Cisco Mobile Workforce Architecture Mobile IP Deployment Guide

May 2011

For further information, questions and comments please contact ccbu-pricing@cisco.com
Contents

Cisco Mobile Workforce Architecture Mobile IP Overview ................................................................. 3
Solution Components .................................................................................................................... 3

Design Considerations: Using VPN ................................................................................................. 4
Accessing Cloud Services with Mobile IP .................................................................................. 4
Using Mobile VPN ..................................................................................................................... 5
Using SafeMove Mobile IP with Cisco VPN Clients .................................................................... 5
Using SafeMove Mobile IP with Native VPN Clients ................................................................... 5

Installing Cisco MWA Mobile IP .................................................................................................. 5
Installation Overview .................................................................................................................. 5
Server Hardware Requirements .................................................................................................. 6
Server Software Installation Steps ............................................................................................... 6
Step 1: Define the Network Parameters ....................................................................................... 6
Step 2: Install and Configure Mobile IP on the Cisco AXP Blade ............................................. 7
System Requirements ................................................................................................................. 7
Installing the Cisco AXP Service Module .................................................................................. 7
Configuring the Cisco AXP Service Module ............................................................................. 7
Configure Cisco IOS Software and Perform Cisco AXP Bootstrapping .................................... 8
Access the Cisco AXP Session and Continued Cisco AXP Configuration ................................... 8
Access the SafeMove Service ...................................................................................................... 9
Configure the SafeMove Service ............................................................................................... 9
Manage and Monitor the SafeMove Service ............................................................................. 10
Configuring the Firewall and NAT ............................................................................................ 10
Firewall Requirements .............................................................................................................. 10
NAT Requirements .................................................................................................................... 10
Step 3: Generate Configurations Using the SafeMove Mobile IP Configuration Utility .......... 12

Appendixes .................................................................................................................................. 14
Appendix A: Client Installation on Microsoft Windows Devices ............................................... 14
Running L2TP and IPSec over Mobile IP ..................................................................................... 15
Appendix B: Client Configuration on Android Devices ............................................................. 17
Appendix C: Client Installation on Nokia Symbian Smartphones ............................................. 17
Appendix D: Client Installation on Microsoft Windows Mobile Devices ..................................... 20
Appendix E: Configuring Home Agent on Cisco IOS Software ................................................ 21
Appendix F: References .............................................................................................................. 22
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 the User 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 Cisco Application Extension Platform (AXP) hardware on Cisco Integrated Services Routers Generation 2 (ISR G2). 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.support@birdstep.com).

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

Solution Components

Figure 2 shows the Cisco MWA Mobile IP solution architecture.
Table 1 lists the Cisco MWA Mobile IP solution components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home Agent</strong></td>
<td>A Mobile IP home agent can run on a Cisco AXP blade or a Cisco IOS Software router (such as a Cisco ISR) 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.</td>
</tr>
<tr>
<td><strong>VPN Gateway</strong></td>
<td>A VPN gateway can be either a Cisco IOS Software router or Cisco Adaptive Security Appliance (ASA) 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.</td>
</tr>
<tr>
<td><strong>Mobile IP Client</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Mobile IP Manager</strong></td>
<td>The Mobile IP Manager is optional server software for managing and monitoring Mobile IP servers and Mobile IP clients running on the Microsoft Windows OS.</td>
</tr>
</tbody>
</table>

**Design Considerations: Using VPN**

This section presents design considerations for implementing Mobile IP in the enterprise network. This section 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 with which your remote-access users are familiar 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 Mobile IP Management Server, you can perform setup automatically simply by entering the required parameters in the web user interface.

This section uses manual configuration steps and presents sample configuration file snippets to help you understand how to integrate Mobile IP with the 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 Cisco Services-Ready Engine (SRE) Modules listed in Table 2.

Table 2. Compatible Cisco SRE Modules

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

SafeMove is also compatible with the Cisco ISR network modules listed in Table 3.

Table 3. Compatible Cisco ISR Network Modules

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NME-APPRE-302-K9</td>
<td>● Network module (NME) form factor</td>
<td>The general-purpose Cisco ISR NME is powerful enough to host a variety of business applications and packet services.</td>
</tr>
<tr>
<td></td>
<td>● 1.0-GHz Intel Celeron processor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 512 MB of RAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 80-GB hard disk</td>
<td></td>
</tr>
<tr>
<td>NME-APPRE-502-K9</td>
<td>● NME form factor</td>
<td>This NME is designed for inline packet services and advanced applications.</td>
</tr>
<tr>
<td></td>
<td>● 1.0-GHz Intel Celeron M processor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 1 GB of RAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 120-GB hard disk</td>
<td></td>
</tr>
<tr>
<td>NME-APPRE-522-K9</td>
<td>● NME form factor</td>
<td>This NME is designed for high-I/O inline packet services and advanced applications. The Cisco AXp NME-522 is supported on the Cisco 3800 Series ISRs for high-powered applications and services.</td>
</tr>
<tr>
<td></td>
<td>● 1.4-GHz Intel Pentium M processor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 2 GB of RAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● 160-GB hard disk</td>
<td></td>
</tr>
</tbody>
</table>

Server Software Installation Steps

The steps to install a Mobile IP client using a Cisco AXp blade are:

1. Define the network parameters.
2. Install and configure Mobile IP on the Cisco AXp blade.
3. Generate configurations using the SafeMove Mobile IP configuration utility.

The following sections describe these steps in detail.

Instructions for installing Mobile IP on Microsoft Windows, Android, Nokia Symbian, and Windows Mobile devices are provided in the appendixes.

Step 1: Define the Network Parameters

Configure the following system parameters:
Mobile IP high-availability address 192.0.2.33: This parameter is a public routed address, with no Network Address Translation (NAT). Firewalls and routers must be configured so that port 434 on this IP address can be reached from all access networks.

IPSec gateway address 192.168.200.10: This parameter can be a private address.

Mobile IP home address pool 10.10.10.0/24: The home agent allocates addresses from this pool to connected mobile nodes. This subnet must be routed first to the IPSec gateway for encryption, and then back to the home agent for tunneling to the mobile node clients.

Mobile IP security association network address ID (NAI) <example.com>; security parameter index (SPI) 256 decimal, which is 0x100 hexadecimal; and shared secret <CHANGEME> ASCII, which is 0x43 48 41 4e 47 45 4d 45 hexadecimal: Set these values.

Domain Name System (DNS) servers 8.8.8.8 and 8.8.4.4: These are the DNS servers for the clients to use when connected to the Mobile IP home agent server.

Step 2: Install and Configure Mobile IP on the Cisco AXP Blade
Selected Mobile IP components, such as the Birdstep Mobile IP server, can also be operated on Cisco hardware by installing a Cisco AXP service module in an existing Cisco ISR chassis. The installation and configuration process for such a setup is described here.

For more detailed instructions about how to set up the Cisco AXP service module, refer to the Cisco AXP 1.5 User Guide.

System Requirements
Cisco AXP Version 1.5.2 or later is recommended. Update Cisco AXP to this version to help ensure successful installation and operation of SafeMove Mobile IP. For instructions on Cisco AXP system installation, refer to the Cisco AXP 1.5 User Guide.

In addition, to help ensure compatibility with Cisco AXP 1.5.2 or later, be sure that Cisco IOS Software Release 12.4(24)T2, 15.0(1)M1, or later is installed on the Cisco ISR. For more information, refer to the release notes for Cisco AXP 1.5.2.

SafeMove directly affects the Cisco AXP routing behavior, so SafeMove should be the only application service on the Cisco AXP host with it is installed. Running other services on the same service module is not recommended because SafeMove may interfere with the operation of these services. For more information, orderability, and support, contact safemove.support@birdstep.com directly.

Installing the Cisco AXP Service Module
To install the Cisco AXP service module, follow the instructions in the Cisco AXP 1.5 User Guide.

Configuring the Cisco AXP Service Module
After the Cisco AXP service module blade is installed in the Cisco ISR chassis, the Cisco IOS Software should be able to identify the new piece of hardware. To verify successful installation of the service module, enter the following commands:

```
   enable
   show diag | include FRU
```
The output should show the model of the Cisco AXP blade:

```
Product   (FRU)   Number   :   NME - APPRE -522 - K9
```

Verify that the service module is correct by entering the following command:

```
show hardware
```

The output should include the following lines:

```
cisco Integrated Service Engine -2(s)
  Application eXtension Platform (AXP) 1.5.2 in slot 1
```

Note that the exact output may vary depending on the service module used and the Cisco AXP host OS version as well as the installation slot of the blade.

If the service module is correctly identified, the installation of SafeMove can proceed.

The following sample setup illustrates the installation process. The service module is inserted into Cisco ISR chassis slot 1 and given internal Cisco ISR IP address 192.0.2.34, sharing the subnet 192.0.2.32/30 with the Cisco AXP Module, configured with address 192.0.2.33. The SafeMove server is allocated home address pool 10.10.10.0/24, used to provide home addresses to SafeMove clients. The FTP server, required for the installation process, is assumed to be deployed at address 192.0.2.21. Using these parameters, the Cisco IOS Software router, Cisco AXP host, and SafeMove Mobile IP virtual guest installation can be performed using the commands shown here.

**Configure Cisco IOS Software and Perform Cisco AXP Bootstrapping**

```
configure terminal
  ! configure internal interface between ISR and AXP
  ! installed in slot 1
  interface Integrated-Service-Engine 1/0
    ! set ISR IP address
    ip address 192.0.2.34 255.255.255.252
    ! set AXP IP address on eth0
    service-module ip address 192.0.2.33 255.255.255.252
    ! set ISR as default router for AXP
    service-module ip default-gateway 192.0.2.34
    ! power interface on
    no shutdown
  exit
  ! add route to address pool maintained by SafeMove
  ip route 10.10.10.0 255.255.255.0 Integrated-Service-Engine 1/0 192.0.2.33
end
  copy running-config startup-config
```

**Access the Cisco AXP Session and Continued Cisco AXP Configuration**

```
enable
  ! open CLI session from IOS to AXP;
```
! if prompted for username and password at this point,  
! enter your IOS administrator credentials  
service-module integrated-service-engine 1/0 session  
! enable forwarding  
configure terminal  
ip forwarding  
end  
copy running-config startup-config  
! assume safemove.5.0.5.pkg and safemove.5.0.5.prt1 are  
! downloadable at ftp://192.0.2.21/pub/  
software install add url ftp://192.0.2.21/pub/safemove.5.0.5.pkg

Access the SafeMove Service

! open CLI session from IOS to AXP;  
! if prompted for username and password at this point,  
! enter your IOS administrator credentials  
service-module integrated-service-engine 1/0 session  
! start service safemove  
app-service safemove  
! open console to the safemove service  
connect console

Configure the SafeMove Service

There are several alternative approaches for configuring the SafeMove server on Cisco AXP. It is strongly recommended that you consult the Birdstep Mobile IP server user’s manual to familiarize yourself with the configuration details before proceeding.

SafeMove deployments using a Birdstep Management Server can use this service for remote configuration and management of all SafeMove components, including SafeMove on Cisco AXP. SafeMove on Cisco AXP uses a SafeMove Manager component co-located with the Birdstep Mobile IP server to locally apply the commands from a remote management server.

For more information, consult the SafeMove installation and administration guide and the Birdstep Management Server administrator's guide.

In deployments lacking a Birdstep Management Server, the SafeMove configuration utility safemoveconfgui.exe can be used to generate compatible client and server configurations, using the co-located SafeMove Manager on the Cisco AXP guest OS for this purpose.

For a minimal Birdstep Mobile IP Cisco AXP setup, configure the Mobile IP SPI, Mobile IP shared secret, Mobile IP home address pool, home agent IP address, home agent private IP address, and the domain part of the Mobile IP NAI. In the example here, the, Mobile IP home address pool corresponds to 10.10.10.0/24. Similarly, both the home agent IP address and home agent private IP address should be set to 192.0.2.33. However, if the Birdstep Mobile IP server is located behind destination NAT (DNAT), the addresses will differ; the home agent IP address will be set to the publicly visible, globally routable IP address, and the home agent private IP address will match the private address.
You can use the safemoveconfigui.exe utility to generate both client and server configurations. You can generate a client configuration using the export option for the desired platform listed in the Export menu. Similarly, you can transmit the matching server configuration to the remote AXP guest using the remotely commit mip.xml to MIP HA action under the Action menu item.

If you are familiar with the format and options of the Birdstep Mobile IP configuration file, you can opt to modify the configuration file /etc/birdstep/mip.xml either locally on the Cisco AXP guest using nano or vi, or remotely using your editor of choice. In the latter case, the configuration file on the Cisco AXP guest must be replaced by the remote copy using either the curl or scp command available in the guest OS.

Following the reconfiguration step, the Birdstep Mobile IP service must be restarted on the AXP guest. If the configuration was updated using the SafeMove Manager component, this action should be performed automatically; otherwise, the service must be restarted manually from the application service console with the following command:

```
/etc/init.d/birdstepmip restart
```

Manage and Monitor the SafeMove Service

Birdstep Management Server is the recommended tool for managing and monitoring previously configured Birdstep Mobile IP services. However, in deployments lacking the Birdstep Management Server, the goctl utility, included in the SafeMove installation on Cisco AXP, can be used to manage and monitor the Birdstep Mobile IP server state. For more information about goctl, refer to the Birdstep Mobile IP 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 an arbitrary number of routers between the SafeMove server and the Internet, and 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, User Datagram Protocol (UDP) port 434 must be opened toward the SafeMove server. Similarly, TCP port 8082 is required for remote management of the SafeMove Cisco AXP service. However, for unlike UDP port 434, global access to TCP port 8082 should not be permitted unless the remote connections are properly protected by SSL/TLS, IPSec, or other such means.

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 private address spaces, such as 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16.

For example, as the address pool from the sample setup is 10.10.10.0/24, source NAT (SNAT) for this subnet is required to help ensure connectivity between mobile nodes and the Internet.
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 port 8082 can reach the Birdstep Mobile IP server private address.

Because configuring NAT rules correctly can be challenging, for the sake of clarity, the following sample listing configures the required rules on the Cisco ISR router hosting the SafeMove Cisco AXP blade. In contrast to the previous sample setup, here the public IP address 192.0.2.33 is configured on the outside interface of the Cisco ISR, rather than on the Cisco AXP blade. The Cisco AXP and Cisco ISR use addresses 172.16.2.33/30 and 172.16.2.34/30, respectively, for internal communication, with the Cisco ISR performing DNAT and SNAT on behalf of the internal SafeMove server. In addition, the Cisco ISR performs SNAT for the entire subnet 10.10.10.0/24, used as an address pool for registered SafeMove clients.

In this sample configuration, the external public IP address on GigabitEthernet 0/0 is mapped to the internal private address used by the Cisco AXP blade residing on Integrated-Service-Module 1/0. Note that unlike in the previous examples, configuration of a SafeMove server behind DNAT requires that you configure the home agent private IP address with the private address (172.16.2.33), rather than with the global address (192.0.2.33).

In addition to the Mobile IP–related NAT rules, the example also illustrates how to enable direct Secure Shell (SSH) connections to the Cisco AXP blade behind DNAT. However, because 192.0.2.33 port 22 is reserved for SSH sessions to the Cisco IOS Software router, SSH sessions to the Cisco AXP blade cannot use the same port number. Therefore, 192.0.2.33 port 2222 is configured for this purpose.

```
configure terminal
interface GigabitEthernet 0/0
   ! configure public IP address on IOS router
   ip address 192.0.2.33 255.255.255.0
   ! enable NAT
   ip nat outside
exit

interface Integrated-Service-Engine 1/0
   ! set ISR IP address
   ip address 172.16.2.34 255.255.255.252
   ! set AXP IP address on eth0
   service-module ip address 172.16.2.33 255.255.255.252
   ! set ISR as default router for AXP
   service-module ip default-gateway 172.16.2.34
   ! enable NAT
   ip nat inside
   ! power interface on
   no shutdown
exit

! add route to address pool maintained by SafeMove
ip route 10.10.10.0 255.255.255.0 Integrated-Service-Engine 1/0 172.16.2.33
!
! configure SNAT rule for MIP address pool
access-list 1 permit 10.10.10.0 0.0.0.255
```
! configure SNAT rule for SafeMove server to allow it to use ftp, scp, etc.
access-list 1 permit 17.216.2.33 0.0.0.3
ip nat inside source list 1 interface GigabitEthernet0/0 overload
!
! configure DNAT for the AXP service
!
! DNAT for MIP server
ip nat inside source static udp 172.16.2.33 434 192.0.2.33 434 extendable
! DNAT for manager
ip nat inside source static tcp 172.16.2.33 8082 192.0.2.33 8082 extendable
! DNAT for SSH (use port 22 for IOS, 2222 for AXP)
ip nat inside source static tcp 172.16.2.33 22 192.0.2.33 2222 extendable
end

Step 3: Generate Configurations Using the SafeMove Mobile IP Configuration Utility
As an alternative to using the SafeMove Management Console, you can configure clients using the SafeMove Configuration Utility. This approach is useful when you are installing Mobile IP only or when you are installing it with an alternative VPN client.

The utility is available as a Microsoft Windows executable file. You start the graphical utility by running safemoveconfigui.exe.

The utility also is available as a compiled Python program. The Python program can be run on systems with Python 2.6 installed. Python can be downloaded from http://www.python.org. The python program is safemoveconfigui.pyc. It must be run using Python Version 2.6. On a Microsoft Windows system, if Python 2.6 is the only Python version installed, you can run the utility by double-clicking the file in Windows Explorer.

The configuration utility’s main window lists the input parameters for configuration file generation (Figure 3). The configuration is generated by filling in the parameters and exporting by selecting the desired output file format from the Export menu. Use care when editing the parameter values because very little error checking is performed. Table 4 lists the current output formats.

Table 4. Configuration Utility Output Formats

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartConnect .dbf</td>
<td>Mobile IP client configuration for Nokia phones</td>
</tr>
<tr>
<td>Nokia mVPN .vpn</td>
<td>VPN configuration package format for Nokia phones</td>
</tr>
<tr>
<td>Nokia mVPN .pol</td>
<td>VPN configuration policy format for Nokia phones</td>
</tr>
<tr>
<td>Birdstep Mobile IP.mip</td>
<td>For Mobile IP client on Microsoft Windows</td>
</tr>
<tr>
<td>Cisco IOS Home Agent CLI .txt</td>
<td>For the home agent running on Cisco IOS Software</td>
</tr>
<tr>
<td>MIP HA .xml</td>
<td>For SafeMove Mobile IP server running on the Cisco AXP blade</td>
</tr>
</tbody>
</table>

The configuration parameters can be saved to an INI file and later loaded using the Save and Open operations on the File menu.
When the utility is launched, the parameter values for the Mobile IP shared secret and the SmartConnect license key are randomly generated. If you have a SmartConnect license key for the organization for which you generate the configuration, enter that key. Otherwise, send the generated license key to your SafeMove account manager for activation.

Figure 3. SafeMove Configuration Utility Main Window
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 4).

![Figure 4. On the Homes Tab, Click Add New](image)

In the Home Network Settings dialog box that opens, enter the parameters as shown in Figure 5.

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.

In the Security Association dialog box, enter the parameters as shown in Figure 6. Then click OK in this dialog box and again in the Home Network Settings dialog box.

Select the Status tab and click New to create a Mobile IP profile as shown in Figure 7. 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.
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 5. 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 6. Security Association Settings

Figure 7. 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 you make a backup of your existing Mobile IP configuration.

4. Verify your Mobile IP connectivity status using the Mobile IP GUI (Figure 8).

![Figure 8. Mobile IP User Interface on Android](image)

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 9). 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.
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 this is the case 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 is information is available in the technical documentation for the phone.

The supported software platforms are:

- 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 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’s 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
11. **FP2**: 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.
12. Add connections (WiFi 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 WiFi access points must be above the 3G access point to make the prioritization work correctly.
13. If no WiFi access points are listed, search for them manually using Scan Wi-Fi and answer to the question add to connection group.
14. If you want, 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 10). Click Yes.

3. If you are asked for the location for installing Mobile IP (Figure 11), choose Device.
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 AXP blade 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.

```plaintext
! 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 HA's 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
deb 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
• SmartConnect User Guide: Available on the SafeMove CD-DVD