Release Notes
RSA Authentication Agent 6.1.4 for Microsoft Windows

March 2013

Introduction

This document lists what's new in RSA® Authentication Agent 6.1.4 for Microsoft Windows. It also includes workarounds for known issues. Read this document before installing the software. This document contains the following sections:

These *Release Notes* may be updated. The most current version can be found on RSA SecurCare® Online at **https://knowledge.rsasecurity.com**.

What's New in This Release

This section describes the major change introduced in this release. For detailed information on additional features in Authentication Agent, see the *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*.

Version 6.1.4

Security vulnerability. In previous versions of this product, the node secret was stored using a weak encryption key and a dated encryption algorithm. This mechanism has been replaced with stronger encryption and stronger keys.

Offline authentication. As of version 6.1.4, RSA Authentication Agent no longer supports offline authentication on Windows 2000 Server platforms

Version 6.1.3

Resolved security vulnerabilities in RSA Security EAP Client Component. Authentication Agent for Microsoft Windows products includes the EAP (Extensible Application Protocol) plug-in component that allows users to log on over Virtual Private Networks (VPNs) or wireless connections to access corporate data. The component allowed several security vulnerabilities that could impact corporate resources. These vulnerabilities no longer exist.

For instructions on how to deploy RSA Security EAP for Microsoft Windows Vista, see the RSA SecurID Wireless Authentication Solution Guide or contact RSA Customer Support at **www.rsa.com/support**.

Required Service Packs and Fixes

For wireless authentication using EAP, access points must support 802.1x authentication.

To use wireless LAN with PEAP, install SP2 for Windows XP or SP2 for Windows Server 2003. If you cannot update to the current service pack, you must install Microsoft hot fix Article ID 827537 on the Windows XP client and the Windows Server 2003 host. To get the fix and installation instructions, see the Microsoft Support Knowledge Base at **http://support.microsoft.com/**.

For Windows Server 2003, if Terminal Services or Citrix Metaframe users are prompted to authenticate with RSA SecurID even though you configured the terminal server for standard Windows authentication, install Microsoft hot fix Article ID 838462 available in the Microsoft Support Knowledge Base at **http://support.microsoft.com/**.

Installing the Upgrade

To upgrade RSA Authentication Agent 6.1 for Microsoft Windows to Authentication Agent 6.1.4 for Microsoft Windows, double-click **Update.exe** to install the update on a single computer.

To install the update on multiple computers, deploy it using Microsoft System Management Server (SMS) or another third-party software product, such as Tivoli, to preserve the RSA Authentication Agent 6.1 for Microsoft Windows configuration settings. For example, to have SMS install the update in silent mode, use this install command:

```
Update.exe /s /v/qn
```

Variations from Microsoft Compliance

RSA Authentication Agent 6.1 for Microsoft Windows complies with Microsoft branding requirements with the following exceptions. The titles and title numbers pertain to the Microsoft compliance documentation.

Cross-Platform Certification Requirements

2.5 Install to Program Files by Default

RSA Authentication Agent 6.1 for Microsoft Windows installs the following shared files in SystemFolder:

- sdconf.rec
- aceclnt.dll
- sdmsg.dll
- rsapwdfilt.dll

Installing the files elsewhere makes the Authentication Agent incompatible with legacy RSA products that share these files. The Authentication Agent also installs unshared files inherited from previous versions of the Authentication Agent to SystemFolder.

The Authentication Agent installs the following files to WindowsFolder\Help:

- sdcontrl.hlp
- sdcontrl.cnt

S5.4 Install using a Windows Installer-Based Package That Passes Validation Testing

The RSA Authentication Agent installation deviates from certification requirements in the following ways:

- Installation sends duplicate files to the destination area of the .exe file. However, the RSA Authentication Agent requires individual instances of all files regardless of whether they are duplicates.
- Installation adds references in the Start menu to components that occur per computer as opposed to per user. This is required because the RSA Authentication Agent can be installed only once on a computer, and all Start menu references must pertain to all users. Therefore, registry key links to these components must originate under HKLM instead of HKCU.

Windows 2000 Server Certification Requirements

3.3 Provide Documented Keyboard Access to all Features

RSA Authentication Agent 6.1 for Microsoft Windows documents all assigned navigation keys in the interface with underlines.

Windows Server 2003 Certification Requirements

S2.8 Terminal Server Requirements

The RSA Authentication Agent 6.1 for Microsoft Windows installation modifies a HKEY_CURRENT_USER value. However, the modification results from Microsoft Windows Installer and not from the Authentication Agent software.

3.8 Services Running as LocalSystem Must Not Present a UI

The **sdagentsvc** service opens the default Microsoft Windows workstation and desktop. However, it does not present a user interface or accept user input or Windows messages.

Windows XP Certification Requirements

2.6: Install Shared Files to the Correct Locations

RSA Authentication Agent 6.1 for Microsoft Windows does not support the side-by-side shared files requirement because it disables the backward compatibility of legacy Agents. Therefore, the following files are installed under the /program files folder/RSA Security/RSA Authentication Agent directory:

- da_svc.exe
- securiduser.exe

The following files must remain in the /system32 directory to ensure backward compatibility with legacy Agents:

- aceclnt.dll
- sdagent2k.dll
- sdmsg.dll
- sdconf.rec

2.7 Support Add or Remove Programs Properly

The RSA Authentication Agent 6.1 for Microsoft Windows uninstaller removes all "non-shared" .dll files and services. It also removes all registry keys associated with the Authentication Agent that are not user configuration settings that must be maintained for future installations. The uninstallation does not remove the following files:

- sdconf.rec - a configuration file that must be preserved
- aceclnt.dll - a shared file removed only if its shared count is 0
- sdagentrt.dll - a shared file removed only if its shared count is 0
- sdmsg.dll - a shared file removed only if its shared count is 0
- sdstatus.12 - a shared configuration file that is preserved for backward compatibility

Package Contents

RSA Authentication Agent is available from **RSA Authentication Agents for Microsoft Windows**.

The RSA Authentication Agent 6.1.4 for Microsoft Windows product folder contains:

File or Folders	Description
Update.exe	This executable upgrades a 6.1.3 Agent to the 6.1.4 Agent, which includes the vulnerability fix concerning Agent/AuthManager communication.

Fixed Issues

The RSA Authentication Agent 6.1.4 for Microsoft Windows patch resolves the following issue:

Tracking Number: AAWIN-1836
Unable to login to domain with *username@domainalias* with 6.1.3 Agent. Agent's domain alias auth was not functioning normally.

Tracking Number: AAWIN-1997
In previous versions of this product, the node secret was stored using a weak encryption key and a dated encryption algorithm. This mechanism has been replaced with stronger encryption and stronger keys.

The RSA Authentication Agent 6.1.3 for Microsoft Windows patch resolves the following issues:

Tracking number: 120750
The RSA EAP component in Authentication Agent for Microsoft Windows products allowed non-administrative access to EAP registry settings. (RSA EAP allows users to use SecurID authentication over a VPN or wireless connection that protects corporate resources.)

Tracking number: 116282
Authentication failed if you used nested groups.

Tracking number: 117639
Authentication Agent took two minutes to log into the domain controller.

Tracking number: 116789
The aceclnt process (aceclnt.dll) caused a protection exception.

Tracking number: 101739
Windows Password Integration intermittently failed.

Tracking number: 116289
Offline authentication failed for non-SecurID challenged users. (Users who did not need to enter a SecurID passcode to authenticate.)

Tracking number: 112627
Authentication failed when winlogon.exe generated an application error.

Tracking number: 109195
Offline challenged domain users (users who were required to enter a SecurID passcode) were not consistently challenged.

Tracking number: 107649
Challenged user could not view offline data using the RSA Security Center options.

Tracking number: 104500
Various changes were made to BackendUISvc.

Tracking number: 106193
Windows Agent DA_SVC.exe had start failures.

Tracking number: 72691
Offline authentication intermittently failed with users who belonged to a domain challenge group.

Tracking number: 69719
LAC (Local Authentication Client) Group Lookup had delays in a large environment.

Tracking number: 101645
Windows Remote Desktop Connection did not function on Windows 2000 Server.

Tracking number: 98874
Autoregistration did not occur when a NIC (Network Interface Card) was disabled.

Tracking number: 71528
Offline authentication required a specific user name format.

Tracking number: 70774
Users with RSA SecurID 800 authenticators (SID 800 tokens) connected to the USB port saw the Microsoft logon prompts instead of the RSA logon prompts when they restarted their computers after their initial logon.

Tracking number: 56252
LAC (Local Authentication Client) did not allow Directory Services Restore Mode challenge exclusion for an administrator.

Tracking number: 59588
Windows Agent challenged users twice when they used Remote Desktop Connection with connect-to-console mode to access a desktop that was locked manually and by the screen saver.

Tracking number: 45774
You could not install wrapped rollup installation kits silently.

Tracking number: 46199
When no authentication occurred, Autoreg included a "Bad offline auth attempt" message.

Tracking number: 56235
Offline authentication message displayed in the log monitor when no offline authentication occurred.

Tracking number: 61184
Trailing spaces in user name were removed for SecurID authentication, but passed to Windows.

Tracking number: 63326
Test authentication failed for domain users.

Tracking number: 63337
Authentication Agent stopped if online, auto-registration failed, and Windows password updated on the domain controller and RSA Authentication Manager.

Tracking number: 63386
Used offline authentication if auto-registration failed to establish a connection.

Tracking number: 68462
Authentication Agent had SSL (Secure Sockets Layer) handshake issues that affected the cryptographic parameters.

Tracking number: 58707
The build number was not correct in the About information of the RSA Security Center.

Tracking number: 40186
More than administrators were allowed DSRM (Directory Services Restore Mode) exclusion.

Tracking number: 40883
Remote Desktop Connection in Console Mode required multiple authentications to successfully gain access.

Tracking number: 45888
Cannot log off from computers with RSA Authentication Agent and Remote Desktop Connection (or Terminal Services Client 6.0) installed.

Tracking number: 55652
Auto-registration did not occur when using an RSA Authentication Manager Replica.

Tracking number: 56318
Could not perform Auto-Registration for non-challenged users.

Tracking number: 57356
Offline authentication failed if an offline download was interrupted.

Tracking number: 57396
Offline authentication took 10 seconds for each RSA Authentication Manager Primary or Replica server used.

Tracking number: 57587
LAC (Local Authentication Client) offline authentication failed for all local users.

Tracking number: 58069
Could not start Authentication Manager Host mode after applying Authentication Agent 6.1.2 (August 2007) patch.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

- After upgrading a 6.1 Agent to 6.1.4, the first request to download offline data might fail for a user who authenticates with a fixed password. This error can be ignored, since subsequent requests to download offline data succeed.
- After upgrading a 6.1 Agent to 6.1.4 on a Domain Client machine, the Client's Domain Controller must be online when a user logs on to the upgraded Domain Client for the first time. Otherwise, if the Client's Domain Controller is offline, the first logon might fail, even if the domain user has previously downloaded SecurID offline data.
- Under certain conditions, clearing a Node Secret on an Agent machine manually through the Security Center might not clear the entire record of the Node Secret. To prevent this, always reboot the Agent machine after clearing the Node Secret.

Repairing a 6.1.4 Agent

To repair a 6.1.4 Agent, use the **Change** button for the product in the main Add/Remove Programs panel. Do not use the **Repair** button on the "Support Information" panel or you will have to re-run the 6.1.4 **Update.exe**.

Automated Registration of Agent Hosts

To enable automated registration of Agent Hosts in environments that use Network Address Translation (NAT), you have to manually copy the failover.dat file from the DATA directory on the RSA Authentication Manager with which the Authentication Agent communicates, and put the file in the Windows System32 directory on the Authentication Agent Host computer.

Interoperability

- The 6.1.4 Agent may be installed on a machine hosting other SecurID products and applications that use an **aceclnt.dll** to communicate with an Auth Manager. In this case, the node secret on the client machine and the Authentication Manager must be deleted after the last SecurID product or application is installed. On the client machine, the name of the node secret is "securid".

  Similarly, after the last SecurID product or application is uninstalled, the node secret on the client machine and on the Authentication Manager must be deleted. After the last uninstall, remaining products or applications may require re-installation in repair mode to reinstate the product's original **aceclnt.dll**.

- The 6.1.4 Agent may be installed on a machine hosting an RSA Web Agent. In this case, offline authentication support must be disabled after installing the 6.1.4 Agent. This ensures that when users authenticate with SecurID to gain access to a SecurID-protected URL, they will not download offline.

  Offline authentication support must be disabled before the required reboot following Agent installation. Therefore, when the installation script prompts to reboot now, respond with "No". To disable offline authentication support, do the following:

  1. Open the system's Services panel.
  2. Right-click **RSA Authentication Agent Offline Local**.
  3. Select **Properties**.
  4. Set **Startup Type** to **Disable**.

- If you install RSA Sign-On Manager on a computer that hosts RSA Authentication Agent 6.1 for Microsoft Windows, RSA Sign-On Manager removes the Authentication Agent installation. If you want to install the Authentication Agent on a computer that hosts RSA Sign-On Manager, you must uninstall RSA Sign-On Manager before installing the Authentication Agent.
- RSA Authentication Agent 6.1 for Microsoft Windows is not compatible with pcAnywhere.

- The RSA SecurID for Microsoft Windows solution does not support smart card-based logon. RSA recommends that you disable the smart card service on client computers that host RSA Authentication Agent 6.1 for Microsoft Windows. If the smart card service on the client computer is not disabled, smart card authentications bypass RSA SecurID authentications.
- To use RSA Authentication Agent 6.1 for Microsoft Windows and Novell on the same computer, you must install Novell before installing the Authentication Agent. When you install the Authentication Agent, the installer warns you that another GINA (the Novell GINA) is already installed. When you are prompted, choose to replace the Novell GINA with the Authentication Agent GINA.
- If you want to replace the RSA Authentication Agent 6.1 for Microsoft Windows GINA with another GINA, uninstall the Authentication Agent before installing the other GINA software.
- If you are using RSA Authentication Agent 6.1 for Microsoft Windows Local Authentication with RSA Keon Web PassPort, and you want to uninstall the Authentication Agent or Web PassPort, you must uninstall the Authentication Agent first, then uninstall Web PassPort. You must then reinstall the component you want to use.

  Important: If you uninstall RSA Keon Web PassPort before you uninstall the Authentication Agent, you cannot log on to the Authentication Agent host computer.

Installation

- In the *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*, the instructions for installing the Authentication Agent assume you are downloading the RSA Authentication Agent 6.1 for Microsoft Windows.zip file and copying the RSA Authentication Agent for Windows files from the .zip file to each computer that will host an Authentication Agent component. However, you may have received the Authentication Agent software on a CD instead of downloading it. If this is the case, copy the RSA Authentication Agent for Windows files from the RSA Authentication Agent 6.1 for Microsoft Windows CD to each computer that will host an Authentication Agent component.
- After installing RSA Authentication Agent 6.1 for Microsoft Windows, you must complete the installation by restarting the Authentication Agent host computer. Installing the Agent modifies the registry to reference the Authentication Agent GINA (AceGina.dll) instead of the Microsoft GINA (msgina.dll).
- Installing or uninstalling RSA Authenticator Utility on a computer that also hosts RSA Authentication Agent requires additional steps if the only Authentication Agent components installed are the Remote Authentication Server component or the RSA Security EAP Client component.

  If you manually installed only the Authentication Agent Remote Authentication Server component or RSA Security EAP Client component, and then install the Authenticator Utility, perform the following steps:

  1. After you install the Authenticator Utility, run the Authentication Agent installation program in Repair mode.
  2. Open RSA Security Center and reconfigure the remote authentication settings.

  If you manually installed only the Authentication Agent Remote Authentication Server component or RSA Security EAP Client component, and then uninstall the Authenticator Utility, perform the following steps:

  1. After you uninstall the Authenticator Utility, run the Authentication Agent installation program in Repair mode.
  2. Open RSA Security Center and reconfigure the remote authentication settings.

  If you silently installed only the Authentication Agent Remote Authentication Server component or RSA Security EAP Client component, and then install the Authenticator Utility, silently reinstall the Authentication Agent components.

  If you silently installed only the Authentication Agent Remote Authentication Server component or RSA Security EAP Client component, and then uninstall the Authenticator Utility, silently reinstall the Authentication Agent components.

- On Windows XP, to use Microsoft Systems Management Service (SMS) to install a silent installation package, you must configure SMS to run under an administrator account on the target computer. If you configure SMS to run under the SMS software installation account on the target computer, silent installation fails. The network installation package creation program assumes that the Windows msiexec.exe file is located in the \system32 directory of the computer from which the installation package will be executed. If the msiexec.exe file is in a location other than the \system32 directory, perform the following steps:

    1. Follow the instructions in the section titled “Creating and Running a Network Installation Package” in the “Installing RSA Authentication Agent 6.1 for Microsoft Windows” chapter of the *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide* to create a network installation package.
    2. Open the SilentInstall.bat file in a text editor.
    3. Edit the file to include the full pathname of the msiexec.exe file (for example, "SystemFolder\msiexec.exe).

- RSA Authentication Agent 6.1 for Microsoft Windows installs and supports local and remote access to Windows operating systems. Administrators can use the RSA Authentication Agent 6.1 for Microsoft 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 and Windows Server 2003. The RSA Authentication Agent 6.1 for Microsoft Windows does NOT install or support web access.

Configuration

For wireless authentication using Cisco, if you mistakenly install Cisco PEAP on a client computer instead of installing Microsoft EAP, perform the following steps:

1. Use the Cisco Installation Wizard to uninstall the Cisco software.

    Important: Do not use **Add/Remove Programs** in the Microsoft Windows Control Panel.

2. Reinstall the Cisco software without PEAP.

Authentication

General Authentication

- The option **Enable RADIUS client check** verifies whether remote authentication requests originate from a device (for example, Microsoft IAS Server, a remote access server, or a network access server) that is registered as an Agent Host in the RSA Authentication Manager database. If the device is not registered as an Agent Host, the authentication request is denied. For example, when this option is enabled, authentication requests originating from network access devices are denied unless the network access devices are registered as Agent Hosts in the Authentication Manager database. By default, this option is disabled. However, this option does not work in environments that use the following protocol set-ups:
    - RSA Security EAP over PEAP
    - RSA Security Protected OTP over PEAP
- If you change the machine name or static IP address of an Authentication Agent host computer, after you restart the computer, you cannot log on to the Authentication Agent host computer, and the system issues the message "Agent Host Not Found." To prevent this, perform one of the following procedures.

    To change the machine name of an Authentication Agent host computer:

    1. On the Authentication Agent host computer, set the RSA SecurID challenge to **None**.
    2. Change the machine name.
    3. Set the challenge to a setting other than **None**, and select the challenge group based on the new machine name.

    If you have already changed the machine name of an Authentication Agent host computer without performing the preceding steps, perform the following steps:

    1. Restart the Authentication Agent host computer in Safe mode.

2. Log on as Administrator.
3. Set the challenge to **None**.
4. Restart the computer.
5. Log on as Administrator.
6. Set the challenge to a setting other than **None**, and select the challenge group based on the new machine name.

To change the static IP address of an Agent host computer:

Change the IP address of the Authentication Agent host computer, then restart the computer.

- RSA Authentication Agent and RSA Authentication Manager do not support leading zeros (for example, 0123) in PINs used for PINPads and software tokens. If a user creates a PIN that contains leading zeros, the PIN is rejected by the Authentication Manager and the system reprompts the user for a passcode. However, the system does not issue a message saying that the PIN is invalid.
- Although the RSA Authentication Manager allows the @ sign as part of a user name, Windows Active Directory does not.

Authentication Using the RSA SecurID SID800 Authenticator USB Token

- When you use a connected RSA SecurID SID800 Authenticator USB token, the **Time Remaining** field on the RSA Security Center View USB Token page shows that the tokencode is valid for a greater amount of time than it actually is valid. Regardless of how long a tokencode has displayed, every time you reopen the View USB Token page, the **Time Remaining** field starts a new count instead of beginning the count at the actual amount of time the tokencode remains valid. Therefore, the **Time Remaining** field and the actual time the tokencode remains valid may differ by as much as 60 seconds.
- When you authenticate with a connected RSA SecurID SID800 Authenticator USB token that is in Next Tokencode mode or New PIN mode, the system may take 30 seconds after the next tokencode displays on the authenticator to submit the next tokencode to the authentication process.
- You can use the RSA SecurID Authenticator Utility on a terminal server to authenticate only to the console. The Authenticator Utility does not work with terminal sessions.

Wireless Authentication

- RSA Security EAP Protected OTP (EAP-32) and RSA Security EAP (EAP 15) are not supported on Microsoft Windows 2000 platforms.
- Remote access authentication with wireless PEAP does not support RSA SecurID authenticators set for 180-second intervals.
- When a computer comes out of hibernation during a wireless connection, the connection can be restored immediately, without waiting for the user to authenticate back into the existing Microsoft Windows session. For greater security, disable hibernation on users' computers and instruct users to log off the network before leaving their desks.
- During an initial wireless authentication, the Authentication Agent prompts you for both a user name and an RSA SecurID passcode. However, during subsequent authentications, the Authentication Agent prompts you for only an RSA SecurID passcode and does not allow you to change the user name. If, during a subsequent authentication, you need to provide a different user name, perform one of the following procedures.

If you are running an active session:

1. Disconnect the wireless service either through the Network Connections list or by right-clicking on the status bar icon and selecting **View Available Wireless Networks**, selecting the wireless network you are using, then clicking **Disconnect**.

   This stops the system from reprompting.
2. Edit the registry to remove the cached EAP information for the authenticating user.

3. Click S**tart > Settings > Network Connections**, and in the Wireless Network Connections dialog box, select your wireless connection and click **Connect**.

The next RSA Security prompt you see should be a user name dialog box. For more information, see Microsoft Support Knowledge Base article #823731 "How to remove cached user credentials that are used for PEAP authentication in Windows XP." This information applies to all RSA Security EAP protocols even if PEAP is not used.

If you are not running an active session:

1. When the system prompts you for an RSA SecurID passcode, click **Cancel**.

   This clears the EAP registry data.
2. At the **Access Denied** message, click **OK**. If the system prompts you again, ignore the prompts and perform the next step.
3. Click **Start > Settings > Network Connections**, and in the Wireless Network Connections dialog box, select your wireless connection and click **Disconnect**.

   This stops the reprompting.
4. In the Wireless Network Connections dialog box, select your wireless connection and click **Connect**.

The next RSA SecurID prompt you see should be a user name dialog box. For more information, see Microsoft Support Knowledge Base Article ID 823731 "How to remove cached user credentials that are used for PEAP authentication in Windows XP." This information applies to all RSA Security EAP protocols even if PEAP is not used.

- If a user logs on to a local computer with a user name and password that matches domain credentials, then successfully establishes an authenticated wireless PEAP connection, the user gains access to domain resources without having to explicitly authenticate to the domain. This behavior is determined by Microsoft Windows.

Remote Authentication

- After initially installing the local authentication client component on a computer, some Authentication Agent features do not work when you are remotely connected to the network unless you do one of the following:
  - Restart the client computer at least once after performing a test authentication or authenticating online.
  - If you cannot connect to the network directly, do the following:
    1. Log on to the local client computer using a reserve password.
    2. Manually install the node secret from the Authentication Manager.
    3. Connect to the network remotely using a VPN client.
    4. At a command line on the client computer, run **sdadmreg -r**.
    5. The next time you connect to the network directly, at a command line on the client computer, run **sdadmreg -r** to update the client IP address in the Authentication Manager database, and restart the client computer.

Offline Authentication

- On some systems, users cannot authenticate offline once the computer has gone into hibernation after being in standby mode. If this occurs, perform the following procedure:

  1. Perform a connected authentication to the RSA Authentication Manager.
  2. If, during authentication, the system prompts the user to recharge offline days, then notifies the user that the recharge failed, determine whether the user's RSA SecurID token is about to expire. If a user authenticates with an RSA SecurID token that is set to expire before the user's offline days expire, the system prompts the user to recharge offline logon days. However, the user cannot recharge offline days under this circumstance, and attempts to do so fail.

- If you reset the number of offline days to a number that is less than the number that was previously set (for example, if you change the number of offline days to 5 from 10), offline users continue to have the greater number of offline days (in this example, 10) until those days expire. When offline users recharge their offline days, the RSA Authentication Manager downloads the new number of offline days (in this example, 5).
- If you clear offline data from an Authentication Agent host, but RSA Security Center still shows available offline days, instruct the user to restart RSA Security Center.
- After a user authenticates offline with an emergency access passcode, the user cannot recharge the offline days remotely. The user must perform a connected authentication to recharge offline days.

Terminal Services Authentication

For Windows XP platforms, remove your RSA SecurID SID800 Authenticator USB token from your computer before you run a terminal services session to the computer. If you leave the token connected to the computer and then run a terminal services session to the computer, you need to restart the computer before you can log on again.

Tracing and Logging

- The first time you use the RSA Security Center to enable tracing and specify a log file as the tracing destination, the system continues to log GINA tracing to the default location, aceclient.log, instead of the specified destination. To solve this problem, restart the computer.
- When you set the tracing destination to **Log File**, then authenticate remotely using dial-up networking, by default the Authentication Agent creates a tracing log file on the client computer with the incorrect filename AceClient.log. The file must be named AceAgent.log. To apply the correct filename, restart the remote authentication server computer.

Windows Password Integration

On Local Authentication Client computers, policy settings are updated every two hours. Therefore, when you enable Windows password integration on a client computer, Windows password integration does not work until the policy has been updated. However, if you cannot wait until the policy is updated automatically, you can force a policy update by restarting the client computer.

Workstation Unlock with RSA SecurID PIN

- Workstation Unlock with RSA SecurID PIN (Quick Workstation Unlock) does not work if you reset your PIN to a character length that is not the same as the former PIN. Although the PIN Unlock dialog box displays, you are not able to unlock your workstation using your new PIN. If you experience this problem, click **Force Logoff,** and unlock the workstation by entering your user name and RSA SecurID passcode.
- On Local Authentication Client computers, if you are in Next Tokencode mode, the Quick Workstation Unlock screen appears, but does not recognize your RSA SecurID PIN. If this situation occurs, click **Force Logoff**, and then unlock the workstation by entering your user name and RSA SecurID passcode.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**www.rsasecured.com**

Trademarks