

Managed Two-Factor Authentication

Virtela offers Managed Two-Factor Authentication services to provide customers added security via an additional means of end-user identification. Our service is based on the RSA/ACE server and RSA SecurID hardware and software tokens, ensuring positive identification of users that access corporate resources.

For hardware tokens, Virtela deploys key fobs. Key fobs are lightweight, water-resistant tokens suited for a variety of environments that authenticate a user's identity, allowing network access to authorized users while locking out hackers. The SecurID key fob token displays a quasi-randomly generated access code that changes every 60 seconds and users login by entering a secret personal identification number (PIN) followed by the current code displayed on the SecurID token. The login process is one simple and quick step, and processing of user credentials is transparent to the user.

Virtela offers Windows-based and Internet Explorer browser based tool bar tokens for customers interested in software token solutions. RSA SecurID software tokens use the same algorithms as the RSA SecurID hardware tokens while eliminating the need for users to carry dedicated hardware devices. Authentication is enabled through familiar interfaces. Software tokens require software to be pre-installed on an end-user's machine.

Committed to providing the highest level of service, Virtela's Global Operations Center (GOC) is staffed 24x7 with a highly trained team of engineers and network experts dedicated to the design, implementation, and maintenance of customers' remote access networks. Virtela will procure and manage the RSA tokens and the ACE server for customers, including token replacement and reset issues.

Hackers are experts at cracking logins and passwords. A single password provides a low proof of authenticity as anyone who overhears the password, sees the end-user type in the password, or captures the password via keystroke logger software, can use it to login and appear to be the actual end-user. The widespread use of public Wi-Fi hotspots compounds this problem. Security administrators need to ensure that the person attempting to access protected files and/or resources is an authentic user vs. an impostor. Remote users need a secure means to authenticate before being allowed access to corporate resources. Two-Factor Authentication adds a second layer of protection requiring proof of identity making the certainty of authenticity exponentially higher as the password changes every 60 seconds.

A major healthcare product developer and manufacturer is currently using Virtela's managed SecurID solution to better secure their remote access users. Virtela took over management of the customer's existing ACE server infrastructure and key fob end-user tokens, significantly reducing the support requirements for the IT staff allowing them to focus on other business critical projects.

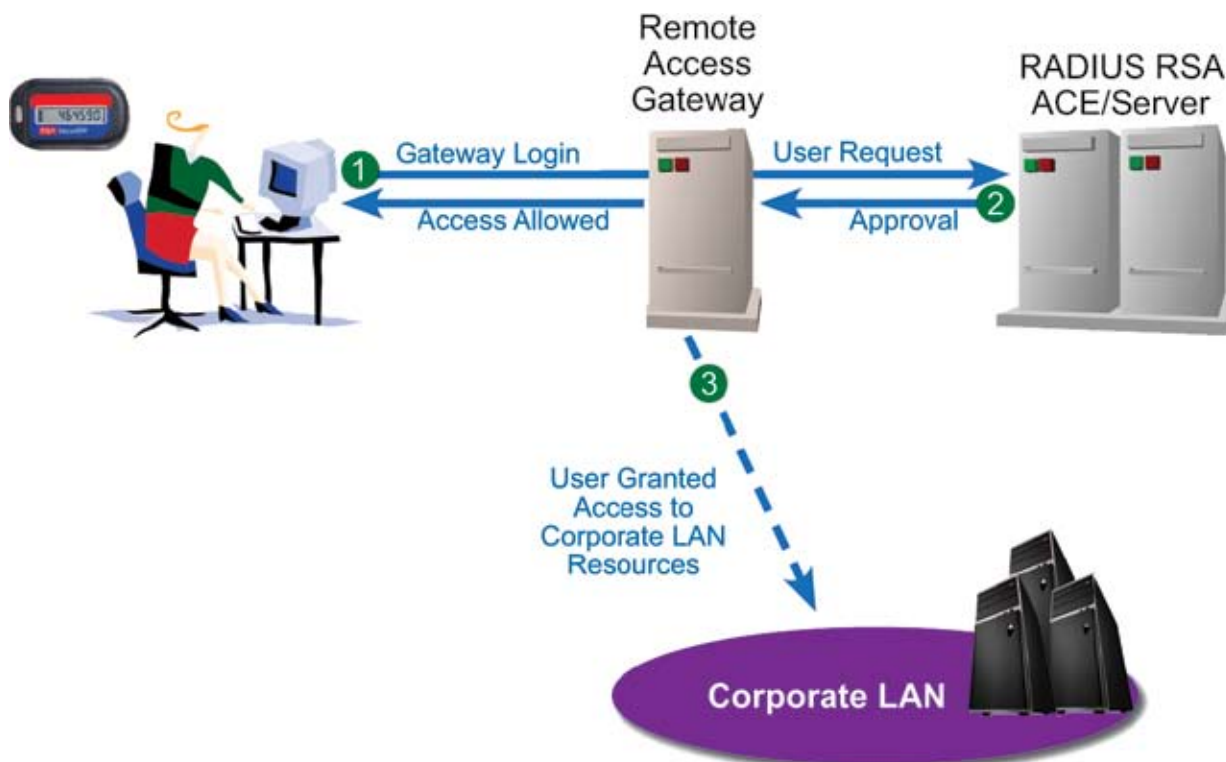


Key Benefits:

- Secure authentication of end-users
- Virtela provided and managed tokens and network based ACE server infrastructure
- Virtela can take over management of existing SecurID infrastructure
- 24x7 Support for PIN or token resets, application issues, & lost token replacement

Managed Two-Factor Authentication

Virtela's Managed Two-Factor Authentication is designed to strengthen and protect end-users' credentials and access to corporate resources. Delivered across our secure global network, Two-Factor Authentication limits risk for multinational enterprises as it can drastically reduce the incidence of fraud or hackers accessing corporate resources.



About Virtela:

Virtela Communications Inc. delivers award-winning network and security solutions to many of the world's largest and fastest-growing multinational companies. Currently serving customers across six continents, Virtela's network reach spans more than 190 countries. Virtela's unique Global Service FabricSM offers the foundation for delivering critical applications via the company's acclaimed service methodology, with a services suite that includes MPLS and IP-based virtual private networks (VPNs), security services, remote monitoring and management of WAN/LAN infrastructure, and converged services (data, video, voice).

