Cisco Mobile Workforce Architecture Mobile IP Implementation Guide

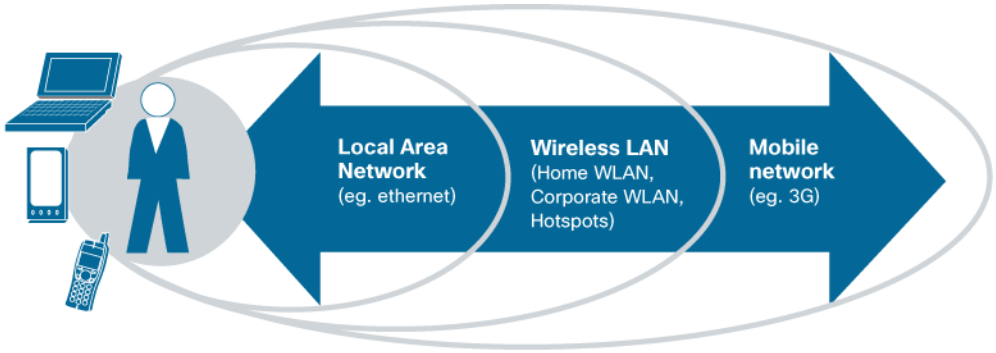
Cisco Mobile Workforce Architecture Mobile IP Overview

This document includes an overview of the benefits of using Mobile IP on mobile devices such as laptops, tablets, and smartphones. It also includes a design guide for the integration of Mobile IP into enterprise network environments.

Mobile IP provides transparent mobility for an outstanding user experience by addressing some of the most common concerns associated with mobile connectivity. Mobile IP enables transparent switching between wireless networks and maintains application sessions during gaps in coverage, offering users a LAN-like experience along with significant cost savings and increased productivity (Figure 1):

- Use of the best connection
- Improved application performance
- Interoperability

Figure 1. Mobile IP Lets You Use the Best Available Network



The Cisco® Mobile Workforce Architecture (MWA) Mobile IP solution uses the Birdstep SafeMove Mobile IP client. This document describes the process for installing SafeMove Mobile IP on mobile devices and the Cisco Unified Computing System™ Express platform. This platform consists of a Cisco Services-Ready Engine (SRE) service module, running the Cisco Services-Ready Engine Virtualization (SRE-V) server virtualization platform powered by VMware vSphere Hypervisor (ESXi), on Cisco Integrated Services Routers Generation 2 (ISR G2) hardware. This document also provides information about accessing Mobile IP home agents on routers running Cisco IOS® Software. Note that software support is provided by Birdstep Technologies directly (for more information, contact SafeMove customer support).

In addition to providing installation instructions, this document serves as a design guide for the integration of Mobile IP, running on Cisco UCS Express, into enterprise network environments.

Solution Components

Figure 2 shows the Cisco MWA Mobile IP solution architecture.

Figure 2. Mobile IP Deployment Architecture

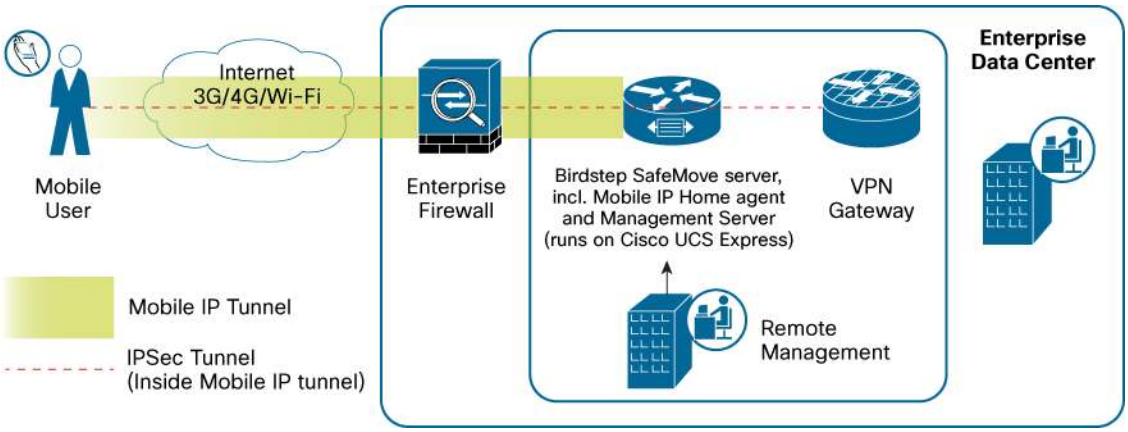


Table 1 lists the Cisco MWA Mobile IP solution components.

Table 1. Solution Components

Component	Description
Home agent	A Mobile IP home agent can run on a Cisco SRE blade or a Cisco IOS Software router (such as Cisco ISR G2) on a home network, serving as the anchor point for communication with clients, or mobile nodes. Each time the IP address of the mobile node changes, for example, because the node has changed locations, the mobile node registers the new address with the home agent, thereby allowing the home agent to forward traffic to the latest location.
VPN gateway	A VPN gateway is, for example a Cisco IOS Software router, Cisco Adaptive Security Appliance (ASA), or SafeMove Crypto IP server on the border of the organization's network. The VPN gateway strongly authenticates the mobile device and provides secure access to protected internal resources. All traffic between the client and the VPN gateway is strongly authenticated and encrypted.
Mobile IP client	A Mobile IP client software suite implements the Mobile IP and, optionally, IP Security (IPsec) protocols as well as software and software configuration management features. The Mobile IP client can be implemented in devices either with or without a VPN client, depending on the use case.
Management Server	The Management Server provides a remote management and monitoring interface for deployed SafeMove components, such as Mobile IP servers running on the Cisco UCS Express and Mobile IP clients running on Microsoft Windows devices.

Design Considerations: Using VPN

This section presents design considerations for implementing Mobile IP in the enterprise network. It also provides guidelines for integrating Cisco VPN with Mobile IP. Depending on the use case, Mobile IP can be implemented either with or without VPN.

Accessing Cloud Services with Mobile IP

With the adoption of cloud-based services, implementation of Mobile IP without VPN is becoming increasingly common. If the entire service portfolio is implemented in the cloud, Mobile IP can be used to help guarantee uninterrupted and transparent access to the cloud services. These applications often employ SSL-based security and do not necessarily require additional VPN software. Real-time collaboration applications such as presence and collaborative editing benefit the most from Mobile IP.

Use the guidelines in subsequent sections to implement Mobile IP without VPN.

Using Mobile VPN

SafeMove can be configured as a full Mobile VPN client and includes an IPsec client with optimized Mobile VPN user experience. The SafeMove IPsec client, Birdstep Crypto IP, is fully interoperable with Cisco IOS Software and Cisco ASA IPsec gateways. Refer to the Quick Installation section in the SafeMove Administration and Install Guide for instructions on implementing the full SafeMove Mobile VPN client, and refer to subsequent sections in this document for instructions on implementing the headend using Cisco IOS Software routers.

Using SafeMove Mobile IP with Cisco VPN Clients

On Microsoft Windows operating systems, you can also use SafeMove Mobile IP together with the Cisco IPsec VPN client or with the Cisco AnyConnect™ VPN client. In addition, you can use the Layer 2 Tunneling Protocol (L2TP) and IPsec client available on the Microsoft Windows OS.

Using SafeMove Mobile IP with Native VPN Clients

On Nokia smartphones, SafeMove Mobile IP integrates with the Nokia mVPN client, which is natively installed on many smartphones.

On Android devices, SafeMove Mobile IP integrates with the native Android VPN client.

In general, when you integrate any of these VPNs with SafeMove Mobile IP, no changes are required in the existing VPN infrastructure. However, certain use cases that your remote-access users are familiar with may change.

The following sections provide more information about how to configure SafeMove Mobile IP and how it may affect VPN use cases. A detailed example showing how to configure Nokia smartphones to use both SafeMove Mobile IP and Nokia mVPN is provided for reference.

Installing Cisco MWA Mobile IP

This section presents a simple deployment example and corresponding configuration options for the various components. Using the SafeMove Management Server, you can perform setup automatically simply by entering the required parameters in the web user interface.

This section describes the manual configuration steps and presents sample configuration file snippets to help you understand how to integrate Mobile IP with Cisco network infrastructure components. The Cisco configuration examples use a format similar to the one used in Cisco configuration files, as shown here:

```
! top - level comment
command
   ! sub - level comment
   Subcommand
```

Installation Overview

This section provides an overview of the installation process and describes the required and optional steps on a high level.

Steps for using the native Cisco IOS Software home agent are described in Appendix E.

Server Hardware Requirements

SafeMove Mobile IP is compatible with the Cisco ISR G2 SRE modules listed in Table 2.

Table 2. Compatible Cisco SRE Modules

Model Number	Configuration	Description
SM-SRE-700-K9 **SM-SRE-710-K9**	• Services module form factor • 1.86-GHz Intel Core 2 Duo processor (single core) • 4 GB of RAM • 500-GB hard disk	Cisco SRE services modules are designed for high-I/O inline packet services and advanced applications supported on the Cisco ISR G2 platform.
SM-SRE-900-K9 **SM-SRE-910-K9**	• Service module form factor • 1.86-GHz Intel Core 2 Duo processor (dual core) • 4 or 8 GB of RAM • 1-terabyte (TB) hard disk • RAID 1 support • Embedded hardware-based cryptography acceleration	Cisco SRE services modules are designed for applications that require the extensive processing capabilities, additional memory, and high availability supported on the Cisco ISR G2 platform.

Server Software Requirements

Cisco SRE-V Version 1.5.1 or later is recommended. Update SRE-V to this version to help ensure successful installation and operation of SafeMove server.

In addition, to help ensure compatibility with Cisco SRE-V 1.5.1, be sure that Cisco IOS Software Release 15.1(4)M or later is installed on the Cisco ISR G2. For the most up-to-date information, refer to the Release Notes for Cisco Services-Ready Engine Virtualization 1.5.

Server Software Installation Steps

The steps to install Mobile IP home agent using a Cisco SRE-V deployment follow:

1. Define the network parameters.
2. Install and configure the SRE module on the ISR G2 chassis.
3. Install and configure SRE-V on the SRE services module.
4. Install and configure a SafeMove server on SRE-V using an Open Virtualization Appliance (OVA) image.
5. Generate configurations using the SafeMove Management Server.

The following sections describe these steps in more detail.

Instructions for installing SafeMove Mobile IP on Microsoft Windows, Android, Nokia Symbian, and Windows Mobile devices are provided in the appendixes. For full SafeMove client installations, please refer to the SafeMove Administration and Install Guide.

Step 1: Define the Network Parameters

Choose and configure the following network parameters:

- Mobile IP home agent address <IP Address>: This parameter is a publicly routed address, with no Network Address Translation (NAT). Firewalls and routers must be configured so that User Datagram Protocol (UDP) port 434 on this IP address can be reached from all access networks. Likewise, to allow extended NAT and firewall traversal in access networks that block normal UDP-based Mobile IP traffic, Transmission Control Protocol (TCP) port 443 should also be opened to the public home agent address. In deployments where the Mobile IP home agent resides behind Destination NAT (DNAT), the home agent must also be allocated an address from the private address space used inside the NAT and appropriate routes and firewall rules must be set up for it.
- VPN gateway address <IP address>: This parameter may be either at a publicly routable or private address. Presuming Mobile IP is used together with VPN, appropriate routes and firewall rules must be configured so the Mobile IP home agent can forward incoming traffic to the VPN gateway and vice versa, unless the two services are co-located on the same router.
- VPN gateway address <IP address>: This parameter may be either at a publicly routable or private address. Presuming Mobile IP is used together with VPN, appropriate routes and firewall rules must be configured so the Mobile IP home agent can forward incoming traffic to the VPN gateway and vice versa, unless the two services are co-located on the same router.
- Mobile IP home address pool: The home agent allocates addresses to connected mobile nodes from a home address pool, e.g., 10.10.10.0/24. Presuming a VPN is used, traffic both to and from this subnet must be routed through the VPN gateway for encryption and decryption, respectively, incoming after it has been decapsulated by the home agent, and outgoing before it is forwarded to the home agent for encapsulation and tunneling to the mobile node clients. However, if the Mobile IP home agent performs Source NAT (SNAT) on the address pool, no additional routes need to be configured, because the addresses are never encountered outside the home agent node.
- Mobile IP security association: The following three parameters need to be set: Network Access Identifier (NAI) pattern, e.g., *@example.com; Security Parameter Index (SPI), e.g., 256 decimal, 0x100 hexadecimal; and shared secret, e.g., “CHANGEME” as ASCII text, 0x43 48 41 4e 47 45 4d 45 as hexadecimal.
- Domain Name System (DNS) servers: These servers are the DNS servers for the clients to use when connected to the Mobile IP home agent server, as well as those possibly required by the SRE-V hypervisor, depending on the configuration.
- Network Time Protocol (NTP) servers: These servers are the NTP servers required by the SRE-V hypervisor and guest instances to maintain their clocks synchronized.

Step 2: Install and Configure the SRE Module on the ISR G2 Chassis

To install the SRE service module, follow the instructions in the guide Installing Cisco Network Modules and Service Modules in Cisco Access Routers, or Installation and Configuration Guide for Cisco Services-Ready Engine Virtualization Software Release 1.5. The initial, application-independent configuration steps are described in the Cisco SRE Service Module Configuration and Installation Guide.

Step 3: Install and Configure SRE-V on the SRE Services Module

For SRE-V system installation and configuration instructions, refer to the Cisco Installation and Configuration Guide for Cisco Services-Ready Engine Virtualization Software Release 1.5 or later.

Additionally, to ensure successful OVA installation on SRE-V, NTP should be enabled, and the clock synchronized on the hypervisor. In some cases, for example, if the NTP server is given by its host name rather than IP address, a DNS server must also be configured. These settings can easily be configured using the VMware vSphere Client, downloadable from the SRE-V hypervisor. Using the vSpere Client, both parameters can be found in the Software menu under the top-level VMware-host-specific Configuration tab. The DNS and NTP settings can be found under “DNS and Routing” and “Time Configuration”, respectively.

Finally, depending on the Cisco ISR G2 configuration and network topology, new routes may need to be added on the router each time a VMware guest is added on the SRE-V hypervisor. Instructions can be found in the Cisco Installation and Configuration Guide for Cisco Services-Ready Engine Virtualization Software.

Step 4: Install and Configure a SafeMove Server on SRE-V Using an OVA Image

Selected Mobile IP components, such as the Birdstep Mobile IP server included in the SafeMove server installation, can also be operated on Cisco hardware by installing them on a guest operating system, running on top of the Cisco SRE-V hypervisor. Because SRE-V is based on VMware vSphere ESXi technology, the installation and configuration steps for both setups are essentially identical. Hence, the instructions for deploying and configuring a SafeMove VMware Appliance provided in the SafeMove administration and installation guide can be used as such. However, some additional configuration steps may have to be taken in a SRE-V environment. For example, in setups that use a Cisco VPN rather than the Birdstep Crypto IP gateway, automatically installed with the SafeMove server, the Crypto IP IPsec gateway should be disabled on the virtual machine. This task can be performed by logging in to the SafeMove server and issuing the following commands:

```
/etc/init.d/birdstecip stop
chkconfig --del birdstepcip
```

Furthermore, depending on the network configuration, some routing, firewall, and NAT settings may be required on the SafeMove server following installation. Please also note that some advanced Birdstep Mobile IP server features are disabled at installation time, and may require post-installation configuration to be enabled. Hence, it is strongly recommended that you also consult the Birdstep Mobile IP server user’s manual to familiarize yourself with the full configuration details.

Step 5: Generate Configurations Using the SafeMove Management Server

The Birdstep Management Server, installed on the SRE-V SafeMove server virtual machine, is the recommended tool for managing and monitoring all Birdstep SafeMove services, including local Mobile IP and Crypto IP servers, as well as remote Mobile IP and Crypto IP clients. For more information, consult the SafeMove installation and administration guide and the Birdstep Management Server administrator’s guide.

Configuring the Firewall and NAT

Successful deployment of SafeMove will in most circumstances require slight modification of corporate firewall rules to help ensure client connectivity. Furthermore, if NAT is employed in the network, configuration of proper address translation rules may also be required during the deployment phase.

Depending on the structure and setup of the deployed network, firewalls and NAT may be configured on any number of routers between the Internet and the virtual SafeMove server, including the SafeMove server itself.

However, selection of the nodes responsible for these tasks is outside the scope of this document. Nevertheless, the following paragraphs list the minimum requirements that SafeMove imposes on both these services.

Firewall Requirements

To allow Mobile IP traffic between the clients and server, UDP port 434 must be opened to the SafeMove server. Similarly, to enable TCP-based Mobile IP NAT and firewall traversal, TCP port 443 has to be opened. In addition, TCP port 8082 is reserved for remote management of SafeMove servers. Likewise, the Birdstep Management Server, if enabled, provides a web-based management interface on TCP port 8080. However, unlike UDP port 434 and TCP port 443, global access to TCP ports 8080 and 8082 should never be permitted unless the remote connections are properly protected by SSL/TLS, IPsec, or other such means. Alternatively, on SRE-V, SafeMove remote management can be performed using suitable graphical VMware remote management tools, such as VMware vSphere Client or Server. In such cases, remote access to ports 8080 and 8082 may be disallowed, because the SafeMove Management Server management interface may be accessed locally using these tools.

NAT Requirements

NAT is not required if public, globally routable IP addresses can be allocated both for the Mobile IP server and its home address pools, but NAT must be used if the required addresses are allocated from any of the private address spaces 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16.

For example, presuming the used address pool is 10.10.10.0/24, SNAT for this subnet is required to help ensure connectivity between mobile nodes and the Internet. The required NAT rules can most easily be set up on either the SafeMove SRE-V virtual machine or the hosting ISR G2 chassis, thereby eliminating the need for any further routing table changes on other routers in the network.

Likewise, if the Birdstep Mobile IP server uses a private address, DNAT must be configured to help ensure that Mobile IP traffic to UDP port 434 and management traffic to TCP ports 8080 or 8082 can reach the Birdstep Mobile IP server private address.

Because configuring NAT rules correctly can be challenging, the following example listing describes the required rules on the Cisco ISR G2 router hosting the SafeMove SRE-V virtual machine. In the example listing, the public IP address <Public IP Address> is configured on the outside interface of the Cisco ISR G2, rather than on the SRE-V virtual machine, while 172.16.2.33/32, reachable through Vlan1, is reserved for the virtual machine, with the Cisco ISR G2 performing DNAT and SNAT on behalf of the virtual SafeMove server. In addition, the Cisco ISR G2 performs SNAT for the entire subnet 10.10.10.0/24, used as an address pool for registered SafeMove clients. However, in scenarios where SNAT is performed by the SafeMove server, the address pool SNAT configuration may be omitted on the ISR G2.

Finally, in addition to the Mobile IP–related NAT rules, the example also illustrates how to enable direct Secure Shell (SSH) Protocol connections to the SafeMove server behind DNAT. However, because <Public IP Address>port 22 may be reserved for SSH connections to the Cisco ISR G2, SSH sessions to the SafeMove virtual machine cannot use the same port number. Therefore, <Public IP Address> port 2222 is configured for this purpose.

```
configure terminal
interface GigabitEthernet 0/0
  ! configure public IP address on IOS router
  ip address <Public IP Address> 255.255.255.0
```

```
  ! enable NAT
  ip nat outside
  exit
! (Optional: add host route to SafeMove server if prefix route isn't available)
! (ip route 172.16.2.33 255.255.255.255 Vlan1)
! add route to address pool maintained by SafeMove
ip route 10.10.10.0 255.255.255.0 Vlan1 172.16.2.33
!
! configure SNAT rule for MIP address pool
access-list 1 permit 10.10.10.0 0.0.0.255
! SNAT rule for SafeMove server to allow it to use http, ftp, scp, etc.
access-list 1 permit 17.216.2.33 0.0.0.0
ip nat inside source list 1 interface GigabitEthernet0/0 overload
!
! configure DNAT for the SRE-V guest service
!
! DNAT for MIP server
ip nat inside source static udp 172.16.2.33 434 <Public IP Address> 434
extendable
! DNAT for manager web interface
ip nat inside source static tcp 172.16.2.33 8080 <Public IP Address> 8080
extendable
! DNAT for manager remote management interface
ip nat inside source static tcp 172.16.2.33 8082 <Public IP Address> 8082
extendable
! DNAT for SSH (use port 22 for IOS, 2222 for SRE-V guest)
ip nat inside source static tcp 172.16.2.33 22 <Public IP Address> 2222
extendable
end
copy running-config startup-config
```

Appendixes

Appendix A: Client Installation on Microsoft Windows Devices

This section describes how to install the Birdstep Mobile IP client on a Microsoft Windows workstation and how to use the user interface to configure the client to connect to the home agent. Installation and manual configuration must be performed as a user with full administrator privileges. Refer to the Birdstep Mobile IP client user's manual for detailed information about installing and configuring the Birdstep Mobile IP client.

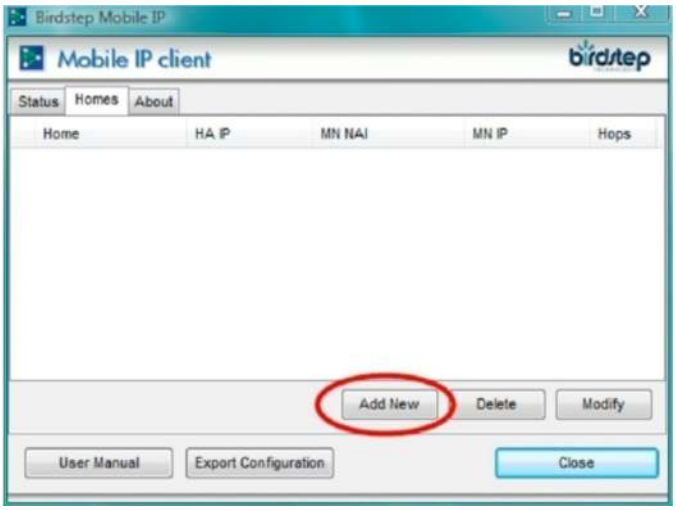
The Birdstep Mobile IP client is delivered as a Microsoft .msi package. It is installed by directly running the file: that is, by double-clicking the file in Windows Explorer.

To configure the client, you can run a .mip file generated using the configuration utility.

Alternatively, you can manually configure the client using the GUI.

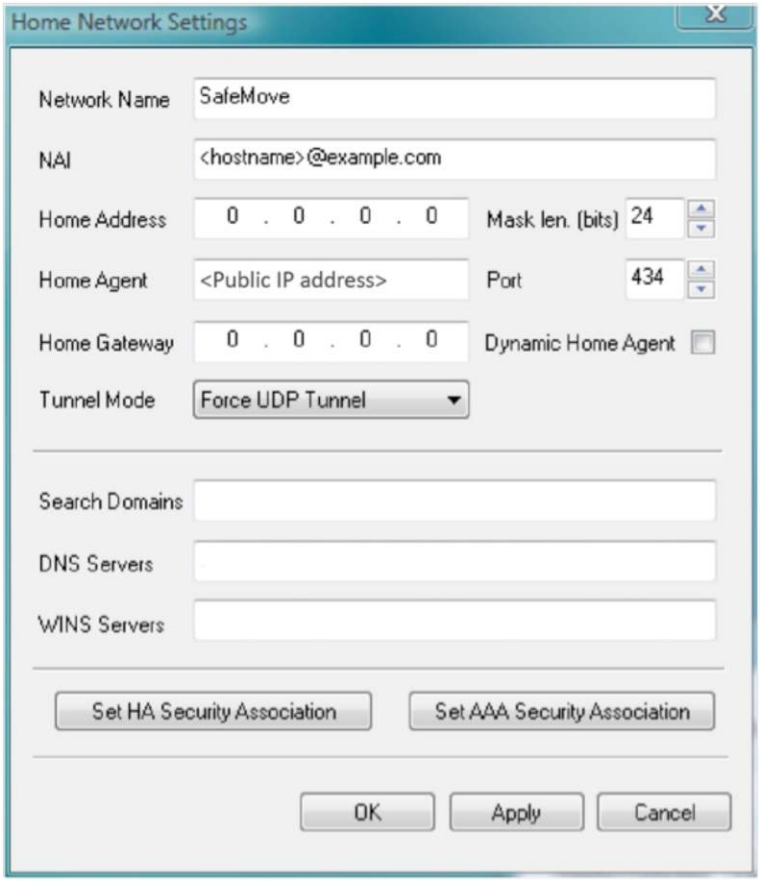
1. To manually configure the client, open the Birdstep Mobile IP GUI. Choose the Homes tab and click Add New (Figure 3).

Figure 3. On the Homes Tab, Click Add New



2. In the Home Network Settings dialog box that opens, enter the parameters as shown in Figure 4.
3. Setting the home address to 0.0.0.0 causes the home agent to allocate a free address from the pool. The client automatically replaces the <hostname> string in the NAI parameter with the Microsoft Windows computer name. Click the Set HA Security Association button to open the next dialog box.
4. In the Security Association dialog box, enter the parameters as shown in Figure 5. Then click OK in this dialog box and again in the Home Network Settings dialog box.
5. Select the Status tab and click New to create a Mobile IP profile as shown in Figure 6. Double-click the home agent configured in the previous step to add it to the profile. It should appear in the In Profile list. Set the registration lifetime to 600 seconds.
6. To export the configuration to a file, click the Export Configuration button on the Status tab in the Birdstep Mobile IP GUI. This step produces a file (.mip) that can be run on other devices to install the same configuration.

Figure 4. Home Agent Settings



Running L2TP and IPsec over Mobile IP

If you need to run L2TP and IPsec over Mobile IP on Microsoft Windows, you need to make a setting in the Microsoft Windows registry. The setting can be made by importing a registry file l2tp.reg after installing and configuring Birdstep Mobile IP. The setting will take effect after you reboot or after you restart the Birdstep Mobile IP service.

Figure 5. Security Association Settings

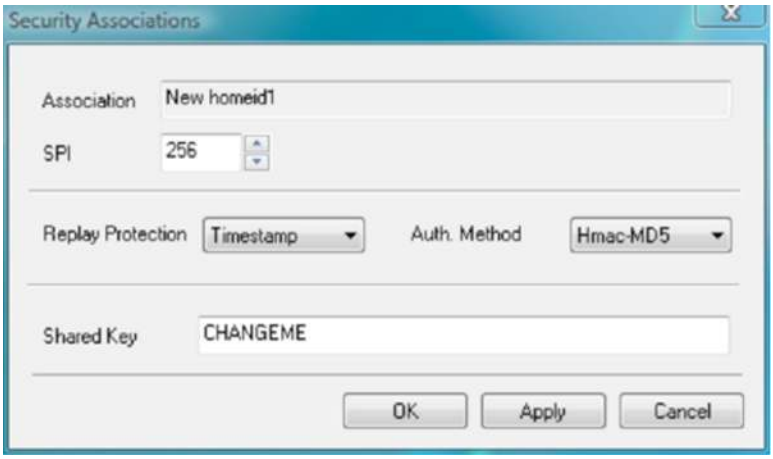
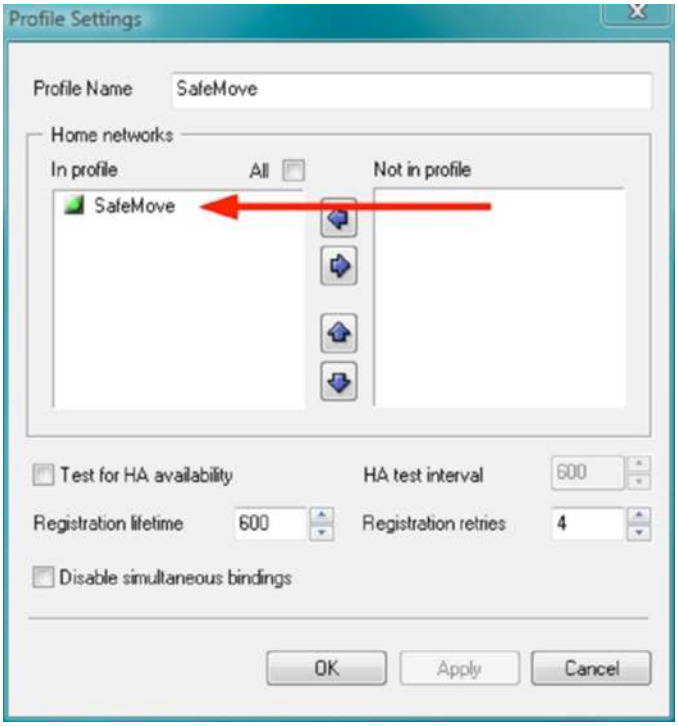


Figure 6. Mobile IP Profile Settings



Appendix B: Client Configuration on Android Devices

On Android devices, you can configure SafeMove Mobile IP with either an .xml or .mip configuration file. The exact method depends on how the SafeMove Mobile IP client was included in the Android system image. However, if you need to change the configuration on your Android device, you need to do the following:

1. Use your system image to verify the exact location of the Mobile IP configuration.
2. Open the adb shell on a rooted device.
3. Replace the current configuration with the one generated with the SafeMove configuration utility.

Note: Make sure that you make a backup copy of your existing Mobile IP configuration.

4. Verify your Mobile IP connectivity status using the Mobile IP GUI (Figure 7).

Figure 7. Mobile IP User Interface on Android

Appendix C: Client Installation on Nokia Symbian Smartphones

This section provides step-by-step instructions for installing and configuring SafeMove on supported Nokia phones (Figure 8). If you use Mobile IP without a VPN, skip the steps relating to Nokia mVPN, IPsec, and .vpn.

On Nokia devices, the installation package is called SmartConnect, and the application is listed as SC on the Nokia S60 menus.

Figure 8. SafeMove on a Nokia Device

This section provides step-by-step instructions for manually installing SafeMove on Nokia smartphones.

Before starting, make sure that you have the required files available:

- smartconnect-<version>.sis
- safemove.dbf
- safemove.vpn
- <user>.p12

Most new phones ship with the VPN client preinstalled. You can determine whether it is by opening Tools > Settings > Connection on the phone. If the VPN client is installed, a VPN entry will appear in this list. Otherwise, you need to get the VPN installation package from Nokia: mVPN-<version>.sisx.

The procedure for configuring SafeMove differs between Nokia software platform versions. You therefore need to determine which version of the supported S60 software platform is used on the phone model. This information is available in the technical documentation for the phone.

The supported software platforms follow:

- S60 3rd Edition (example phones: E65)
- S60 3rd Edition Feature Pack 1 (example phones: E51, E63, E71, and E90)
- S60 3rd Edition Feature Pack 2 (example phones: E52, E55, E72, and E75)
- S60 5th Edition (example phones: N97 and N97mini)

In this appendix, information related to S60 3rd Edition and 3rd Edition Feature Pack 1 is identified with FP1. Information for a phone with software platform S60 3rd Edition Feature Pack 2 or 5th Edition is identified with FP2.

All additions, imports, and execution during the installation is performed using the File Manager application on the phone. To open the File Manager, choose Menu > Office > File Mgr. To open or run a file, select the file and choose Options > Open in the menu.

After transferring the files to the mobile phone, you perform the subsequent steps on the mobile phone.

1. Transfer the required files to the phone. For example, you can use the location c:\data\.
2. Open the File Manager on the mobile phone by choosing Menu > Office > File Mgr. The files should be in the directory to which you transferred them. If you used the c:\data\ location, you should see the files in the root of the phone File Manager.
3. Add the user certificate to the phone certificate store by choosing Options > Open for the PKCS#12 (.p12 file). When prompted, enter the password you received along with the certificate file.
4. If prompted to do so, create a key store password (with a minimum of six: for example 123456). This password is needed when establishing the VPN connection. If the key store has been created already, use the password used when initially creating it. Select the VPN option when prompted for the purpose of the imported certificate.
5. If VPN is not already installed on the phone, install the Nokia mVPN-client and follow the instructions on the phone display.
6. Install SmartConnect and follow the instructions on the phone display.

7. Reboot the phone at the end of the installation. You will receive a notification when the installation is complete. You must reboot the phone because SafeMove for Nokia smartphones will not work if the phone is not rebooted.
8. Import the VPN policy .vpn and follow the instructions on the phone display.
9. Import the .dbf for SmartConnect and follow the instructions on the phone display.
10. FP1: Create a new VPN access point by choosing Menu > Tools > Settings > VPN > Options > New Access Point.
    - Connection name: SafeMove
    - VPN policy: Choose the VPN policy from the list
    - Internet access point (IAP): SafeMove Mobile IP
    - Back

    Edit the VPN policy in the intranet destination to point to the SafeMove Mobile IP IAP by choosing Menu > Control Panel > Settings > Connection > Destinations > Intranet > SafeMove Policy > Internet Access Point.
11. Add connections (Wi-Fi and 3G) to SmartConnect. In FP1, SmartConnect can be found by choosing Menu > Installations > SC. In FP2, SmartConnect can be found by choosing Menu > Applications > SC. Choose SafeMove MIP and then Options > Add Connections and choose the access points you want to use. Note that the Wi-Fi access points must be above the 3G access point to make the prioritization work correctly.
12. If no Wi-Fi access points are listed, you may search for them manually using the “Scan Wi-Fi” function. Then, when a new access point is defined, you will be prompted whether you want to add the access point to a connection group.
13. If you want to, you can define the SafeMove access point so that it starts automatically when you open any connection. In the web browser, choose Web > Options > Settings > General > Access point. You can also have the browser always prompt for the access point by setting the Always Ask option for the access point. When an application prompts for the access point to use, choose SafeMove from the list. This approach helps ensure that the optimal connection is always selected.

Appendix D: Client Installation on Microsoft Windows Mobile Devices

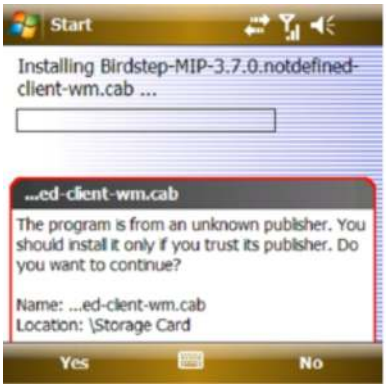
You can use the SafeMove Configuration Utility to create the configuration, or you can export the configuration from a Microsoft Windows computer.

To do the latter, on the Status tab in the Birdstep Mobile IP GUI (in Microsoft Windows), click the Export Configuration button. This step produces a file (.mip) that can be transferred to a Microsoft Windows Mobile device.

After you have the configuration, you can proceed to install the client and then to actually configure the device.

1. Move the installation files, safemove_codesign.cab and Birdstep-MIP-X.Y.Z-client-wm.cab, to the device and click the files in the File Explorer in this same order.
2. During the installation of safemove¬_codesign.cab, you may encounter a query about trusting the software publisher (Figure 9). Click Yes.

Figure 9. Trusting the Software Publisher



3. If you are asked for the location for installing Mobile IP (Figure 10), choose Device.

Figure 10. Choosing the Location for the Mobile IP Installation

4. After installing Birdstep Mobile IP, soft reset the device when prompted.
5. After the soft reset completes, run the configuration file (.mip) using the File Manager on the device. This step will import and apply the configuration.

Appendix E: Configuring Home Agent on Cisco IOS Software

To run a Mobile IP home agent on Cisco IOS Software, you will need a license for either Advanced IP services (advipservices) or Advanced Enterprise services (adventerprise).

This section describes the most basic Cisco IOS Software command-line interface (CLI) implementation of the sample setup.

Note that SafeMove relies on special extensions in the Birdstep Mobile IP home agent to implement some SafeMove features. Some examples of features that cannot be implemented using Cisco IOS Software home agent are listed here:

- Internal network detection
- Mobile device battery-life optimizations
- Simultaneous bindings for optimizing handover performance

Because of these extensions, use of a SafeMove Mobile IP home agent running on a Cisco SRE-V virtual machine is recommended over running SafeMove Mobile IP on a native Cisco IOS Software home agent.

When configuring a Cisco device, the whole command needs to be entered on a single line.

```
! enable mobile ip on the router
router mobile

! Mobile IP Home Address pool
! The subnet network and broadcast addresses are not
! included in the pool and 10.10.10.1 is the HAs address on
! the virtual network.
ip local pool safemove-mip-pool 10.10.10.2 10.10.10.254

! make the home-agent accept nat traversal
ip mobile home-agent nat traversal forced accept
! make the home-agent accept reverse tunneling
ip mobile home-agent reverse-tunnel private-address

ip mobile virtual-network 10.10.10.0 255.255.255.0 address 10.10.10.1

! SA and address mapping information
ip mobile host nai @example.com address pool local safemove-mip-pool virtual-
network 10.10.10.0 255.255.255.0
ip mobile secure host nai @example.com spi decimal 256 key hex 4348414e47454d45
algorithm hmac-md5
```

To verify or troubleshoot the Mobile IP home agent function on Cisco IOS Software, enable logging to the terminal as follows:

```
terminal monitor
debug ip mobile host
```

To view the status of mobile clients, the following commands are useful:

```
show ip mobile bindings
show ip mobile host
```

Appendix F: References

- SafeMove administration and installation guide: Available on the SafeMove CD-DVD
- Installing Cisco Network Modules and Service Modules in Cisco Access Routers: http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/InstNetM.html
- Cisco SRE Service Module Configuration and Installation Guide: http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/ism-sm-sre.html
- Release Notes for Cisco Services-Ready Engine Virtualization 1.5: http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/sre_v/1.5/release/notes/sre_v_release.html
- Installation and Configuration Guide for Cisco Services-Ready Engine Virtualization Software Release 1.5: http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/sre_v/1.5/user/guide/sre_v.html
- Birdstep Mobile IP server administrator's guide: Available on the SafeMove CD-DVD
- SmartConnect User Guide: Available on the SafeMove CD-DVD

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-677831-01 11/11