GoToMyPC Corporate and RSA SecurID Integration

Enabling employees to work remotely improves their productivity and facilitates the growth of your organization by giving them access to the data they need, when they need it. However, mitigating security risks is an important consideration when using a remote access product. Many of the most damaging security breaches are the result of one thing: the theft of passwords to gain access to corporate information. For most organizations, the use of passwords alone may be sufficient to safeguard access to common applications and non-critical systems, but organizations with sensitive applications, data and systems demand an increased level of protection.

For these organizations, GoToMyPC Corporate provides secure, managed remote access to the desktop that reduces the costs and complexity associated with traditional remote access solutions while offering administrators the highest levels of security and centralized control. With a rapid deployment cycle and a clientless solution that requires minimal end-user training and ongoing maintenance, GoToMyPC Corporate provides SMS-based 2-step verification, which an administrator can configure. As an additional layer of security, GoToMyPC Corporate can also be seamlessly integrated with RSA Security's SecurID to provide unparalleled protection for remote access to company PCs.

True two-factor authentication

Single-factor authentication methods, such as a password requirement, provide a low-level proof of authenticity because anyone who overhears or steals the password will appear genuine. It is the addition of a second, physical proof of authenticity that makes the certainty of user authentication exponentially higher.

The ATM card is an example of a widely used form of two-factor authentication. It requires the owner to possess both a PIN and a valid ATM card. In the case of GoToMyPC's SMS-based 2-step verification feature, the user's phone serves as the physical authenticator.

For GoToMyPC Corporate users, RSA SecurID can provide another method of authentication via a SecurID token, which is a tamper-proof hardware device encased in a key fob or smart card. The token displays a token code that changes once every minute. The token and the SecurID server are the only parties that know the sequence of token codes.

How SecurID works

- From the SSL-secured GoToMyPC Corporate administration center, your organization's designated administrator sets the authentication policy to require SecurID at the organization, group or individual level.

- Your administrator configures each participating user's computer with the SecurID server(s) name, SecurID user name and RADIUS encryption key.
- When the user attempts to connect to the host computer from the client computer, the user is challenged for the PASSCODE, which is securely transmitted to the host via Advanced Encryption Standard using 128-bit keys.
- The host computer communicates with the SecurID Server using RADIUS, which verifies the PASSCODE and authenticates the user for the connection.

System requirements

- An existing installed RSA SecurID system running RSA Authentication Manager version 5.0.01 or later with RADIUS server support
- Purchase of GoToMyPC Corporate
- Host PC: Microsoft Windows XP or later. (Mac integration not yet available.)

Contact us

To learn more about how the GoToMyPC Corporate option can meet your needs for enhanced security, please call us toll-free at 1 888 646 0016 or direct dial +1 805 690 5780. Or, visit our website at www.gotomypc.com.