey

Logon password

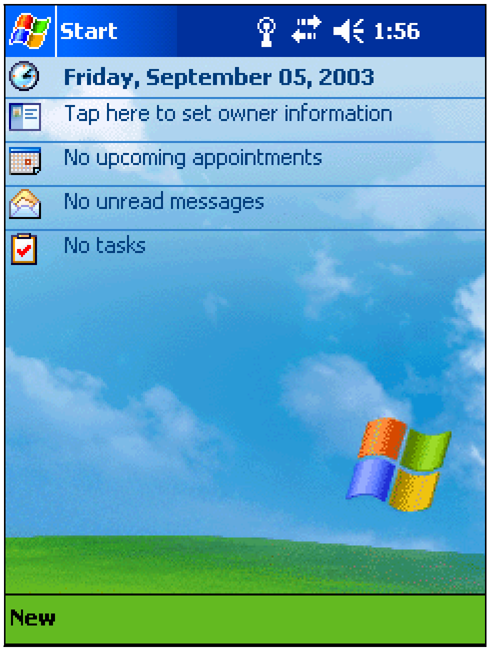
☑ Save password (required for automatic sync)

Connection | Rules

1. Enter Username and Password in the appropriate box. Checking the box to save password will store the password on the PocketPC2003/SmartPhone device.
2. Rules for ActiveSync can be configured by tapping the Rules tab.
3. Tap **OK** to save your changes.

F. Product Operation

1. From the **Today** screen on a Pocket PC 2003 or SmartPhone device, the user taps **Start > ActiveSync**



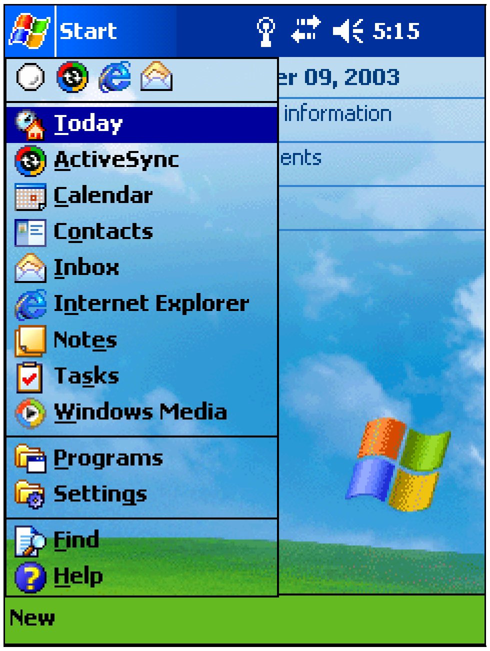
Friday, September 05, 2003

Tap here to set owner information

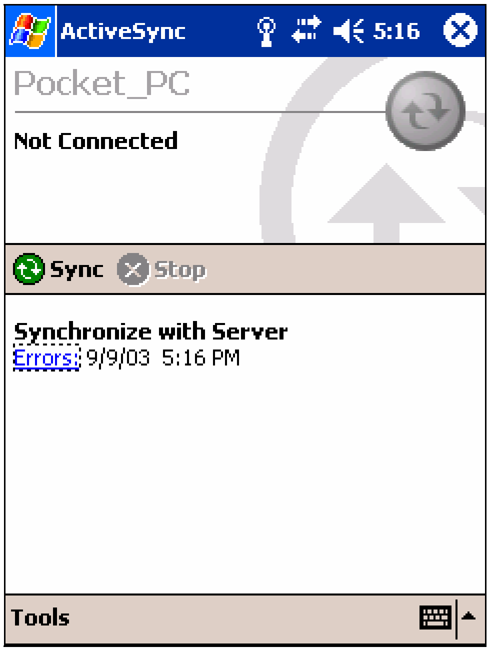
No upcoming appointments

No unread messages

No tasks



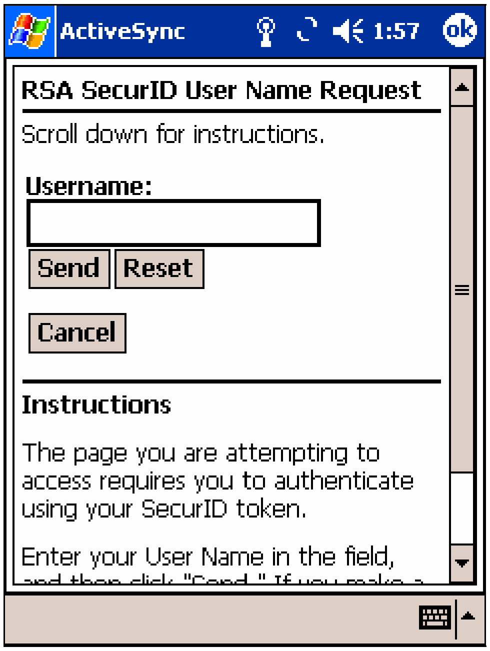
2. To synchronize with the Exchange 2003 server, tab **Sync.**



Pocket_PC

Not Connected

Synchronize with Server
Errors: 9/9/03 5:16 PM



RSA SecurID User Name Request

Scroll down for instructions.

Username:

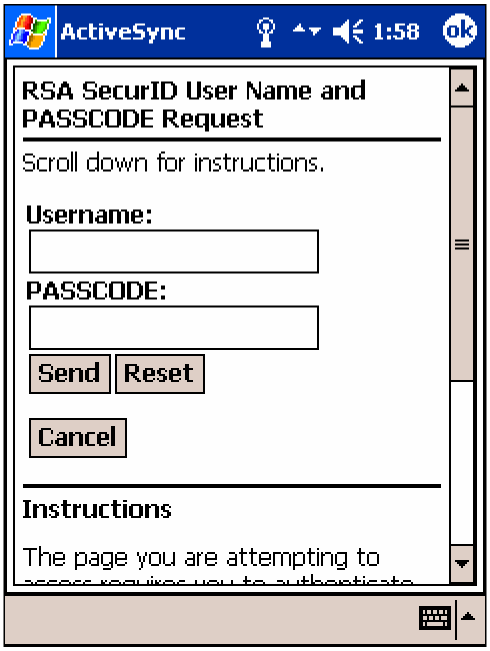
Instructions

The page you are attempting to access requires you to authenticate using your SecurID token.

Enter your User Name in the field, and then click "Send." If you make a

3. Enter your username when prompted and click Send.

4. You will be prompted for your Username and PASSCODE.
5. Enter the appropriate information and click Send



RSA SecurID User Name and PASSCODE Request

Scroll down for instructions.

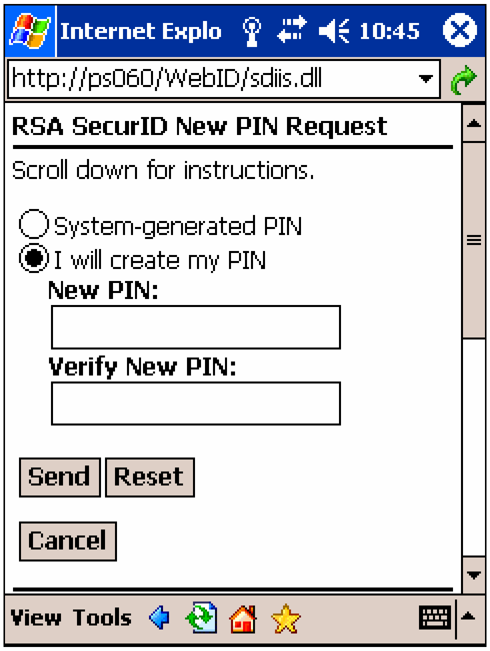
Username:

PASSCODE:

Instructions

The page you are attempting to

6. If this is the first time you are authenticating, you will be prompted for a new PIN.



http://ps060/WebID/sdiis.dll

RSA SecurID New PIN Request

Scroll down for instructions.

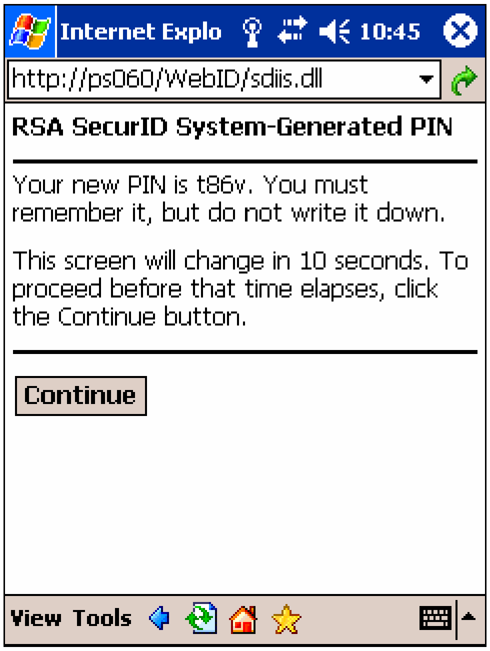
○ System-generated PIN
● I will create my PIN

New PIN:

Verify New PIN:

7. You can choose to create your own PIN or accept one generated by the ACE/Server.

System generated PIN

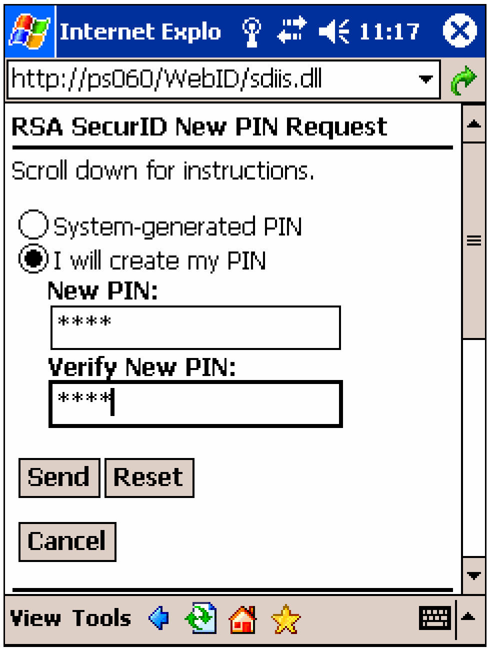


RSA SecurID System-Generated PIN

Your new PIN is t86v. You must remember it, but do not write it down.

This screen will change in 10 seconds. To proceed before that time elapses, click the Continue button.

User created PIN



RSA SecurID New PIN Request

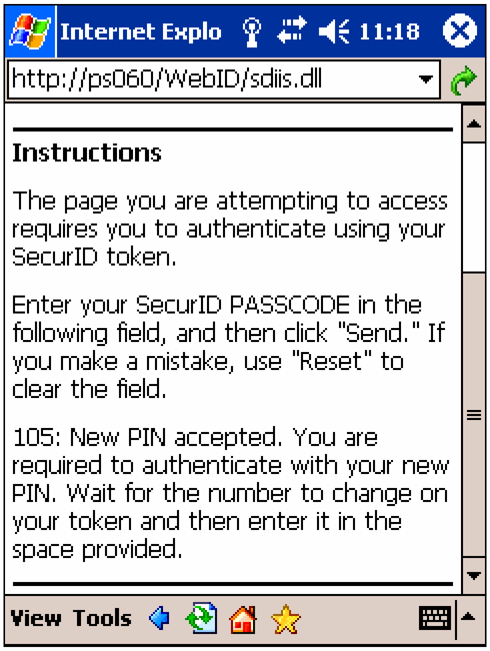
Scroll down for instructions.

○ System-generated PIN
● I will create my PIN

New PIN: ****

Verify New PIN: ****

New PIN accepted



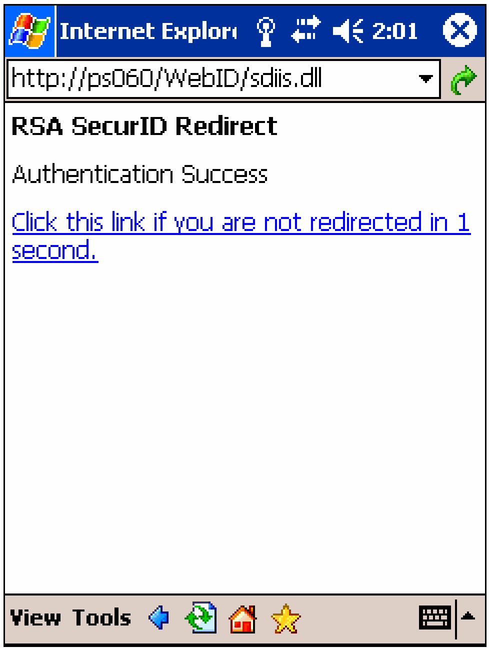
Instructions

The page you are attempting to access requires you to authenticate using your SecurID token.

Enter your SecurID PASSCODE in the following field, and then click "Send." If you make a mistake, use "Reset" to clear the field.

105: New PIN accepted. You are required to authenticate with your new PIN. Wait for the number to change on your token and then enter it in the space provided.

Once you have successfully authenticated with the ACE/Server, ActiveSync completes synchronization.

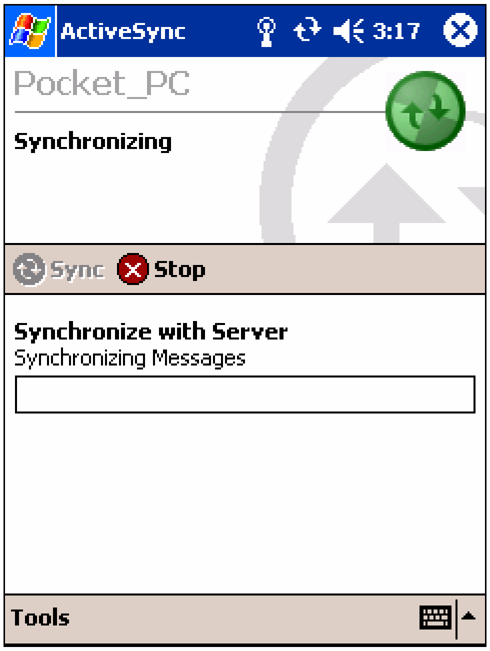


http://ps060/WebID/sdiis.dll

RSA SecurID Redirect

Authentication Success

Click this link if you are not redirected in 1 second.

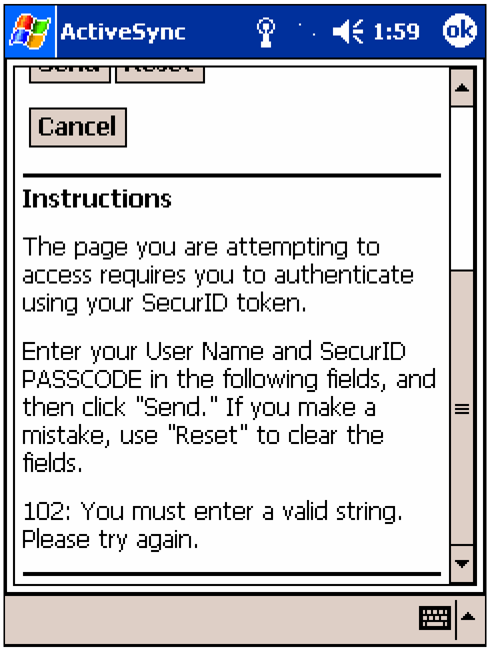


Pocket_PC

Synchronizing

Synchronize with Server
Synchronizing Messages

Access denied



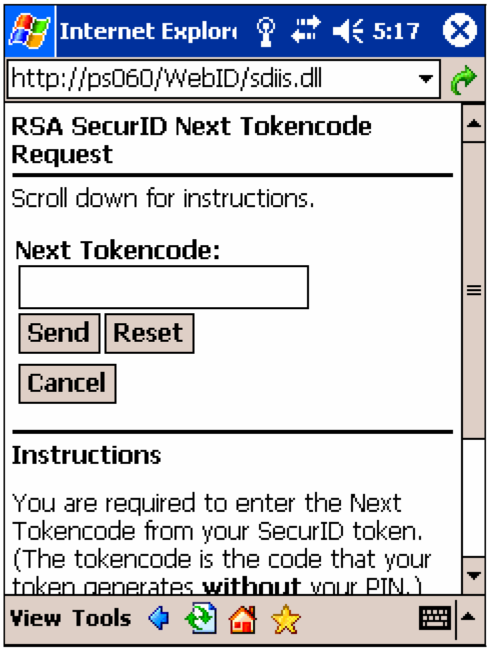
Instructions

The page you are attempting to access requires you to authenticate using your SecurID token.

Enter your User Name and SecurID PASSCODE in the following fields, and then click "Send." If you make a mistake, use "Reset" to clear the fields.

102: You must enter a valid string. Please try again.

Next TOKENCODE



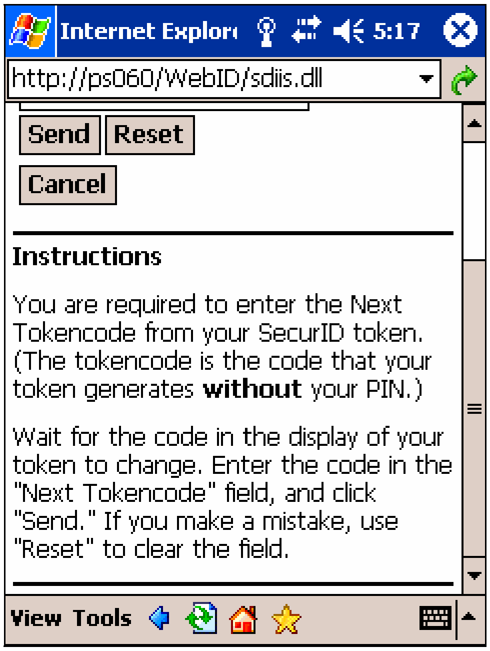
RSA SecurID Next Tokencode Request

Scroll down for instructions.

Next Tokencode:

Instructions

You are required to enter the Next Tokencode from your SecurID token. (The tokencode is the code that your token generates **without** your PIN.)



Instructions

You are required to enter the Next Tokencode from your SecurID token. (The tokencode is the code that your token generates **without** your PIN.)

Wait for the code in the display of your token to change. Enter the code in the "Next Tokencode" field, and click "Send." If you make a mistake, use "Reset" to clear the field.

7. Certification Checklist

Date Tested: September 2, 2003

Product	Tested Version
RSA ACE/Server	5.1
RSA ACE/Agent	5.03
Microsoft Exchange ActiveSync	2003
Microsoft IIS	5.0

Test	ACE	RADIUS
1st time auth. (node secret creation)	P	N/A
New PIN mode:		
System-generated		
Non-PINPAD token	P	N/A
PINPAD token	P	N/A
User-defined (4-8 alphanumeric)		
Non-PINPAD token	P	N/A
Password	P	N/A
User-defined (5-7 numeric)		
Non-PINPAD token	P	N/A
PINPAD token	P	N/A
SoftID token	P	N/A
Deny 4 digit PIN	P	N/A
Deny Alphanumeric	P	N/A
User-selectable		
Non-PINPAD token	P	N/A
PINPAD token	P	N/A
PASSCODE		
16 Digit PASSCODE	P	N/A
4 Digit Password	P	N/A
Next Tokencode mode		
Non-PINPAD token	P	N/A
PINPAD token	P	N/A
Failover	P	N/A
User Lock Test (RSA ACE Lock Function)	P	N/A
No RSA ACE/Server	P	N/A

PJV

Pass, Fail or N/A (N/A=Non-available function)

8. Known Issues

There are limitations between IIS 6 and the RSA ACE Agent that prevent a solution in an IIS 6 environment when using the RSA ACE/Agent 5.2 for IIS.

To complete the integration, please obtain the RSA ACE/Agent 5.3.1 for IIS from RSA Security Technical Support or RSA SecureCare Online. As this integration is now fully supported by the RSA ACE/Agent for IIS, additional instructions regarding the configuration are available in the product documentation.