Splashtop
Splashtop for Business

RSA SecurID Ready Implementation Guide

Last Modified: January 22, 2014

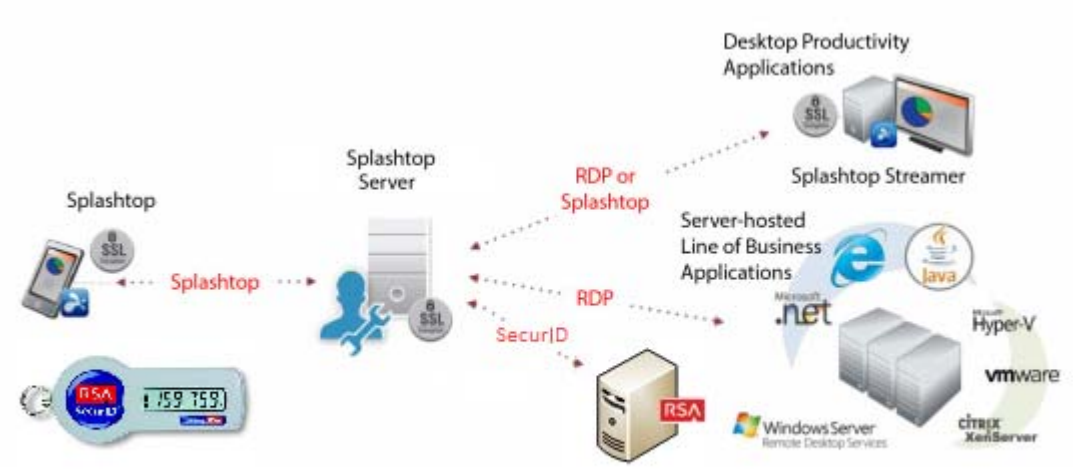
Partner Information

Product Information	
Partner Name	Splashtop
Web Site	www.splashtop.com
Product Name	Splashtop for Business
Version & Platform	2.3.5.14 Windows
Product Description	Splashtop for Business is a remote desktop application which allows administrators to control access through the Splashtop Gateway.

Solution Summary

Splashtop for Business is a remote desktop application which allows administrators to control access through the Splashtop Gateway. Splashtop leverages RSA SecurID to provide OTP access to protect access to hosted workstations and servers.

RSA Authentication Manager supported features	
Splashtop for Business 2.3.5	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Splashtop will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	C:\Windows\SysWOW64
Node Secret	C:\Windows\SysWOW64
sdstatus.12	C:\Windows\SysWOW64
sdopts.rec	C:\Windows\SysWOW64

Note: The appendix of this document contains more detailed information regarding these files.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Splashtop for Business with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Splashtop components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Splashtop Center Configuration

RSA Authentication Manager

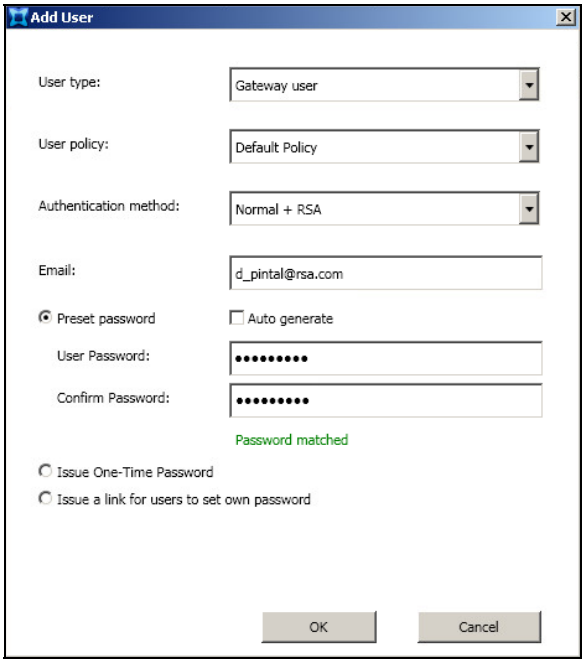
- Collect the sdconf.rec file from the RSA Authentication Manager.
- Create/Collect a password protected nodesecret.rec from the RSA Authentication Manager.
- Create an RSA SecurID protected Splashtop user.
- Configure Splashtop for RSA SecurID Authentication.

Create an RSA SecurID protected Splashtop User

1. Open the Splashtop Center and select **Add**.

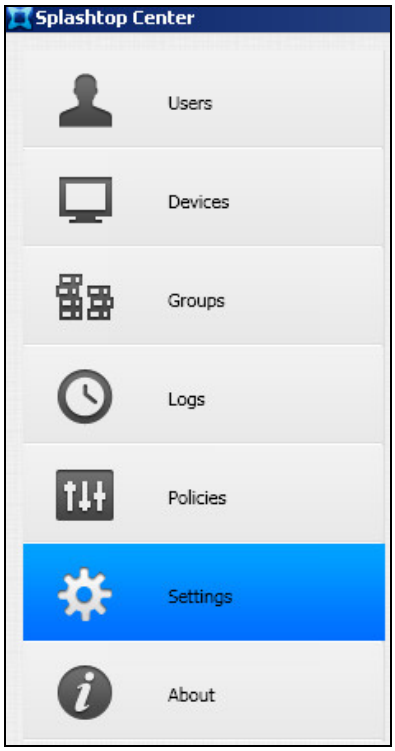
Note: The Splashtop User account must match the RSA Authentication Manager user account created for this client.

2. Select the drop down list for User Policy and select **Normal + RSA**, enter the **Email**, **User Password** and **Password Confirmation**. Select **OK** to continue.

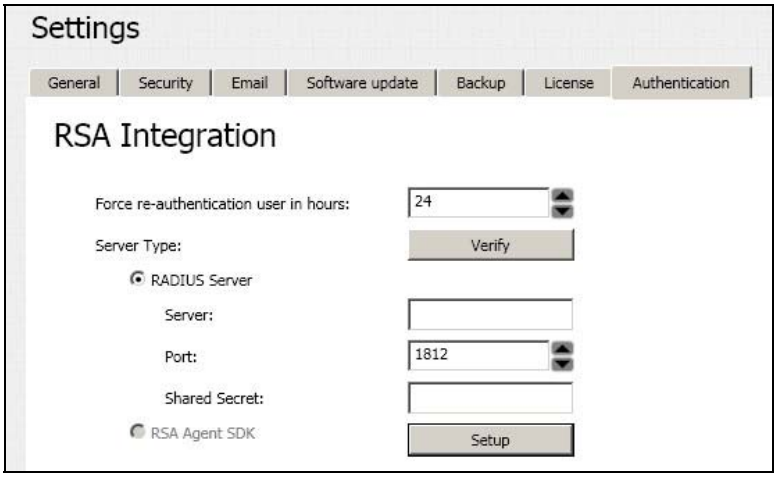


Splashtop RSA SecurID Configuration

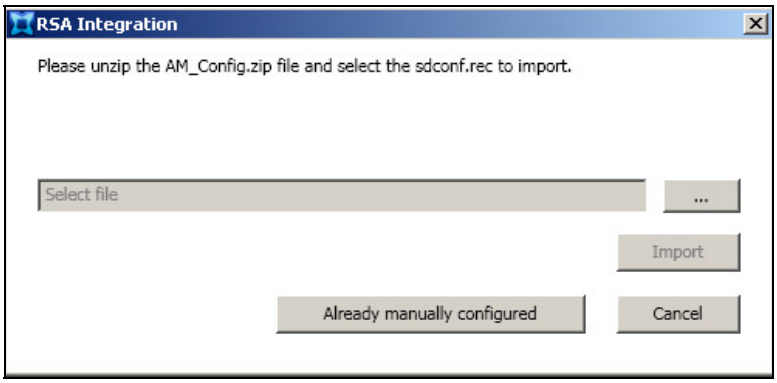
1. Open the Splashtop Center and select **Settings**.



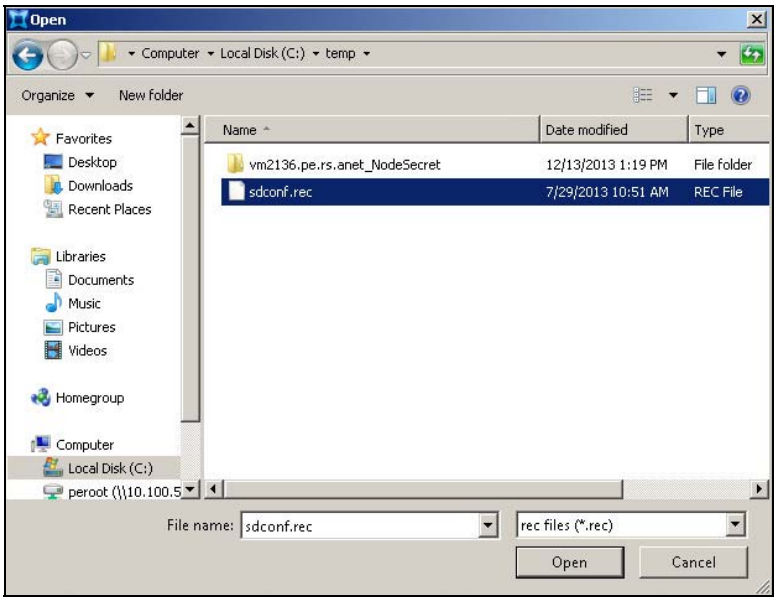
2. Within the Settings Menu select the Authentication tab, and select **Setup**.



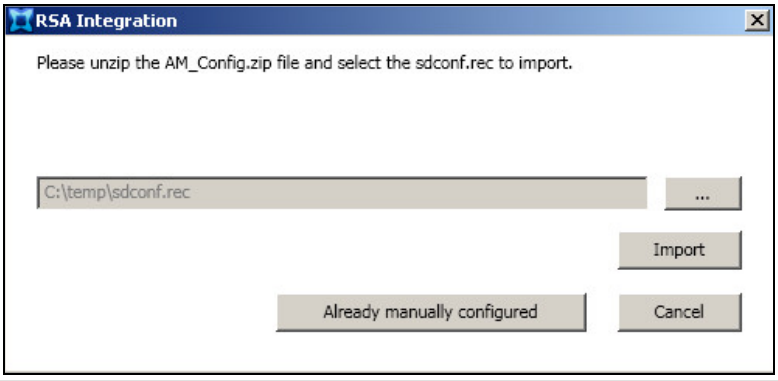
3. Import the sdconf.rec using the ... button.



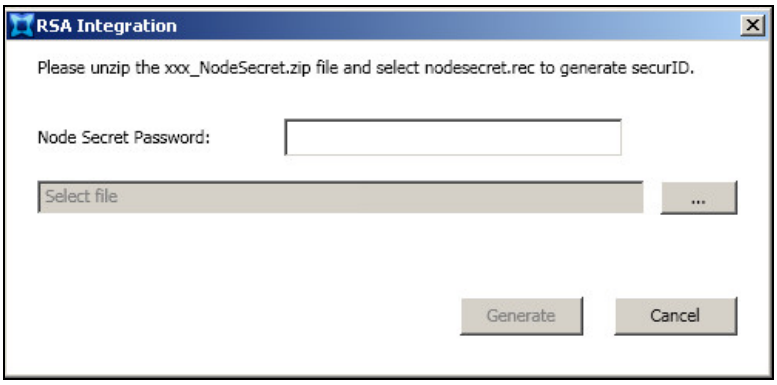
4. Browse to the location of the sdconf.rec file, select **sdconf.rec** file to be imported into Splashtop and select **Open**.



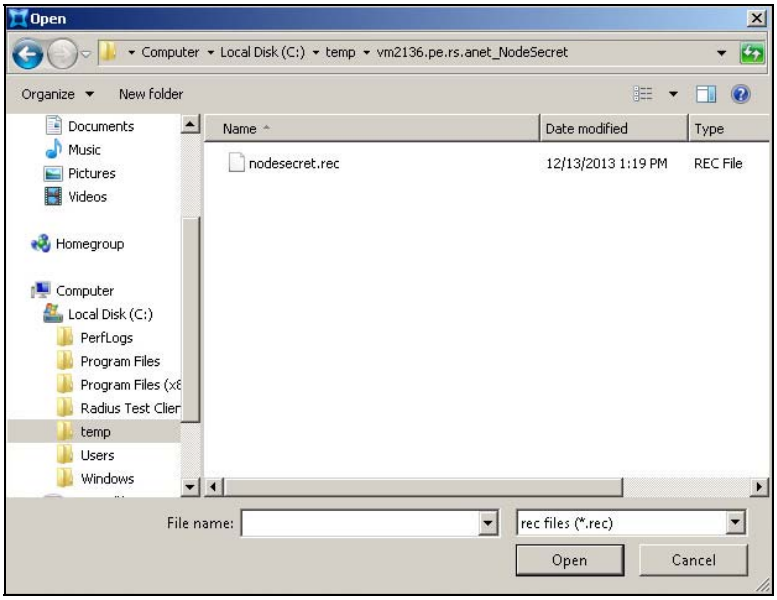
5. Select **Import**.



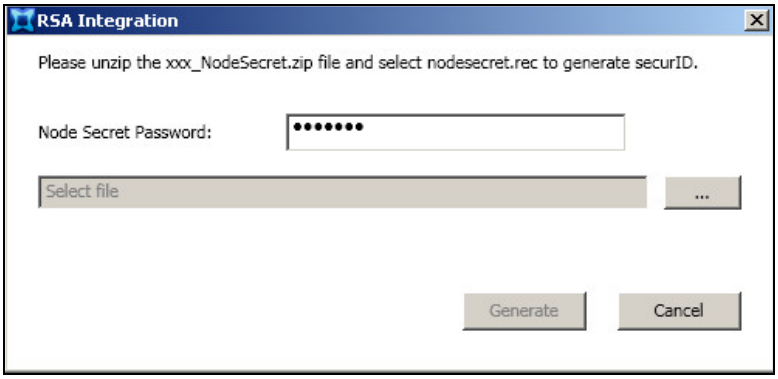
6. Import the Node Secret by selecting the ... button.



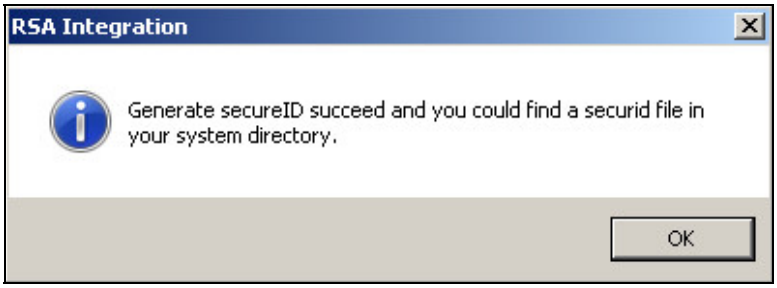
7. Browse to the location of the nodesecret.rec, select **nodesecret.rec** and select **Open**.



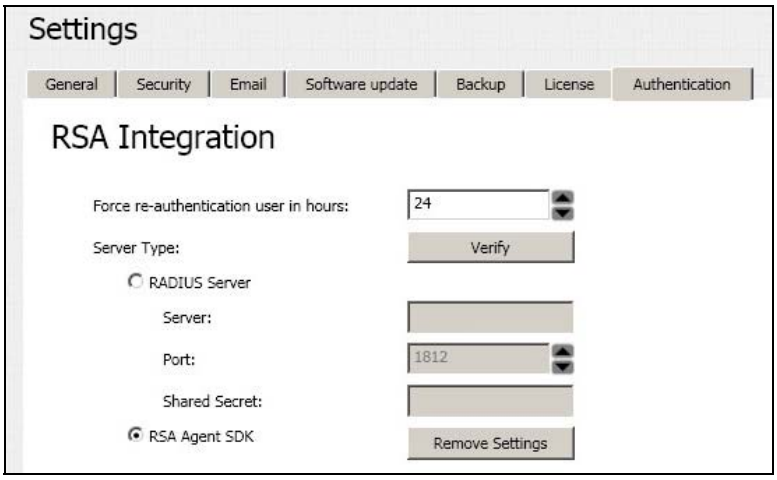
8. Enter the Node Secret Password.



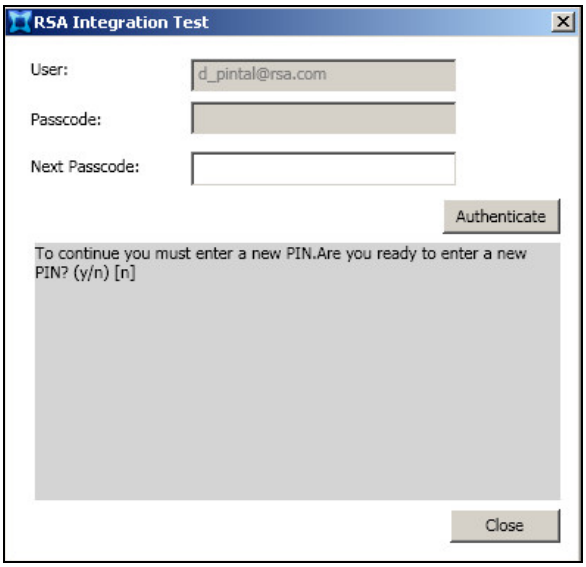
9. Select **OK** to complete the RSA SecurID configuration process.



10. Select **RSA Agent SDK**.

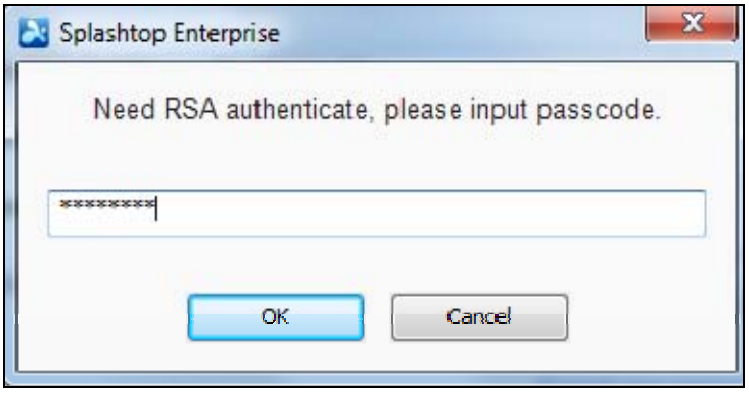


11. Perform a test authentication using either the Splashtop Client or alternatively select **Verify** within the Authentication Tab of the Splashtop Center.

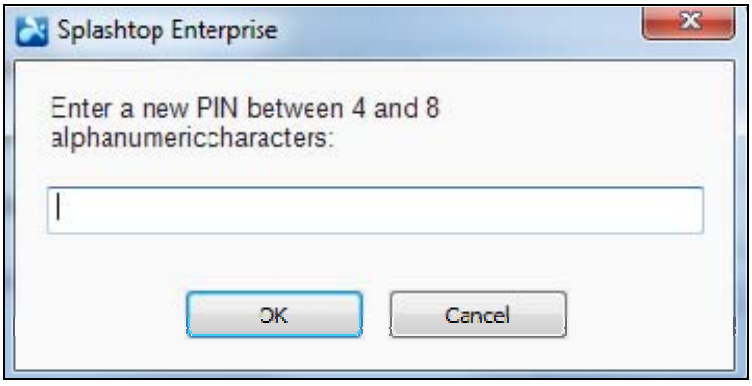


RSA SecurID Login Screens

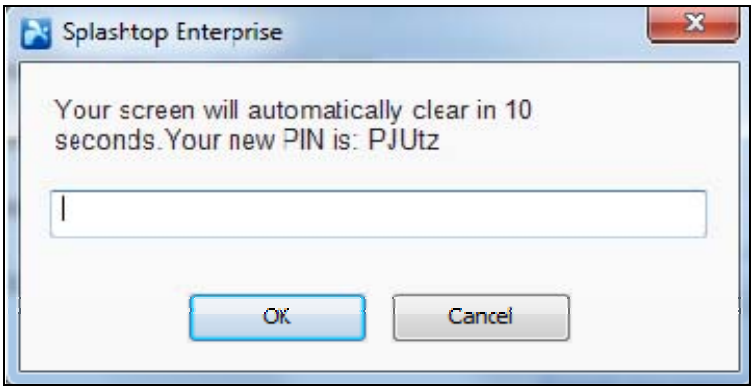
Login screen:



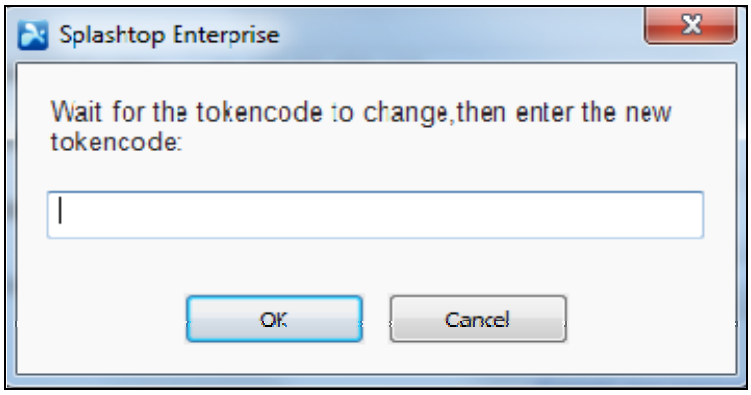
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: January 22, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Splashtop for Business	2.3.5.14	Windows 7 SP1 x64
Splashtop for Business Client	2.3.10	Windows 7 SP1 x64

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Deny PIN Reuse	✓	Deny PIN Reuse	N/A
Passcode			
16-Digit Passcode	✓	16-Digit Passcode	N/A
4-Digit Fixed Passcode	✓	4-Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	N/A
On-Demand New PIN	✓	On-Demand New PIN	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

DRP / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Appendix

Partner Integration Details	
RSA SecurID API	Auth Agent SDK v8.1
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	Yes
Agent Tracing	Yes

Node Secret:

Delete the **securid** file from **C:\Windows\SysWOW64**.

sdconf.rec:

Delete **sdconf.rec** from **C:\Windows\SysWOW64**.

sdopts.rec:

Create or delete **sdopts.rec** from **C:\Windows\SysWOW64**.

sdstatus.12:

Delete **sdstatus.12** from **C:\Windows\SysWOW64**.

Windows Agent Tracing:

Using Regedit locate the HKEY_LOCAL_MACHINE\Software\SDTI\ACECLIENT key and create 2 DWORD values: **tracelevel** and **tracedest.**

> **Note: SDTI\ACECLIENT and all sub values will need to be created when setting up for Windows 64 bit.**

The value tracelevel specifies the verbosity and the categories of messages produced by the code. The value tracedest controls the output destination of the trace messages.

tracedest VALUES:

```
SDITRACE_EVENT_LOG  0x00000001   // messages to event log
SDITRACE_CONSOLE    0x00000002   // messages to console
SDITRACE_LOGFILE    0x00000004   // messages to logfile (aceclient.log)
SDITRACE_DEBUGGER   0x00000008   // messages to debugger output
SDITRACE_NOFILELINE 0x80000000   // no file and line information
```

The SDITRACE_NOFILELINE value can be combined with any of the other values to stop the display of file and line number information. The logfile is SYSTEMROOT%\ACECLIENT.LOG but can be changed by creating a **REG_SZ:tracefile** value and specifying the file pathname.

tracelevel VALUES:

```
SDITRACEING_OFF     0x000000000  // All messages off
SDITRACEING_ON      0x000000001  // All messages marked with this level on
SDITRACEING_ENTRY   0x000000002  // All entrypoints use this
SDITRACEING_EXIT    0x000000004  // All function returns use this
SDITRACEING_FLOW    0x000000008  // All logic flow control use this (ifs)
SDITRACEING_GRP1    0x000000010  // Old SDITRACE macros use this (see dbglib.h)
```

The hex value 0xF gives the complete set of tracing. The values can be combined to produce multiple sets of trace messages.

> **Note: Using the SDITRACE_CONSOLE value can cause the service applications to access violate during logoff. Use only for real time debugging.**