SMSPASSCODE Installation Guide

Article Number: 429 | Last Updated: Mon, Dec 14, 2015 2:24 PM

Prerequisites: Windows Server 2003 SP1 with Domain Controller (Active Directory, e.g. smspasscode.local; e.g. *Administrator\test\email\Netop123!)* Microsoft .NET 3.5 SP1 Framework (addition: e.g. Chrome browser) **Â Installing the Internet Authentication Service (IAS)** Go to the Control Panel and click on **Add/Remove Programs.** Click on **Add/Remove Windows Components**: A list of Windows Components appears. Scroll down to **Networking Services**. Mark **Networking Services**. Click the **Details** button A list of **Networking Services** appears. Check **Internet Authentication Service**. Click the **OK** button. Click the **OK** button. Click the **Next** button. Click the **Finish** button. IAS has now been installed. Â **Configuring RADIUS Protection on Windows Server 2003** Configure all RADIUS clients in the usual way by specifying the **IAS server** as the RADIUS server. If you are in doubt how to perform the configuration, please refer to the configuration guide of the specific RADIUS client in question. Â **Important**! The user experience is best for RADIUS clients supporting *Challenge Response*. If *Challenge Response* support is configurable on the RADIUS client, please enable it. Start the IAS Management Console: In the Windows Start menu, select **Runâ€¦** Enter **ias.msc**. Click **OK** To create a RADIUS Client: Right-click the **RADIUS Clients** node. Select **New RADIUS Client** The **New RADIUS Client** dialog appears. Enter a â€œfriendly nameâ€• of the RADIUS Client. Enter the IP address of the RADIUS Client. Click **Next** New fields appear in the **New RADIUS Client** dialog. a. Enter and confirm the **Shared Secret**. It must match the shared secret configured on the RADIUS Client. b. Click **Finish**. **Installing SMSPASSCODE** (version SmsPasscode-700-x86.exe) Log on to the machine using a user account with local administrator rights Copy **SmsPasscode-700-x86.exe** (32-bit) or **SmsPasscode-700-x64.exe** (64-bit) to a local path on the machine. A Welcome dialog appears. Click the **Next** button. An End-User License Agreement (EULA) appears. Please read the agreement carefully. If you accept the EULA: Click on **I accept the terms in the license agreement**. Click the **Next** button. A dialog for **component** selection appears. This is where you decide which components are to be installed on the current machine. Make your component selections. **Please note**: The selections you make are not permanent. You can always run the installation again afterwards and change your selections. Select Database Service, Web Administration Interface, Transmitter Service, Load Balancing Service. Click the **Next** button. If a dialog for entering license information appears: Enter the license code from the license e-mail. Use copy and paste. Click the **Next** button. If a dialog for selecting the installation folder appears: It is recommended to use the proposed default installation folder. In case you want to change the path, click the **Change** button and select a new path. Click the **Next** button. If a dialog for specifying the default prefix appears: Specify the default prefix for phone numbers. All phone numbers without an explicit prefix will have this prefix automatically added (e.g. +40) Click the **Next** button. If a dialog for setting up the **Web Administration Interface** appears: It is recommended to use the proposed default path for the **Web Administration Interface** installation folder. If you want to change the path, click the **Change** button and select a new path. It is recommended to use the proposed default TCP port for the **Web Administration Interface** site. If you want to change the TCP port, e.g. because of a port conflict with another application or another web site, then enter a different TCP port. Click the **Next** button. A dialog for selecting **Authentication Clients** appears. Select **RADIUS Protection**. Click the **Next** button. Enable ASP.NET 20 (dialog). At some stage during the installation the **SMS PASSCODEÂ® Configuration Tool** is automatically started (except during an upgrade, because in this case the settings from the previous installation are preserved): Radius Client Protection Authentication: add default domain Authorization: Active directory resolve provider -> select LDAP Network -> enter shared secret **Post installation** After having completed the SMS PASSCODEÂ® installation you should perform some configurations, before SMS PASSCODEÂ® is ready for use: **(! If the SMS PASSCODE USERS is not created, you can added from AD Users and Computers)** Use the **Web Administration Interface** for the following tasks: **Settings** -> General: Misc. Settings -> AD integration (enabled) Authentication monitoring (enabled) Globalization options -> Email, Token, Personal passcode (selected) Save. **Policies**-> User Integration Policies: Data Source -> LDAP,Â AD credentials Data Filtering-> Phone number andÂ email required Save. In **AD Users and Computers**: Add user: test with Telephone number and email details. Member of SMS Passcode Administrator and Users (addition: Domain Users, Administrator, Remote Desktop

Users). Use the **Web Administration Interface** for the following tasks: **Users** -> Maintain Users: Sync now **Transmission**-> Email Dispatchers 1Â Â Â Â Â Â Â Add new email dispatcher -> SMTP: 10.202.0.2; Sender email: email@company.com; transmitter hosts â€“ enabled **Policies**->Token Policies Default Token Policy: **Token mode**: OATH/TOTP; **Token type**: Software Token (enable Show QR code forâ€¦). Email Token: **Token mode**: OATH/TOTP; **Token type**: Software Token. **Policies** ->Passcode Policies Default Passcode Policy: **Passcode composition**: Digits only. Email Policy: **Passcode composition**: Digits only. **Policies** ->User Group Policies Default User Group Policy (sms token). Add new-> Email Group Policies. **Users** -> Maintain Users: Email user->User Group Policy Settings: User Group Policy: email group policies Passcode policy: email policies Auth. Policy: default Token Policy: email token Passcode type: one-time passcode (OTP) Dispatch type: send passcode by email Token auth.: Allow test user->User Group Policy Settings: Token auth.: Allow

Posted - Mon, Dec 14, 2015 2:24 PM.
Online URL: https://kb.netop.com/article/smspasscode-installation-guide-429.html