Summer 2010

A Security Assessment of Mobikey for Remote Access

Joseph Brooks
Regis University

A SECURITY RISK ASSESSMENT OF MOBIKEY FOR REMOTE ACCESS

A THESIS

SUBMITTED ON 19 OF JUNE, 2010

TO THE DEPARTMENT OF INFORMATION TECHNOLOGY

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

COMPUTER INFORMATION TECHNOLOGY

BY

Joseph Brooks

APPROVALS

Robert Bowles, Thesis Advisor

D. M. Likarish

Daniel Likarish

Douglas I. Hart

Douglas I. Hart

Abstract

Today, it is very common for employees to need to work when outside of the office. For various reasons, it’s important that they be able to work anytime and anywhere. However, this raises security concerns about how this is accomplished. There are many options, such as virtual private networks (VPNs) and remote desktop solutions, but each comes with its own risks. A newer option is the MobiKEY from Route1, which allows users to connect to their work resources from anywhere.

Route1 touts the MobiKEY, powered by MobiNET, as a much more secure method of remote access. How does it stack up against other solutions? This paper examines the advantages of MobiKEY from a security perspective as contrasted with other options. The author performed a risk assessment of the device based upon guidelines from the National Institute of Technology (NIST) and obtained a MobiKEY from Route1 for the purposes of testing. This paper documents those findings.

Acknowledgements

I wish to thank the faculty and my fellow students with whom I've had the fortune to work with over the past three years. I've enjoyed the opportunity to learn and interact with all of you. In particular, I would like to thank my thesis advisor, Robert Bowles, for all of his assistance. I've enjoyed my studies in the area of information security most of all.

Additionally, I would like to thank my parents, as well as other family and friends, who have supported me through this journey.

Table of Contents

List of Figures

Chapter 1 – Introduction

1.1 Statement of Problem

In today's world, it is very common for employees to need remote access to their work computer and network resources while outside of the office. Employees often need the ability to work wherever and whenever they want. However, remote access inherently creates some security risks. Employees may carry a laptop that contains private or proprietary information. If this equipment is lost or stolen, then it creates a security breach for the organization. Employees may also connect back to their organization's internal network via a virtual private network (VPN) connection or via some other remote desktop solution such as GoToMyPC or Laplink Everywhere. A newer option is MobiKEY, a portable validation device from Route1, which allows users to remotely access their work computer from any other computer that has a USB port utilizing their TruOFFICE service.

It is important for organizations and their members to recognize the risks posed by any form of remote access. There usually is a legitimate business need to have remote access, whether this involves telecommuting from a home office or doing work while traveling for business. At the same time, it's important to have some mechanisms in place in order to protect the confidentiality, integrity, and availability of resources. It's important to strive to achieve a balance between reasonable access to resources while protecting against threats (Whitman and Mattord, 2005). The question is how to do this most effectively while allowing employees to have remote access. It is important to keep this in mind while evaluating different options for remote access, whether it using a VPN, remote desktop, or MobiKEY.

Route1 positions MobiKEY and the TruOFFICE service in the marketplace as an option to securely access digital resources from anywhere at any time. After an initial setup procedure on the work computer, remote connections are possible from any computer with an Internet connection and a USB port. The device uses no drivers and leaves no trace of the session on the computer used for remote access, providing security and simplicity. This seems like a great solution, but the question remains as to how it stacks up against other remote access solutions from a security standpoint.

1.2 Thesis Statement

When evaluating remote access solutions, security must be a primary concern. Any time that resources are accessed or taken out of an organization's trusted network, there is a possibility that these resources may be compromised. It's important to utilize solutions that can effectively minimize the risk of this occurring. This involves examining the strength of authentication and encryption provided by a solution, as well as investigating any vulnerabilities that may exist within the solution. For purposes of this study, the author focused on the MobiKEY solution offered by Route1 in order to evaluate the level of security provided. The key question of this study is to examine the security advantages of using MobiKEY over other remote access applications, such as virtual private networks and other remote desktop solutions.

1.3 Statement of Goals and Objectives

The goal of this project was to investigate the level of security offered by the MobiKEY product from Route1 in comparison with other solutions currently available, such as VPN solutions and remote desktop products such as GoToMyPC and Laplink Everywhere.

1.4 Work Plans, Methods and Procedures

This project examined the security advantages of using MobiKEY for remote access utilizing the risk assessment portion of the risk management methodology. As defined by the

National Institute of Standards and Technology (NIST), there are nine steps to the risk assessment process (Stoneburner, Goguen, & Feringa, 2002). These steps are:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

The author employed these steps to perform an analysis of the risks involved with MobiKEY as a remote access solution. The analysis was conducted as an individual user, rather than testing the solution in a business environment. The author did not have access to any testing environment where this could be validated for an entire organization, although the results can be utilized by any organization to assist in their own research of the security advantages of the product.

Additionally, the author obtained a MobiKEY device from Route1 directly, for the purposes of first hand testing and evaluation of the security of the solution. While the review of security literature and product documentation gave a good basis for the analysis, actual use of the product was necessary in order to perform comprehensive testing.

Chapter 2 – Review of Literature and Research

2.1 Value of Information

To begin, it's important to understand why security is such an important issue when dealing with remote access. Information security is designed to protect data by addressing three elements: confidentiality, integrity, and availability (Pfleeger & Pfleeger, 2007). These elements make up what is commonly referred to as the C.I.A. Triangle, and they are the characteristics that provide information with its value. Confidentiality ensures that information is only accessed by those who have permission to do so. The goal of maintaining confidentiality is to make certain that no unauthorized parties are able to obtain such data. Integrity of information means that it is available in its original form and has not been altered by any unauthorized parties. Availability is important so that information can be accessed when needed. Failure to ensure availability may create costly downtime for an organization. Protecting all three of these characteristics of data is crucial to protecting its value.

Additionally, there are other characteristics of information that are also important; these include accuracy, authenticity, utility, and possession (Whitman & Mattord, 2005). Accuracy of information means that there are no errors in the information and that it's what the end user expects. If the information's accuracy is in doubt, then the information's value is diminished. Authenticity means that information is in its original form and is what it appears to be. Utility means that information has value to the user and can be used for a specific purpose. Possession means that a user has access to and control over information in order to use it effectively. These characteristics are very important when dealing with information in any context. However, when considering these elements within the context of remote access, their importance is even more apparent. Information that is accessed and/or transmitted remotely may be susceptible to intercept or attacks that compromise one or more of the above characteristics, thus diminishing or destroying its value. Taking adequate steps to address the security of remote access is critical for these reasons.

2.2 Encryption

In order to protect information and ensure its value, data should be encrypted. Encryption is performed using cryptography, which involves hiding the true content of information. According to Ciampa, cryptography provides for information security in five ways: providing confidentiality so that only authorized users can view it; providing authentication so that the sender can be verified as genuine and trusted; providing integrity so that the receiver can verify that information has not been altered; offering nonrepudiation, so that no one can deny that the information has been sent or received; and offering access control so that the availability of information can be restricted (Ciampa, 2005). It's critical to utilize encryption for information that will be accessed remotely, particularly while in transport. This requires that the other party be able to decrypt the message and determine its contents.

2.2.1 Symmetric Encryption

There are two primary categories of encryption. The first is symmetric encryption, which is also known as private key encryption. In symmetric encryption, the same key is used both to encrypt and decrypt a message. The most commonly used form of symmetric encryption today is the Advanced Encryption Standard (AES), which was adopted by United States National Institute of Technology (NIST) in 2000 and published as Federal Information Publishing (FIP) Standards Publication 197 in 2001. AES was adopted after the previous forms of symmetric encryption, Data Encryption Standard (DES) and Triple DES (3DES), proved to be too weak for top-secret communications and their keys proven too easy to break (Whitman & Mattord, 2005).

AES uses a block size of 128-bits of data, and can utilize key sizes of 128, 192, or 256 bits. The larger the key size, the more difficult it is to break the encryption. Data goes through four steps of encryptions for several rounds, with the number of rounds increasing based upon the key size (FIPS 197, 2001). In order to encrypt data using AES, it is first converted to a 128-bit hexadecimal format and then processed into a 4x4 square format, where each block represents one byte of data. The process then goes through multiple rounds, where the number depends upon the key size. The first step is to add a round key, and then the data goes through four steps (NIST, 2001):

1. SubBytes
2. ShiftRows
3. MixColumns
4. AddRoundKey

This process repeats for ten, twelve, or fourteen rounds, depending on whether they key size is 128, 192, or 256, respectively. The process begins by substituting bytes according to pre-defined substitution table (SubByes), and then proceeds through steps of shifting rows (ShiftRows), mixing columns(MixColumns), and adding a round key(AddRoundKey). Each round serves to scramble the data further.

AES is considered more secure than other forms of encryption, although there have been indications that it can potentially can be attacked by solving algebraic equations that are the heart of its predefined tables (Courtois & Pieprzyk, 2002). However, it remains the US government standard for encryption and is widely-used in private industry as well.

2.2.2 Asymmetric encryption

The other category of encryption is asymmetric encryption, which is commonly known as public key encryption. In asymmetric encryption, there is a pair of keys that are used to encrypt and decrypt information. One key is public and can be made freely available, while the private key is held by a user. This method of encryption allows users to send a message and authenticate that it comes from a valid source. This protects the keys from accidental exposure while being transmitted over the internet, since the private key never has to be transmitted.

Common forms of asymmetric encryption include the Diffie-Hellman method of key exchange; the Rivert, Shamir, and Adleman (RSA) algorithm for encryption; and the Digital Signature Algorithm (DSA), which is the United States Federal Information Processing Standard (FIPS) for digital signatures. Diffie-Hellman allows two users to securely exchange a secret key over an insecure network, and is used in the Secure Shell (SSH) protocol (Ciampa, 2005). RSA is commonly used in operating systems and secure communications, including Secure Sockets Layer and (SSL) Transport Layer Security (TLS). Finally, a digital signature is included in a message in order to verify the authenticity of the sender. A digital signature must be unforgettable, authentic, unalterable, and non-reusable in order to be effective (Pfleeger & Pfleeger, 2007). This frequently makes use of a trusted third party, known as a certificate authority (CA), to verify the authenticity of the signature.

2.3 Remote Access Methods

No remote access solution is completely free from risk. It’s important to bear this in mind and perform careful risk analysis when looking at the various methods of remote access. The National Institute of Standards and Technology outlines four common methods of remote access (Scarfone, Hoffman, and Souppaya, 2009):

1. Tunneling
2. Application Portals
3. Remote Desktop Access
4. Direct Application Access

Tunneling typically involves a client-based virtual private network (VPN), while application portals are typically web-based. Remote desktop access encompasses MobiKEY as well as solutions such as GoToMyPC and desktop virtualization. The fourth option, direct application access specifically allows access to a particular application, such as email. As this final method allows more limited access than the other options, it is not addressed further due to the scope of this paper.

2.3.1 Virtual Private Networks (VPNs)

One of the more common methods of remote access is via VPN. A VPN allows a remote user to establish a secured tunnel between their computer or network device back to an organization's network. This allows the user to access network resources through this connection. There are typically two types of VPNs: Internet Protocol Security (IPSec) VPN and Secure Sockets Layer (SSL) VPN (Scarfone and Souppaya, 2007). An IPSec VPN uses client software that is installed on the user's PC, while an SSL VPN more typically utilizes a web-based connection. Utilizing VPN for remote access is common today, but these solutions are not perfect from a security standpoint. NTA Monitor performed a three year study of VPNs that found a number of common vulnerabilities across vendors, including VPN fingerprinting, which allows an attacker to identify the device or software version; insecure storage of login credentials by VPN clients; username enumeration vulnerabilities, which allows attackers to obtain valid usernames; and poor default configurations (Hills, 2005). While these findings apply to client-based IPSec VPNs, SSL VPNs have their own vulnerabilities. For example, the United States

Computer Emergency Readiness Team (US-CERT) issued a vulnerability note in 2009 stating that clientless VPN products from several vendors, including Cisco, Citrix, Juniper, Microsoft, Nortel, and others operate in a way that breaks web browser security mechanisms (Warren & Giobbi, 2009).

2.3.2 Remote Desktop Access

Remote desktop options for remote access may take several forms, from MobiKEY to solutions such as GoToMyPC.com, Laplink Everywhere, and desktop virtualization solutions. The specifics of MobiKEY will be addressed in detail in chapter 4. It's also important to understand remote desktop alternatives to place MobiKEY in the proper context. Remote desktop solutions may be either hosted or may be managed internally.

GoToMyPC is a hosted service from Citrix Online that allows remote access to desktop resources from any remote computer using a web browser. The service requires users to register the host PC with GoToMyPC. This process installs a small server on the host that registers it with the GoToMyPC broker in Citrix Online's data center. Once this is established, users can log in to GoToMyPC.com using any web browser and initiate a log-in with their username and password. The broker receives the request and initiates an SSL-encrypted session to the host PC. The remote desktop session is then passed through a communication server that is also located at Citrix Online's headquarters. These connections occur over TCP ports 80, 443, and/or 8200 using 128-bit Advanced Encryption Standard (AES) (Phifer, 2010). Port 80 is commonly used for Hypertext Transfer Protocol (HTTP), while port 443 is typically used for Hypertext Transfer Protocol over SSL/TLS (HTTPS) and is more secure. Port 8200 is not an industry standard, but is specifically used for the GoToMyPC solution.

Laplink Everywhere is a solution similar to GoToMyPC and is offered by Laplink. According to the company's website at http://www.laplink.com/le5, this solution offers three ways of accessing a user's PC remotely: via a toolbar that can be installed on a remote computer and allows searching and accessing files on the work PC; via any PC's web browser by logging into their website at lle5.ll2go.com; or via any smart phone with a web browser. Like GoToMyPC, all connections are brokered through hosted servers at Laplink's facility using 128-bit AES encryption. The product utilizes Microsoft Remote Desktop Protocol (RDP), which is a standard protocol for remote desktop access in Microsoft terminal servers. Also with Laplink Everywhere, the user can create guest access accounts for sharing and can easily transfer files from the work PC to the client PC. The website's demo of the product also indicates that all signs of the remote session are erased from the client PC once the session is ended.

Desktop virtualization involves solutions where PCs access an image that resides on a central server. This is a form of thin-client computing, where the client PCs access applications that are running on a server that is located elsewhere. There are a number of vendors who offer these types of solutions, including Microsoft, Citrix, and VMware. From a security standpoint, this may seem more secure than other solutions because everything resides at a central location. However, there may be a lot of unknowns because attackers have not yet begun to target these solutions (Cummings, 2008). These solutions are more typically managed internally, as opposed to the hosted solutions offered by vendors such as Route1, Citrix Online, and Laplink.

Now that there is some context for understanding remote desktop solutions, the author will turn to an analysis of MobiKEY in the next chapters.

Chapter 3 – Methodology

This project examined the security advantages of utilizing MobiKEY for remote access utilizing the risk assessment portion of the risk management methodology. As defined by the National Institute of Standards and Technology (NIST), there are nine steps to the risk assessment process (Stoneburner, Goguen, & Feringa, 2002). These steps are:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Each of these steps plays an important role in determining the risk level of the solution and whether deploying the solution is within the realm of acceptable risk. See figure 3.1 for an overview of the process. Following is an explanation of what is entailed in each step of the process.

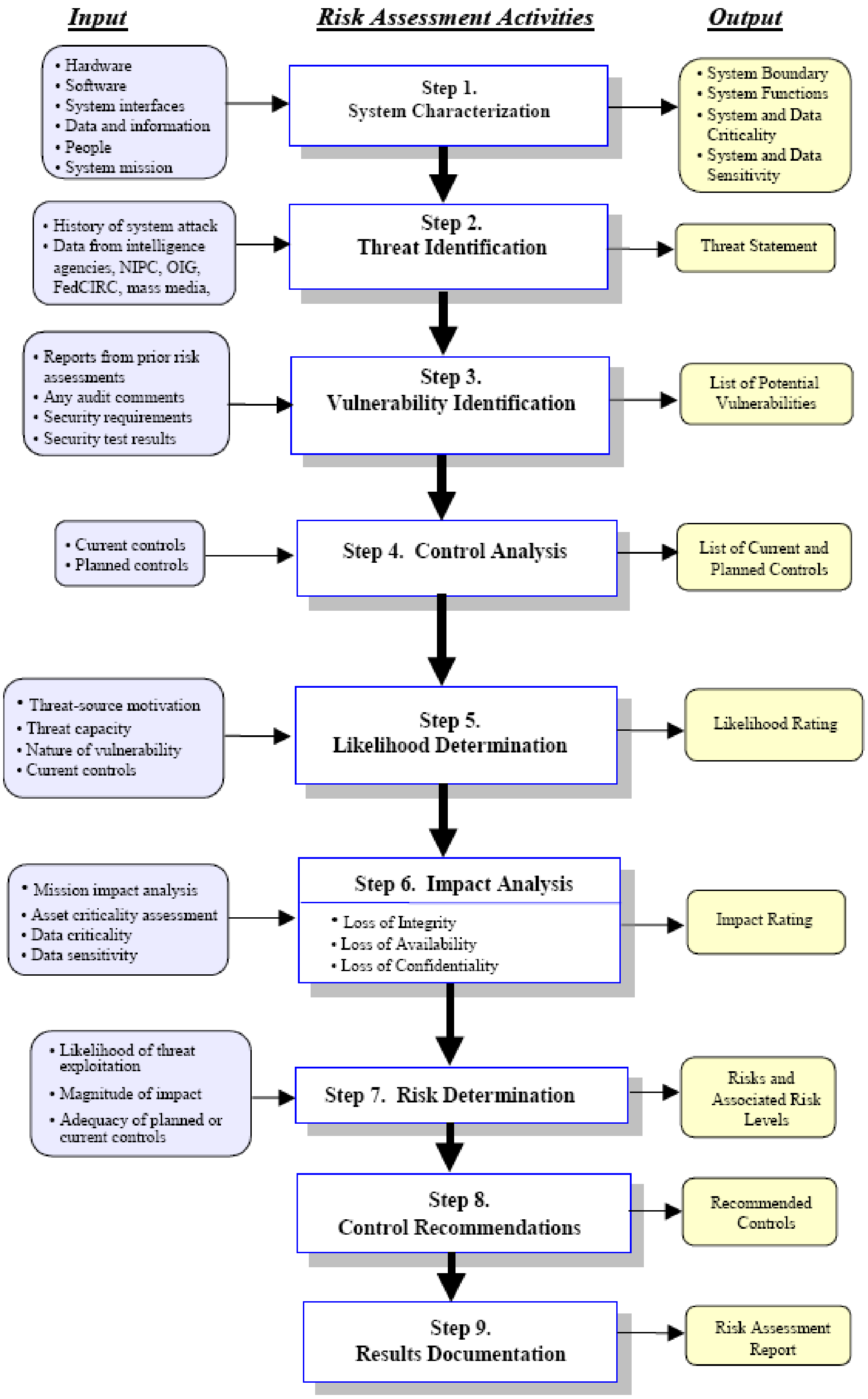


Figure 3.1: Risk Assessment Methodology

3.1 System Characterization

System characterization involves outlining the components that make up the environment of the system. This involves gathering data about all elements that make up this environment, including:

- Hardware
- Software
- System Interfaces, which are used to connect to the system
- Data and information
- People who support and use the system
- System mission or how the system is functionally utilized.

This data is used to develop an understanding of all involved systems and the general design of the operating environment.

3.2 Threat Identification

This step involves identifying any threats that may be able to exploit vulnerabilities in the environment. Threats may come from any number of sources, and may be either deliberate or accidental. A threat in computing terms means something that can potentially cause loss or harm (Pfleeger & Pfleeger, 2007). Threats may be posed by individuals both inside and outside of an organization, or by computers themselves, such as when there are software or hardware failures. Threats can also be posed by environmental factors or natural disasters. The end result of threat identification is to compile a list of potential threats that may cause harm to the system.

3.3 Vulnerability Identification

The goal of this step is to compile a list of vulnerabilities that could be exploited by a threat. A vulnerability is defined as “a flaw or weakness in the system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or violation of the system’s security policy” (Stoneburner, Goguen, & Feringa, 2002).

3.4 Control Analysis

During this step, the goal is to identify any controls that are in place within the system environment. Controls are used to decrease the chance that a system vulnerability will be exploited. They can also be used to minimize the impact if such an event occurs.

3.5 Likelihood Determination

As the header suggests, this step involves identifying how likely it is that a particular vulnerability may be exploited and cause harm to the system. The likelihood may be high, medium, or low.

3.6 Impact Analysis

This step involves determining how much of an impact the exploitation of a vulnerability will have on an IT system's mission. Any loss of confidentiality, integrity, and availability of data must be considered in terms of the impact that this will have.

3.7 Risk Determination

This step is designed to determine the risk level, which is defined as high, medium, or low. The risk level is determined from the likelihood that a threat will be exploited; the level of impact to the organization if a breach occurs; and the effectiveness of any planned or current controls in mitigating the risks of any security breach.

3.8 Control Recommendations

After completing all of the other steps, the result is a recommendation of controls that should be put in place in order to mitigate the risks posed by the likelihood of a vulnerability being exploited.

3.9 Results Documentation

This final step involves creating a risk assessment report from the data gathered during the previous eight steps. In this case, this document will be the end result.

3.10 Methods of Information Collection and Sources

In researching this project, the author has utilized multiple sources of information. The sources include information security books, web articles, journals, and vendor-specific sources of information. This provided a good background, as well as an understanding of the advantages and disadvantages of different options. However, the best way to determine the security advantages of MobiKEY is by first-hand testing. The author obtained a MobiKEY, along with a 30-day trial to TruOFFICE, from Route1 for testing purposes.

Chapter 4 – MobiKEY Analysis

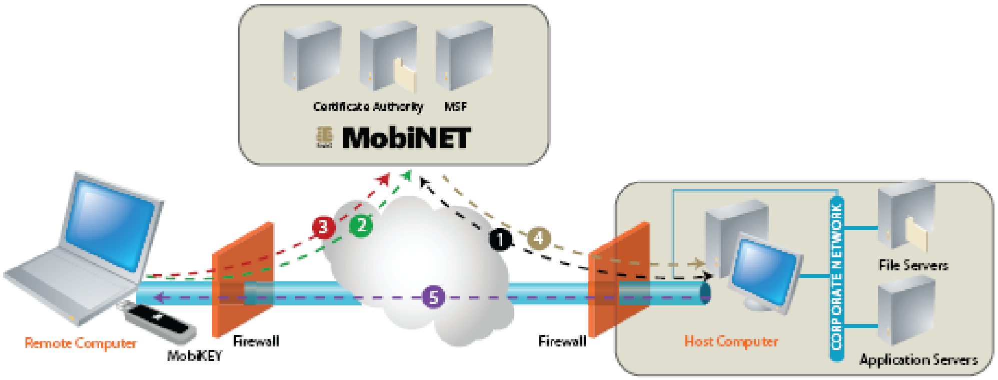
The MobiKEY from Route1 offers an alternative to other forms of remote access, such as VPN connectivity and remote desktop solutions, such as GoToMyPC. The primary question is whether MobiKEY is a better alternative from a security standpoint.

4.1 MobiKEY: How it works

MobiKEY is a small device that connects to the USB port of any computer. MobiKEY works in conjunction with MobiNET. MobiNET is a hosted identity management solution that authenticates users and allows them to access resources that they are authorized to use. MobiKEY must be registered with MobiNET, configured and setup before users can access resources with the device. This entire process is typically completed in a matter of minutes and without any reconfigurations to the PC or any firewalls.

First, the MobiNET Agent software is installed the host computer. This software issues digital X.509 certificates to identify the users and what resources they are authorized to access. The MobiNET Agent software must be installed on all resources that are going to be accessed using the MobiKEY. Once this has been configured, the user can use the MobiKEY to access resources remotely.

The MobiKEY device can be plugged into a USB port of any internet-connected computer. The computer can be anywhere, as long as there is a wired or wireless internet connection. Once the MobiKEY is connected to the computer, the user is prompted to enter their MobiNET password. There is a smartcard built into the MobiKEY that authenticates the user’s password with MobiNET’s certificate authority. Once this is done, the user is presented with a list of resources that he or she is authorized to access. These resources are all hosts that have been configured with the MobiNET Agent. A user can be authorized to access multiple resources, not just their own work computer. These resources need to be predefined within MobiNET. The user does this by connecting the MobiKEY to a computer and configuring it as a host. Once the user selects a resource with which to connect, the MobiKEY sends this request to MobiNET. MobiNET then initiates the connection back to the MobiNET Agent on the host. The Agent initiates a secured SSL connection with the MobiKEY. This connection runs entirely on the MobiKEY without placing any files or leaving any trace on the client computer that is used to connect. See figure 4.1, taken from the Route1 website, for a depiction of this entire process.



1. Host Computer is Registered with MobiNET: The MobiNET Agent can be installed and activated on multiple Host computers. MobiNET manages a user's identity and the services they are authorized to access by issuing to Route1 subscribers, digital X.509 certificates.

2. MobiNET Authentication: Plug your MobiKEY, with TruOFFICE, into the USB port of any Internet-enabled PC. Enter your MobiNET password, which is validated by the smart card embedded on MobiKEY. Once authenticated, MobiNET presents your list of Hosts and their availability.

3. Connection Request and Notification: Selecting the desired Host computer initiates a connection request to MobiNET which, in turn, provides the connection information back to the MobiNET Agent.

4. Session Request and Mutually Authenticated TLS (SSL): MobiNET Agent establishes a secured TLS(SSL) connection with the MobiKEY. This mutually authenticated end-to-end session eliminates any man-in-the-middle vulnerabilities.

5. Secure Computing Session Established

Figure 4.1: The MobiKEY connection process

The communications between the host and MobiNET, as well as the MobiKEY and MobiNET, all occurs over port 443. As previously noted, port 443 is used for Hypertext Transfer Protocol Secure (HTTPS) and is used for secure transactions. The use of this port allows MobiKEY to be used without any reconfigurations to corporate firewalls, since this port is commonly used for highly secure web transactions, such as financial transactions. Many other applications require firewall reconfigurations to allow them to punch through for communications, but this is not the case with MobiKEY.

TruOFFICE is the solution offered by Route1 that allows remote control of the work desktop. The MobiKEY allows the user to launch the TruOFFICE session and the user then accesses the work PC from the client, with everything remaining behind the corporate firewall and no file transfer allowed between the work computer and the client. All keystrokes that are sent to the work computer are encrypted, and all screen changes that are sent from the work computer to the MobiKEY are also encrypted.

4.1.1 Necessary components for MobiKEY deployment

MobiKEY simplifies the components needed for remote access. Users still have work computers, but it is not necessary that this be a laptop that the user takes with them when leaving the office. The work computer has the MobiNET agent installed and be accessed from anywhere. In order for this to work, the work computer must remain on. This increases the importance of physical security. Control to the physical premises where the computer is stored must be maintained in order to prevent unauthorized access. The user must make sure to lock the computer when not in the office; this is also good security practice even when in the office but away from the computer. Locking the computer also mitigates risk by requiring an attacker to possess local login credentials in order to access any protected information.

Additionally, steps should be taken on the work computer to harden it against security threats. There are several steps that can be taken to achieve this, including installing anti-virus software; installing a personal firewall; utilizing encryption for critical files; and shutting down any unnecessary services on the laptop. The work computer should also be patched with any operating system and application software updates and patches that are available to address any known vulnerabilities. These are all good practice for general security and aren't specifically needed because of MobiKEY. However, it is important to address them in all cases to protect the computer from threats.

Along these same lines, it's critical that if this is a computer that is part of an organization's trusted network that proper steps be taken to protect the network. This should include the user of a corporate firewall that is properly configured. It may also involve the user of a demilitarized zone (DMZ), which adds an additional layer of security between the open Internet and trusted internal resources. The internal network should always have proper security mechanisms in place to protect it, regardless of the remote access solution that is being used.

Since the computer needs to remain on and have an internet connection in order to be accessed via MobiKEY, it's also important that the site where the resources are kept has provisions for backup power and disaster recovery. Again, this should also be part of planning for any remote security option, but it becomes more critical with MobiKEY. No resources ever leave the company's premises, so they must remain in service or the remote user is completely cut off.

4.1.2 Additional Features of MobiKEY

MobiKEY offers several security features that make it an attractive remote access option. First, MobiKEY offers two-factor authentication (2FA.) In order to access the remote resources, the user must both possess the MobiKEY device and know the correct password in order to authenticate with MobiNET. This is 2FA based upon what the user has and what the user knows. Only when possessing both is the user able to access any resources. This offers a stronger form of authentication than simply accessing with one of the methods. This stands in contrast to web-based remote access options such as GoToMyPC or an SSL VPN portal that depend only upon one factor (username/password.)

Additionally, MobiKEY runs entirely off the USB token and is completely clientless and driverless. No trace of the user session is left on the client computer that is used to access internal network resources. This simplifies the need to secure the client computer and protects the internal network from accidental exposure to threats. Since the session is running off of the MobiKEY token, there is no need to take extraordinary security measures to protect the client before connecting. The client computer may be the user's home PC or even a PC in an internet café. The session is not impacted by any viruses, malware, or key loggers that may be running on the client PC, because it's all running on the MobiKEY token itself. This protects the trusted network from being exposed to any of these threats via the remote access session.

4.2 MobiKEY Threat Identification

Any remote session that involves accessing private or confidential information across the Internet is open to some form of threat. It's important to understand the types of attackers and attacks that such a solution may face before deployment. In the case of MobiKEY, many of these are not as much of a threat as they are when deploying other forms of remote access.

4.2.1 Types of Attackers

There are a number of types of individuals who may attack computer systems. These include hackers, crackers, disgruntled or dishonest employees, terrorists, or spies (Ciampa, 2005). It's important to distinguish among the various types to understand the threat that they pose.

A hacker is someone who accesses computer systems for relatively benign reasons. A hacker will attempt to access a system without authorization just to prove that he or she can do it.

Closely related to the hacker is the cracker, who is someone who accesses systems without authorization with the intention to do harm.   In the mainstream media, the term hacker is often used to describe both.   In computer security, it's important to understand the distinction. The hacker without bad intentions may also be called a white hat, while the cracker is commonly referred to as a black hat. However, both hackers and crackers are attempting to access resources and systems without authorization, so both pose a security risk. The ethical implications of both are the same; regardless of motivation, someone is accessing resources without the authorization to do so and should be considered a potential threat.

Employees can also be attackers, and are one of the more dangerous forms of attacker. If an employee wishes to do harm for some reason, whether it's because they are disgruntled or are interested in some form of financial or personal gain, then it is difficult to stop them. The employee has the advantage of being a trusted resource with authorized access.

Terrorists are also an increasingly common form of attacker. Terrorists may attempt to utilize computers as targets or methods of attack, as well as to spread propaganda (Pfleeger & Pfleeger, 2007). Terrorists may seek to deface websites or deny resources to legitimate users in order to further their cause.

Finally, spies are another common form of attacker. Spies are out to obtain information without being detected.

Any attacker needs method, opportunity, and motive to launch an attack on a system (Pfleeger & Pfleeger, 2007.) From the standpoint of computer security, it's easier to address solutions to deny the effectiveness of methods or opportunities to launch an attack.

4.2.2 Common Attacks

There are a number of common attacks that may target a remote access user. Among these are man-in-the-middle attacks; malicious code or malware; password guessing; and social engineering. Each of these is examined in turn.

A man-in-the-middle attack involves eavesdropping on a connection between two endpoints. This may commonly be performed with a packet capture device that records traffic to and from a particular IP address. The traffic captured may be saved and replayed later, or it may be intercepted and altered before being sent on to the final destination. In any case, the confidentiality and integrity of the data is compromised.

Malicious code, or malware, is software that is installed on a user's machine without the user's permission. There are a number of types of malware, including viruses, worms, logic bombs, Trojan horses, and backdoors (Ciampa, 2005). A virus is software that causes disruption when a program is run or an email attachment is downloaded. The virus infects the computer when this is done and then attempts to spread to other computers. A worm is a similar type of attack, but it propagates itself to other users and doesn't usually require action by the user in order to spread. A logic bomb is a type of malware that will launch with a triggering event, such as when a specific date/time is reached. Trojan horses are programs that are downloaded and appear to be innocuous, such as a screensaver. However, Trojan horses hide some other software with malicious intent. Lastly, a backdoor program is one that allows users to enter a system without the owner's knowledge or consent.

Password guessing is form of attack in which an unauthorized user attempts to access a system with another's credentials. Such attacks may take the form of a dictionary attack, where the attacker attempts passwords based upon words in the dictionary, or a brute force attack, where the attack attempts to guess any password based upon the password guidelines. If an attacker is able to obtain the user’s username and password, the attacker can then access any resources that the authorized user can. They can steal, destroy, or alter any data that the user can access.

Social engineering is a type of attack where the user tricks an unauthorized user into providing access. The attacker does this by posing as someone who should have access or by convincing an authorized user to provide information that allows them to have such access. This can involve gaining physical access or obtaining passwords in order to access remote systems.

4.3 Vulnerability Identification

Once the potential threats are recognized, it’s important to identify any vulnerabilities that may exist within the systems and solution. A vulnerability is a flaw within a solution that may be exploited by an attacker. Such a flaw may exist in the design, implementation, or in security procedures. Vulnerabilities can be identified from previous risk assessments, running automated scanning tools, or by reviewing security white papers.

For a remote access solution, vulnerabilities may exist in the equipment used to access the secure network remotely; within the secure network, where access from the outside may be exploited; or by actions taken by the trusted employee who is attempting to access resources remotely. The latter is the greatest risk. If an employee is careless, then it’s possible that attackers may be able to gain access to any equipment that is taken out of the office by the employee. For example, an employee may take a company laptop or a USB drive and these may be stolen. If the data on these is not encrypted, then an attacker can very easily compromise confidential data.

With MobiKEY, the user only has to take the MobiKEY device offsite. If this device is lost or stolen, it can be deactivated by the administrator so that it becomes inoperable, per information from Route1's website. An expedited replacement can then be supplied by Route1. While there is some risk if an unauthorized user has access to both the password and the MobiKEY for some period of time, this risk is much less than if a device that actually contains files is lost or stolen. Additionally, the attacker must also have login credentials to the host machine. This actually requires the unauthorized users to possess three factors in order to compromise trusted resources. This makes the potential vulnerability from using MobiKEY much less likely than other solutions.

In other ways, MobiKEY also seems to be less vulnerable than other remote access solutions, such as GoToMyPC or Laplink Everywhere. These services work in a very similar manner to MobiKEY, but work from a web browser. The remote user does not have to possess any device, but simply can log in from any computer with web access. However, since the session is initiated from the remote PC, the security of the remote PC is more of an issue than with MobiKEY, where the session is initiated from the device. It's possible that the remote PC may have keylogging software, which captures all key strokes made by the user, or may be compromised by not having firewall or anti-virus protection. Additionally, web browsers are still subjected to many attacks. In SANS's top cyber security risks in September 2009, the organization identified browsers and client-side applications that are launched from browsers as among the most commonly targeted by attackers (SANS, 2009.)

While considering multiple remote access methods, MobiKEY appears to have less exploitable vulnerability than other options that are currently available. This gives the MobiKEY option an advantage over other remote access methods.

4.4 Control Analysis

Control analysis involves examining any current or planned controls to guard against security risks. In the case of MobiKEY, there are many controls offered. As already noted, MobiKEY utilizes 2FA based upon something the user has (the MobiKEY) and something that the user knows (the accompanying password.) Without possession of both, an unauthorized user cannot gain access to the internal network. However, there are also a number of other controls offered by the solution. Among these controls are: a public key infrastructure (PKI) and integrated smart card to provide secure authentication and connection, and a highly secure SSL connection to protect data that is transferred during the remote access session.

MobiNET offers a PKI infrastructure that handles all access, authentication, and authorization for users. Certificates are issued by MobiNET for the MobiKEY and any hosts running MobiNET Agent, and the MobiNET manages the identities of all components. MobiNET also manages what users are authorized to access via a particular MobiKEY device. If the device is lost or stolen, then the PKI can be used to revoke the certificates, as described in the previous section. This is more a more secure method of identifying and authenticating users than by using passwords alone. Additionally, the integrated smart card on the MobiKEY is used to store the certificate and connection information in an encrypted format. This protects the information from attackers, even in the event that they obtain the MobiKEY device. These items serve to provide the user with a secure way to authenticate and prevent attackers from even accessing any secure resources.

Additionally, data is protected during transit by creating a highly secure client-server SSL conversation between the MobiKEY and the host. These communications occur over SSL port 443, and all communication is encrypted. Any keystrokes from the client with MobiKEY are encrypted, as is the screen presentation from the host running MobiNET Agent. Since the user is actually working off the host PC, all information stays behind the corporate firewall and there is no opportunity for man-in-the-middle attacks.

According to Route1's website, there are a number of other security advantages offered by MobiKEY and MobiNET. These include:

- Smart Card, Common Criteria EAL4+ certified
- Private key never leaves the smart card
- 1024 to 4096-bit asymmetric keys
- FIPS 140-2
- TLS 1.0 (SSL 3.1)
- 128-bit/256-bit AES
- RSA/SHA-1/SHA-2 signing algorithm
- Evaluated by ICSA labs.

This information was obtained from an information sheet at Route1's website (http://www.route1.com/mobinet/documents/Route1_Security.pdf), and it's worth discussing a few of these items in more detail to clarify their meaning. The following paragraphs elaborate on Common Criteria and FIPS 140-2.

Common Criteria certified refers to an international standard for computer security certification. Common Criteria security evaluation is specified in International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408. (Common Criteria, 2009) Products go through an evaluation process and are assigned one of seven Evaluation Assurance Levels (EALs). This credential indicates that the MobiKEY product went through this testing process.

FIPS 140-2 refers to Federal Information Processing Standard 140-2, which is a standard published by the National Institute of Standards and Technology. This document, first published as FIPS 140-1 in 1994 and updated to FIPS 140-2, defines standards for the design and implementation of a cryptographic module (FIPS 140-2, 2001). This standard defines four levels, numbered one through four. Level one is the lowest level while level four is the highest. Route1 achieved level 1 FIPS 140-2 certification for their cryptographic module on July 17, 2008 (NIST, 2008).

The security controls offered by MobiKEY and MobiNET are used by Route1 as one of the biggest selling points for the product. Based upon the information available, the authentication and encryption features offered by Route1 do provide strong protection against any attacks.

4.5 Likelihood Determination

Based upon the analysis to this point, it seems unlikely that remote access via MobiKEY will result in a security breach. As noted previously, an attacker would need to gain access to both the MobiKEY device and the user’s password in order to use it to gain access to the internal network. This would require careless behavior on the part of the user, or compliance on the part of the user in such an attack. In the case of the former, the device can quickly be deactivated by contacting Route1 and having the MobiKEY’s security certificate revoked. This can be prevented by educating users about the importance of keeping passwords secure, as well of the importance of immediately reporting if the device is lost or stolen. In the latter case, it is very difficult to defend against an attack by a trusted user. In this event, MobiKEY would not seem to provide significant advantages over other forms of remote access.

Additionally, the security provided by the SSL session between the host computer and the MobiKEY makes it unlikely that the session will be compromised by man-in-the-middle attacks or any vulnerabilities on the machine used for remote access. Most of the most common attacks are circumvented by the authentication and connection process.

By comparison, other remote access solutions seem more likely to fall victim to exploitation. Any remote access solution that involves taking resources out of the workplace is exposed to physical loss, whether by accident or intentional theft. A device that is used to access the network via an IPSec or SSL VPN may not be properly protected from viruses, malware, and threats, and may expose the internal trusted network to these threats. Overall, the information obtained by the author indicates that the likelihood of a security breach with MobiKEY is much lower than other alternatives.

4.6 Impact Analysis

Any security breach that occurs as a result of a remote access solution has the potential to compromise the confidentiality, integrity, and availability of critical information. The impact of any such breach depends upon the value of the information to the organization. All data has value, but some data has more value than others. This depends upon the nature of the business and how critical the information is to that business. The impact can range from losing advantage because a competitor has access to sensitive information, to facing legal and civil penalties if the data compromised is protected by a law such as the Health Insurance Portability and Accountability Act (HIPAA). In order to determine the impact, a careful analysis must be performed to determine the criticality and sensitivity of the data, as well as any associated systems. This step must occur independently of the remote access solution chosen, although the results will be considered along with other factors in the next step of the risk assessment process.

4.7 Risk Determination

The risk determination stage involves determining the risks and levels of risk associated with a solution. In determining the risk, any organization should consider the likelihood of threat exploitation, the magnitude of impact, and the adequacy of any controls. In the case of MobiKEY, the likelihood of threat exploitation is low while the adequacy of controls is high. As explained in section 4.2 and 4.3, there are few threats that seem likely to successfully exploit any vulnerabilities in the product. Likewise, the controls provided make it unlikely that any attacker can successfully compromise any data unless they can obtain the MobiKEY device, the corresponding password, and have the loss of the MobiKEY go unreported for some time. While no solution is ever full-proof, MobiKEY does stand at an advantage versus other remote access solutions.

4.8 Control Recommendations

The MobiKEY itself, used in conjunction with TruOFFICE, provides strong controls to prevent any attacks. This allows all data to remain inside the trusted network and within the confines of the workplace. Depending on the nature of the data, it may also be advisable to block local printing and utilize AES-256 for all TruOFFICE connections. The simplicity of this solution stands in stark contract when compared to SSL VPN or other web-based remote access solutions.

4.9 Results Documentation

As noted previously, this document is the results documentation for this risk assessment of MobiKEY. If this were being performed for a specific organization, then the results would be documented and kept as part of the organization’s security policy. This risk assessment may also be reviewed periodically in order to maintain security policy and ensure that the risk does not change over time.

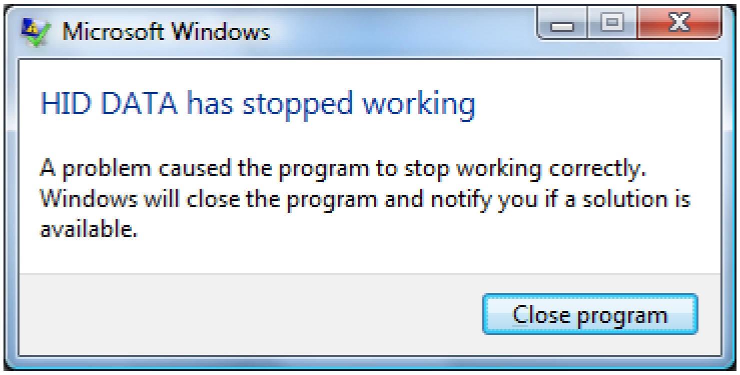
After performing this overview of the solution, the next step was to obtain the MobiKEY and perform product testing to validate its security advantages. The testing of the product was not as easy as expected, but did provide the author with enough information to draw conclusions.

Chapter 5 – Analysis and Results: MobiKEY testing

The author determined that the best way to evaluate the security aspects of MobiKEY was to test it. It was relatively simple to obtain the device for testing. Route1's website instructs visitor's to contact the company directly via telephone at +1-416-848-8391. The author contacted Route1 at this number and was connected to a sales representative, Neville Thomas. Neville advised that the MobiKEY can be obtained for a fee of $175 plus shipping, along with a 30 day trial of TruOFFICE. The sales representative also advised that if the author chose to continue with TruOFFICE past the 30 day trial, the cost would be $300 for one year. Once the author advised that he wished to proceed with the purchase for testing purposes, the sales representative emailed a contract that required the author to provide shipping and payment information, along with a valid signature. This contract can be viewed in appendix A. The MobiKEY was received by the author on the following day, so it only took a period of 24 hours to purchase and have the device in hand.

5.1 MobiKEY host installation

During the research process, the author found multiple sources, including Breeden (Breeden, 2006) and Marsan (Marsan, 2009), who indicated how easy the installation and setup process for MobiKEY is to perform. The author installed the MobiKEY on a Hewlett Packard model HP Pavilion DV7 laptop. Unfortunately, this process was not entirely seamless, and this appeared to be related to issues with the test computer. Upon inserting the MobiKEY in an available USB port, the author was presented with a window with an error message, "HID DATA has stopped working" (see figure 5.1.)



HID DATA has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

Figure 5.1 Error message from Windows Vista on test machine

Despite this error, the MobiKEY installation was able to proceed normally. Further complications were encountered after installion, but that will be addressed later. For screen shots of the installation process, please see appendix B. Upon insertion into the USB port, the executable file on the device ran and the user was prompted with a window requesting that the user enter the license key, which is provided by Route1 along with the MobiKEY device.

After entering the license key, the user hits the "Next" button in the window provided and moves to a window where the MobiNET password must be created. The MobiNET password must be between 8 and 16 characters in length. The user must enter the password twice, and a warning in the window notes that during login, the user has a limited number of times to enter the password before the MobiKEY is locked.

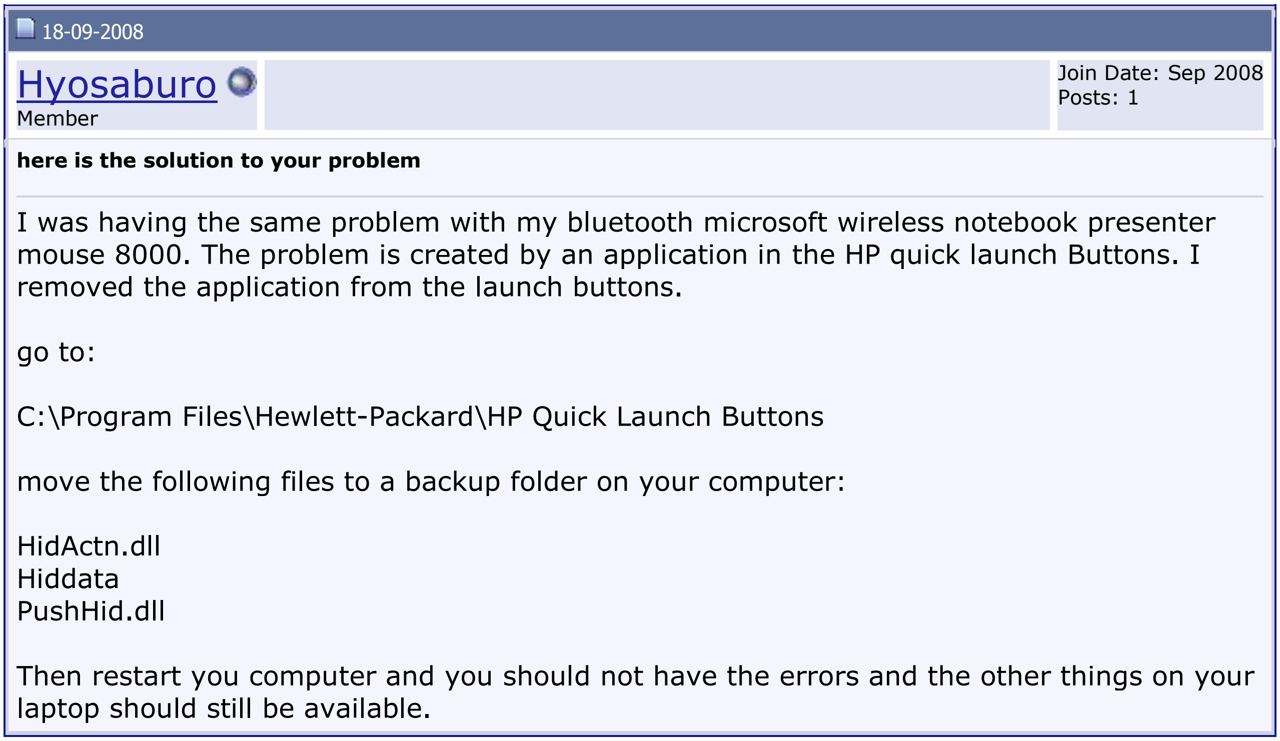
The window following password creation prompts the user to create a security question/answer pair that can be used to verify a user's identity. Unlike many websites that provide a list of standard questions, Route1 allows the user to create their own question and answer. This is yet another way that the product is more secure than other options.

Once the question and answer pair is entered, the user clicks the "Next" button and then must wait a few seconds while the information is transmitted to MobiNET. Once that is complete, the user is prompted to enter their information. Finally, once this is completed, the user is provided with a window displaying the user id and providing prompting to add a host to access using the MobiKEY.

In order to add a host, the user clicks continue and is prompted to add either this computer or another remote host. In the case of the author's testing, the existing computer was used. The next step is to install the MobiNET host software on the computer. The MobiNET host software is installed via an Install Shield wizard that launches separately. The user is provided with the license agreement, which must be accepted in order to complete installation. The next step is to specify where the program will be installed (or accept the default location). Once these steps are completed, the MobiNET host software is installed and the user can then exit the wizard to return to the MobiKEY wizard.

The user is prompted to enter the host name so that the resource can be identified when initiating a remote session. In this case, the author chose the host name "Joe-Host PC" since this describes the resource that was used for testing purposes. After this is done, the program advises that the host was successfully added and prompts the user to reboot the PC to complete installation.

In the author's testing environment, the post-installation required significant issues. Windows Vista failed to restart on the test PC, and the author launched Windows recovery to get the PC back into an operational state. Ultimately, the author had to restore to an earlier state that wiped out the installation of MobiKEY and MobiNET agent. Upon inserting the MobiKEY into a USB port after recovery, the author was again prompted with an error from the machine indicating "HID DATA has stopped working." A Google search of technical support forums found that this issue relates to a program on the laptop for HP Quick Launch Buttons. The author took two actions in an attempt to remedy the situation. First, this error message seems to be commonly associated with installing a blue tooth mouse on HP laptops running Windows Vista. At the support forum located at URL http://forums.techarena.in/vista-hardware-devices/1023595.htm, the author found a recommendation to move several dynamic link library (DLL) files that related the HP Quick Launch Button program (see figure 5.2). Additionally, a search of the manufacturer website led the author to http://h10025.www1.hp.com/ewfrf/wc/document?docname=c01712518&cc=us&lc=en&dlc=en, where the user followed instructions to download a new version of the HP Quick Launch Button software. These two actions allowed the author to restore the test host to a functional state in order to test the MobiKEY. However, this state only lasted until the host machine was rebooted once again. Upon the next reboot of the PC, the system received a Windows Blue Screen and would not boot. The system rebooted and went into system recovery once again, where the



18-09-2008

Hyosaburo
Member

Join Date: Sep 2008
Posts: 1

here is the solution to your problem

I was having the same problem with my bluetooth microsoft wireless notebook presenter mouse 8000. The problem is created by an application in the HP quick launch Buttons. I removed the application from the launch buttons.

go to:

C:\Program Files\Hewlett-Packard\HP Quick Launch Buttons

move the following files to a backup folder on your computer:

HidActn.dll
Hiddata
PushHid.dll

Then restart you computer and you should not have the errors and the other things on your laptop should still be available.

Figure 5.2 Solution recommendation for test PC

solution was to restore the PC to an earlier state. At this point, MobiNET agent would no longer function, and any attempt to access the MobiKEY from a remote PC would show the host as being offline. The author made several attempts to reinstall the MobiNET agent software, but the results were the same. Ultimately, this only allowed the author to make one successful test session of the MobiKEY. All indications are that the issues encountered are specific to the test machine, and the author did not perform an exhaustive attempt to make this work again. For example, the author considered reloading the test PC or upgrading to a newer operating system, Windows 7. However, limitations of time due to the author's commitments professionally and to a deadline for this project made both of these options improbable. The author was also limited to testing MobiKEY with his personal PC, as this was the only machine to which he had access. While the author did have access to another computer that is provided by his employer, the employer's security policy specifically prohibited him from installing the MobiNET agent software on that machine as a host. The author performed a follow-up with Route1 about two months after testing the solution. The original contact, Neville Thomas, was no longer with the organization, so the follow-up was conducted with Tanieu Tan, Vice President of Marketing and Communication. Ms. Tan indicated that the author could have sought assistance from the Route1 technical support team for the installation issues. The author's own background with computers and technical support made him decide not to do this initially. Ultimately, the author also determined that the initial test session provided adequate information to test the security aspects of MobiKEY, so the PC-specific issues did not hinder the analysis.

5.2 Remote Session Using MobiKEY

Once the test machine had MobiNET agent installed and was functional, the next step was to test the solution by plugging the MobiKEY into another computer. In this instance, the author utilized another laptop that was temporarily connected to the same network as the host computer. This laptop will subsequently be referred to as the remote computer. Please see appendix C for screenshots showing the results that are discussed in the following section.

Upon inserting the MobiKEY into the remote computer, the author was provided with a login window that prompts the user to enter the MobiNET password associated with the MobiKEY. Once the password was entered, the author was provided with a list of resources that he is authorized to access. In this case, that was limited to the host computer. Once the author clicked on the “connect” button, he was provided with a full screen window of the host computer. The host computer also is administered with a login password, so the remote session also prompted the user to enter this password. Once the password was entered, the user was presented with the desktop of the host computer. He had the ability to open and run any programs or access any documents on the host PC using the remote session. The author observed that this was no different than accessing the PC locally.

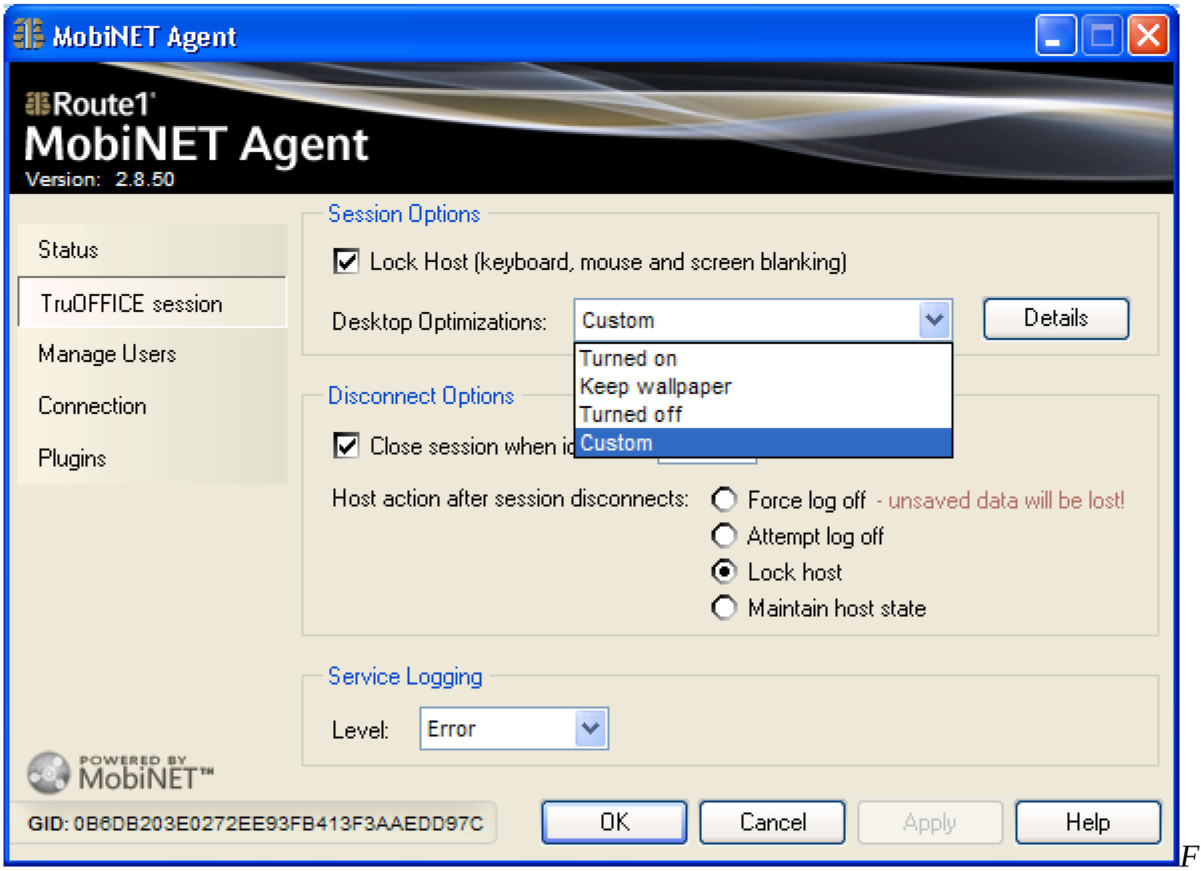
While running this session, the author also ran a packet capture on each machine using Wireshark, a free protocol analyzer available for download from www.wireshark.org. This tool allows the user to capture traffic that is occurring in both ways from the point of capture. On the remote computer, the author observed that Wireshark showed all traffic between MobiNET and the remote computer was in the Transport Layer Security version 1.0 (TLSv1). The remote computer initiates a client hello to the MobiNET server, and the two engaged in a handshaking and certificate exchange process. Next, the author observed that MobiNET initiates this same communication to the host computer. Once the session is mutually authenticated, the traffic was exchanged between the remote and host computer IPs directly. This information remained encrypted using TLS/SSL for the duration of the session. The packet capture on the host machine was consistent with what was seen on the remote computer. As noted earlier, these communications all occur over port 443.

Additionally, the author observed that the MobiKEY session indicates that the connection is authenticated using AES-256. Under the settings tab in the session window, the user can specify whether to use AES-256 or AES-128. This option is located under the "TruOFFICE Session" tab within the settings window. The default setting was set for the more secure AES-256 option.

More security is also provided under the "Presentation" tab of the settings window. The user has the option to be warned at startup if the computer has any remote access applications or screen capture applications running. These are selected by default, and provide further protection against anyone capturing any data that is transferred during the session.

By default, nothing is installed or transferred to the remote computer. There is an option in settings to turn on logging. There are three levels of logging (error, info, and debug), and these will write data to the remote computer. The user is warned of this before enabling logging. During the follow-up conversation with Tanieu Tan, the author learned that the logging feature is included in order for their technical support staff to diagnose any issues. Otherwise, the session is disconnected and disappears when the MobiKEY is disconnected from the USB port of the remote computer. There is no trace of the session left behind on the remote computer.

Since the author tested the machine in the same physical location, he was able to observe the host computer during the session. Since this is a remote access option, the keystrokes and actions taken on the remote computer could be observed in real-time on the host computer. As indicated previously, this makes it very important that the host computer be in a secured location. Otherwise, someone anyone with physical access to the host would be able to observe any actions taken, just as they would with any other remote desktop sharing solution. However, the risks are less than if the user takes the host computer out of the work location or transfers files to a USB drive that can easily be lost or stolen. Because this was the biggest security issue found with the product, the author mentioned this to Tanieu Tan. Tanieu provided information indicating that with MobiNET Agent version 2.8.50, the host is locked by default. This can be changed by the user, although obviously this is not recommended because of the increased risk it introduces. See figure 5.3 for a screenshot from MobiNET Agent showing where this can be changed in MobiNET Agent. Unfortunately, the author was unable to test this because of the issues encountered on the test machine. However, the information provided from Route1 is sufficient to indicate that this option provides increased protection from the standpoint of physical security as well.



MobiNET Agent

Route1

MobiNET Agent

Version: 2.8.50

Session Options

☑ Lock Host (keyboard, mouse and screen blanking)

Desktop Optimizations: Custom

Disconnect Options

☑ Close session when id

Host action after session disconnects:

○ Force log off - unsaved data will be lost!

○ Attempt log off

● Lock host

○ Maintain host state

Service Logging

Level: Error

GID: 0B6DB203E0272EE93FB413F3AAEDD97C

Figure 5.3 MobiNET Agent program TruOFFICE Session options

5.3 Observations

Based upon the test session that was successfully completed, the author observed that utilizing the MobiKEY for remote access seems to be a secure and very user-friendly method of remote access. Initial setup was actually very simple, other than the system issues that were encountered on the test PC. The session was secure and appeared to be no different than sitting directly in front of the host computer, with the exception that the host machine's desktop wallpaper was not visible. However, this likely could have been tweaked by changing the MobiKEY's color settings, if the author had been able to perform additional testing. This is a very minor issue, though, that had no impact on productivity or security. Overall, the process was secure and effective.

Despite the issues with installation, which the author recognizes as being specific to the PC, the author concluded that MobiKEY and TruOFFICE are a highly effective and secure method of remote access. If in a position to select a remote access solution for an organization, the author would highly recommend it based upon the security aspects. The fact that data never leaves the physical location and the trusted network helps to ensure greater security for the data while at rest. At the same time, the security of Route1's solutions helps to protect the information in transit and makes it nearly impossible for any intruders to compromise the session in progress. The solution is innovative and secure, and offers many advantages over other forms of remote access.

Chapter 6 – Conclusions

The reality of today's business world is that employees often do have a legitimate business need for remote access. Employees may need to work off hours from home, or access work resources while traveling for business. It may also provide advantages to companies by having their employees "go green" by not commuting to and from the office on certain days of the week. Remote access is here to stay, but the security implications of solutions to enable this must be carefully considered.

The purpose of this project was to evaluate the security advantages of MobiKEY from Route1 for remote access over other remote access solutions, such as VPN solutions and other remote desktop solutions, such as GoToMyPC and Laplink Everywhere. Based upon an analysis of existing literature and first-hand testing of the MobiKEY device, the author concludes that this product does indeed offer many significant advantages over other remote access solutions. The risks of using the MobiKEY are lower than those of other remote solutions. Among the key advantages are: two factor authentication; strong encryption of both the authentication process and the remote session; and physical security. Based upon this investigation, the author recommends MobiKEY as a remote access solution for organizations seeking a solution with maximum security.

Two-factor authentication is one of the greatest strengths of MobiKEY. Many remote desktop solutions simply depend upon a login and password in order to access resources remotely. With this solution, the user must possess both the password and the MobiKEY that is verified against the certificate authority within MobiNET in order to access resources remotely. Having possession of either the password or the device only is useless, as there is no way to access trusted resources without both. This is a significant advantage over browser-based solutions, which only utilize one factor and are potentially susceptible to browser-based vulnerabilities.

Additionally, MobiKEY offers strong encryption. The remote session using MobiKEY can be encrypted with either 128 or 256 bit AES. Most of the other alternatives that were investigated would only support 128 bit AES at this time. This level of encryption, combined with the use of the MobiNET to mutually authenticate the session, provides strong security.

Physical security is another huge advantage of the MobiKEY solution. No files ever leave the company's location, so there is no concern about lost or stolen laptops or USB sticks, or relying on user diligence to comply with security policies. Additionally, MobiKEY does not allow file transfer, so everything truly does stay behind the corporate firewall. The only way that anything leaves the trusted network is via local printer support, but even this is an option that may be disallowed if the administrator prefers. By actually working off the computer that is behind the protected firewall, MobiKEY offers a solution that protects data both at rest and in transit.

Ideally, the author would have been able to do more testing with the MobiKEY solution, if it were not for issues with the test PC. However, the testing done was significant enough to validate the advantages of this solution. The available literature on similar solutions, such as GoToMyPC and Laplink Everywhere, was significant enough to determine the similarities and differences among the products. While these other solutions do offer some similar advantages, Route1's offering seems far more secure for the reasons previously specified.

Additionally, it may have been beneficial to do hands on testing with VPN solutions for more comparison, but the author did not readily have access to any such solution. The costs and logistics of testing any such solution were prohibitive of any first-hand comparison, although this could provide the basis for future work.

Overall, the information gathered allowed the author to come to the conclusion that MobiKEY is a more secure solution than other remote access solutions. If placed in a position to select a remote access solution for an organization, the author would highly recommend MobiKEY for its security aspects.

Finally, remote access solutions seem likely to only become more prevalent in the future. As this occurs, new security concerns will arise and the need for strong security will increase. MobiKEY offers a secure solution for computer access, but their competitor, Laplink Everywhere, already has addressed the ability to access corporate data on smart phones. It seems that this is an area where there may be increased demand in the future. Technology is always evolving, and security must always be considered in order to preserve the value of information.

When considering any new remote access solution, security must be carefully considered. Any breach of the confidentiality, availability, or integrity of information can have devastating impacts on an organization. It’s important to balance convenience and productivity against the risks in order to minimize the likelihood of any such incident occurring. Organizations must find a happy medium between solutions that allow everything to be wide-open and those that are locked down to the point of being unusable.

References

Breeden, J. I. (2006). The key to mobile access. Retrieved December 29, 2009, from http://www.gcn.com/Articles/2006/11/16/The-key-to-mobile-access.aspx

Ciampa, M. (2005). *Security+ Guide to Network Security Fundamentals* (Second.). Thomson Course Technology.

Common Criteria for Information Technology Security Evaluation. (2009). Retrieved from http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Courtois, N. & Pieprzyk. (2002) *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations.* Retrieved 4/10/08 from http://eprint.iacr.org/2002/044.pdf

Cummings, J. (2008) Three caveats for desktop virtualization. Retrieved March 20, 2010 from http://www.networkworld.com/supp/2008/ndc5/081808-ndc-desktop-virtualization-caveats.html

Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules. (2001). . National Institute of Standards and Technology. Retrieved April 13, 2010 from http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Federal Information Processing Standards Publication 197. (2001) Retrieved March 20, 2010, from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Hills, R. (2005). Common VPN Security Flaws. Retrieved December 29, 2009, from http://www.nta-monitor.com/posts/2005/01/VPN-Flaws-Whitepaper.pdf

Marsan, C. D. (2009, October 19). Secure telework without a VPN - Network World. Retrieved December 29, 2009, from http://www.networkworld.com/news/2009/101909-telework-security-mobikey.html

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in Computing* (Fourth.). Prentice Hall.

Phifer, L. (2010) GoToMyPC Technology Security White Paper. Retrieved April 14, 2010, from https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Security_White_Paper.pdf

Scarfone, K., Hoffman, P., & Souppaya, M. (2009, June). NIST Special Publication 800-46, Revision 1: Guide to Enterprise Telework and Remote Access Security: Recommendations of the National Institute of Standards and Technology. Retrieved from December 29, 2009 from http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

Scarfone, K., & Souppaya, M. (2007). NIST Special Publication 800-114: User's Guide to Securing External Devices for Telework and Remote Access: Recommendations of the National Institute of Standards and Technology. Retrieved from December 29, 2009 from http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf

Stephenson, P. (2007). MobiKEY and MobiNET. *SC Magazine*. Retrieved December 29, 2009 from http://www.scmagazineus.com/mobikey-and-mobinet/review/1095/

Stoneburner, G., Goguen, A., & Feringa, A. (2002). NIST Special Publication 800-30 Risk Managment Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. Retrieved January 9, 2010 from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

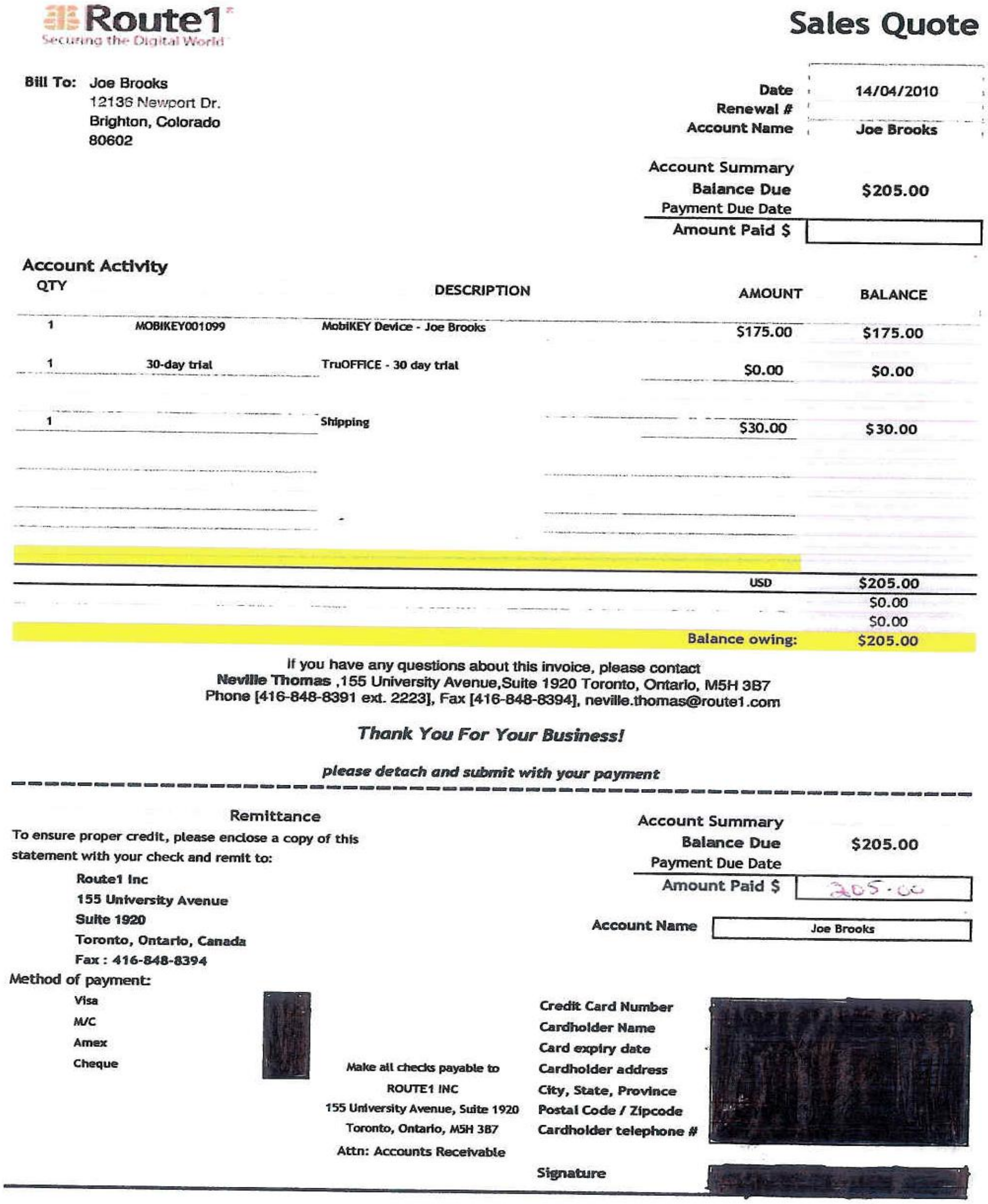
The Top Cyber Security Risks. (2009) Retrieved April 11, 2010 from http://www.sans.org/top-cyber-security-risks/

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules. (2008). . Retrieved April 13, 2010, from http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm

Warren, D., & Giobbi, R. (2009). *US-CERT Vulnerability Note VU#261869 Clientless SSL VPN products break web browser domain-based security models*. Retrieved January 9, 2010 from https://www.kb.cert.org/vuls/id/261869

Whitman,, M. E., & Mattord, H. J. (2005). *Principles of Information Security*. Thomson Course Technology.

Appendix A MobiKEY sales contract



Route1
Securing the Digital World

Sales Quote

Bill To: Joe Brooks
12136 Newport Dr.
Brighton, Colorado
80602

Date	14/04/2010
Renewal #	
Account Name	Joe Brooks

Account Summary

Balance Due	$205.00
Payment Due Date	
Amount Paid $	

Account Activity

QTY		DESCRIPTION	AMOUNT	BALANCE
1	MOBIKEY001099	MobiKEY Device - Joe Brooks	$175.00	$175.00
1	30-day trial	TruOFFICE - 30 day trial	$0.00	$0.00
1		Shipping	$30.00	$30.00

USD	$205.00
	$0.00
	$0.00
Balance owing:	$205.00

If you have any questions about this invoice, please contact
Neville Thomas ,155 University Avenue,Suite 1920 Toronto, Ontario, M5H 3B7
Phone [416-848-8391 ext. 2223], Fax [416-848-8394], neville.thomas@route1.com

Thank You For Your Business!

please detach and submit with your payment

Remittance

To ensure proper credit, please enclose a copy of this statement with your check and remit to:

Route1 Inc
155 University Avenue
Suite 1920
Toronto, Ontario, Canada
Fax : 416-848-8394

Account Summary

Balance Due	$205.00
Payment Due Date	
Amount Paid $	205.00
Account Name	Joe Brooks

Method of payment:
Visa
M/C
Amex
Cheque

[redacted]

Make all checks payable to
ROUTE1 INC
155 University Avenue, Suite 1920
Toronto, Ontario, M5H 3B7
Attn: Accounts Receivable

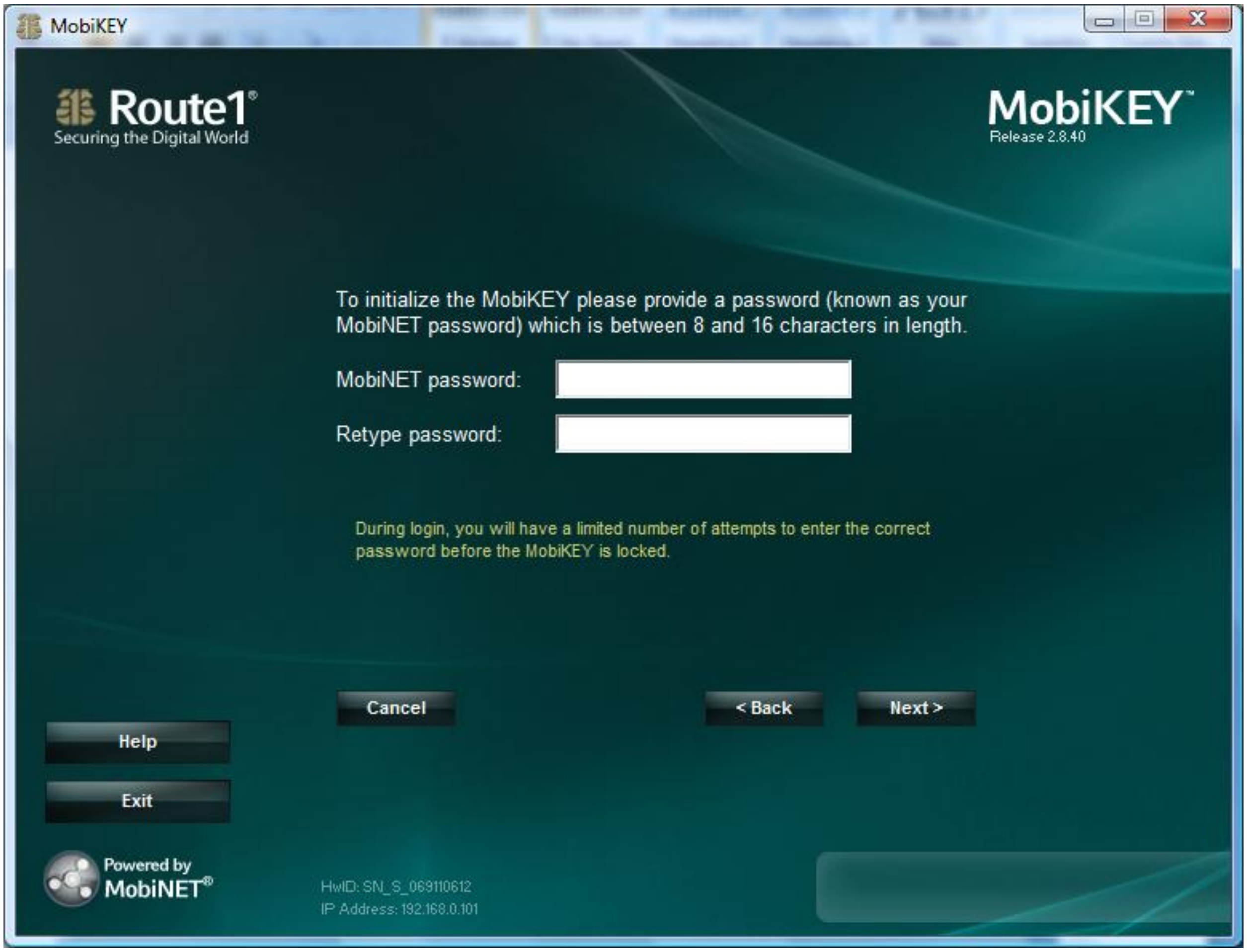
Credit Card Number
Cardholder Name
Card expiry date
Cardholder address
City, State, Province
Postal Code / Zipcode
Cardholder telephone #

[redacted]

Signature [redacted]

Appendix B Screenshots of MobiKEY installation

When MobiKEY is inserted, the executable file runs and you are prompted to enter the license key, provided by Route1 with purchase of the device.



To initialize the MobiKEY please provide a password (known as your MobiNET password) which is between 8 and 16 characters in length.

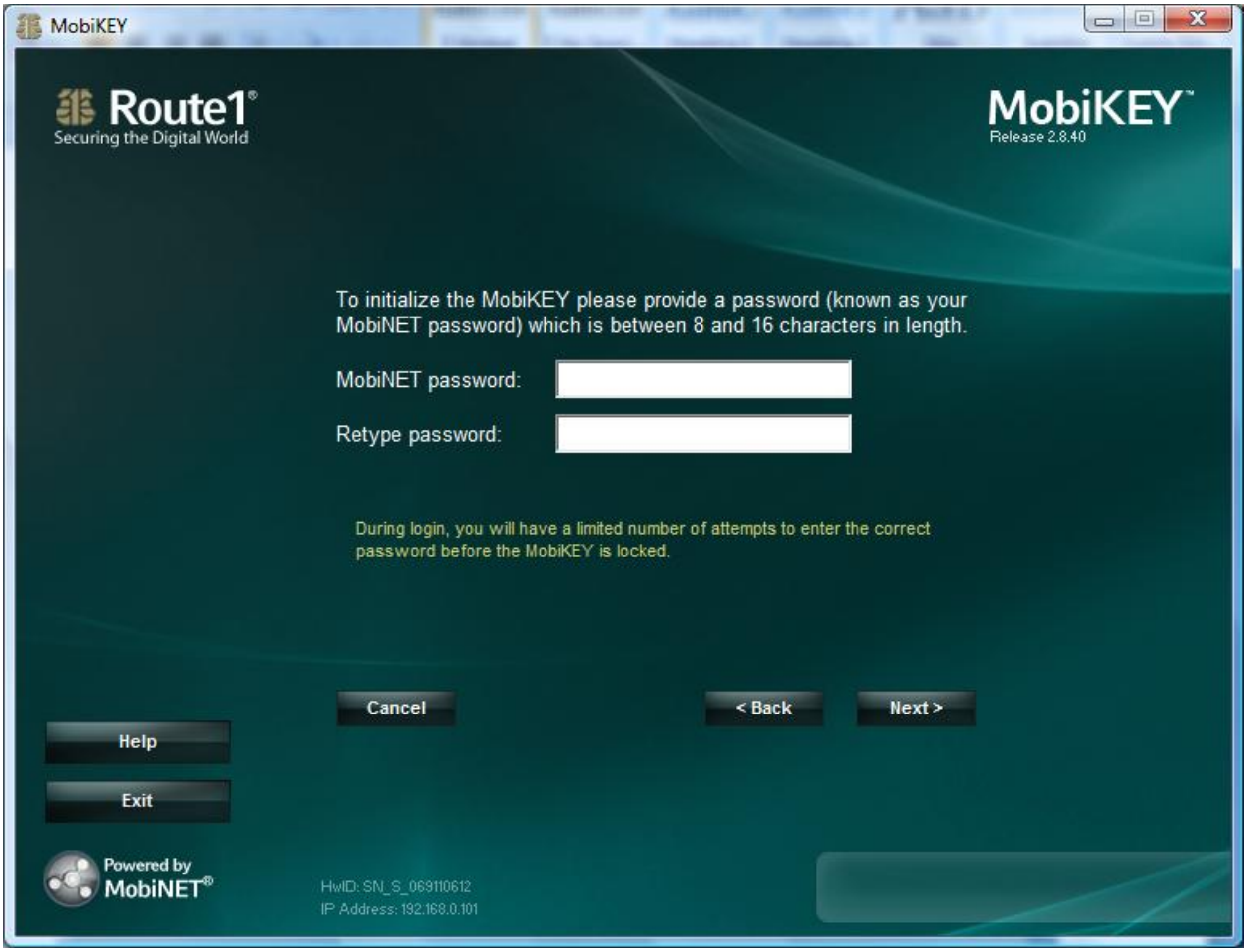
MobiNET password:

Retype password:

During login, you will have a limited number of attempts to enter the correct password before the MobiKEY is locked.

HwID: SN_S_069110612
IP Address: 192.168.0.101

After entering the product key, the user is prompted to create the MobiNET password. This password must be between 8 and 16 characters in length.



To initialize the MobiKEY please provide a password (known as your MobiNET password) which is between 8 and 16 characters in length.

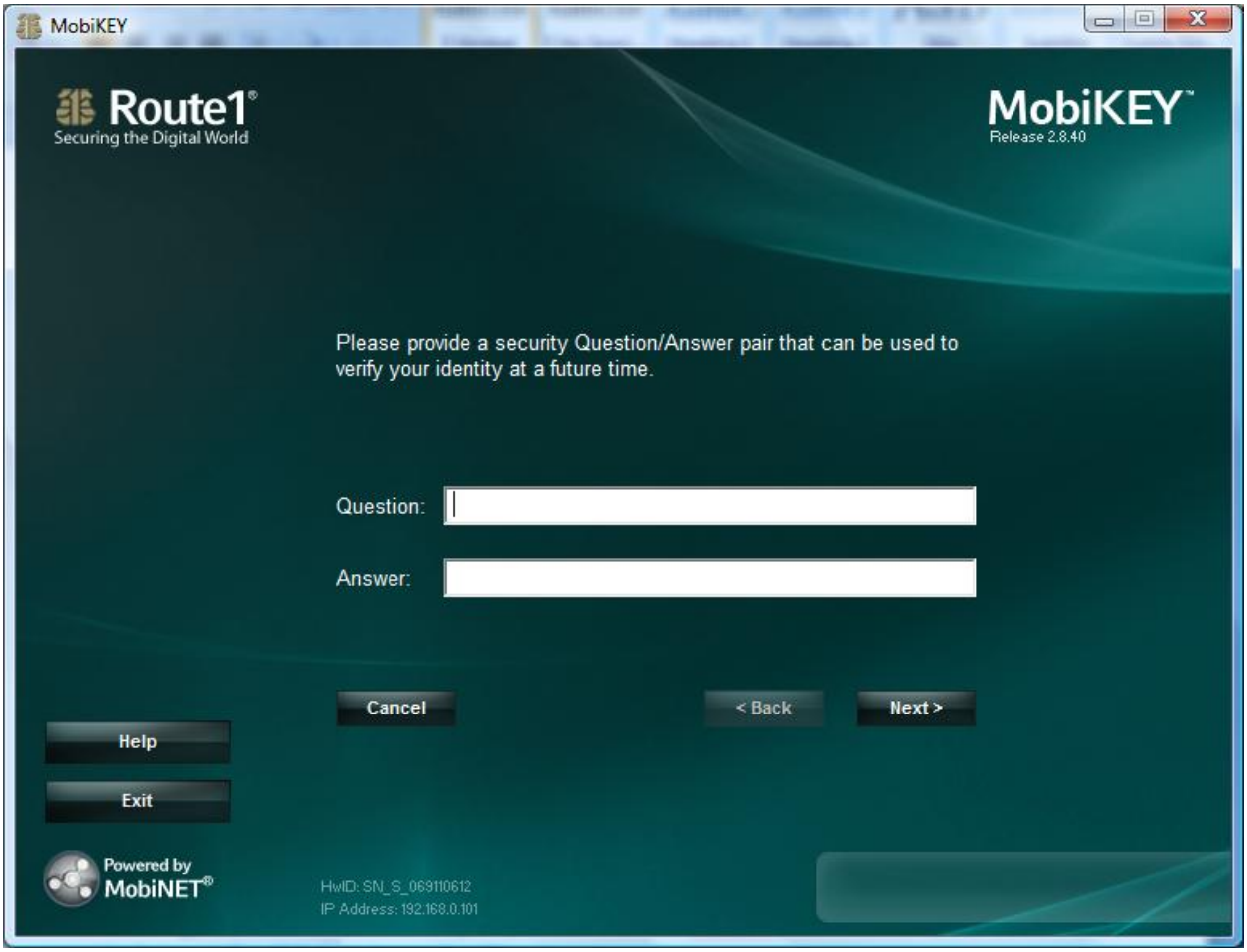
MobiNET password:

Retype password:

During login, you will have a limited number of attempts to enter the correct password before the MobiKEY is locked.

HwID: SN_S_069110612
IP Address: 192.168.0.101

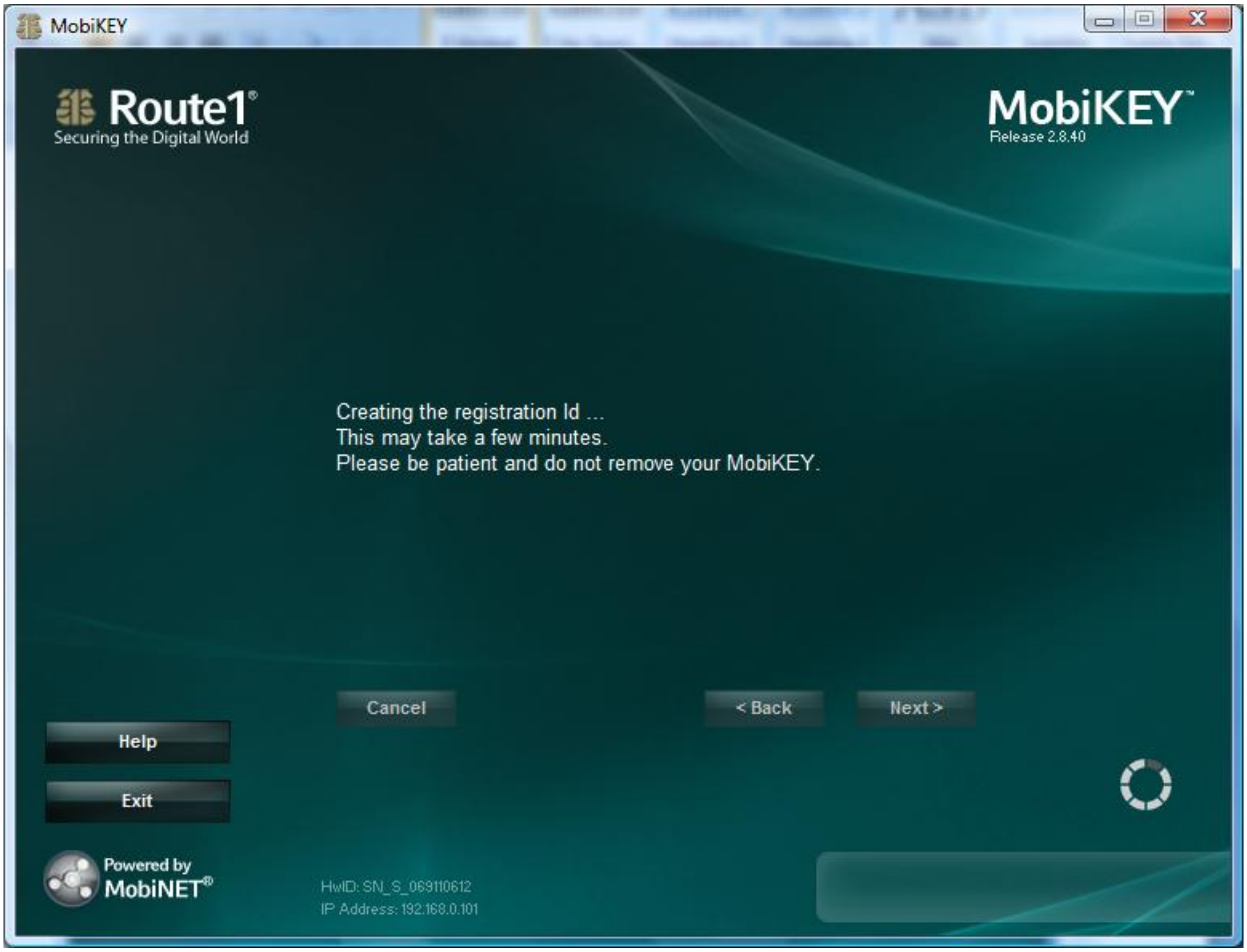
Next the user is prompted to create a security Question/answer pair to validate identity. Again, this is more secure that providing a standard question or a series of standard questions. Route1 allows you to create your own security question and answer.



Please provide a security Question/Answer pair that can be used to verify your identity at a future time.

HwID: SN_S_069110612
IP Address: 192.168.0.101

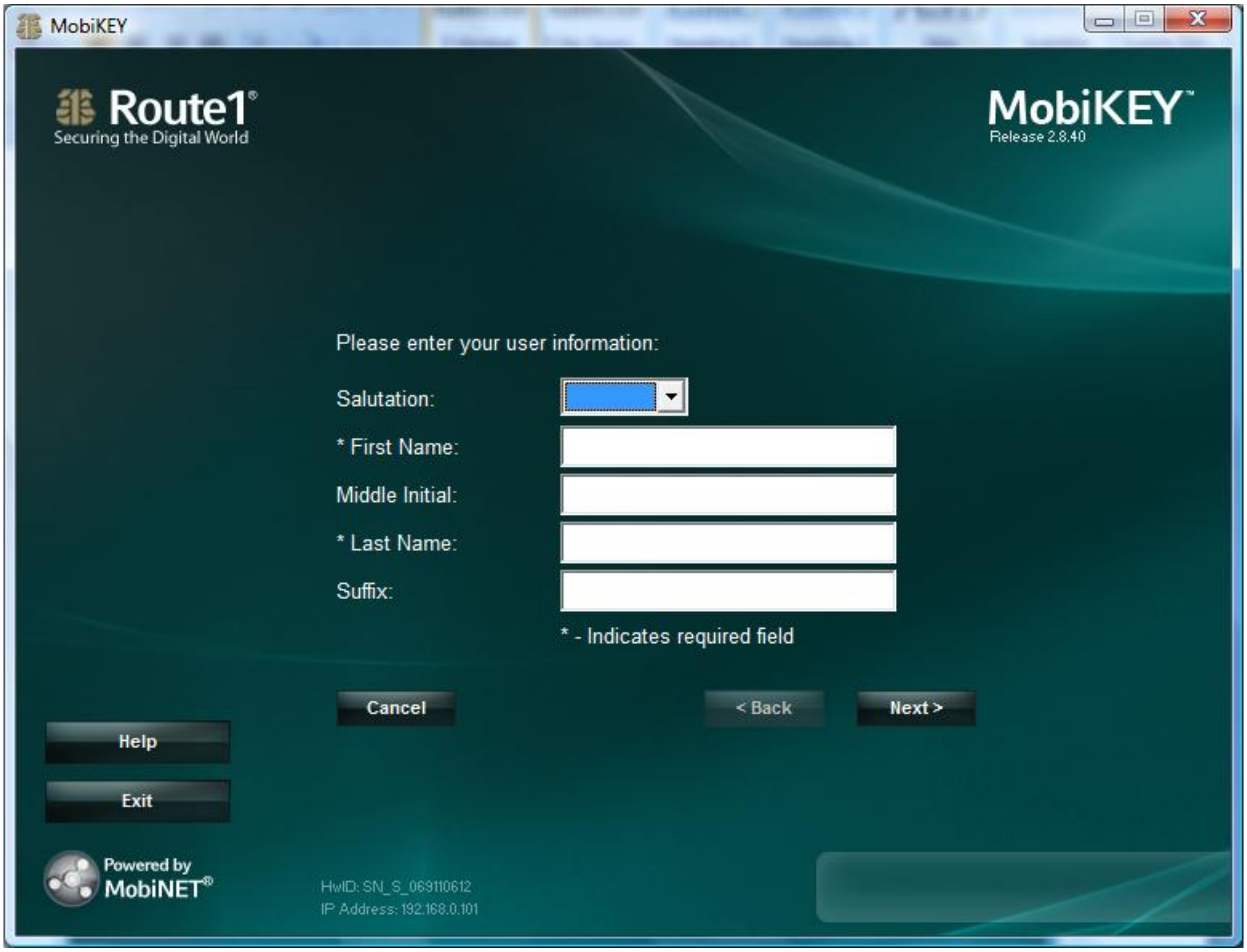
Next, the user waits a few seconds while information is transmitted to MobiNET.



Creating the registration Id ...
This may take a few minutes.
Please be patient and do not remove your MobiKEY.

HwID: SN_S_069110612
IP Address: 192.168.0.101

Next, the user is prompted to enter contact information on the following two screens.



Please enter your user information:

Salutation:

* First Name:

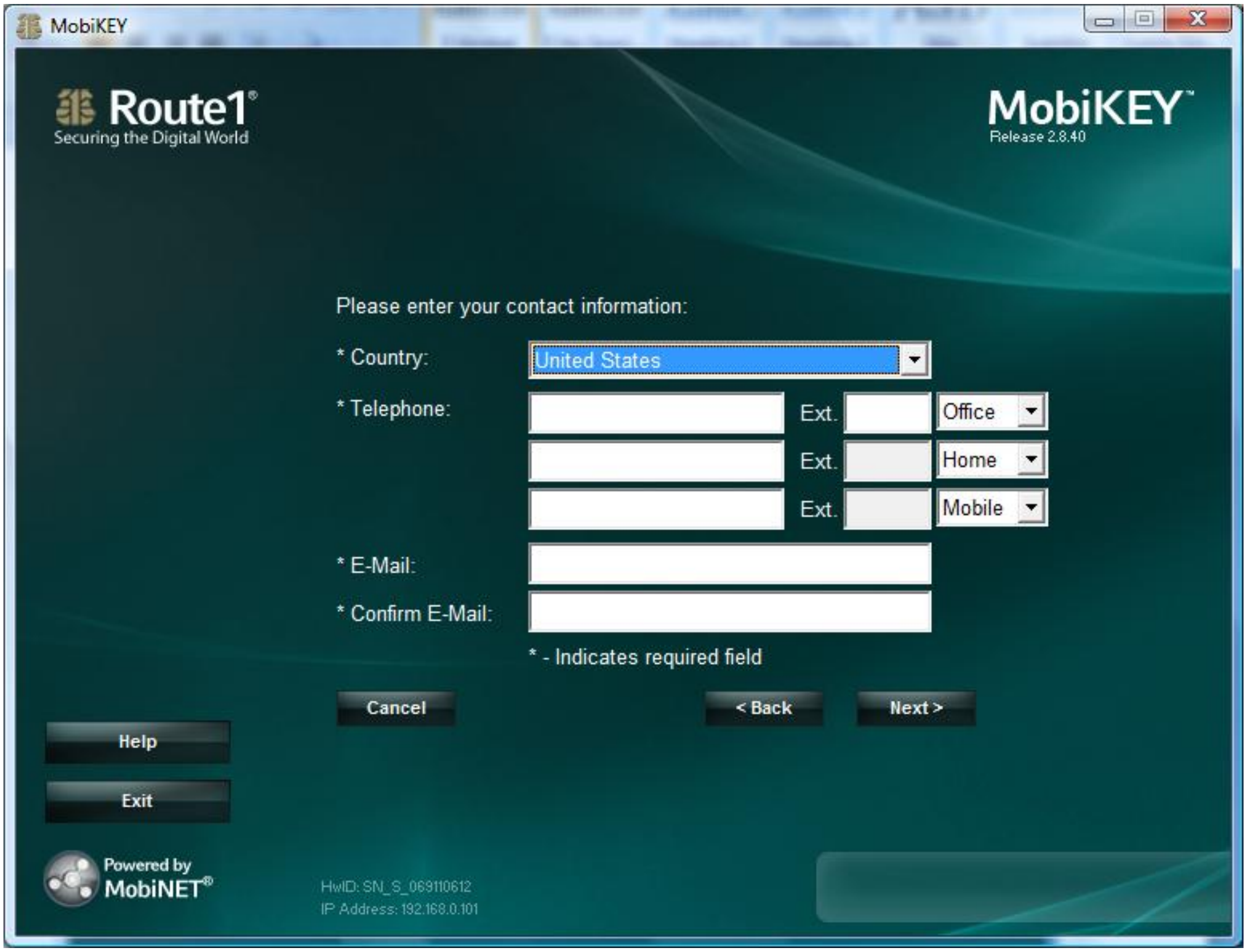
Middle Initial:

* Last Name:

Suffix:

* - Indicates required field

HwID: SN_S_069110612
IP Address: 192.168.0.101



Please enter your contact information:

* Country: United States

* Telephone: Ext. Office
Ext. Home
Ext. Mobile

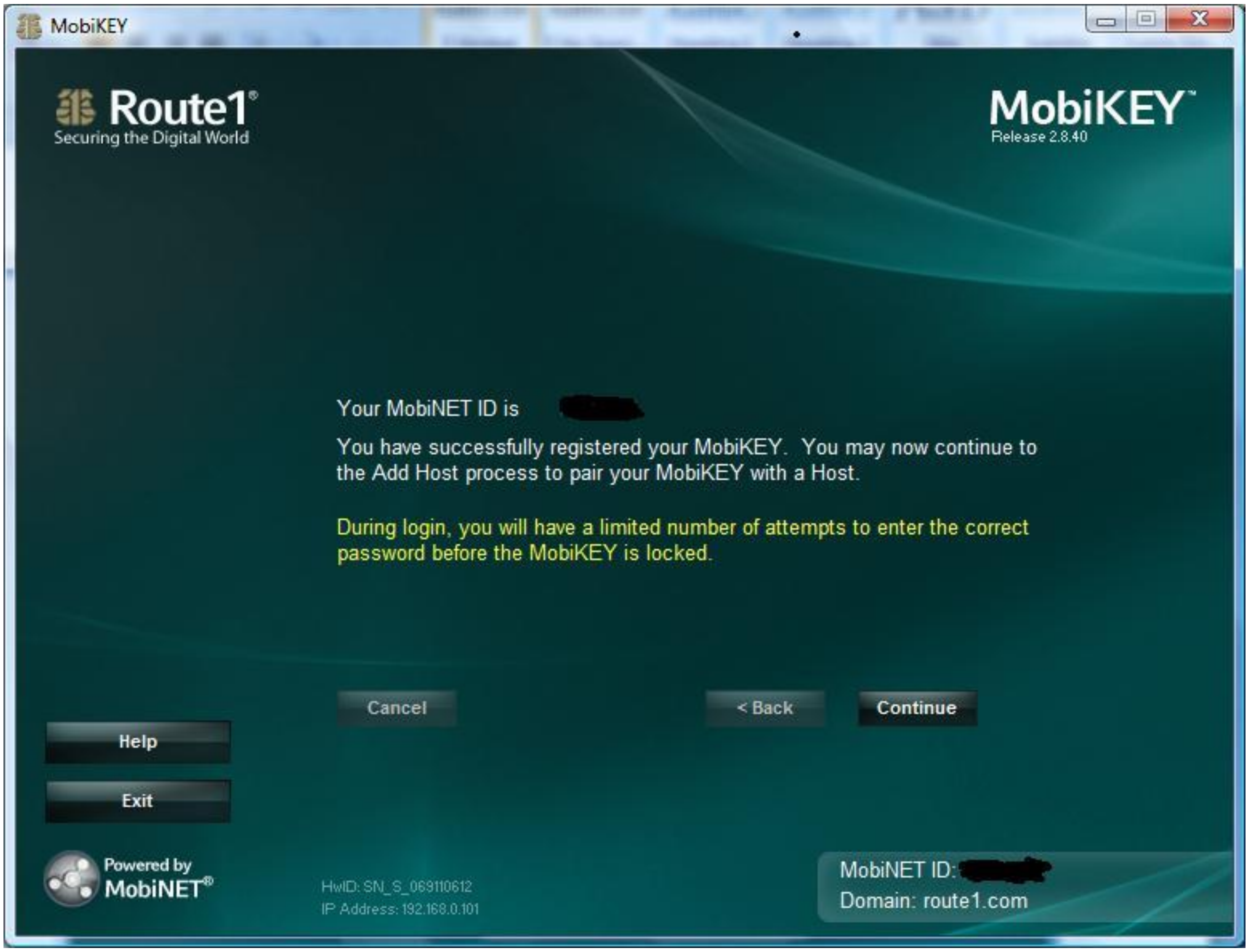
* E-Mail:

* Confirm E-Mail:

* - Indicates required field

HwID: SN_S_069110612
IP Address: 192.168.0.101

After successful registration, the user is presented with the MobiNET user ID (obscured here for the author’s security) and prompted to add a host for remote access.



Your MobiNET ID is [redacted]

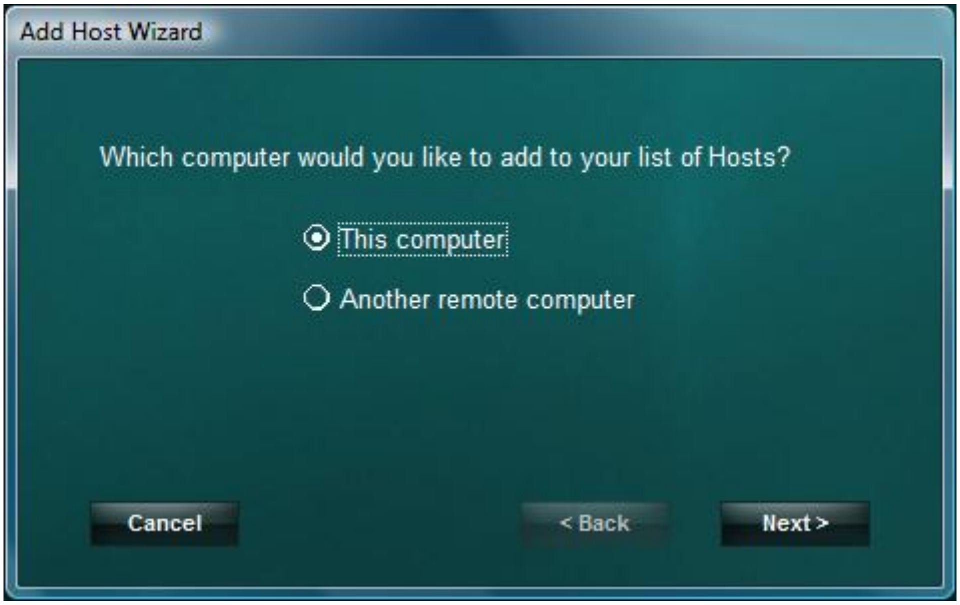
You have successfully registered your MobiKEY. You may now continue to the Add Host process to pair your MobiKEY with a Host.

During login, you will have a limited number of attempts to enter the correct password before the MobiKEY is locked.

HwID: SN_S_069110612
IP Address: 192.168.0.101

MobiNET ID: [redacted]
Domain: route1.com

The software then prompts you to install the Host software, if this is the first time that it's being registered with MobiNET.

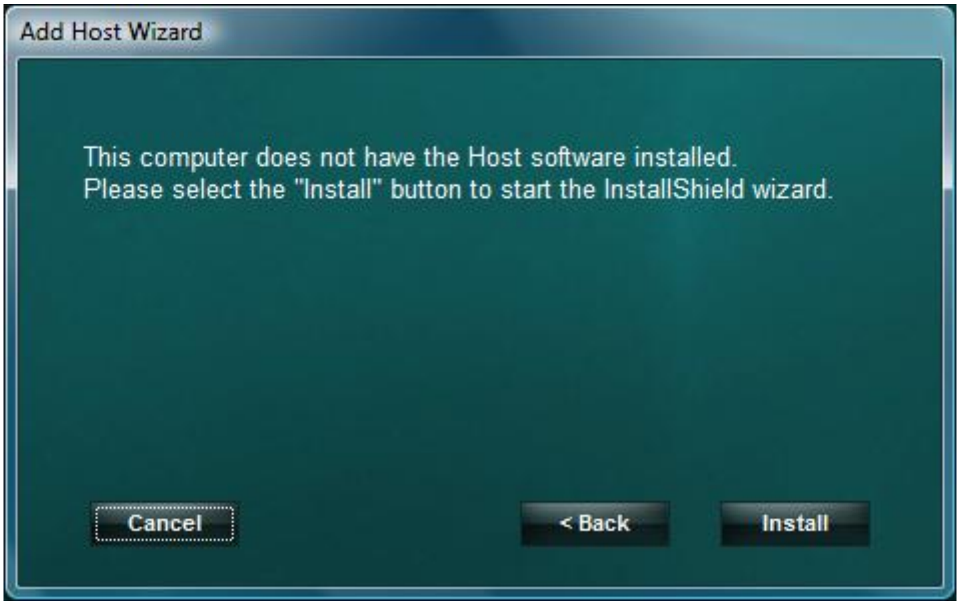


Add Host Wizard

Which computer would you like to add to your list of Hosts?

● This computer

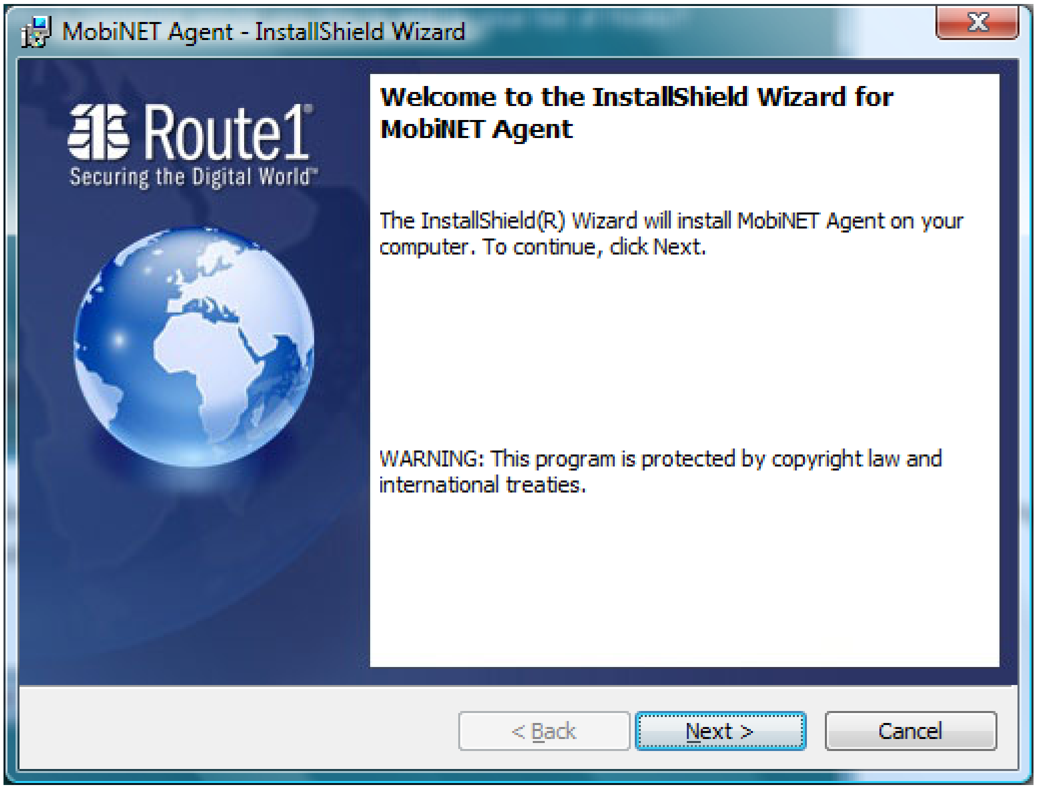
○ Another remote computer



Add Host Wizard

This computer does not have the Host software installed.
Please select the "Install" button to start the InstallShield wizard.

The following screens show what the user sees while installing MobiNET agent.

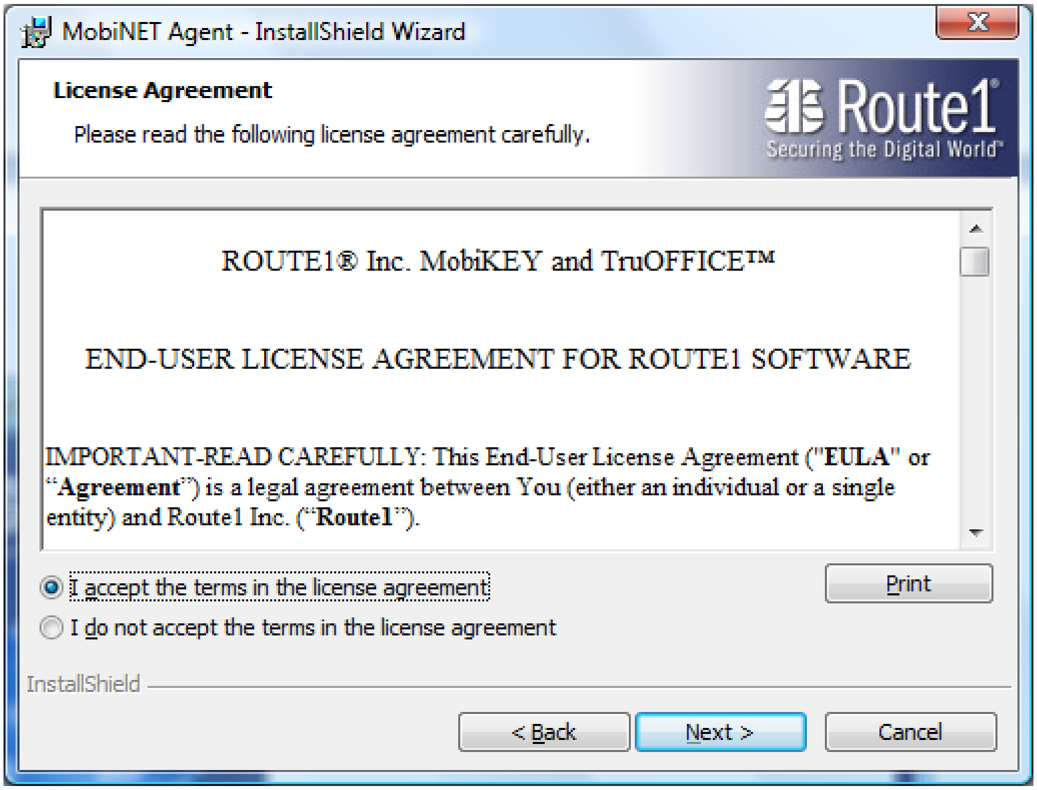


MobiNET Agent - InstallShield Wizard
Route1
Securing the Digital World

Welcome to the InstallShield Wizard for MobiNET Agent

The InstallShield(R) Wizard will install MobiNET Agent on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.



MobiNET Agent - InstallShield Wizard
Route1
Securing the Digital World

License Agreement

Please read the following license agreement carefully.

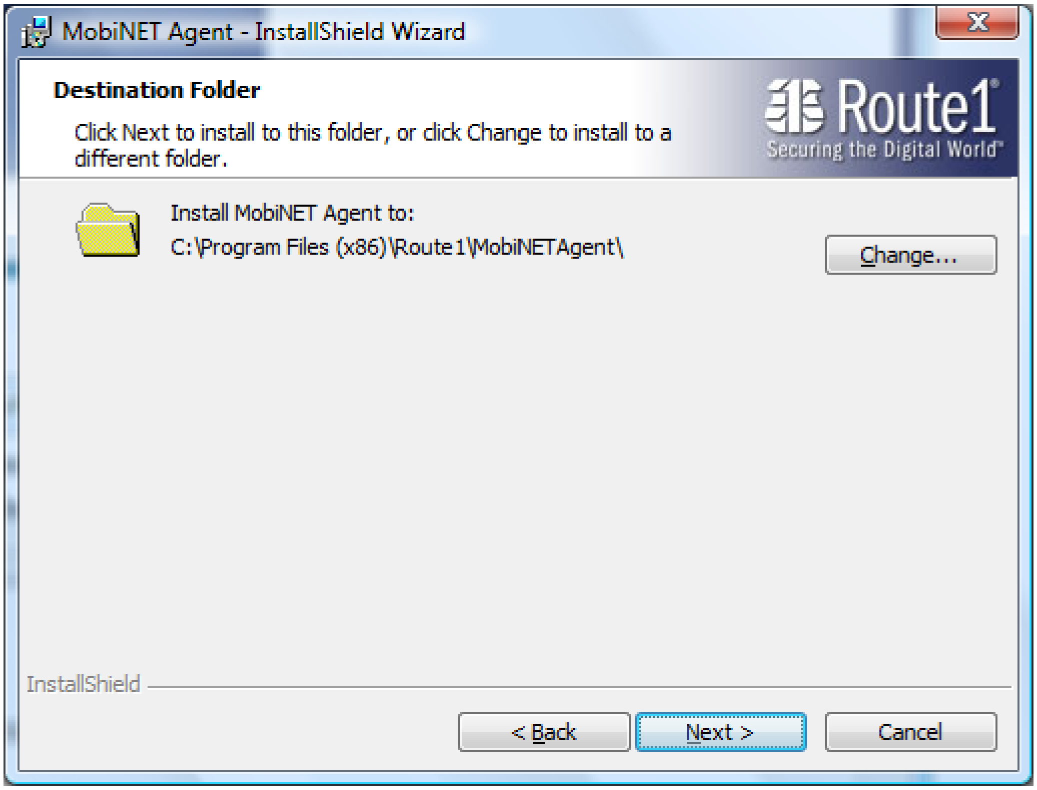
ROUTE1® Inc. MobiKEY and TruOFFICE™

END-USER LICENSE AGREEMENT FOR ROUTE1 SOFTWARE

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("**EULA**" or "**Agreement**") is a legal agreement between You (either an individual or a single entity) and Route1 Inc. ("**Route1**").

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

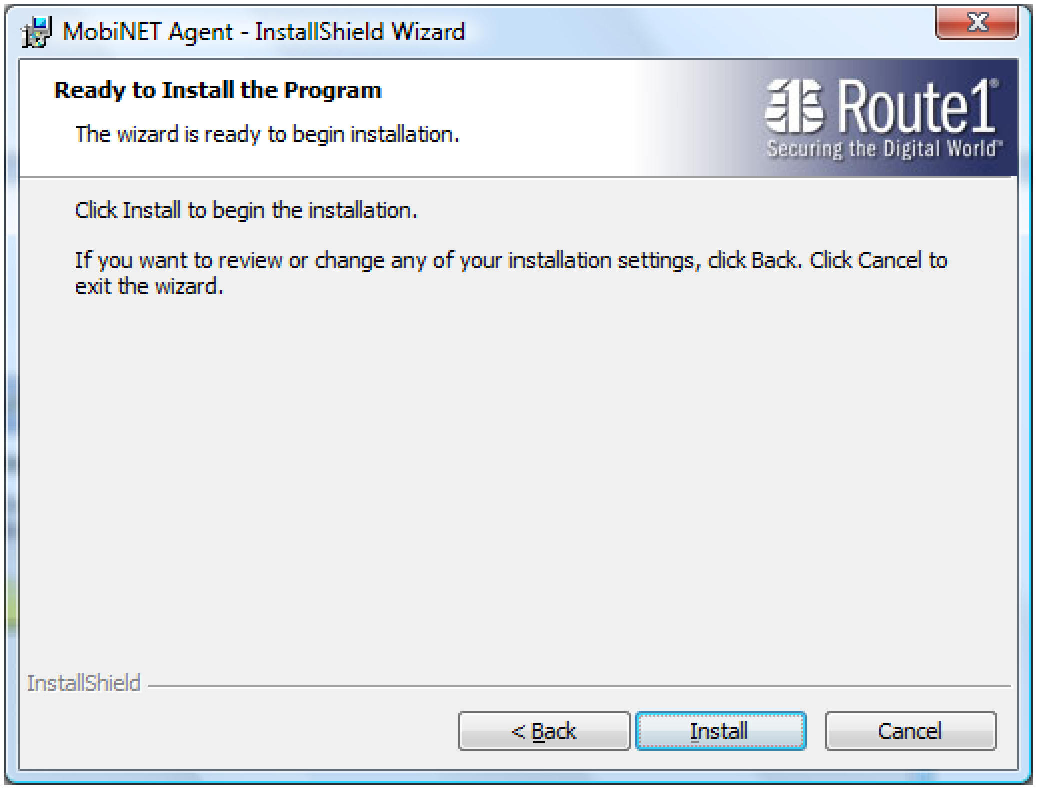


MobiNET Agent - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install MobiNET Agent to:
C:\Program Files (x86)\Route1\MobiNETAgent\



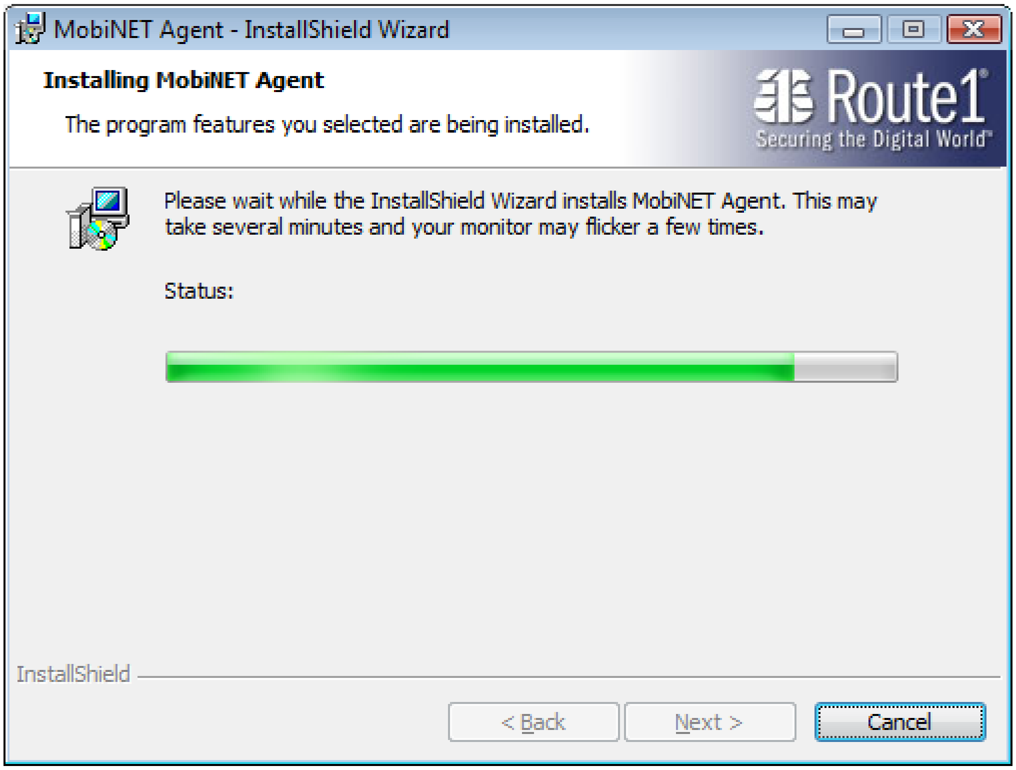
MobiNET Agent - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.



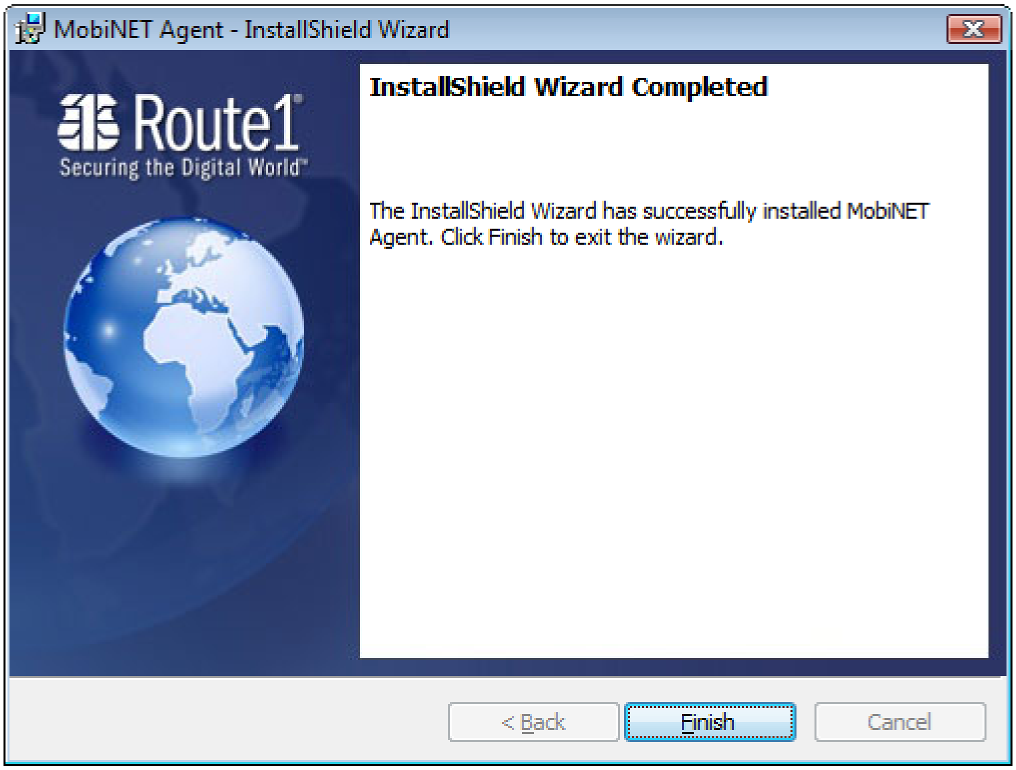
MobiNET Agent - InstallShield Wizard

Installing MobiNET Agent

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs MobiNET Agent. This may take several minutes and your monitor may flicker a few times.

Status:

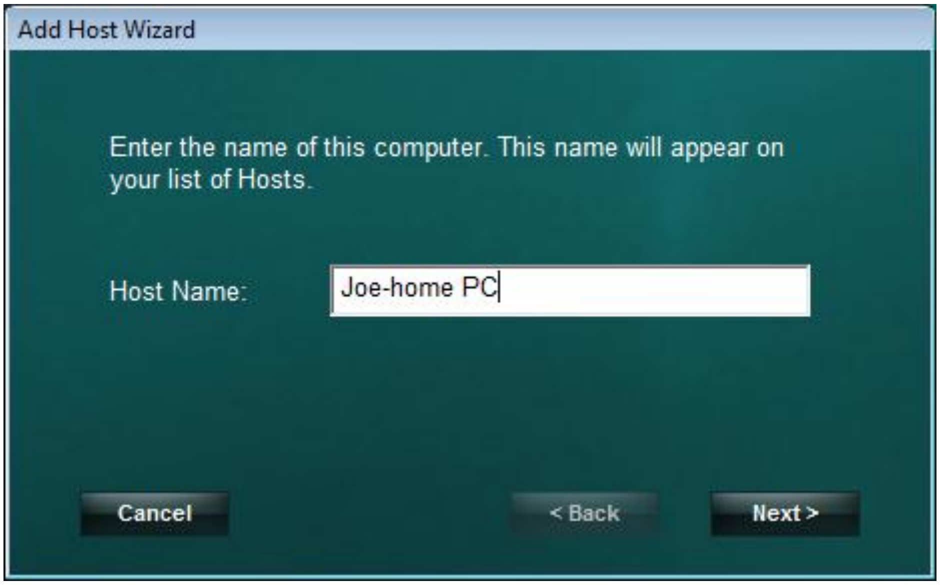


MobiNET Agent - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed MobiNET Agent. Click Finish to exit the wizard.

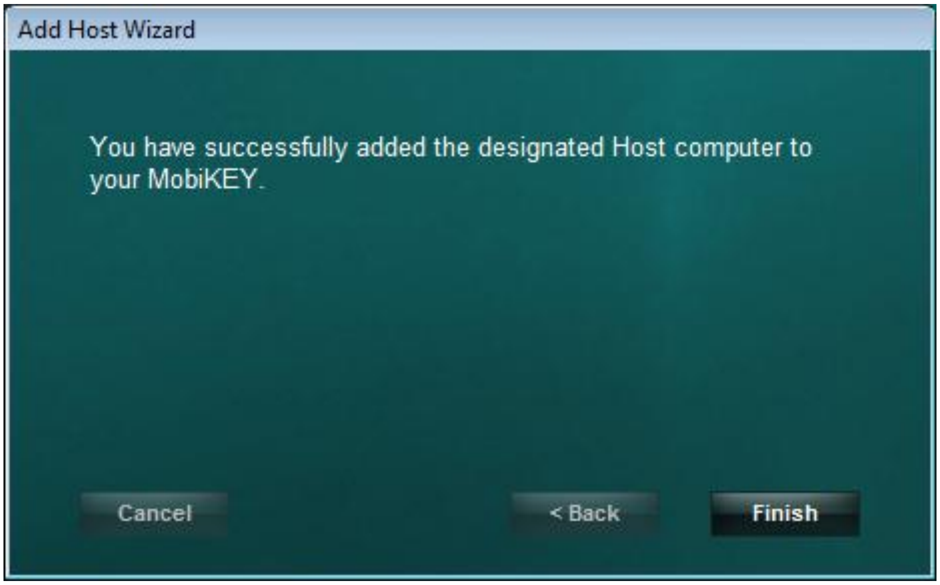
After completion of MobiNET agent installation, the user returns to the wizard to name the host.



Add Host Wizard

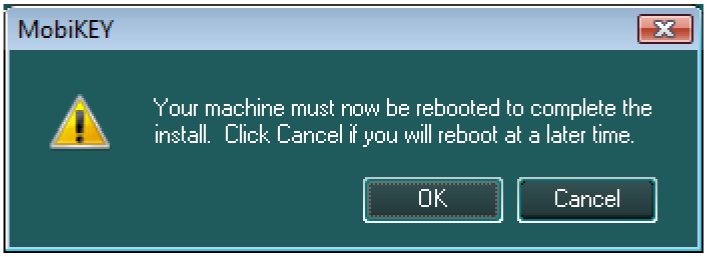
Enter the name of this computer. This name will appear on your list of Hosts.

Host Name: Joe-home PC



You have successfully added the designated Host computer to your MobiKEY.

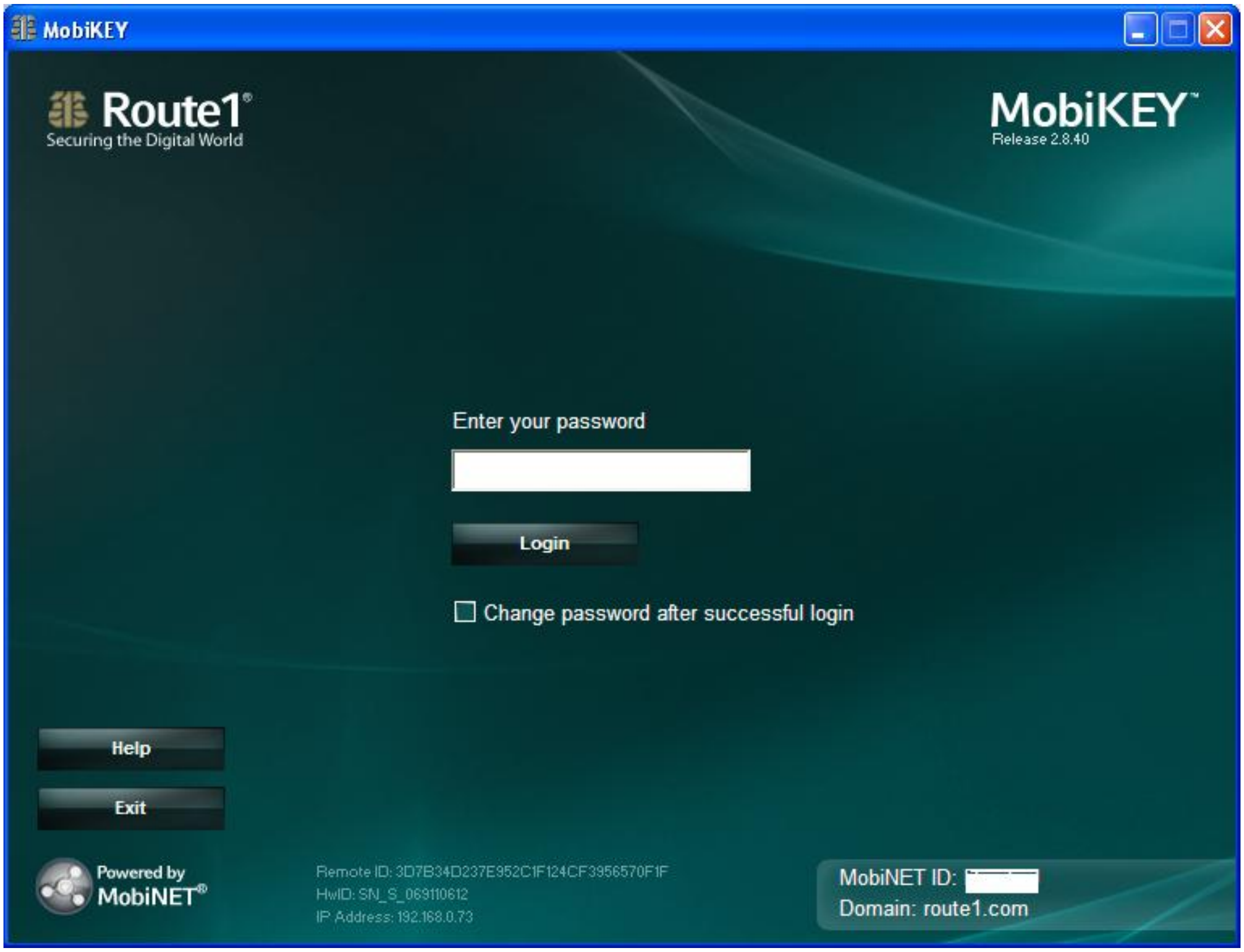
Finally, the host computer must be rebooted to complete installation.



Your machine must now be rebooted to complete the install. Click Cancel if you will reboot at a later time.

Appendix C Remote Access using MobiKEY

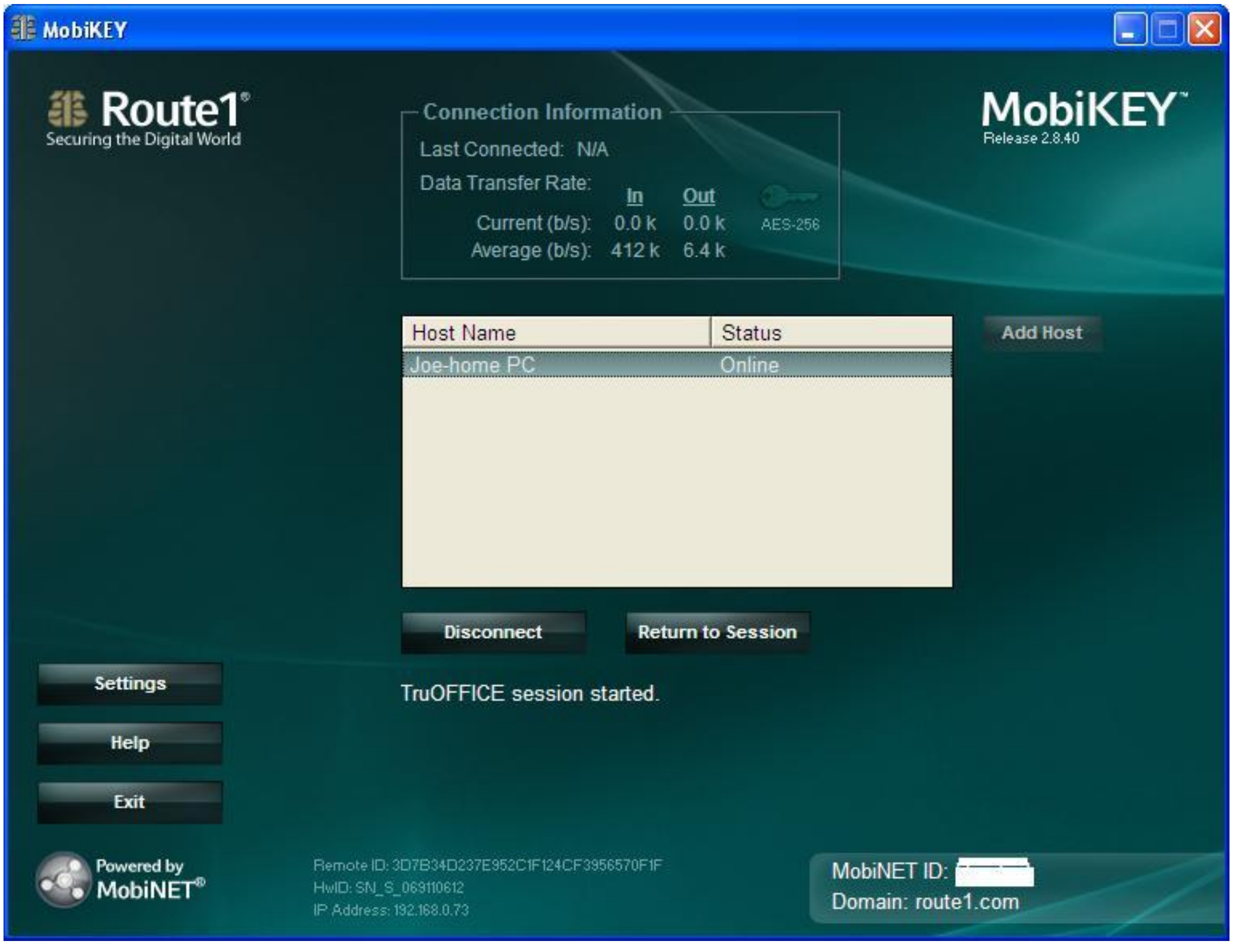
When plugging the MobiKEY into the remote computer, the user is prompted with a window requesting that he/she enter the appropriate MobiNET password.



Remote ID: 3D7B34D237E952C1F124CF3956570F1F
HwID: SN_S_069110612
IP Address: 192.168.0.73

MobiNET ID: [redacted]
Domain: route1.com

After successful authentication, the user is prompted with a list of authorized resources.



Connection Information

Last Connected: N/A

Data Transfer Rate:

	In	Out	
Current (b/s):	0.0 k	0.0 k	AES-256
Average (b/s):	412 k	6.4 k	

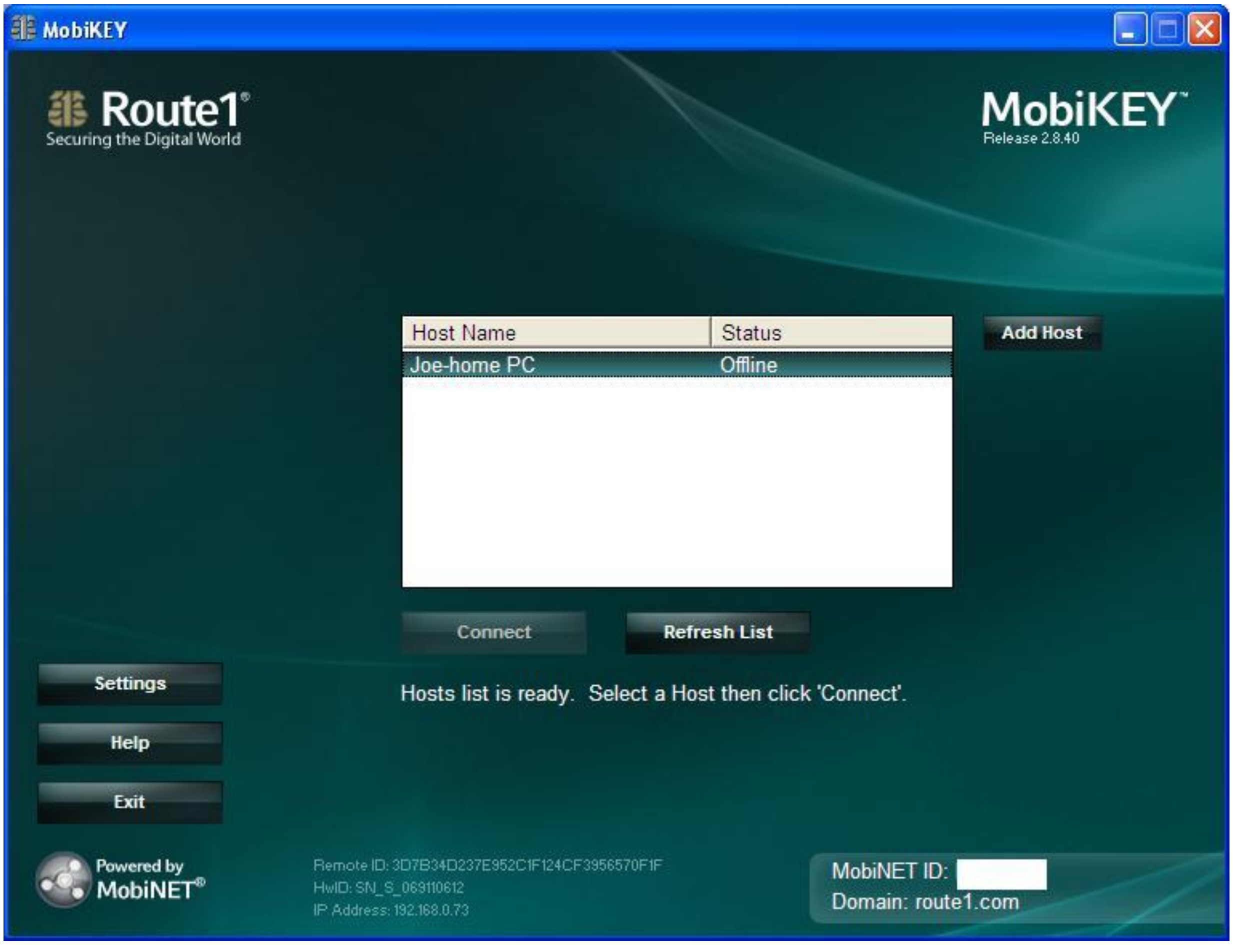
Host Name	Status
Joe-home PC	Online

TruOFFICE session started.

Remote ID: 3D7B34D237E952C1F124CF3956570F1F
HwID: SN_S_069110612
IP Address: 192.168.0.73

MobiNET ID: [redacted]
Domain: route1.com

If the remote host is not available, then the user will see this in the window as well.



Host Name	Status
Joe-home PC	Offline

Hosts list is ready. Select a Host then click 'Connect'.

Remote ID: 3D7B34D237E952C1F124CF3956570F1F
HwID: SN_S_069110612
IP Address: 192.168.0.73

MobiNET ID:
Domain: route1.com