



Readme

RSA ACE/Agent 5.5 for Windows

December 2002

Introduction

This document contains important configuration and installation information for the RSA ACE/Agent 5.5 for Windows. It also contains information about problems in the software found too late to be included in the standard documentation. Read this document before installing the RSA ACE/Agent 5.5 for Windows software.

Installation

The RSA ACE/Agent 5.5 for Windows installs and supports local and remote access to Windows operating systems. Administrators can use the RSA ACE/Agent 5.5 for Windows to authenticate users accessing their computer desktops, as well as users accessing the network remotely through Routing and Remote Access Server (RRAS) or Internet Authentication Server (IAS) on Windows 2000 Server.

The RSA ACE/Agent 5.5 for Windows does NOT install or support the following authentication components:

- Web access
- Network access

Caution: DO NOT install RSA ACE/Agent 5.5 for Windows if your current installation is RSA ACE/Agent 4.x or later with either the Network access or the Web access authentication components installed, and you want to continue to implement these types of authentication. Installing the RSA ACE/Agent 5.5 for Windows removes any prior versions of web and network access, and installs local and remote access ONLY.

Configuration

When you configure remote client computers to use RSA Security EAP, the Properties button in the Advanced Security Settings dialog box appears to be enabled, but in fact, there are no configurable properties when you choose RSA Security EAP.

Authentication

If a new PIN is not accepted by the RSA ACE/Server when authenticating through RSA Security EAP (Extensible Authentication Protocol), there is no specific message indicating that the new PIN was accepted or rejected; instead, only the message "Access Denied" is displayed. In this situation, you should check with the RSA ACE/Server administrator to determine if the new PIN was either accepted or rejected.

This release does not allow for group challenges using RSA Security EAP. In addition, only the following group deployments are allowed when using post-dial terminal based authentication, or local authentication:

- Local groups in a local computer's Security Accounts Manager, including
 - all users in the local group
 - all users in a domain global group that is part of the local group
- Domain local groups that are part of a domain into which a user is logged, including
 - all users in the local group
 - all users in the domain global group that is part of the local group.
- Domain global groups that are part of a domain into which a user is logged, including all users in that domain group.

Domain trust groups are NOT supported. RSA Security recommends that you test all group environments to ensure that they work properly with RSA SecurID.

RSA Security recommends that you enable a reserve password for use with local authentications. Doing so will ensure that users are not locked out of their desktops in the event of a failed network connection.

On Windows XP machines, if you configure Local access authentication to challenge groups with either the "Users In" or "All Users except" settings, there may be instances where every user is challenged when the machine is re-booted for any reason. This is caused by a delay in relaying necessary group information from the Windows XP operating system to the RSA ACE/Agent 5.5 for Windows. Instruct any user who is inappropriately RSA SecurID challenged to do the following:

1. Click **Cancel** in the RSA SecurID challenge window, then click **OK** in the Access Denied message.
2. Repeat the login process. This second time, users will not be RSA SecurID challenged.

Getting Support and Service

RSA SecurCare® Online

www.rsasecurity.com/support/securcare

Technical Support Information

www.rsasecurity.com/support

© 2002 RSA Security Inc. All rights reserved.
First printing: December 2002

Trademarks

ACE/Agent, ACE/Server, Because Knowledge is Security, BSAFE, ClearTrust, JSAFE, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, RSA Security, SecurCare, SecurID, Smart Rules, The Most Trusted Name in e-Security, Virtual Business Units, and WebID are registered trademarks, and the RSA Secured logo, SecurWorld, and Transaction Authority are trademarks of RSA Security Inc. in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.