

Legal Information

End-User License Agreement

The use of the products described in these materials is subject to the then current end-user license agreement, which can be found at the Stonesoft website:

www.stonesoft.com/en/support/eula.html

Third Party Licenses

The StoneGate software includes several open source or third-party software packages. The appropriate software licensing information for those products at the Stonesoft website:

www.stonesoft.com/en/support/third_party_licenses.html

U.S. Government Acquisitions

If Licensee is acquiring the Software, including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense ("DoD"), the Software is subject to "Restricted Rights", as that term is defined in the DOD Supplement to the Federal Acquisition Regulations ("DFAR") in paragraph 252.227-7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government's rights in the Software will be as defined in paragraph 52.227-19(c) (2) of the Federal Acquisition Regulations ("FAR"). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions.

Product Export Restrictions

The products described in this document are subject to export control under the laws of Finland and the European Council Regulation (EC) N:o 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology (as amended). Thus, the export of this Stonesoft software in any manner is restricted and requires a license by the relevant authorities.

General Terms and Conditions of Support and Maintenance Services

The support and maintenance services for the products described in these materials are provided pursuant to the general terms for support and maintenance services and the related service description, which can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/terms/

Replacement Service

The instructions for replacement service can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/return_material_authorization/

Hardware Warranty

The appliances described in these materials have a limited hardware warranty. The terms of the hardware warranty can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/warranty_service/

Trademarks and Patents

The products described in these materials are protected by one or more of the following European and US patents: European Patent Nos. 1065844, 1189410, 1231538, 1259028, 1271283, 1289183, 1289202, 1304849, 1313290, 1326393, 1379046, 1330095, 131711, 1317937 and 1443729 and US Patent Nos. 6,650,621; 6 856 621; 6,885,633; 6,912,200; 6,996,573; 7,099,284; 7,127,739; 7,130,266; 7,130,305; 7,146,421; 7,162,737; 7,234,166; 7,260,843; 7,280,540; 7,302,480; 7,386,525; 7,406,534; 7,461,401; 7,721,084; and 7,739,727 and may be protected by other EU, US, or other patents, or pending applications. Stonesoft, the Stonesoft logo and StoneGate, are all trademarks or registered trademarks of Stonesoft Corporation. All other trademarks or registered trademarks are property of their respective owners.

SSL VPN Powered by PortWise.

Disclaimer

Although every precaution has been taken to prepare these materials, THESE MATERIALS ARE PROVIDED "AS-IS" and Stonesoft makes no warranty to the correctness of information and assumes no responsibility for errors, omissions, or resulting damages from the use of the information contained herein. All IP addresses in these materials were chosen at random and are used for illustrative purposes only.

Copyright © 2011 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

TABLE OF CONTENTS

GETTING STARTED

CHAPTER 1

Using StoneGate Documentation	11
Objectives and Audience	12
Typographical Conventions	12
Documentation Available	13
Product Documentation	13
Support Documentation	13
Contact Information	13
Licensing Issues	13
Technical Support	14
Your Comments	14
Security Related Questions and Comments	14
Other Queries	14

CHAPTER 2

What's New	15
New Feature in SSL VPN 1.5.1	16
Linux Access Client	16

CHAPTER 3

Feature Overview	17
Introduction	18
Assessment	18
Authentication	19
Authorization	19
Access	20
Auditing	20
Abolishment	21

CHAPTER 4

Technical Overview	23
Introduction to System Services	24
Default Listening Ports	24
Administration Service	25
Access Point	25
Mirroring	25
Trusted Gateways	25
Cipher Suites	26
Link Translation and DNS Mapping	26
Policy Service	26
Resources	26
Standard Resources	27
Access Rules	27

Single Sign-On	28
Authentication Service	28
Internal Authentication	28
Directory Service and User Storage	29

CHAPTER 5

Planning	31
Getting Started with Planning SSL VPN Deployment	32
Security Audit/Planning	32
System Architecture Review	32
Public Key Infrastructure	32
User Management Strategy	33
Analyzing Your Environment	33
Directory Service Requirements	34
Password Management	34
Use of Special Characters	34
Resource Access	35
Access Strategies	35
Using Groups	35
Naming Conventions	35
Select Authentication Methods	35
Pre-Installation Checklist	36

CHAPTER 6

GUI Overview	37
Getting Started with SSL VPN Graphical User Interface	38
SSL VPN Administrator	38
Online Help	39
Navigating in StoneGate SSL VPN Administrator	39
Top Menu	39
Monitor System	39
Manage Accounts and Storage	40
Manage Resource Access	41
Manage System	43
SSL VPN Web Console	45
Navigating in StoneGate SSL VPN Web Console	45
System	45
Networking	46
Hardware	46
SSL VPN Application Portal	47

INITIAL CONFIGURATION

CHAPTER 7

Configuring the System After Installation 51

Getting Started with SSL VPN Configuration 52

Configuration Overview 52

Integrating the SSL VPN With the SMC 52

Configuration Overview 52

Creating an SSL VPN Gateway Element 53

Saving the Initial Configuration 53

Making Initial Contact 53

Importing SSL VPN License Into the SMC 53

Applying the Configuration 54

Configuring a Directory Service 54

Adding an External User Storage Location 55

Updating an External User Storage 56

Further Configuration Steps 57

CHAPTER 8

Configuring Mirroring 59

Getting Started with Configuring Mirroring 60

Configuration Overview 60

Preparing for Mirroring 61

Configuring Basic System Services for Mirroring 61

Configuring the Policy Service for Mirroring 61

Configuring the Authentication Service for Mirroring 62

Configuring the Access Point Service for the Primary Appliance 62

Configuring the Access Point Service for the Secondary Appliance 62

Selecting the Access Points for Mirroring 63

Configuring Administrator Web Resources for Mirroring 64

Setting Up Registered Authentication Method Servers 64

Setting Up the Administrator Service for Mirroring 65

Setting Up Appliances as Primary and Secondary 66

Configuring the Primary Appliance 66

Configuring the Secondary Appliance 66

Configuring Server Pool Monitoring Agents 67

CHAPTER 9

Customizing the Application Portal 69

Getting Started with Application Portal Customizations 70

Configuration Overview 70

Working with Customization Files 71

Finding the Root Folder for Customization Files 71

Editing or Replacing Customization Files 72

Customizing Application Portal Text 73

Customizing Application Portal Images 74

Customizing Application Portal Colors and Layout 75

Customizing HTML Templates 76

Page Template Variables 79

Customizing the StoneGate Web Authentication Script 80

DAILY MANAGEMENT

CHAPTER 10

Managing User Accounts 85

Getting Started with Managing User Accounts 86

Configuration Overview 86

Managing Global User Account Settings 86

General Settings 87

User Linking Settings 88

Auto Repair Settings 92

Managing User Storage Locations 92

Managing User Accounts 92

Creating User Accounts 92

Adding Users 93

Linking Users 94

Linking Users Automatically 94

Linking Users Manually 94

Repairing User Links 95

Repairing User Links Manually 95

Enabling Automatic User Link Repair 95

Creating a File for Importing Users 96

Importing Users 98

Modifying Users 99

Deleting Users 99

Managing User Groups 99

Adding User Groups 100

Adding a User Location Group 100

Adding a User Property Group 100

Searching User Groups 101

Editing User Groups 101

Deleting User Groups 101

Getting Started with Delegated Management 102

Configuring Delegated Management 102

Managing Self Service 103

Task-specific Self Service Challenges	103	Configuring Global SMS and Screen Message Settings	132
Activating Self Service	105		
Managing System Challenges	105	CHAPTER 13	
Adding Challenges to Self Service Tasks	106	Defining Access Rules	133
CHAPTER 11		Getting Started with Access Rules	134
Managing Authentication Methods	107	Configuration Overview	134
Getting Started with Authentication Methods	108	Defining the Global Access Rule	135
Configuration Overview	108	Editing Access Rules	136
Authentication Methods	108	Adding a New Registered Access Rule	137
StoneGate Authentication Methods	108	Modifying a Registered Access Rule	137
Additional Authentication Methods	111	Selecting Criteria for Access Rules	138
Managing Authentication Methods	112	Defining Authentication Method Access Requirements	139
Adding Authentication Methods	112	Defining User Group Membership Access Requirements	139
Modifying Authentication Methods	115	Defining IP Address Access Requirements	140
Deleting Authentication Methods	116	Defining Client Device Access Requirements	140
Enabling Authentication Methods for Self Service	116	Defining Time-Based Access Requirements	141
Managing RADIUS Configuration	117	Defining User Storage Access Requirements	142
Adding RADIUS Clients	117	Defining Assessment Access Requirements	142
Adding RADIUS Back-End Servers	117	Defining Abolishment Access Requirements	143
Managing OATH Configuration	118	Defining Access Point Access Requirements	144
Importing Tokens	118	Defining Identity Provider Access Requirements	144
Backing Up the OATH Token Database	119	Defining Custom Access Requirements	144
Scheduling Automatic OATH Backups	119	Finishing the Add Access Rule Wizard	146
Restoring an OATH Token Database Backup	120		
Defining OATH Database Connection	120	CHAPTER 14	
Getting Started with Certificates	121	Standard Resource Configuration	147
Managing Certificates	122	Getting Started with Standard Resources	148
Adding a Certificate Authority	122	About the Application Portal	149
Adding Server Certificates	123	Creating an IMAP/SMTP or POP3/SMTP Resource	149
Adding a Client Certificate	123	Creating a Microsoft Outlook Web Access Resource	150
CHAPTER 12		Creating a Microsoft Outlook Client Resource	150
Managing Authentication Services	125	Creating a Domino Web Access Resource	151
Getting Started with Authentication Services	126	Creating a Microsoft Terminal Server Resource	152
Configuration Overview	126	Creating a Microsoft Windows File Share Resource	152
Managing Authentication Services	126	Creating an Access to Home Directory Resource	153
Adding an Authentication Service	126	Creating a Salesforce Resource	154
Modifying an Authentication Service	127	Creating a StoneGate SSL VPN Administrator Resource	154
Deleting an Authentication Service	128	Creating a Citrix MetaFrame Presentation Server Resource	155
Configuring Global Authentication Service Settings	128	Creating a Microsoft Sharepoint Portal Server Resource	156
Configuring Global RADIUS Authentication Settings	128		
Configuring Global Password/PIN Settings	129		
Configuring Global E-mail Message Settings	131		

CHAPTER 15

Web Resource Configuration	157
Getting Started with Web Resources	158
Configuration Overview	158
Creating Web Resources	158
Adding Alternative Hosts	159
Selecting Single Sign-On (SSO) Options for Web Resources	160
Making Web Resources Available in the Application Portal	161
Selecting Resource Access Rules	161
Defining External Sites	162
Customizing Web Resource Authorization Settings	162
Setting the Web Resource Encryption Level	163
Configuring Link Translation	164
Configuring Resource Link Translation	165
Configuring Global Link Translation	165
Configuring Global DNS Name Pool Settings	166
Adding a DNS Name for the Access Point	166
Adding a DNS Name to the Pool	167
Configuring Internal Proxies	167
Configuring Resource Internal Proxy Settings	167
Configuring Global Internal Proxy Settings	168
Filter Scripts	168
Adding a Filter	168
Mapping Filter Variables	170

CHAPTER 16

Tunnel Resource Configuration	171
Getting Started with Tunnel Resources	172
About the Application Portal	172
About Alternative Hosts	172
Configuration Overview	172
Creating Tunnel Resource Networks	173
Creating Tunnel Resource Hosts	174
Creating and Modifying Tunnel Sets	175
Adding a New Tunnel Set	175
Adding a Static Tunnel to a Tunnel Set	176
Adding a Dynamic Tunnel to a Tunnel Set	176
Specifying a Startup Command	177
Selecting Tunnel Resource Access Rules	177
Configuring Tunnel Resource Authorization Settings	178
Configuring IP Address Pools	179
Defining the IP Address Pool	179

Defining the Access Point Dynamic Pool IP Address	179
Enabling the Dynamic IP in the Tunnel Set	179
About the Access Client	180
Windows Native Access Client	180
Windows Vista/Windows 7-specific Configuration	180
Linux Native Access Client	181
Preparing for Linux Access Client Installation on Ubuntu Linux	181
Preparing for Linux Access Client Installation on Suse Linux	182
Installing the Linux Access Client	182
ActiveX Access Client Loader	183
Configuring Internet Explorer for the ActiveX Access Client Loader	183
Java Applet Access Client Loader	183
Pure Java Access Client	183

CHAPTER 17

Client Security	185
Getting Started with Client Security	186
Configuration Overview	186
Configuring Device-Specific Controls	186
Adding Custom Device Definitions	186
Registering Device Settings	187
Configuring Device Access Restrictions	189
Configuring Assessment	190
Assessment Configuration Overview	190
Enabling Assessment	191
Defining Client Scan Paths	191
Enabling Real Time Scan	192
Hiding Resources Before Assessment Client Scan	192
Enabling Silent Assessment	193
Modifying Assessment Client Loader Order	193
Adding Assessment Plug-Ins	193
Configuring Abolishment	194
Abolishment Configuration Overview	194
Configuring File Removal	195
Configuring Cache Clean-Up	196
Hiding Resources Before Abolishment Client Scan	196
Enabling Silent Abolishment	197
Modifying the Abolishment Client Loader Order	197

CHAPTER 18
Managing Single Sign-On and Identity Federation 199

Getting Started with Single Sign-On	200
Creating Single Sign-On (SSO) Domains	200
Adding an SSO Domain	200
Adding Domain Attributes	201
Selecting the SSO Access Rule	202
Getting Started with Identity Federation	202
Managing Identity Federation Settings	203
Configuring Service Provider Settings	204
Configuring ADFS Settings	204
Configuring SAML 2.0 Settings	205
Reading User Certificate Attributes	207
Configuring Identity Provider Settings	208
Configuring ADFS Settings	208
Configuring SAML 2.0 Settings	209
Troubleshooting Identity Federation	210

CHAPTER 19
Monitoring in the SSL VPN Administrator 211

Introduction to Monitoring SSL VPN	212
About System Status Overview	212
Status Overview	212
Event Overview	213
Monitoring System Status	213
Monitoring General Status	213
Access Points	214
Policy Services	215
Authentication Services	215
Monitoring Current User Sessions	216
Viewing Current User Sessions	216
Closing Current User Sessions	216
Viewing Logs in the SSL VPN Administrator	217
Configuring Alert Notifications	218
Adding Alerts	218
Specifying Alert Event Types	218
Specifying Alert Receivers	219
Generating Reports	219
Configuring Logging	220
Configuring Logging for a Registered Server . .	220
Additional Options for HTTP Logs on	
Access Points	221
Additional Options for Audit Logs on	
Access Points	223
Configuring Global Logging Settings	224
Enabling Debug Logging	224

MAINTENANCE

CHAPTER 20
Licenses 227

Getting Started with Licenses	228
SSL VPN License Contents	228
Installing and Updating Licenses Through SSL	
VPN Administrator	229
Installing and Updating Licenses Through SMC	229

CHAPTER 21
Working With Backups 231

Getting Started With Backing up and Restoring	
SSL VPN	232
Backing up and Restoring StoneGate SSL VPN in	
the Web Console	232
Backing up StoneGate SSL VPN in the Web	
Console	232
Restoring a Backup in the Web Console	232
Backing up and Restoring StoneGate SSL VPN on	
the Command Line	232
Accessing the Command Line Interface	232
Backing up StoneGate SSL VPN on the	
Command Line	233
Restoring a Backup on the Command Line	234

CHAPTER 22
Configuring Basic System Settings 235

Getting Started With Configuring Basic System	
Settings	236
Setting the System Time	236
Configuring Network Interfaces	236
Configuring Routing and Gateways	237
Defining the Default Router	237
Defining other Routes	237
Configuring the Host Name and DNS Client	238
Configuring Host Addresses	238

CHAPTER 23
Upgrading 239

Getting Started With Upgrading SSL VPN	240
Upgrading Stand-alone SSL VPN	240
Upgrading SSL VPN with SMC	241

APPENDICES

APPENDIX A
Default Listening Ports 245

Glossary	249
Index	259

GETTING STARTED

In this section:

Using StoneGate Documentation - 11

What's New - 15

Feature Overview - 17

Technical Overview - 23

Planning - 31

GUI Overview - 37

CHAPTER 1

USING STONEGATE DOCUMENTATION

Welcome to the StoneGate SSL VPN by Stonesoft Corporation. This chapter provides you with an overview to this guide, to other information resources available to you, and the contact information for reaching Stonesoft.

The following sections are included:

- ▶ [Objectives and Audience](#) (page 12)
- ▶ [Documentation Available](#) (page 13)
- ▶ [Contact Information](#) (page 13)

Objectives and Audience

The StoneGate SSL VPN Administrator's Guide covers all aspects of StoneGate SSL VPN and is intended for both administrators and system integrators. Most sections in this guide begin with an overview ("Getting Started with...") to the subject at hand.

The guide continues from where the Appliance Installation Guide ends. The chapters in this guide are organized according to administrative tasks. Each chapter focuses on one area of administration. As a general rule, the chapters proceed from basic configuration tasks to more advanced topics. Although overviews are provided, the emphasis in this guide is more on completing specific tasks than developing a deep understanding of how the system works.

To launch the Online Help system in the SSL VPN Administrator, click the **Help** button on the top of the Administrator window, or click the question mark on screen in any window or dialog.

Typographical Conventions

The following conventions are used throughout the documentation:

Table 1.1 Typographical Conventions

Formatting	Informative Uses
User interface text	Text you see in the User Interface (buttons, menus, etc.) and any other interaction with the user interface are in bold-face .
<i>References, terms</i>	Cross-references and first use of acronyms and terms are in <i>italics</i> .
Command line	File names, directories, and text displayed on the screen are monospaced.
User input	User input on screen is in monospaced bold-face .
<i>Command parameters</i>	Command parameter names are in <i>monospaced italics</i> .

We use the following ways to indicate important or additional information:



Note – Notes prevent commonly-made mistakes by pointing out important points.



Caution – Cautions prevent breaches of security, information loss, or system downtime. Cautions always contain critical information that you must observe.

Tip – Tips provide additional helpful information, such as alternative ways to complete steps.

Example Examples present a concrete scenario that clarifies the points made in the adjacent text.

Example Examples clarify points made in the adjacent text.

Documentation Available

The StoneGate SSL VPN Administrator's Guide covers all areas related to StoneGate SSL VPN Administrator. The initial setup and configuration tasks are explained in the *Appliance Installation Guide* delivered with the appliance.

Product Documentation

The table below lists the available guides. PDF versions of the *Administrator's Guide* and the *Appliance Installation Guide* are available at <http://www.stonesoft.com/support/>.

SSL VPN Administrator user interface also has a link to the *SSL VPN Administrator's Guide* on the front page.

Table 1.2 Product Documentation

Guide	Description
Online Help	Detailed instructions for configuration and use. An HTML-based system is available in the StoneGate SSL VPN Administrator through help links and icons.
Administrator's Guide	This document. Describes how to configure and manage the system step-by-step. Explains also comprehensively the operation and features of StoneGate SSL VPN. Demonstrates the general workflow and provides example scenarios.
Appliance Installation Guide	Instructions for installing, maintaining and initially configuring StoneGate SSL VPN (for example, rack mounting, cabling, installation of certificates and licenses).

Support Documentation

The StoneGate support documentation provides additional and late-breaking technical information. These technical documents support the StoneGate guide books, for example, by giving further examples on specific configuration scenarios.

The latest StoneGate technical documentation is available on the Stonesoft website at <http://www.stonesoft.com/support/>.

Contact Information

For street addresses, phone numbers, and general information about StoneGate and Stonesoft Corporation, visit our Web site at <http://www.stonesoft.com/>.

Licensing Issues

You can view your current licenses at the License Center section of the Stonesoft Web site at <https://my.stonesoft.com/managelicense.do>.

For license-related queries, e-mail order@stonesoft.com.

Technical Support

Stonesoft offers global technical support services for Stonesoft's product families. For more information on technical support, visit the Support section at the Stonesoft Web site at <http://www.stonesoft.com/support/>.

Your Comments

We want to make our products suit your needs as well as possible. We are always pleased to receive any suggestions you may have for improvements.

- To comment on software and hardware products, e-mail feedback@stonesoft.com.
- To comment on the documentation, e-mail documentation@stonesoft.com.

Security Related Questions and Comments

You can send any questions or comments relating to StoneGate SSL VPN and network security to security-alert@stonesoft.com.

Other Queries

For queries regarding other matters, e-mail info@stonesoft.com.

CHAPTER 2

WHAT'S NEW

This section lists major changes in previous releases. Most new or reworked features in the software are listed here. Changes that do not significantly affect the way StoneGate is configured are not listed. For a full list of changes in the software, consult the *Release Notes*.

The following sections are included:

- ▶ [New Feature in SSL VPN 1.5.1](#) (page 16)

New Feature in SSL VPN 1.5.1

Linux Access Client

The Access Client is now available as a Linux application.

- For more information, see [Linux Native Access Client](#) (page 181).

CHAPTER 3

FEATURE OVERVIEW

This chapter provides an overview to the benefits you gain from the StoneGate SSL VPN solution. It lists and describes the six core principles of security, starting from assessing the end-user devices and ending with removing all traces of access from user devices at the end of the session.

The following sections are included:

- ▶ [Introduction](#) (page 18)
- ▶ [Assessment](#) (page 18)
- ▶ [Authentication](#) (page 19)
- ▶ [Authorization](#) (page 19)
- ▶ [Access](#) (page 20)
- ▶ [Auditing](#) (page 20)
- ▶ [Abolishment](#) (page 21)

Introduction

StoneGate SSL VPN provides access to applications and information from virtually any location and device. To provide this access securely, the SSL VPN gateway covers entry-to-exit security by following six core principles of security:

- *Assessment*: Inspect user devices to ensure they comply with the corporate security policy.
- *Authentication*: Verify that users are who they claim to be.
- *Authorization*: Check that the conditions for giving access are met and determine the level of access that can be granted separately for each session.
- *Access*: Create a secure encrypted network link between users' devices and the application or information that the authenticated user is authorized to utilize in this session.
- *Audit*: Record and monitor user activities.
- *Abolishment*: Remove all traces of access from the user devices at the end of the session to prevent information leaks.

Assessment

StoneGate SSL VPN assesses client devices to ensure they comply with your corporate security policy.

Requirements may include the assessment of:

- Firewall and anti-virus software.
- Operating systems and patches.
- Spyware checking.
- Device type.
- Network configuration.
- Hardware (NIC MAC addresses, hardware serial numbers).

Based on the assessment results, devices may be refused entry, or be referred to software update sites.

How Does It Work?

When activated, Assessment runs a software component on the client computer to inspect it. Assessment criteria can be set as a condition of access in Access Rules, and you can also configure assessment to run at intervals throughout the user session to ensure compliance throughout the entire session.

For more information, see [Configuring Assessment](#) (page 190).

Authentication

StoneGate SSL VPN includes a variety of authentication features. Several single sign-on (SSO) methods are supported. Users can access different resources with a single log-in even for services that do not actually share the same login details. You can also use any combination of different authentication methods together for highly robust access control.

How Does It Work?

The SSL VPN gateway provides six internal authentication methods:

- *StoneGate Challenge*: End-users receive a challenge code from the web portal and enter that along with their personal PIN code in the StoneGate MobileID software installed, for example, on their mobile phone. MobileID then produces a one-time password for the log in.
- *StoneGate Mobile Text*: End-users enter their personal PIN code on a login page in their web browser. The SSL VPN Gateway sends them a text message that contains a one-time password for the actual login.
- *StoneGate OATH*: End-users enter a one-time password from an OATH-compliant hardware token. OATH-compliant tokens are available from several manufacturers and must be purchased separately. The action required to produce the password depends on the type of token used.
- *StoneGate Password*: End-users enter their password.
- *StoneGate Synchronized*: End-users enter their personal PIN code in the StoneGate MobileID software installed, for example, on their mobile phone. MobileID then produces a one-time password for the log in.
- *StoneGate Web*: End-users enter their personal PIN code using a secure virtual keypad in their web browser.

Additionally, a variety of external authentication methods are supported, such as LDAP, SafeWord, RSA Secure ID, and others.

For more information, see [Getting Started with Authentication Methods](#) (page 108).

Authorization

Access rules are lists of one or more conditions for access. Access Rules can contain a combination of different conditions, which gives you detailed control over the resources that are available in each user session.

How Does It Work?

The following types of access criteria can be set in access rules:

- **Authentication method**: The end-user must authenticate using the method(s) you specify.
- **User group membership**: The end-user's account must be included in the group(s) you specify.
- **IP address of incoming client**: The source IP address of the end-user's connection must be within a range you specify.
- **Client device**: The end-user's request is matched to a Device Definition that you have configured in the system, with different options for taking action depending on the results.
- **Date, day and/or time**: The end-user must connect within the time period(s) you define.
- **User storage**: The end-user's account must be stored in the user storage location(s) you specify.
- **Assessment**: The end-user's device must pass the security scans you specify.

- **Abolishment:** The end-user's device must be compatible with abolishment (trace removal).
- **Access Point:** The end-user must connect through the Access Point (SSL VPN appliance) you specify.
- **Identity Provider:** The end-user must connect through the Identity Provider you specify.
- **Custom-defined:** Allows you to define information paths and client data requirements yourself instead of using a plug-in. You can define requirements for Windows and Mac OS X clients.

For more information, see [Getting Started with Access Rules](#) (page 134).

Access

The SSL VPN gateway provides authorized end-users SSL-encrypted, secure access to resources. Resources can be, for example, applications, network drives, individual files, or simple web pages. Resources do not have to be web-enabled to work: the Access Client component can create a secure encrypted network tunnel between the end-user device and the SSL VPN gateway.

The SSL VPN gateway offers a customizable, dynamically populated Application Portal front-end that allows the end-user access to resources. The application portal contains different items and can be made to look different for each end-user session depending on various criteria you set.

How Does It Work?

For more information, see [Getting Started with Web Resources](#) (page 158), [Getting Started with Tunnel Resources](#) (page 172), and [Getting Started with Standard Resources](#) (page 148).

Auditing

The advanced auditing features in StoneGate SSL VPN provide:

- Permanent, centralized record of application access.
- Real-time and historical reports covering all areas of end-user and administrator activities, as well as system and performance reports.

The auditing, log processing and reporting capabilities of StoneGate SSL VPN can be further enhanced by sending the data to the StoneGate Management Center, where it can be processed in more detail and correlated between several separate SSL VPN appliances or other security and networking products in your organization's network.

How Does It Work?

For more information on viewing the gathered information, see [Introduction to Monitoring SSL VPN](#) (page 212).

For more information on the logging and reporting features in the StoneGate Management Center, see the main *StoneGate Administrator's Guide*.

Related Tasks

- ▶ [Integrating the SSL VPN With the SMC](#) (page 52)

Abolishment

On the completion of the end-user session, all traces of access to your organization's network can be removed. Browsers leave a trail of information during an access session, including:

- Cookies.
- URL history.
- Cached Pages.
- Registry Entries.
- Downloadable Components.

All these can be removed.

How Does It Work?

When activated, Abolishment runs a software component on the client computer to clean-up the traces at the end of the end-user session. Compatibility with abolishment can be set as a condition of access in Access Rules.

For more information, see [Configuring Abolishment](#) (page 194).

CHAPTER 4

TECHNICAL OVERVIEW

This chapter introduces the services that comprise the StoneGate SSL VPN system. It also describes the SSL VPN network topology, and how the services are connected.

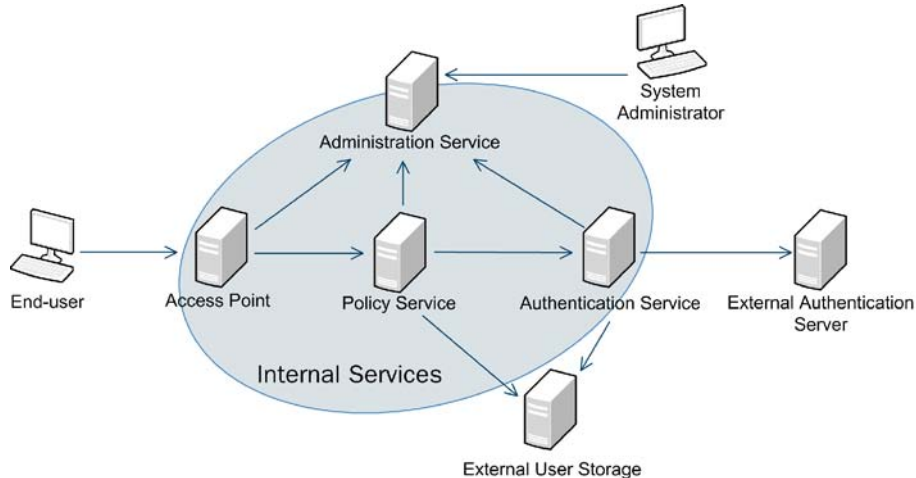
The following sections are included:

- ▶ [Introduction to System Services](#) (page 24)
- ▶ [Default Listening Ports](#) (page 24)
- ▶ [Administration Service](#) (page 25)
- ▶ [Access Point](#) (page 25)
- ▶ [Policy Service](#) (page 26)
- ▶ [Authentication Service](#) (page 28)
- ▶ [Directory Service and User Storage](#) (page 29)

Introduction to System Services

The system services in the StoneGate network are illustrated below.

Illustration 4.1 StoneGate Network



It is recommended to locate the Appliance in the DMZ. The Access Point Service interacts with the Policy Service to validate queries and authorize access. The Administration service allows configuring the appliance. These are always internal in the appliance.

The Authentication Service may be internal or external. In the latter case, it is placed on the internal LAN.

A directory service is used for authorization and authentication purposes. An external (LDAP) user storage is required. To facilitate testing, the system also includes a basic internal LDAP directory service.



Note – Do not use the internal LDAP user storage and Directory Server for anything other than short-term testing. They lack maintenance features necessary to keep the database usable in the long term.

Default Listening Ports

Before installing StoneGate SSL VPN, ensure that the Access Point has access to internal applications, and can be made accessible to external traffic. Connectivity to any external services also must be verified.

For more information on the default listening ports used for traffic to and from the services in the StoneGate network, see [Default Listening Ports](#) (page 245).



Note – All registered services must be able to communicate with the Administration Service.

Administration Service

StoneGate SSL VPN is a complete network of services, with the Administration Service as the hub, and the web-based *StoneGate SSL VPN Administrator* its interface. All these services work together as a self-contained unit in each StoneGate SSL VPN appliance. Optionally, authentication and user storage may be handled by external servers.

You publish all updates in the StoneGate SSL VPN Administrator to the different services, and monitor and manage all user activity in real-time.

Refer to the Online Help for detailed information on how to configure and manage the different services, directory services, and resources.

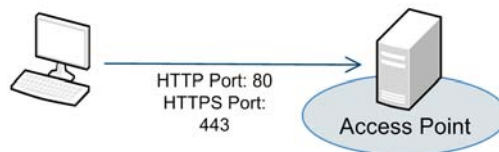


Note - Regular backups of the Administration Service are strongly recommended.

Access Point

As the gatekeeper for all resource and access requests, the Access Point constantly listens for incoming communication.

Illustration 4.2 Default Listening Ports for the Access Point



All requests are logged, filtered, encrypted, and forwarded to the Policy Service or a resource host depending on the type of request.

Mirroring

You can set up a pair of Access Points so that the configuration is automatically copied from the designated primary appliance to the secondary appliance. An external load-balancer can then balance the incoming traffic to either appliance to share the load and to provide a backup for the primary appliance, for example, during scheduled maintenance. The user sessions are shared between the appliances, so that requests can be processed correctly no matter which appliance receives the request.

The mirrored configuration can be used even without the load-balancer, with each appliance's Access Point keeping its own IP address. The replication of configuration and authenticated user sessions takes place as usual.

Trusted Gateways

A client connecting to the Access Point may not have a secure connection, but incoming traffic from the trusted gateway (a specified IP address and port) is assumed to have a specified level of security.

Cipher Suites

When an SSL connection is initialized, the client and server determine a common cipher value to be used for key exchange and encryption. Various cipher values offer different types of encryption algorithms and levels of security.

Link Translation and DNS Mapping

Link translation is used to ensure that all traffic to registered Web resource hosts is routed through the Access Point, which enables the use of SSL and a secure connection.

A link can sometimes be divided into subsets, for example by protocol, host, and path, and then dynamically put together by the browser to form a link. In that case, the Access Point cannot interpret the link and consequently cannot translate it.

To solve this, *DNS mapping* is used. A DNS name or an IP address pointing to the Access Point is mapped to an internal host and protocol: a mapped DNS name.

All mapped DNS names are added to a DNS name pool. From there, you map Web hosts to DNS names using one of two methods:

1. Reserved DNS mapping - the Web resource is mapped to a specific DNS name in the DNS name pool.
2. Pooled DNS mapping - the Web resource is assigned the first available DNS name from the DNS name pool.

Policy Service

The Policy Service is an important part of StoneGate SSL VPN authentication, authorization, and auditing. All authentication methods are configured in the Policy Service, so when a request comes in, the Policy Service evaluates the appropriate access rules and forwards the request to its destination.

Resources

In StoneGate SSL VPN, applications, folders, files, and URLs are registered as Web or tunnel resources. Web-enabled applications are registered as Web resources, and client-server applications that are not Web-enabled are registered as tunnel resources.

For users to be able to access a resource, you must configure a resource host and specify whether it is available in the Application Portal. A resource host can have one or several paths.

There are three different types of resource hosts:

- Web Resources.
- Tunnel Resources.
- Customized Resources.

Tunnel Resources are collected into Tunnel Sets where each tunnel in the set points to a tunnel resource.

Standard Resources

Several of the most frequently used resources are available as Standard Resources. The purpose of this is to minimize your configuration time.

File Sharing Resources

- Microsoft Windows File Share
- Access to Home Directory

Mail

- IMAP/SMTP
- POP3/SMTP
- Outlook Web Access 5.5
- Outlook Web Access 2000
- Outlook Web Access 2003
- Outlook Web Access 2007
- MS Outlook Client 2000/2003/2007

Portal Resources

- Citrix Metaframe Presentation Server
- Microsoft Sharepoint Portal Server 2003

Administration Resources

- StoneGate SSL VPN Administrator

Remote Controlling Resources

- Microsoft Terminal Server 2000
- Microsoft Terminal Server 2003

Other Web Resources

- Salesforce

You can edit the standard resource settings just as easily as any other type of resource. For more information, see the Online Help and [Getting Started with Standard Resources](#) (page 148).

Access Rules

StoneGate SSL VPN authorization makes the access decisions using access rules.

These rules rely on:

- who is requesting access.
- what resource or service is requested.
- what communication channel (or device) is used.
- which authentication methods are most suitable.

Access rules protect resources by allowing or denying access, and specify the requirements for a particular user, resource group, or communication channel. Additionally, business-related conditions can be customized for services. For example, only customers who are allowed credit are able to use the ordering function.

See the Online Help and [Getting Started with Access Rules](#) (page 134), for detailed information on how to add and use Access Rules.

Single Sign-On

Single Sign-On (SSO) permits users to enter their credentials once, giving them access to several resources without the need to re-authenticate when accessing each resource.

All resources using the same user credentials can be defined in a SSO domain. When user credentials are modified, the changes apply to all resources in the SSO domain.

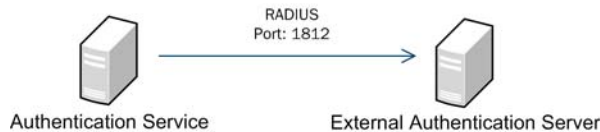
When using the system for the first time, the users are usually prompted for SSO credentials (user ID and password). The SSO credentials are stored per user account and retrieved whenever the user accesses resources registered in a SSO domain. If credentials are changed, the user is prompted for authentication.

For more information, see [Getting Started with Single Sign-On](#) (page 200).

Authentication Service

The Authentication Service provides mobile users with strong authentication methods that can be used regardless of device and location.

Illustration 4.3 Authentication Service as RADIUS proxy



The Authentication Service can proxy the authentication request to another RADIUS server.

Internal Authentication

Internal authentication refers to the Authentication Service using the StoneGate Mobile Text, Web, Challenge, Password, Synchronized, and OATH authentication methods.

When using the Synchronized or Challenge methods, users install Mobile ID client applications on their computer or mobile phone. When using the Web authentication method, the client is either an ActiveX component or a Java applet, used within a browser.

All StoneGate authentication methods can be used in combination or on their own to access any type of resource. The order, in which the different authentication methods are presented to the user is configurable.

See the Online Help and [Getting Started with Authentication Methods](#) (page 108) for detailed information on how to configure and use the different authentication methods.

Directory Service and User Storage

The Directory Service is used to store the data of the user accounts. To use features like Single Sign-On (based on Single Sign-On domains) or StoneGate Authentication methods, you must have a Directory Service enabled.

The Directory Service is separate from any User Storage locations you may have, and it is where StoneGate authentication-specific items are stored for the StoneGate users. However, the Directory Service and User Storage can be in the same directory (for example, in Microsoft Active Directory).

The User Storage location links the users in your Directory Service to SSL VPN user accounts, and uses the Directory Service as the storage for user accounts and credentials for authorization and authentication. You can define multiple User Storage locations.



Caution – Do not use the internal SSL VPN Directory Service and user storage for anything other than short-term testing. Configure an external Directory Service and user storage as explained in [Configuring a Directory Service](#) (page 54) and [Adding an External User Storage Location](#) (page 55).

CHAPTER 5

PLANNING

This chapter presents some general security recommendations for planning the deployment of StoneGate SSL VPN.

The following sections are included:

- ▶ [Getting Started with Planning SSL VPN Deployment](#) (page 32)
- ▶ [Security Audit/Planning](#) (page 32)
- ▶ [User Management Strategy](#) (page 33)
- ▶ [Resource Access](#) (page 35)
- ▶ [Pre-Installation Checklist](#) (page 36)

Getting Started with Planning SSL VPN Deployment

The most important goal of the planning phase is to make sure that:

- End-user and administrator needs are addressed by the services you deploy.
- Service prerequisites that affect installation and initial setup are identified.

Security Audit/Planning

The phases in the security planning process are as follows:

1. Define your security goals.
2. Make preliminary decisions about your security architecture.
3. Determine which users need which permissions to which resources, and develop a strategy for creating access rules.

System Architecture Review

Find potential security problems related to the system architecture. This includes going through existing design documentation and high-level descriptions of the system.

Typical areas of investigation are:

- Where and how sensitive information is stored.
- Identify “trusted” components.
- Communication paths and their protection.
- Identify single-points of failure and components likely to hit Denial Of Service (DOS) attacks.

Public Key Infrastructure

A well-defined public key infrastructure (PKI) enables your organization to secure critical internal and external processes.

Deploying a PKI allows you to perform tasks such as:

- Digitally signing files such as documents and applications.
- Securing e-mail from unintended viewers.
- Enabling secure connections between computers, even if they are connected over the public Internet or through a wireless network.
- Enhancing user authentication through the use of smart cards.

If your organization does not currently have a public key infrastructure, begin the process of designing a new PKI by identifying the certificate requirements for your organization.

Designing a PKI for your organization involves defining your certificate requirements, creating a design for your infrastructure, creating a certificate management plan, and deploying your PKI solution.

A PKI consists of the following basic components:

Component	Description
Digital certificates	Electronic credentials (public keys), which are used to sign and encrypt data. Digital certificates provide the foundation of a PKI.
One or more certificate authorities (CAs)	Trusted entities or services that issue digital certificates. When multiple CAs are used, they are typically arranged in a carefully prescribed order and perform specialized tasks, such as issuing certificates to subordinate CAs or issuing certificates to users.
Certificate policy and practice statements	Two documents that outline how the CA and its certificates are to be used, the degree of trust that can be placed in these certificates, legal liabilities if the trust is broken, and so on.
Certificate repositories	A directory service or other location where certificates are stored and published. In a Windows Server 2003 domain environment, the Active Directory service is the most likely publication point for certificates issued by Windows Server 2003–based CAs, although the system also supports other LDAP-based locations, such as, OpenLDAP, Novell eDirectory, and others. For a complete list of solutions supported, see the StoneGate SSL VPN Release Notes.
Certificate Revocation Lists (CRL)	Lists of certificates that have been revoked before reaching the scheduled expiration date.

User Management Strategy

This section presents a few general security recommendations regarding user management.

Analyzing Your Environment

Your user management settings should complement your particular environment, including:

- The size and distribution of your network.
- The number of users who will access your network.
- The kind of clients users will use to connect.
- Which clients are mobile?
- Which users must have administrator privileges?
- Which users must have access to particular computers?
- What services and resources do users need?
- How you might divide users into groups.
- A password strategy.
- The principle of least privilege: the users must be able to access only those resources that are necessary to their legitimate purpose.

Directory Service Requirements

Identify the directories that will be used for the user repository: user and group information used for authorization.

If you already have an Active Directory or LDAP server set up, you might be able to take advantage of existing records.

Use the following guidelines:

- If you are using Microsoft Active Directory, you can manage users and computers across domains and forests. Active Directory uses the Kerberos version 5 protocol for authentication. This provides a high level of security.
- If you are using UNIX, you can use a UNIX Kerberos Key Distribution Centre (KDC) to provide authentication services for a realm. It is as secure as an Active Directory environment.
- You can also use the Security Accounts Manager (SAM) and NTLM to authenticate local users. This option is not as secure as the first two.

For general guidelines on what to consider when securing the Directory Service, see <http://blogs.sans.org/it-audit/checklists/active-directory-security-checklist/>.

Password Management

StoneGate SSL VPN does not store passwords or encryption keys in unprotected configuration files, LDAP directories, or other system storages. The passwords are stored in the Directory Service in encrypted format.

Encryption keys are automatically generated by the system. A minimum key length of 128 random bits is used for stream and block ciphers. For RSA, a minimum of 1024 bits is used.

Block ciphers use cipher-block-chaining to avoid cut-and-paste attacks.

Encryption keys that are not automatically generated use a secure encryption key generation function to derive the key from a password.

Systems administrators are advised to implement a password policy:

- Password dictionary with banned passwords.
- Password history saving already used passwords.
- Password validity time (not before, not after).
- Password minimum length.
- Constraints on characters, for example, passwords must contain a capital letter and a number.

Use of Special Characters

Avoid special characters (å, ä, ö, ^, ", ~, etc.) in user names and/or passwords.

Since Active Directory treats å and ä as equal to a, and ö as equal to o, we recommend that these characters not be used for account names. The user "Åke" for example may otherwise be able to log on using "Ake", "Äke", or "Öke". StoneGate SSL VPN creates separate user accounts for all three examples, which can cause problems with SSO, for example.

The login page uses UTF-8 by default. To use special characters, you must edit the templates to use other encoding systems.

Resource Access

An authorization strategy enables you to effectively manage users' access to different resources.

Access Strategies

The first part of this process is identifying your users by workgroup, job function, or a combination of workgroup and job function. You can then identify the different types of resources that users access, such as departmental or job-specific data. Consider the policies that determine who is allowed to create user groups, how they are named, and how they are administered.

In StoneGate SSL VPN, the basic strategy for controlling access to resources is to create access rules. Access Rules protect resources by combining requirements such as user group memberships or date and time ranges, and authentication methods such as StoneGate Web or Challenge.

Using Groups

It is recommended to assign permissions to groups, rather than to individual accounts, according to the principle of least privilege.

Example All users in the HR department might need access to privileged personnel records. To protect these, group every member of the HR department into a user group that is authorized to access those files and create access rules of the type User Group.

Naming Conventions

A naming convention decreases the potential for simple mistakes when adding or removing user accounts and selecting the correct group. The consequences of granting access to the wrong group can be serious, causing members to have access to restricted resources or to be denied access to resources that are necessary for job tasks.

When establishing a security group naming convention for your organization, ensure that names:

- Differentiate each group from similar groups
- Allow group names to be sorted into organized lists

Select Authentication Methods

Some resources require a stable set of common permissions. The different user groups may also have different requirements on mobility, which demands different authentication methods. A user belonging to a group with full permission for file share, may also need a strong authentication method enabling mobile access from different clients.

Example A file share typically requires full permissions for very few people, read-write permission for more people, and read-only permission for most people. In this situation, you might create three user groups, one for each of the three common access levels.

The combinations are more or less infinite, which further emphasizes the need for thorough planning.

Pre-Installation Checklist

The following list is by no means exhaustive. You must establish your own checklist for the necessary steps for your deployment.

Table 5.1 Pre-Installation Check List

Check	Activity	Comment
<input type="checkbox"/>	Identify and resolve user management issues	Environment analyzed Directory service secured Password strategy in place External user storage defined (<i>optional</i>)
<input type="checkbox"/>	Identify and resolve security issues	Public Key Infrastructure Operating systems secured File system secured Shared resources secured Physical environment secured Auditing strategy in place Backups and recovery strategies in place
<input type="checkbox"/>	Ensure that existing network has necessary power supplies, switches, and other network components	
<input type="checkbox"/>	Perform time synchronization	Set the clock on the appliance through the basic Web Console (<a href="https://<SSL VPN IP address>:10000">https://<SSL VPN IP address>:10000 if accessed directly through eth0). If you are using a Virtual Appliance, ensure that the hosting platform does not overrule the Virtual Machine-specific time synchronization settings.

CHAPTER 6

GUI OVERVIEW

This chapter is a general introduction to the StoneGate SSL VPN administrator and user interfaces.

The following sections are included:

- ▶ [Getting Started with SSL VPN Graphical User Interface](#) (page 38)
- ▶ [SSL VPN Administrator](#) (page 38)
- ▶ [SSL VPN Web Console](#) (page 45)
- ▶ [SSL VPN Application Portal](#) (page 47)

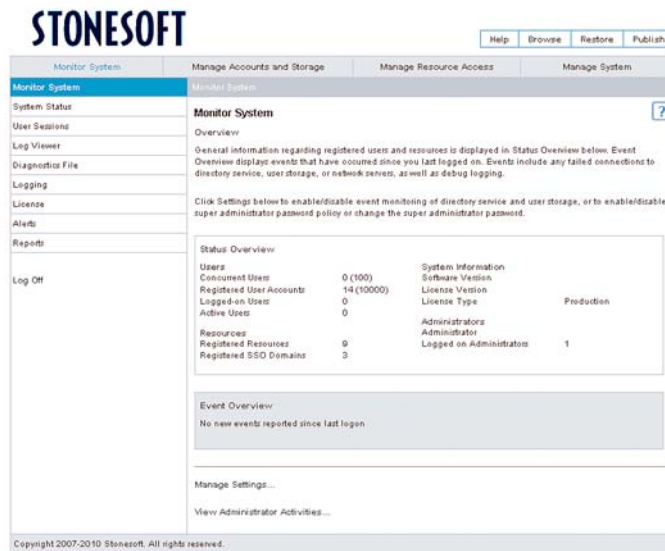
Getting Started with SSL VPN Graphical User Interface

The SSL VPN Graphical User Interface consists of three different views: the Web Console, the SSL VPN Administrator, and the Application Portal.

You use the Web Console and SSL VPN Administrator for configuring and managing the SSL VPN system. The Application Portal is used by end-users to access the resources you make available for them.

SSL VPN Administrator

The StoneGate SSL VPN Administrator is the Web-based administration interface for setting up and managing SSL VPN features.



The basic features in StoneGate SSL VPN Administrator include:

- Web-based administration interface
- Task-oriented approach
- Wizards for common tasks
- Interface adapted to features included in the license
- Context-sensitive online user assistance

To log in to the Administrator, enter `https://<SSL VPN IP Address>:8443` in a web browser. Login with the following credentials:

- **User:** admin.
- **Password:** the password defined for the admin user.

Online Help

You can access the information in the Online Help in different ways. If you click the question mark on a specific page, you access context-sensitive information concerning that page. You can expand the Help window to use the Table of Contents and tabs. If you click the **Help** button in the top menu of the Administrator, you access the start page of the Online Help, with the Table of Contents and help tabs already visible.

The **Getting Started** section of the Online Help contains instructions for how to complete a basic working setup after the initial configuration. The section also contains instructions for getting started with the different features.

Navigating in StoneGate SSL VPN Administrator

The StoneGate SSL VPN Administrator has the following types of menus:

- Top menu
- Main menu
- Left-side menu

The Main menu is divided into four sections: [Monitor System](#) (page 39), [Manage Accounts and Storage](#) (page 40), [Manage Resource Access](#) (page 41), and [Manage System](#) (page 43). Each section has a left-side menu, allowing you to manage your configuration in a flexible and structured environment.

The Administrator is task-oriented. When you click an **Add** link, a wizard guides you through the process of adding user accounts, resources, and so on. You can always cancel a wizard by selecting a different menu item or by simply closing your browser. No changes are saved until you click **Finish Wizard**.

Top Menu

- Use the **Publish** button to distribute changes in the configuration to the entire StoneGate network. When there are unpublished changes in the configuration, the **Publish** button is highlighted.
- Use the **Restore** button to revert to a previous configuration.
- Use the **Browse** button to browse the centrally stored files. The **Browse** dialog displays the schema, templates, and applets stored in the Administration Service. The browser allows you to create directories, and create, move, copy, and delete files in the directory structure.
- Use the **Help** button to access the *Online Help*. Each page in the StoneGate SSL VPN Administrator has a corresponding help page.

Monitor System

- Use the **Manage Settings** link to enable/disable Event Monitoring and to edit the Super Administrator logon credentials.
- Use the **View Administrator Activities** link to see the logon times of all system administrators.
- **Status Overview** displays the current user, resource, and system information.
- **Event Overview** lists events occurred since last logon.

The following navigation options are available in the left-side menu:

Table 6.1 Left-side Menu Options

Option	Description
System Status	System Status contains status information presented on four tabs: General Status, Access Points, Policy Services, and Authentication Services. For additional information, see Monitoring System Status (page 213).
User Sessions	Search for sessions using all or specific authentication methods to view or delete current user sessions. For additional information, see Monitoring Current User Sessions (page 216).
Log Viewer	Search for specific log events from all logs and configuration files for all servers. For additional information, see Viewing Logs in the SSL VPN Administrator (page 217).
Diagnostics File	Create a zip-compressed diagnostics file containing the configuration and logs for all services. The diagnostics file must be included, when submitting a bug report to Stonesoft.
Logging	Manage settings for logging of all or specific servers in the StoneGate network. You can set log collection interval, debug mode, and which time zone to use for timestamps. For more information, see Configuring Logging (page 220).
License	View the contents of the current license. For more information, see SSL VPN License Contents (page 228).
Alerts	Manage alerts used to notify administrators of different types of events. For more information, see Configuring Alert Notifications (page 218).
Reports	Generate reports containing statistics and run-time information on access, authentication, authorization, accounts, and system. For more information, see Generating Reports (page 219).

Manage Accounts and Storage

- **User Accounts**, displays the number of registered users.
- **User Groups** lists the number of registered user groups, sorted by type.
- **User Storage** displays the registered user storage locations.

The following navigation options are available in the left-side menu:

Table 6.2 Left-side Menu Options

Option	Description
User Accounts	Add user accounts using the Add User Account wizard. To edit settings for a specific user account, you can search for registered user accounts and users. For more information on managing user accounts, see Managing User Accounts (page 92).

Table 6.2 Left-side Menu Options (Continued)

Option	Description
User Linking	Create user accounts by linking from user storage. For more information on linking users, see Linking Users (page 94).
User Link Repair	Repair broken links used in User Linking. For more information on repairing user links, see Repairing User Links (page 95).
User Import	Create user accounts by importing a file with existing user information. For more information on importing users, see Creating a File for Importing Users (page 96).
User Groups	Add user groups using the Add User Group wizard. To edit settings for a specific user group, you can search for registered user groups. For more information, see Adding User Groups (page 100).
User Storage	Add user storage locations using the Add User Storage Location wizard. To edit settings for a specific user storage, you can search for registered user storage locations. For more information, see Adding an External User Storage Location (page 55).
Global User Account Settings	Manage global default settings for all registered user accounts. The General Settings tab contain default account settings for logon to the Application Portal and StoneGate authentication settings. Enable automatic and/or manual linking on the User Linking tab. Enable auto repair to update links to the directory service in the Auto Repair tab. For more information, see Managing Global User Account Settings (page 86).
Self Service	Self Service is used when some user administration tasks are allowed to be performed by the end-user. Currently the following scenarios can be left to the end-user: <i>Auto Activation</i> , <i>Forgotten Password</i> , and <i>Forgotten User Name</i> . Self Service must be enabled and configured separately. For more information, see Managing Self Service (page 103).

Manage Resource Access

Use the Add Resource wizards to add Web and tunnel resources. All registered resource hosts and paths can be edited or deleted here.

The following navigation options are available in the left-side menu:

Table 6.3 Left-side Menu Options

Option	Description
Standard Resources	Use the Add Standard Resources wizards to select standard resources from the list and to add standard resources. For more information, see Getting Started with Standard Resources (page 148).
Web Resources	Add Web resources using the Add Web Resource Host wizard. To manage settings for a specific Web resource host or path, use the + sign to display detailed resource information. For more information, see Creating Web Resources (page 158).

Table 6.3 Left-side Menu Options (Continued)

Option	Description
Tunnel Resources	Add tunnel resources using the Add Tunnel Resource Host wizard or Add Tunnel Resource Network wizard. To manage settings for a specific tunnel resource host or path, use the + sign to display detailed resource information. For more information, see Creating Tunnel Resource Hosts (page 174) and Creating Tunnel Resource Networks (page 173).
Tunnel Sets	Add tunnel sets using the Add Tunnel Set wizard. To edit settings for a tunnel set, select tunnel set in the list. For more information, see Creating and Modifying Tunnel Sets (page 175).
Client Firewall	Add client firewalls consisting of Internet firewall configurations using the Add Internet Firewall Configuration wizard. An Internet firewall configuration is a collection of rules that control traffic to and from the Access Client. Each configuration is connected to a corresponding tunnel set.
Customized Resources	Add customized resources using the Add Customized Resource Host wizard. To manage settings for a specific customized resource host or, use the + sign to display detailed resource information.
Access Rules	Add access rules available for several resources and/or SSO domains using the Add Access Rule wizard. To edit settings for an access rule, select access rule in the list. For more information, see Editing Access Rules (page 136).
Application Portal	Add Application Portal items using the Add Application Portal Item wizard. To edit settings for a specific item, select item in the list. For more information, see Getting Started with Application Portal Customizations (page 70).
SSO Domains	Add SSO domains using the Add SSO Domain wizard. To edit settings for a specific SSO domain, select SSO domain in the list. For more information, see Adding an SSO Domain (page 200).
Identity Federation	Add SAML 2.0 and ADFS identity providers using the Add Identity Provider wizard and service providers using the Add Service Provider wizard. Use the Manage Global Identity Federation Settings to manage global identity federations. For more information, see Managing Identity Federation Settings (page 203).

Table 6.3 Left-side Menu Options (Continued)

Option	Description
Global Resource Settings	<p>Manage global default settings for all registered resources. Global resource settings are managed on the following tabs:</p> <ul style="list-style-type: none"> • Specify internal proxy hosts on the General Settings tab. • In the DNS Name Pool tab you can add DNS names for Access Points and Pools. • On the Filters tab, you add and manage filters used to filter specific pages or requests to specific resources. • Edit headers used for filtering on the Link Translation tab. • In the Client Access tab you manage Client Access Settings and Device Control Settings (= device settings and device access restriction settings). • In the Trusted Gateways tab you can add and delete trusted gateways to the system. • In the Advanced tab you can define what type of information to add to internal requests and whether cache control is used for Internet Explorer users.

Manage System

The **Manage System** section allows you to add, edit and delete services, certificates, authentication methods, RADIUS back-end servers and clients, as well as configure directory service settings. It is also possible to enter global settings which apply to all Access Points, Policy Services, and Authentication Services, and general settings for notifications and SMS distribution.

The following navigation options are available in the left-side menu:

Table 6.4 Left-side Menu Options

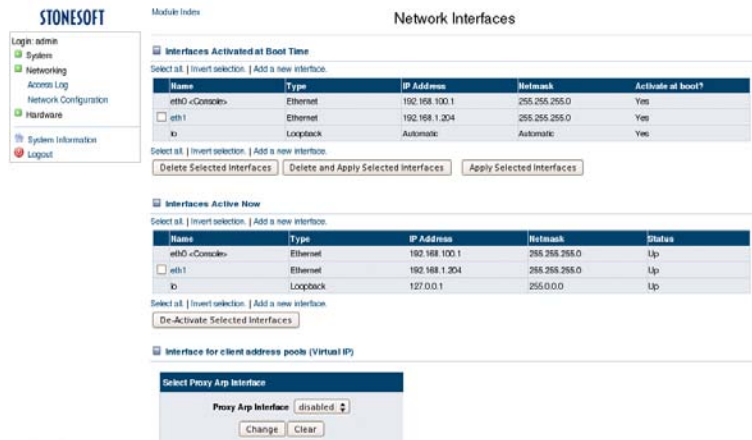
Option	Description
Authentication Methods	<p>Add authentication methods using the Add Authentication Method wizard. To edit settings for extended properties and/or RADIUS replies for a specific authentication method, select authentication method in the list. For more information, see Managing Authentication Methods (page 112).</p>
Certificates	<p>Add, edit or delete Certificate Authorities, Server Certificates and Client Certificates. For more information, see Getting Started with Certificates (page 121).</p>
Abolishment	<p>Define actions performed on a client computer when using an abolishment access rule. Actions include the monitoring of downloaded files and deleting of internet browser history and browser cache. For more information, see Configuring Abolishment (page 194).</p>
Assessment	<p>Define user client computer assessment activities. Activities include: client scan, setup of reference machines, and use of plug-ins in assessment access rules. For more information, see Configuring Assessment (page 190).</p>

Table 6.4 Left-side Menu Options (Continued)

Option	Description
RADIUS Configuration	Add RADIUS clients using the Add RADIUS Client wizard. To edit settings for a specific RADIUS client, select client in the list. Click the Manage RADIUS Back-end Servers link to add and edit RADIUS back-end servers. These RADIUS clients and back-end servers are used by the Authentication Service. For more information, see Managing RADIUS Configuration (page 117).
Notification Settings	Manage settings for notification message channels: SMS, e-mail, and/or E-mail/Screen. The notification channel settings are also used for alerts. For more information, see Configuring Alert Notifications (page 218).
Device Definitions	Manage definitions of how HTTP headers in requests are interpreted to identify devices by the Access Point. Add definitions using the Add Device Definition wizard. To edit the definition of a specific device, select device in the list. For more information, see Configuring Device-Specific Controls (page 186).
Delegated Management	Manage administrative roles with different privileges and responsibilities. For more information, see Configuring Delegated Management (page 102).
Access Points	Add Access Points using the Add Access Point wizard. To edit settings for a specific Access Point, select Access Point in the list. For more information, see Access Point (page 25).
Policy Services	Add Policy Services using the Add Policy Service wizard. To edit settings for a specific Policy Service, select Policy Service in the list. Click the Manage Global Policy Service Settings link to edit default global communication settings. For more information, see Policy Service (page 26).
Authentication Services	Add Authentication Services using the Add Authentication Service wizard. To edit settings for a specific Authentication Service, select Authentication Service in the list. Click the Manage Global Authentication Service Settings link to display global default RADIUS authentication and password and/or PIN settings. For more information, see Managing Authentication Services (page 126).
Administration Service	Manage internal communication settings (in the StoneGate network) and external communication settings (with the client). For more information, see Administration Service (page 25).
Directory Service	Manage general settings for the directory service. You can change type of directory service here, test the connection to the directory service, and enable SSL communication. For more information, see Configuring a Directory Service (page 54).
OATH Configuration	Manage the OATH configuration for importing tokens from file, backing up and restoring of database, and for configuring scheduled backups. For more information, see Managing OATH Configuration (page 118).

SSL VPN Web Console

The Web Console allows you to configure basic operating-system-level settings for the StoneGate SSL VPN appliance, such as, for example, configuring network interfaces, enabling IP address pool, and configuring routing.



▼ To log in to the Web Console

1. Enter `https://<SSL VPN IP Address>:10000` in a web browser.
2. Log in with the following credentials:
 - **User:** admin.
 - **Password:** <password set for admin user>).

Navigating in StoneGate SSL VPN Web Console

The SSL VPN Web Console consists of the following configuration views:

- System
- Networking
- Hardware

System

Use the System settings for making basic system settings, such as setting and changing passwords, and making initial contact to the SMC. The following configuration options are available in the System settings:

Table 6.5 Configuration Options in System Settings

Option	Description
Admin Password	Define the new administrator password for the appliance.
Backup Management	Create, restore, and delete SSL VPN backups.
Initial Contact	Define the contact management IP address and one time password for initial contact. On this page you can also switch SSL VPN to standalone mode.

Table 6.5 Configuration Options in System Settings (Continued)

Option	Description
Mirrored Pair	Check the current appliance configuration, define the mode of the appliance, and download a CA certificate.
Remote Upgrade	Upgrade the SSL VPN appliance. When the initial contact has been made to the SMC, the backups can also be restored through it.
Root Password	Define the new root password for the appliance.
Services	Reboot the appliance, restart services separately, enable SSH daemon, activate OATH, and internal LDAP

Networking

Use the Networking settings to define network configuration and to check access logs. The following configuration options are available in the Networking settings:

Table 6.6 Configuration Options in the Networking Settings

Option	Description
Access Log	Check the latest access logs of the appliance.
Network Configuration	Define the network configuration of the appliance. The settings include the setting of Network Interfaces, Routing and Gateways, Hostname and DNS Client, Host Address, and the activation of IP address pool functionality on OS level.

Hardware

Use the Hardware settings to set system time and change the time zone.

- Set the system time/hardware time, and change the time zone of the appliance.

SSL VPN Application Portal

The StoneGate SSL VPN Application Portal is Web-based end-user interface, that lists the resources that the end-user is allowed to access. You can also set up an access for yourself to manage the SSL VPN system remotely.

STONESOFT

Help Logged On: Log Off

StoneGate SSL VPN Application Portal

Welcome to the StoneGate SSL VPN Application Portal. The resources you have access to are displayed below. To start a resource, click the corresponding icon.

Resources



Intanet

▼ To log in to the SSL VPN Application Portal

- ↪ Enter `https://<SSL VPN Domain>:10000` in a web browser.

Example `https://ssl.example.com:10000`.



Note - Do not use the SSL VPN IP address for logging into the Application Portal. In StoneGate SSL VPN, the licenses are assigned by domains and not by IP addresses, and attempting to login to the Application Portal using the SSL VPN IP address and port 10000 results in a “403: Unknown Host Header” error message.

INITIAL CONFIGURATION

In this section:

[Configuring the System After Installation - 51](#)

[Configuring Mirroring - 59](#)

[Customizing the Application Portal - 69](#)

CHAPTER 7

CONFIGURING THE SYSTEM AFTER INSTALLATION

This chapter describes how to configure the SSL VPN system after it has been installed as shown in the *SSL VPN Appliance Installation Guide*.

The following sections are included:

- ▶ [Getting Started with SSL VPN Configuration](#) (page 52)
- ▶ [Integrating the SSL VPN With the SMC](#) (page 52)
- ▶ [Configuring a Directory Service](#) (page 54)
- ▶ [Adding an External User Storage Location](#) (page 55)
- ▶ [Further Configuration Steps](#) (page 57)

Getting Started with SSL VPN Configuration

Prerequisites: Appliance has been installed as instructed in the *Appliance Installation Guide*

Required Configuration

After you have installed the appliance as explained in the *SSL VPN Appliance Installation Guide*, you must configure an external Directory Service and an external User Storage Location. The basic internal LDAP database is meant to facilitate basic single-appliance testing only, and is not suitable for long-term production use or any type of mirrored configuration.

You can also optionally configure the StoneGate Management Center (SMC) to monitor the SSL VPN gateway.

Configuration Overview

1. (Optional) Configure the SMC to monitor the SSL VPN gateway as explained in [Integrating the SSL VPN With the SMC](#) (page 52).
2. Configure an external Directory Service to work with SSL VPN. See [Configuring a Directory Service](#) (page 54).
3. Add an external user storage to the SSL VPN. See [Adding an External User Storage Location](#) (page 55).

What's Next?

- ▶ If you want to use the SSL VPN with the SMC, begin by [Integrating the SSL VPN With the SMC](#) (page 52).
- ▶ Otherwise, begin by [Configuring a Directory Service](#) (page 54).

Integrating the SSL VPN With the SMC

Prerequisites: Appliance has been installed as instructed in the *Appliance Installation Guide*

To monitor the SSL VPN Gateway in the Management Client, you must create an SSL VPN Gateway element to represent the gateway in the SMC.

You must also make initial contact with the Management Server in the SSL VPN Gateway's Administrator interface, import the license to the SMC, and apply the configuration.

Configuration Overview

1. Create an SSL VPN Gateway element in the SMC. See [Creating an SSL VPN Gateway Element](#) (page 53).
2. Save the initial configuration information in the SMC. See [Saving the Initial Configuration](#) (page 53).
3. Make an initial contact between the appliance and the Management Server. See [Making Initial Contact](#) (page 53).
4. Import the gateway's license into the SMC. See [Importing SSL VPN License Into the SMC](#) (page 53).
5. Apply the configuration to the SSL VPN element you created in the SMC. See [Applying the Configuration](#) (page 54).

Creating an SSL VPN Gateway Element

▼ To create an SSL VPN Gateway Element

1. Log in to the StoneGate Management Client.
2. Right-click **Monitored Elements** and select **New**→**SSL VPN Gateway**.
3. Give a **Name** to your SSL VPN Gateway, and double-click the **IP Address** field to open the Node Properties dialog.
4. Enter the **IP Address** and the **Application Portal URL**. Entering the Application Portal URL here allows you to open the Application Portal through a shortcut in the Management Client.
5. Click **OK**.

Saving the Initial Configuration

▼ To save the initial configuration

1. Expand the SSL VPN branch until you can see the node under the Gateway.
2. Right-click the SSL VPN Gateway element you created and select **Save Initial Configuration**. The Initial Configuration dialog opens.
3. Right-click the one-time password and select **Copy Password**. The password is copied to the clipboard.
4. Click **Close**.

Making Initial Contact

▼ To make initial contact

1. Log in to the Web Console at `https://<SSL VPN IP Address>:10000`.
2. Browse to **System**→**Initial Contact**. The Initial Contact page opens.
3. Enter the IP address of the StoneGate Management Server as the **Management IP Address**.
4. Paste the one-time password you copied in [Saving the Initial Configuration](#).
5. Click **Contact**. The SSL VPN appliance sends the initial contact request to the Management Server. When the initial contact is successfully completed, a confirmation appears.

Importing SSL VPN License Into the SMC

▼ To import a license to the SMC

1. In the StoneGate Management Client, Browse to **File**→**System Tools**→**Install Licenses**. The Install License File(s) dialog opens.
2. Browse to the SSL VPN license file, and click **Install**. The license is imported.

Applying the Configuration

▼ To apply the configuration

1. Right-click the SSL VPN Gateway element you created and select **Apply Configuration**. The Policy Upload Task Properties dialog opens.
2. Select your SSL VPN from the list on the left and click **OK**. The Send Configuration tab opens and shows the progress of the upload.
3. When the upload has finished, check from the System Status view that the state of your SSL VPN Gateway element changes to green (OK).

Configuring a Directory Service

Prerequisites: Appliance has been installed as instructed in the *Appliance Installation Guide*

Configure an external Directory Service to operate with the SSL VPN. For a list of supported Directory Services, see the *Release Notes*.

▼ To configure a Directory Service

1. In the appliance's StoneGate SSL VPN Administrator interface, browse to **Manage System**→**Directory Service**. The Manage Directory Service page opens.
2. Configure the following Directory Service server settings:

Setting	Description
Primary Host	The IP address of the primary Directory Service server.
Secondary Host	The IP address of the backup Directory Service server.
Port	The listening port of the Directory Service server.
Account	The administrator DN of the Directory Service server.
Password	The administrator password of the Directory Service server
Location DN	The base DN for the storage in the Directory Service server. For Active Directory, the Location DN must start with an Organizational Unit (OU="..."...). Configure the Location DN to set the Organizational Unit as not part of a container. For example, OU=Accounts,DC=DOMAIN,DC=COM or OU=Accounts,OU=SSLVPN, DC=DOMAIN,DC=COM
Time-out	The connection time-out of the Directory Service server.
Enable change of directory service type	Select this to change the Directory Service type.
Directory Service Type	The type of directory service used in your environment.
Use SSL	(Optional) Use the SSL protocol for the communication with the Directory Service

3. Click **Test Connection** to verify that the settings are correct, and that the Directory Service is reachable.
4. Click **Save**. You are prompted to confirm the changes in the Directory Service settings.

5. Click **Yes**.

Adding an External User Storage Location

Prerequisites: Appliance has been installed as instructed in the *Appliance Installation Guide*

A User Storage Location is a user database that is queried by the Policy Service as part of the authorization process.

▼ To add an external User Storage Location

1. Enter the following command on the server's command line to check that the server listens to port 389 for LDAP and/or port 636 for LDAPS for incoming queries:
 - `netstat -an|find "<port number>"`
2. Log in to the SSL VPN Administrator at `https://<SSL VPN IP Address>:8443`.
3. Browse to **Manage Accounts and Storage**→**User Storage**. The Manage User Storage page opens.
4. Click **Add User Storage Location** and select the type of user storage. Click **Next**.
5. Fill in the following fields and leave the other parameters set to their default values.:

Field	Description
Display Name	The name of the user storage.
Host	The IP address of the user storage server.
Secondary Host	The IP address of the backup user storage server (Leave the field empty if there is no secondary host).
Port	Listening port number (389 for LDAP or 636 for LDAPS).
Account	An account with read-write permissions. For example, <i>administrator@example.com</i> .
Password	The account's password.
Timeout	The timeout in seconds after which a query is considered unanswered.
Use SSL	(Optional) Use the SSL protocol for the communication with the Directory Service. Select Use SSL if LDAPS is used.
Follow referrals	Redirects requests from one Directory Service to another. Referrals are linked between different Directory Services or within the same directory server.
Nested Group Search	(Microsoft Active Directory only) Include Active Directory nested user groups in user information search.

6. Click **Next**.
7. Click **Test Connection to User Storage** to verify the correct connectivity with the user storage, using the parameters you defined. If the connection succeeds, proceed to define search scopes for user accounts and groups.
8. Click **Add User Search Rule** to add the DN (Distinguished Name) that defines where user accounts are searched for when this user storage is used.

9. Click **Show Tree** to display directory structure and select the DN where user accounts you are interested in are located. If necessary, configure an additional filter to limit and a different search scope to restrict or extend the query operation.
10. Click **Next** to return to the previous screen.
11. Click **Add User Group Search Rule** and define the scope of the query when searching for groups.
12. Click **Finish Wizard** and verify that the state of the external User Storage is *Connected*. To activate the changes, click **Publish** at the top of the page.

Updating an External User Storage

▼ To update an external user storage location

1. Browse to **Manage Accounts and Storage**→**User Storage**. The Manage User Storage page opens.
2. Click the user storage location to be updated under Registered User Storage Locations. The General Settings tab opens, showing the previously entered general settings of the user storage location.
3. Modify the settings of the selected Directory Service type:

Field	Description
Display Name	The name of the user storage.
Host	The IP address of the user storage server.
Secondary Host	The IP address of the backup user storage server (Leave the field empty if there is no secondary host).
Port	Listening port number (389 for LDAP or 636 for LDAPS).
Account	An account with read-write permissions. For example, <i>administrator@example.com</i> .
Password	The account's password.
Timeout	The timeout in seconds after which a query is considered unanswered.
Use SSL	<i>(Optional)</i> Use the SSL protocol for the communication with the Directory Service. Select Use SSL if LDAPS is used.
Follow referrals	Redirects requests from one Directory Service to another. Referrals are linked between different Directory Services or within the same directory server.
Nested Group Search	<i>(Microsoft Active Directory only)</i> Include Active Directory nested user groups in user information search.

4. Click the Search Rule tab. Define the user and user group search rules.
5. Click the Directory Mapping tab. Define the user storage attributes used in directory mapping.
6. Click **Save** to save the changes. To activate the changes, click **Publish** at the top of the page.

Further Configuration Steps

Prerequisites: [Configuring a Directory Service](#), [Adding an External User Storage Location](#)

After completing the basic configuration as explained in this chapter, you can proceed with setting up the working configurations:

- To configure two appliances for a load-balanced setup, see [Configuring Mirroring](#) (page 59).
- To set up access to resources, see [Daily Management](#) (page 83).

CHAPTER 8

CONFIGURING MIRRORING

This chapter describes how to set up mirroring between two StoneGate SSL VPN appliances.

The following sections are included:

- ▶ [Getting Started with Configuring Mirroring](#) (page 60)
- ▶ [Preparing for Mirroring](#) (page 61)
- ▶ [Configuring Basic System Services for Mirroring](#) (page 61)
- ▶ [Configuring Administrator Web Resources for Mirroring](#) (page 64)
- ▶ [Setting Up the Administrator Service for Mirroring](#) (page 65)
- ▶ [Setting Up Registered Authentication Method Servers](#) (page 64)
- ▶ [Setting Up Appliances as Primary and Secondary](#) (page 66)
- ▶ [Configuring Server Pool Monitoring Agents](#) (page 67)

Getting Started with Configuring Mirroring

A pair of SSL VPN appliances can be set up so that the configuration is automatically copied from a designated primary appliance to a secondary appliance to provide a backup for the primary appliance, for example, during a scheduled maintenance break.

To achieve a load-balanced or standby solution, you must configure an external load balancing product of your choice, for example, StoneGate Firewall/VPN system with Server Pool Load Balancing.

All configuration is done on the primary appliance. The information is then exported from the primary appliance and imported to the secondary appliance. It is recommended to use a dedicated interface for mirroring on each appliance.

What Do I Need to Know Before I Begin?

The primary and secondary roles defined for the appliances are permanent. You cannot change the roles without re-installing and reconfiguring primary and secondary appliances. In mirrored configuration, the StoneGate SSL VPN Administrator is not available on the secondary appliance.

After the appliances are set up for mirroring, all day-to-day configuration is done through the primary appliance and the configuration changes are automatically synchronized to the secondary appliance.

The internal LDAP in StoneGate SSL VPN can be used only for evaluation purposes or small scale implementations without mirroring. When mirroring is used with StoneGate SSL VPN, an external User Storage must always be configured, and OATH must be either disabled in the Web Console or configured to use an external database as described in [StoneGate SSL VPN Technical Note #5342](#).

Configuration Overview

1. Set up the appliances so that they are ready for mirroring. See [Preparing for Mirroring](#) (page 61).
2. Configure the Policy, Authentication, and Access Point services. See [Configuring Basic System Services for Mirroring](#) (page 61).
3. Configure remote administrator access. See [Configuring Administrator Web Resources for Mirroring](#) (page 64).
4. Complete the configuration by setting up the StoneGate SSL VPN Administrator. See [Setting Up the Administrator Service for Mirroring](#) (page 65).
5. Set up registered Authentication Method Servers. See [Setting Up Registered Authentication Method Servers](#) (page 64).
6. Configure the network-level settings and pair the appliances together. See [Setting Up Appliances as Primary and Secondary](#) (page 66).

Preparing for Mirroring

▼ To prepare for mirroring

1. Make sure both appliances are installed and configured with their basic interface settings as instructed in the *SSL VPN Appliance Installation Guide* (delivered with each appliance). The dedicated interface on both appliances must have a static IP address. Any more advanced configuration on the secondary appliance (done in the StoneGate SSL VPN Administrator) is overwritten when the appliances are paired together for mirroring.
2. If the appliances are already configured and there are services running on the mirroring interface of the primary appliance, consider reconfiguring the appliance so that there is a dedicated mirroring interface. If there are no free ports, a shared interface can be used.
3. Make sure the primary appliance is configured to use an External User Storage (**Manage Accounts and Storage**→**User Storage**) and Directory Service (**Manage System**→**Directory Service**) because the internal LDAP server information is not mirrored between the appliances and is stored only on the primary appliance.
4. Connect the appliances together through their dedicated interfaces.
5. Make sure the communications with external services (for example, the user database) are routed correctly so that both appliances can use them.

Configuring Basic System Services for Mirroring

First, you must configure the Policy, Authentication, and Access Point services to run on the normal static IP address of the dedicated interface instead of the default loopback address and add identical services with the IP address of the secondary appliance.

All configuration is done on the primary appliance.

Configuring the Policy Service for Mirroring

▼ To configure the Policy Service for mirroring

1. Log in to the Administration Service (port 8443) on the appliance that will be the primary appliance.
2. Click **Policy Services** in the left-hand menu.
3. Click the IP address 127.0.0.1 under **Internal Host**.
4. Enter the dedicated interface **Internal Host** IP address of the primary appliance.
5. Click **Add Policy Service** and create an identical service, but with the secondary appliance's dedicated interface IP address in the **Internal Host** field.
6. Click **Save**.

Configuring the Authentication Service for Mirroring

▼ To configure the Authentication Service for mirroring

1. Click **Authentication Services** in the left-hand menu.
2. Click the IP address 127.0.0.1 under **Internal Host**.
3. Type the dedicated interface IP address of the primary appliance in the **Internal Host** field.
4. Click **Add Authentication Service** and create an identical service, but with the secondary appliance's dedicated interface IP address in the Internal Host field.
5. Click **Save**.

Configuring the Access Point Service for the Primary Appliance

▼ To configure the Access Point service for the primary appliance

1. Click **Access Points** in the left-hand menu.
2. Give a **Display Name** for the Access Point.
3. Click the IP address 127.0.0.1 under **Internal Host**.
4. Type the dedicated interface IP address of the primary appliance in the **Internal Host** field.
5. Select **Listen on All Interfaces**.
6. Click **Add Additional Listener**.
7. Enter general settings:

Example Value	Description
Host	The dedicated interface IP address of the primary appliance.
Port	16972
Server Certificate	None Selected
Type	Load Balance

8. Select **Listen on All Interfaces**.
9. Click **Add**.
10. Click **Save**.



Note - Ensure that the **Listen on All Interfaces** option is selected both in basic configuration and when defining Additional Listeners.

Configuring the Access Point Service for the Secondary Appliance

▼ To configure the Access Point service for the secondary appliance

1. Click **Add Access Point**.
2. Give a **Display Name** for the Access Point.

3. Type the dedicated interface IP address of the secondary appliance in the **Internal Host** field.
4. Type the loopback address 127.0.0.1 in the **Application Portal Host** field.
5. Select **Listen on All Interfaces**.
6. Make sure the other settings are identical with the primary appliance's Access Point service.
7. Click **Add Additional Listener**.
8. Enter general settings:

Example Value	Description
Host	The dedicated interface IP address of the secondary appliance.
Port	16972
Server Certificate	None Selected
Type	Load Balance

9. Select **Listen on All Interfaces**.
10. Click **Add**.
11. Click **Save**



Note – Ensure that the **Listen on All Interfaces** option is selected both in basic configuration and when defining Additional Listeners.

Selecting the Access Points for Mirroring

▼ To select the Access Points for mirroring

1. Click **Access Points** in the left-hand menu.
2. Click the **Configure Load Balancing** link.
3. Select **Enable multi-host sessions**.
4. Click the link **Add Pair of Mirrored Access Points** at the bottom of the page, under Mirrored Access Points.
5. In the window that opens, select the two Access Points to be mirrored in the **Primary server** and **Secondary server** menus.
6. Click **Update**. The pair of mirrored Access Points is saved.

If you are doing basic testing without an external user storage and Directory Service, you must replace the loopback address for those services with the dedicated interface address of the primary appliance. Configure the loopback address temporarily as the Secondary Host for the directory service to keep the service available during the reconfiguration.



Caution – If you use the internal user storage, the secondary appliance must fetch user information from the primary appliance and the secondary appliance cannot function without the primary appliance.

What's Next?

- ▶ To allow remote access to administration resources in a mirrored environment, proceed to [Configuring Administrator Web Resources for Mirroring](#) (page 64).
- ▶ Otherwise, proceed to [Setting Up the Administrator Service for Mirroring](#) (page 65).

Configuring Administrator Web Resources for Mirroring

To use the StoneGate SSL VPN Administrator and Web Console services remotely, configure also these services to the normal static IP addresses. If the resource is configured using the default loopback address, the resource uses whichever appliance the load-balancer happens to select for your connection.

▼ To configure remote administrator access for a mirrored appliances

1. Browse to **Manage Resource Access**→**Web Resources**. The Manage Web Resources page opens.
2. Change the **Host** IP address of the resource for the StoneGate SSL VPN Administrator (HTTP port 8443) from the loopback address to the dedicated interface IP address of the primary appliance. The secondary appliance does not run this service since both nodes are configured through the primary appliance.
3. Click **Save**.
4. Change the **Host** IP address of the resource you have created for the Web Console (HTTP port 10000) to the dedicated interface IP address of the primary appliance and rename the service accordingly (for example, *Web Console on Primary*).
5. Click **Save**.
6. Create a new **Web Resource Host** for the Web Console (HTTP port 10000) of the secondary appliance using the dedicated interface IP address of the secondary appliance and name the service accordingly (for example, *Web Console on Secondary*).
7. Click **Save**.

Setting Up Registered Authentication Method Servers

In a mirrored configuration, it is mandatory to set up two registered Authentication Method Servers for all authentication methods. If two registered Authentication Method Servers have not been set up, the authentication will not work from the secondary appliance if the primary appliance goes down.

▼ To set up a registered Authentication Method Server

1. Browse to **Manage System**→**Authentication Methods**. The Manage Authentication Methods page opens.
2. Select the authentication method for which the Authentication Method Server is set up (StoneGate Web, StoneGate Challenge, StoneGate Synchronized, StoneGate Mobile Text, or StoneGate Password).
3. Click **Add Authentication Method Server**.

4. Enter the general settings for the primary Authentication Method Server (Select **Host** from the drop-down menu and leave **Port** to its default value):

Example Value	Description
Display Name	The display name of the primary/secondary appliance.
Host	The dedicated interface IP address of the primary/secondary appliance.
Port	18123

5. Click **Add**.
6. Set up the secondary Authentication Method Server in the same manner as described in steps 3-5.
7. Click **Save**.
8. To activate the changes, click **Publish** at the top of the page.

For additional information on Authentication Method Servers, see [Getting Started with Authentication Methods](#) (page 108).

Setting Up the Administrator Service for Mirroring

When you have configured all other settings, you can change the IP address of the Administration service. Depending on your setup, Administration service may become unreachable until the rest of the configuration is complete.

▼ To configure the Administration service IP address

1. Click **Administration Service** in the left-hand menu.
2. Replace the IP address 127.0.0.1 in **Internal Host** with the dedicated interface IP address of the primary appliance.
3. Click **Save**.
4. Click **Publish**.



Note - If available, the status display for all services shows them as not connected, since the access rules remain unchanged at this point. The access rules are changed automatically and the services return to their normal status when you complete the configuration as explained below.

Setting Up Appliances as Primary and Secondary

If the primary appliance must be replaced, the secondary appliance can be used to handle the traffic, but it must be paired to the replacement primary appliance. For this reason, we strongly recommend that you make sure you always back up your most recent configuration on the primary appliance and keep the backup in a secure location to be prepared for a complete loss of the primary appliance (see [Working With Backups](#) (page 231)). There is no need to back up the secondary appliance.

Configuring the Primary Appliance

▼ To configure the primary appliance

1. Log in to the Web Console on the primary appliance with a direct connection through eth0 (<https://<SSL VPN IP Address>:10000>).
2. Browse to **System**→**Mirrored Pair**.
3. Under **Available Modes**, select **Primary** and click **Change**.
4. On the page that opens, click **Download** to export the configuration file for the secondary appliance.

Configuring the Secondary Appliance

▼ To configure the secondary appliance

1. Log in to the Web Console on the secondary appliance with a direct connection through eth0 (<https://<SSL VPN IP Address>:10000>).
2. Browse to **System**→**Mirrored Pair**.
3. Under **Available Modes**, select **Secondary** and click **Change**.
4. On the page that opens, **Browse** to the configuration file.
5. Click **Import** and confirm to upload the configuration file that you saved on the primary appliance.

What's Next?

- ▶ The mirroring configuration is complete.

Configuring Server Pool Monitoring Agents

Monitoring Agents are part of the StoneGate Firewall/VPN's Server Pool feature. A Server Pool Monitoring Agent is installed by default on each SSL VPN appliance. The Monitoring Agent starts automatically when initial contact between the SMC and the SSL VPN appliance has been established. The SSL VPN Server Pool Monitoring Agent has a default basic configuration that can be used out-of-the-box. If you need to reconfigure the Server Pool Monitoring Agent, follow the guidelines below.

▼ To configure the SSL VPN Server Pool Monitoring Agent

1. Access the SSL VPN engine command line in one of the following ways:
 - Physically through a serial console using a null-modem cable.
 - Physically by connecting a display and keyboard directly to the engine machine.
 - By using an SSH client.
2. Log in as `root` and enter the engine password.
3. Temporarily disable the running StoneGate Monitoring Agent daemon:
`msvc -d sgagentd`
4. As the default permissions of `sgagent.conf` do not allow editing, make the file editable:
`/usr/lib/stonegate/sslgw_set sgagent.conf editable`
5. Use the included vi editor to open the `sgagent.conf` file for editing:
`vi /data/config/sgagentd/confdir/sgagent.conf`
6. Modify the `sgagent.conf` file. For modification examples, see the *StoneGate Administrator's Guide*.
7. Save your changes with command: `wq`
8. Restart the StoneGate Monitoring Agent daemon:
`msvc -u sgagentd`
9. Change the `sgagent.conf` file permissions back to the default value:
`sslgw_set sgagent.conf default`

For configuration instructions and additional information on the operation of Server Pool Monitoring Agents, see the *StoneGate Administrator's Guide*.

CHAPTER 9

CUSTOMIZING THE APPLICATION PORTAL

The Application Portal provides an end-user interface to resources. You can customize the Application Portal text, colors, and layout.

The following sections are included:

- ▶ [Getting Started with Application Portal Customizations](#) (page 70)
- ▶ [Working with Customization Files](#) (page 71)
- ▶ [Customizing Application Portal Text](#) (page 73)
- ▶ [Customizing Application Portal Images](#) (page 74)
- ▶ [Customizing Application Portal Colors and Layout](#) (page 75)
- ▶ [Customizing HTML Templates](#) (page 76)
- ▶ [Customizing the StoneGate Web Authentication Script](#) (page 80)

Getting Started with Application Portal Customizations

Prerequisites: None

The Application Portal provides a simple interface for end-user resource access. You can modify the Application Portal to match the look-and-feel of your organization. In addition to stylistic and graphical elements, you can also change the layout of the content, and edit the text that is presented to the end-users.

You can brand these parts of the Application Portal:

- The logon pages.
- The main Application Portal page.
- The Application Portal Online Help.
- The StoneGate Web authentication applet (virtual keypad).

What Do I Need to Know Before I Begin

Customization does not affect which resources the user is shown. Use Access Rules to determine which resources each user can see. The available resources are displayed dynamically based on what a user is allowed to access in each session.

Some labels and the icons for resources can be changed directly in the configuration in the StoneGate SSL VPN Administrator. There is no need to change these through the customization process described here.

Some customizations require you to manually edit HTML and CSS files. Familiarity with HTML and CSS is required.

Configuration Overview

1. Locate the customization files as instructed in [Finding the Root Folder for Customization Files](#) (page 71).
2. Follow the general workflow outlined in [Editing or Replacing Customization Files](#) (page 72) to make the customizations. Check the task-specific file locations and names from the following sections:
 - [Customizing Application Portal Text](#) (page 73)
 - [Customizing Application Portal Images](#) (page 74)
 - [Customizing Application Portal Colors and Layout](#) (page 75)
 - [Customizing HTML Templates](#) (page 76)
 - [Customizing the StoneGate Web Authentication Script](#) (page 80)

Working with Customization Files

Prerequisites: None

Files on the SSL VPN appliance can be accessed through the command line or through a graphical file browser in the SSL VPN Administrator interface.

The command line interface supports standard Linux commands and tools, such as `scp` and `ftp` for connecting to a compatible file server, `cp` for copying files, and `mkdir` for creating folders.

Unless otherwise specified, the instructions in this chapter assume you are using the graphical file browser.

Finding the Root Folder for Customization Files

There is a separate folder structure for your custom files, with the same structure as the default folder. Any file that is put into the custom folder is used without destroying the original file.

All default style sheets, images, and template files are located in the following folder:

- When accessed through the command line
`/data/portwise/administration-service/files/access-point/built-in-files/wwwroot/wa/`
- When accessed through the SSL VPN Administrator file browser
`/opt/portwise/administration-service/files/access-point/built-in-files/wwwroot/wa/`



Caution – Do not directly edit the original default files; copy the files to the custom files directory and edit the copies. Do not directly edit the HTML/WML files for the Application Portal pages.

These two paths refer to the same folder even though the display name of the root folder is slightly different depending on the access method. The `files` folder is the lowest level in the hierarchy that you can access through the graphical file browser.

Place all customized files in the correct sub-folder in the following folder:

- When accessed through the command line
`/data/portwise/administration-service/files/access-point/custom-files/wwwroot/wa/`
- When accessed through the SSL VPN Administrator file browser
`/opt/portwise/administration-service/files/access-point/custom-files/wwwroot/wa/`

Editing or Replacing Customization Files

You can customize style sheets, images, and template files. The following table provides more information about the correct folders and files to edit.

Table 9.1 Customization Options

What you Can Customize	How to do It	File Name
Application Portal labels and text	Edit the text. See Customizing Application Portal Text (page 73)	Multiple. Refer to the instructions for details.
Logon page text or buttons	Edit individual template files. See Customizing HTML Templates (page 76).	Multiple. Refer to the instructions for details.
Logon page background	Replace the current background image. See Customizing Application Portal Images (page 74).	background_img.gif
Logon page colors and fonts	Edit the style sheet for logon pages. See Customizing Application Portal Colors and Layout (page 75).	common.css
Application Portal logo	Replace the standard Stonesoft logo. See Customizing Application Portal Images (page 74).	logo_bg.gif
Application Portal resource icons	Replace the images used. See Customizing Application Portal Images (page 74).	[symbol_color].gif
Application Portal colors and fonts	Edit the Application Portal style sheet. See Customizing Application Portal Colors and Layout (page 75).	access_portal.css
Application Portal Online Help page colors and fonts	Edit the Application Portal Online Help page style sheet. See Customizing Application Portal Colors and Layout (page 75).	default.css
Application Portal Online Help page contents	Edit the Online Help HTML page. See Customizing Application Portal Colors and Layout (page 75).	access_portal_help.html
StoneGate Web authentication applet graphics	Replace the current skin. See Customizing Application Portal Images (page 74).	WebSkin.zip
StoneGate Web authentication applet text, layout, and behavior	Edit the parameters explained in Customizing the StoneGate Web Authentication Script (page 80).	Web.js

▼ To edit or replace a customization file

1. Log on to the StoneGate SSL VPN Administrator.
2. Click **Browse** in the top menu. The file browser opens.
3. Browse to the default file in you want to duplicate under the `/access-point/built-in-files/wwwroot/wa/` folder (see [Table 9.1](#)).
4. Download files in one of the following ways:
 - Through the right-click menu for the correct file link (browser-specific menu).
 - By selecting the checkboxes for the correct files and clicking **Download selected files as zip**.
5. Modify the downloaded default file(s) or create your custom file.
6. Browse to the folder under `/access-point/custom-files/wwwroot/wa/` where you want to store your customized files or enter a folder name and click **Create Dir** to create a new folder.
7. Click **Browse** and navigate to the folder on your computer where your customized files are located.
8. Select a custom file and click **Open**. The path to the selected file is displayed next to the Browse button.
9. Click **Upload** to place your image in the displayed folder.
10. Close the file browser window. To activate the changes, click **Publish** at the top of the page.

Log on to the Application Portal to ensure that the changes are displayed correctly. You may have to refresh the page to see the changes.

Customizing Application Portal Text

Prerequisites: [Finding the Root Folder for Customization Files](#)

When the Application Portal pages are shown to end-users, the text from these files is automatically included in the pages. To customize the text in the Application Portal pages, create and edit custom copies of the text files. The customized text is automatically included in the Application Portal pages.

▼ To customize Application Portal text

1. (Optional) Download the default files you want to customize as instructed in [Editing or Replacing Customization Files](#) (page 72).
2. Modify the text in relevant parts in the files described in the table below:

Table 9.2 Text Customization Options

File Name	Description
authAD.txt	The heading for the Active Directory Login page. Appears on every Active Directory Template. Note that the other authentication methods use their Display name and therefore do not need a branding text file.
authselect.txt	The heading for the Select Authentication Method page.

Table 9.2 Text Customization Options (Continued)

File Name	Description
authweb.txt	The name of the StoneGate Web authentication method. This is used in JavaScript dialogs that explain how to accept the StoneGate Web ActiveX or Java applet.
company.txt	The name of your organization. Appears in the application portal.
company_about_url.txt	The link to information about your organization.
company_contact_url.txt	The link to your organization's contact information.
copyright.txt	Copyright notice.
portal.txt	The name of the Application Portal. Appears on the Application Portal and on its help page.
product.txt	The name of the StoneGate SSL VPN product. Appears on the title of each page.
tunnel.txt	The name of the Access Client. This is used in JavaScript dialogs that explain how to accept the Access Client ActiveX or Java Applet loader.

3. Upload the modified files as instructed in [Editing or Replacing Customization Files](#) (page 72).

Customizing Application Portal Images

Prerequisites: [Finding the Root Folder for Customization Files](#)

You can replace or edit image files to customize the graphics used on logon pages, the application portal items, the main logo, and the StoneGate Web authentication applet.

▼ To customize Application Portal images

1. (Optional) Download the default files you want to customize as instructed in [Editing or Replacing Customization Files](#) (page 72).
2. Edit or replace the images as described in the table below:

Table 9.3 Images

Directory Location	File Name	Description
access-point/custom-files/ wwwroot/wa/img	background_img.gif	Background image for logon pages.
	logo_bg.gif	The StoneGate SSL VPN logo.
access-point/custom-files/ wwwroot/wa/img/icons	multiple files	Icons that you can select for resources (applications) in the Application Portal.

Table 9.3 Images (Continued)

Directory Location	File Name	Description
access-point/custom-files/ wwwroot/wa/authmech/base/ WebSkin.zip	mask.gif	Controls the position of buttons and labels in StoneGate Web authentication. This image must be in the GIF format (indexed palette) and it must have the same dimensions in pixels as the down.jpg and up.jpg images.
access-point/custom-files/ wwwroot/wa/authmech/base/ WebSkin.zip	down.jpg	StoneGate Web authentication skin without the background and with the buttons depicted as pressed. This image must have the same dimensions in pixels as the mask.gif and the up.jpg images.
access-point/custom-files/ wwwroot/wa/authmech/base/ WebSkin.zip	up.jpg	StoneGate Web authentication skin with the background and with buttons depicted as not pressed. This image must have the same dimensions in pixels as the mask.gif and the down.jpg images.

3. Upload the customized images as instructed in [Editing or Replacing Customization Files](#) (page 72).

Customizing Application Portal Colors and Layout

Prerequisites: [Finding the Root Folder for Customization Files](#)

You can customize style sheets to control colors and fonts in the Application Portal, on the associated logon pages, as well as in the Application Portal Online Help.

▼ To customize Application Portal colors and layouts

1. (Optional) Download the default files you want to customize as instructed in [Editing or Replacing Customization Files](#) (page 72).
2. Edit the style definitions in the style sheets listed below.

Table 9.4 Style Sheets

Directory Location	File Name	Description
/access-point/custom-files/ wwwroot/wa	access_portal.css	Controls colors, fonts, as well as location and size of different page objects (e.g. the logotype) in the Application Portal (_menu.html/wml and _welcome.html/wml).
	common.css	The color and font definitions for logon pages.
/access-point/custom-files/ wwwroot/wa/help	default.css	The color and font definitions for the Application Portal Online Help page.

3. Upload the modified files as instructed in [Editing or Replacing Customization Files](#) (page 72).

Customizing HTML Templates

Prerequisites: [Finding the Root Folder for Customization Files](#)

You can edit template files to customize details such as text and buttons on individual logon pages. Text on the Login pages are defined by Template Specifications, configured in StoneGate SSL VPN Administrator. However, the heading of each login page is defined by the display name that you give the Authentication Method.

The template files are available in two different formats: HTML and WML. HTML files are used for Web logon, WML files for WAP logon. Files used for Web authentication are HTML files with .html suffixes and files used for WAP authentication are WML files with .wml suffixes. The file names are the same, regardless of format

For descriptions of the user variables included in the files, see [Page Template Variables](#) (page 79).

▼ To customize HTML templates

1. (Optional) Download the default files you want to customize as instructed in [Editing or Replacing Customization Files](#) (page 72).
2. Edit the template files in the `~/wwwroot/wa/` directory as described in the table below:

Table 9.5 Template files in `~/wwwroot/wa/`

File Name	Description	Variables
<code>_auto_reauthmessage</code>	Page displayed when the user must log off and re-authentication is required.	
<code>_chooseAuthmech</code>	Page displayed when authentication method is to be selected.	name displayname
<code>_closedown_message</code>	Page displayed when user is timed out from the Access Point.	
<code>_deleteLogonCred</code>	Page displayed when password database has been cleared.	
<code>_error</code>	Error message displayed to the user.	errmsg
<code>_InternalAuthentication</code>	The Internal Authentication form.	ihost iuid idom
<code>_logoutPage</code>	Page displayed when user has logged off.	
<code>_menu</code>	The actual Application Portal page (called from <code>welcome.html</code>).	
<code>_no_session</code>	Page displayed when a session has timed out.	
<code>_popup_msg</code>	Page used to display a popup message to the user.	location errmsg
<code>_reauthmessage</code>	Time-out message displayed to user.	
<code>_refresh_top</code>	Page displayed when a user needs to refresh the browser.	
<code>_securitywarning</code>	Page displayed for security warnings.	errmsg

Table 9.5 Template files in ~/wwwroot/wa/ (Continued)

File Name	Description	Variables
_TimeoutPage	Page displayed when a user is temporarily locked until a specific time out occurs (currently concerns only SecurID).	auth_timeout
_webclient.html	Page displayed when clicking on a tunnel set in the access portal. Detects and loads the Access Client ActiveX if possible, otherwise loads the Java Applet.	
_webclientjavaobj.html	Holds an instance of the Access Client Java Applet.	
_webclientobj.html	Holds an instance of the Access Client ActiveX.	
_welcome	Page displayed subsequent to a successful logon.	
302	Page displayed to redirect the user when a page has moved.	location
302_top	Page displayed to redirect the user when a page has moved.	location
400	Page displayed subsequent to a bad request.	
401E	Page displayed subsequent to external authentication failure due to mismatching credentials if the authentication method on the device is set to Basic authentication.	authmech location
401I	Page displayed subsequent to an internal authentication failure due to mismatching credentials if the authentication method on the device is set to Basic authentication.	
401WIL	Displayed when a user fails to log on using Windows Integrated Login.	
403	Page displayed when a client requests a forbidden resource, that is, Access Control denies the resource to be accessed.	eprot ehost uri
404	Page displayed when a requested file on the Access Point does not exist.	eprot ehost file
405	Page displayed when a HTTP-method which is not allowed has been used in a client request.	eprot ehost uri method allow
500	Page displayed when a server error occurs.	errmsg
pocketclient	Starts the installation of the Access Client for Pocket PC.	
TestLogonLoginPage	Logon page for TestLogon, that is, when a user requests http://127.0.0.1:19146/wa/auth?authmech=TestLogon on the local computer where the Access Point is installed.	

3. Edit the template files in the `~/wwwroot/wa/authmech/base` directory as described in the table below:

Table 9.6 Template files in `~/wwwroot/wa/authmech/base`

File Name	Description	Variables
GenericForm.<file extension>	Base Template for logon forms used in conjunction with Template Specifications of type GenericForm. The template specifications form the appearance of the log page for the authentication method by supplying the content of the user variables.	heading errmsg explanation message authmech textText textName textValue readonlyText readonlyName readonlyValue passwordText passwordName checkboxText checkboxName checkboxValue
Dialog.<file extension>	Base template used in conjunction with template specifications of type Dialog.	heading errmsg explanation message authmech buttonText hiddenName hiddenValue
Applet.html	Base template used in conjunction with template specifications of type Applet. Only used by StoneGate SSL VPN Web.	heading errmsg explanation message authmech buttonText hiddenName hiddenValue username vendorBase64 arg1 arg2

4. Upload the modified files as instructed in [Editing or Replacing Customization Files](#) (page 72).

Page Template Variables

When an HTML/WML page is displayed to an end-user, the variables in the template file are dynamically populated with content as explained in the table below.

Table 9.7 Page Template Variables

Variable	Description
allow	Comma-separated list of allowed HTTP methods for the current host and URI.
auth_timeout	Number of seconds left of the period of time a user is locked from logging in (used in combination with SecurID logon).
authmech	The authentication method for an authenticated user.
authtimeout	Number of seconds remaining before an authenticated user is logged out. Used in the timeout warning page.
do	Used as a parameter for handling input data.
ehost	External host name, that is, the HTTP Host in the client request to the Access Point (for example mvpn.theseurecompany.com). General variable that can be used in all templates.
eprot	External protocol, that is, the protocol between the client and the Access Point: HTTP or HTTPS. General variable that can be used in all templates.
errmsg	Error message from the Access Point.
explanation	Explanatory text in Template Specification.
final_timeout	Number of minutes remaining before the configured maximum lifetime of the current session is reached and the session ends.
heading	Main heading text in Template Specification.
idom	The internal domain.
ihost	Internal host (alias) currently accessed by the user (not necessarily the same as the HTTP Host header in the Access Point request to the internal host).
input-heading	Heading text for an input field in Template Specification.
iprot	Internal protocol currently accessed by the user: HTTP or HTTPS.
iuid	Internal UserID (uid filtered through NameMapper.wascr). General variable that can be used in all templates.
iuri	Internal URI, in requested from Access Point to host.
location	A URI or a URL specifying where to redirect during logon.
maxSessionTimeout	Maximum time in minutes for a user session. The value is specified in the configuration.
message	Message from the Authentication Service.
method	HTTP method in a GET request.
ntdomain	NT domain name.

Table 9.7 Page Template Variables (Continued)

Variable	Description
pin	PIN for authentication.
protocol	An Access Client URL parameter for the protocol for the tunnel: EESSP or SSL.
reauth_uid	User ID used on RADIUS pages.
redirect	URL parameter for the Access Client.
replyMsg	RADIUS reply message.
servername	Logon challenge number from the Authentication Service.
title	Heading text.
tunnelCipherIv	The Base64 encoded cipher IV. Generated dynamically in the system.
tunnelCipherKey	The Base64 encoded cipher key. Generated dynamically in the system.
upd	The value of the UPD cookie used for session handling in a mirrored environment. Generated dynamically in the system.
uid	The UserID for an authenticated user. General variable that can be used in all templates.
uri	The URI that the client requested from the Access Point.
waak	The session handling method selected on the Advanced tab of the Global Access Point settings.
warningtimeout	Number of seconds remaining before a warning message or another logon page is displayed to the user.
wasid	The unique user session identifier. Generated dynamically in the system.

Customizing the StoneGate Web Authentication Script

Prerequisites: [Finding the Root Folder for Customization Files](#)

The StoneGate Web authentication applet can be customized by changing the values of parameters that are set in a configuration script. The values are all set in the JavaScript from values supplied by the server. A \\ value in a parameter indicates a newline character.



Note - Some of the optional parameters may not have any effect when used with the ActiveX version of the authentication applet.

▼ To customize the StoneGate Web authentication script

1. (Optional) Download the default files you want to customize from the `.../access-point/built-in-files/wwwroot/wa/authmech/base/Web.js` directory as instructed in [Editing or Replacing Customization Files](#) (page 72).

2. Edit the values of the required parameters for StoneGate Web authentication.

Table 9.8 Required Parameters for StoneGate Web Authentication

Parameter Name	Description
UserName	User ID of authenticating user.
Config	Configuration parameters.
Challenge	Challenge from the Authentication Service.
Modulus	Encryption Modulus.
PostURL	URL to which the result is posted.

3. (Optional) Edit the values of the optional parameters.

Table 9.9 Optional Parameters for StoneGate Web Authentication

Parameter Name	Usage	Default Value
ShowPress	If set to true, the buttons are rendered in a down state when pressed.	true
UseFrame	If set to true, the applet uses a free-floating frame.	true
FrameName	Name of frame to open redirect URL in.	
SkinFile	Name of the skin file.	WebSkin.zip
EchoChar	Character to echo when a character has been typed.	*
GuideChar	Character to echo to guide the user on how many characters should be entered.	-
AutoEnter	If set to true, an automatic enter is submitted when the maximum number of characters is reached.	false
ShadeMultiply	Multiplication factor used for shading disabled buttons.	0x50
FrameTitle	Used as the title for the free-floating applet.	StoneGate SSL VPN Web Authentication
DefaultText	Text displayed right after login.	Powered by PortWise
MustChange	The prompt that is displayed when the end-user must change passwords.	You must change password\\Enter new password
OldPwd	Field label for current password verification.	Enter current password
NewPwd	Field label for new password.	Enter new password
VerifyPwd	Field label for re-entering new password.	Verify new password

Table 9.9 Optional Parameters for StoneGate Web Authentication (Continued)

Parameter Name	Usage	Default Value
VerifyFailed	Message shown when the two new password fields do not match.	Verify failed. Try again
SyntaxError	Message shown when the password does not meet the configured password requirements.	Pwd must contain {0} letters \\and {1} numerals. Try again
Login	Message shown during login.	Login in progress...
Expired	Message shown when the client session has expired.	Expired
NoUseKeyboard	Popup message shown when users try to enter numerals through their physical keyboard.	Client configured not to \\accept numerals from \\keyboard

4. Upload the modified files to the `/access-point/custom-files/wwwroot/wa/authmech/base/Web.js` directory as instructed in [Editing or Replacing Customization Files](#) (page 72).

DAILY MANAGEMENT

In this section:

- Managing User Accounts - 85**
- Managing Authentication Methods - 107**
- Managing Authentication Services - 125**
- Defining Access Rules - 133**
- Standard Resource Configuration - 147**
- Web Resource Configuration - 157**
- Tunnel Resource Configuration - 171**
- Client Security - 185**
- Managing Single Sign-On and Identity Federation - 199**
- Monitoring in the SSL VPN Administrator - 211**

CHAPTER 10

MANAGING USER ACCOUNTS

This chapter describes the management of user accounts, user groups and Self Service.

The following sections are included:

- ▶ [Getting Started with Managing User Accounts](#) (page 86)
- ▶ [Managing Global User Account Settings](#) (page 86)
- ▶ [Managing User Accounts](#) (page 92)
- ▶ [Managing User Groups](#) (page 99)
- ▶ [Configuring Delegated Management](#) (page 102)
- ▶ [Managing Self Service](#) (page 103)

Getting Started with Managing User Accounts

In StoneGate SSL VPN, users and user accounts are separate. User accounts are required for access to registered resources, and the accounts are connected to actual users. However, not all users in your directory service need to have registered StoneGate SSL VPN user accounts. StoneGate SSL VPN user accounts are linked to user information already stored in your directory service. A user storage link establishes a connection to your local user information.

What Do I Need to Know Before I Begin?

Before adding user accounts, you must have configured an external Directory Service and an external user storage to work with SSL VPN as described in sections [Configuring a Directory Service](#) (page 54) and [Adding an External User Storage Location](#) (page 55).

Configuration Overview

1. Define global user account settings for creating new accounts with the Add User Account wizard or through User Linking. See [Managing Global User Account Settings](#) (page 86).
2. Add user and administrator accounts. See [Adding Users](#) (page 93).
3. Add user groups. See [Adding User Groups](#) (page 100).

Managing Global User Account Settings

Prerequisites: None

Global user account settings are used by default for new user accounts created with the Add User Account wizard or through User Linking. When a user account is created through User Import, these settings are used by default if nothing else has been specified in the import file.



Note – Changes made in settings for specific user accounts override the global default configuration.

▼ To manage global user account settings

1. Browse to **Manage Accounts and Storage**→**Global User Account Settings**.
2. Select one of the following tabs depending on which settings you want to configure:
 - **General Settings:** Includes default settings for user account validity, StoneGate authentication, and time-outs.
 - **User Linking:** Includes default settings for link repair methods, and for each applicable authentication method.
 - **Auto Repair:** Allows you to automatically repair user links when the users access the system.

What's Next?

- ▶ To define general user account settings, proceed to [General Settings](#) (page 87).
- ▶ To define settings for user linking, proceed to [User Linking Settings](#) (page 88).
- ▶ To enable/disable automatic user link repair, proceed to [Auto Repair Settings](#) (page 92).

General Settings

The following general settings can be configured globally for all user accounts:

Table 10.1 Default Account Settings

Setting	Description
Max Retries	Maximum number of invalid login attempts allowed (1-999) before the user account is locked for authentication. You can override the global setting for specific user accounts. When set to 0, the user account is never locked. This setting is used for both default account configuration and for StoneGate authentication. Set to 10 by default.
Account Expires In	<i>(Optional)</i> The number of days a user account is valid. This is used as default when a new user account is created. When set to 0, the user account never expires. Set to 0 by default.

The following default account setting for StoneGate authentication must be defined:

Table 10.2 Required Default Account Settings for StoneGate Authentication

Setting	Description
Max Retries	Maximum number of invalid login attempts allowed (1-999) before the user account is locked for StoneGate authentication. Set to 9 by default.

Optional default account settings for StoneGate authentication include:

Table 10.3 Optional Default Account Settings for StoneGate Authentication

Setting	Description
Use groups	<i>(Optional)</i> When selected, user group names are supported. If supported, a group name can be connected to a user when managing user accounts. This group information is sent to the RADIUS client. The RADIUS client can then be configured to use this attribute for authorization.
Use framed IP	<i>(Optional)</i> When a framed IP address has been configured, this IP address is sent to a network access point from the Authentication Service upon successful authentication. This information can be used in authorization decisions made by the access point.
Time Lock Time-Out	The length of time users are locked out from attempting to log on after the number of failed logon attempts specified in Time Lock Interval. Set to 120 by default.
Time Lock Interval	Number of consecutive incorrect logon attempts allowed before the user account is time-locked. Set to 3 by default.
Change Password/PIN Notification	Number of days (1-19) before users are asked to change password/PIN. Set to 7 by default.

Time-out settings are used as default values when a Web resource is created. To edit or specify any or all of these settings for a specific resource, go to the Web Resource Host Advanced Settings page.

You set the maximum user inactivity time before re-authentication is required, validity time for a session in the system, time since the user was last authenticated with required authentication method before re-authentication is required, and time before users are warned and prompted to re-authenticate.

Table 10.4 Time-Out Settings

Setting	Description
Max Inactivity Time	Maximum user inactivity time in minutes (0-1440) before re-authentication is required. Set to 15 by default.
Session Time-out	Validity time in minutes (0-1440) for a session in the system. Set to 30 by default.
Absolute Time-out	Time in minutes (0-1440) since the user was last authenticated with required authentication method, before re-authentication is required, independent of user activity. Set to 720 by default.
Time-out Warning	Time in seconds (0-3600) before user is warned and prompted to re-authenticate. Set to 60 by default.
Active Users Time-out	Time in minutes (0-1440) allowed for the user to re-authenticate after a re-authentication prompt is triggered. Set to 15 by default.

User Linking Settings

User linking can be performed manually or automatically. These default settings apply to both methods of user linking. Default global settings are configured for user linking for each StoneGate authentication method. These default settings include:

Table 10.5 Global Settings for User Linking

Setting	Description
Enable authentication method after user linking	Defines whether an authentication method is enabled after user linking.

Table 10.5 Global Settings for User Linking (Continued)

Setting	Description
Generate password/ PIN	<p>When selected, the password/PIN is created automatically when user linking is used.</p> <p>Password/PIN can be retrieved automatically if a user storage attribute has been specified on the Directory Mapping tab in the Manage User Storage section.</p> <p>Select Generate Password for an automatically created password. When selected, directory mapping is not performed.</p>
Password/PIN never expires	<p>When selected, the password/PIN does not expire when user linking is used</p>
User cannot change password/PIN	<p>When selected, users cannot change the password/PIN when user linking is used</p>
User must change password/PIN at next logon	<p>When selected, users are required to change password/PIN at next logon when user linking is used</p>
Use password from directory service	<p>When selected, the password used in the applicable directory service is used for authentication when user linking is used</p> <p>This option is only available for the following authentication methods: StoneGate Mobile Text and StoneGate Password.</p>

The general settings for user linking allow you to define when StoneGate authentication is enabled for user linking, and to select the notification method.

Table 10.6 StoneGate Authentication Settings for User Linking

Setting	Description
Enable Stonegate Authentication When Manually Linking the User	<p>Select to enable StoneGate Authentication when manually linking the user.</p>
Enable Stonegate Authentication When Automatically Linking the User	<p>Select to enable StoneGate Authentication when automatically linking the user.</p>
Notification	<p>When StoneGate authentication is enabled for automatic user linking, you are also required to select notification method. Available options are: By E-mail and By SMS.</p>

Enabling StoneGate authentication for manual or automatic user linking makes the list of authentication methods visible. Optional settings for each authentication method are displayed when the authentication method is enabled. The following settings are available:

Table 10.7 Optional Settings for StoneGate Mobile Text

Setting	Description
Enable StoneGate Mobile Text	Defines whether Mobile Text authentication is enabled after user linking.
Generate password	Defines whether a password is automatically created for the user.
Password never expires	When selected, the password is always valid.
User cannot change password	Defines whether the user can change the password.
User must change password on next logon	When selected, the user must change the password at the next logon.
Use password from directory service	Defines whether the password from the directory service is used.

Table 10.8 Optional Settings for StoneGate Web

Setting	Description
Enable StoneGate Web	Defines whether Web authentication is enabled after user linking.
Generate password	Defines whether a password is automatically created for the user.
Password never expires	When selected, the password is always valid.
User cannot change password	Defines whether the user can change the password.
User must change password on next logon	When selected, the user must change the password at the next logon.

Table 10.9 Optional Settings for StoneGate Challenge

Setting	Description
Enable StoneGate Challenge	Defines whether Challenge authentication is enabled after user linking.

Table 10.9 Optional Settings for StoneGate Challenge (Continued)

Setting	Description
Generate PIN	Defines whether a PIN is automatically created for the user.
PIN never expires	When selected, the PIN is always valid.
User cannot change PIN	Defines whether the user can change the PIN.
User must change PIN on next logon	When selected, the user must change the PIN at the next logon.
Generate seed	Not editable.

Table 10.10 Optional Settings for StoneGate Password

Setting	Description
Enable StoneGate Password	Defines whether Password authentication is enabled after user linking.
Generate password	Defines whether a password is automatically created for the user.
Password never expires	When selected, the password is always valid.
User cannot change password	Defines whether the user can change the password.
User must change password on next logon	When selected, the user must change the password at the next logon.
Use password from directory service	Defines whether the password from the directory service is used.

Table 10.11 Optional Settings for StoneGate Synchronized

Setting	Description
Enable StoneGate Synchronized	Defines whether Synchronized authentication is enabled after user linking.
Generate PIN	Defines whether a PIN is automatically created for the user.
PIN never expires	When selected, the PIN is always valid.
User cannot change PIN	Defines whether the user can change the PIN.

Table 10.11 Optional Settings for StoneGate Synchronized (Continued)

Setting	Description
User must change PIN on next logon	When selected, the user must change the PIN at the next logon.
Generate seed	Not editable.

Auto Repair Settings

Auto Repair automatically updates user links when users with invalid directory links try to access the system,

Table 10.12 Auto Repair Users

Setting	Description
Auto repair user links when the users access the system	Defines whether the directory link is automatically updated if the system detects that the directory link is not the same one as saved on the user account when the user tries to access the system.

Managing User Storage Locations

User storage is the location where users are stored and used by the Policy Service as part of the authorization process. An internal user storage is included on the appliance by default for testing purposes, but you must configure an external user storage for the SSL VPN before bringing it to production use, as described in [Adding an External User Storage Location](#) (page 55).

What's Next?

- ▶ To add user accounts, proceed to [Adding Users](#) (page 93).
- ▶ To add user accounts by linking, proceed to [Linking Users](#) (page 94).
- ▶ To add user accounts by importing, proceed to [Creating a File for Importing Users](#) (page 96).

Managing User Accounts

Prerequisites: [Managing User Storage Locations](#)

Creating User Accounts

There are three different ways to create user accounts in StoneGate SSL VPN:

- Adding User Accounts
- Linking Users
- Importing Users

User import and user linking are both alternatives to using the Add User Account wizard to create user accounts. To create a number of user accounts simultaneously, with a minimum of manual intervention, you can import a file containing user information.

User Linking is used when you quickly want to create a basic user account based on an existing user in user storage. You add user accounts according to your default settings in Global User Account Settings with links to the appropriate user storage.

Not all users in your directory service need to have registered StoneGate SSL VPN user accounts. StoneGate SSL VPN user accounts are linked to user information already stored in your Directory Service. A user storage link establishes a connection to your local user information.

Adding Users

We recommend enabling the default authentication methods on the Global User Account Settings page as described in [User Linking Settings](#). If no default authentication methods are enabled, you must enable authentication methods separately for each user account.

▼ To add a user account

1. Browse to **Manage Accounts and Storage**→**User Accounts**. The **Manage User Accounts** page opens.
2. Click **Add User Account**. The Add User Account page opens.
3. Add the general user information in one of the following ways:
 - Enter the **User ID** and click **Link User** to automatically retrieve user information stored in your Directory Service.
 - Enter the **User ID** and **Display Name** to manually add user information.
4. Click **Next**.
5. Select one or more of the StoneGate Authentication methods.
6. Enter any contact information that was not retrieved automatically in step 3. Click **Next**.
7. Enter and verify the password/PIN for each of the selected authentication methods.
 - By default, the password must be between 6 and 16 characters long, with at least 2 numerals.
 - By default, the PIN must be 6 digits.
8. Define the Password Properties for each authentication method:

Setting	Description
Generate password	A password is automatically created for the user.
Password never expires	The password is always valid.
User cannot change password	Prevents the user from changing the password.
User must change password on next logon	Requires the user to change the password at the next logon.

9. Select the **Notification** method for sending the new password/PIN to the user.
10. Select the authentication notification **Message Set** that is shown to the user.
11. Click **Finish Wizard**. The user account is added and the user can access the Application Portal.

Linking Users

User Linking allows you to quickly create a basic user account based on an existing user in the user storage.

Users can be linked automatically or manually. With automatic linking, user accounts are created automatically when users who are located in the user storage, but do not have corresponding user accounts in StoneGate SSL VPN, attempt to log in to the system.

Linking Users Automatically

Automatic user linking is enabled on the User Linking tab in Manage Global User Account Settings. All default settings for user accounts created through import or linking are retrieved from the Global User Account Settings section.

When a user tries to access a resource using StoneGate authentication and no matching user account exists, a StoneGate SSL VPN user account is automatically created and the user information is linked from the user storage location to the new user account. When other authentication methods are used, the user must exist in the user storage in order for a user account to be created.

▼ To link users automatically

1. Browse to **Manage Accounts and Storage**→**Global User Account Settings**. The Manage Global User Account Settings page opens.
2. Switch to the **User Linking** tab.
3. Select **Enable StoneGate Authentication When Automatically Linking the User**.
4. Select the **Notification** method for sending the new password/PIN/seed to the user.
5. Select the authentication methods that are enabled when the new user is linked. For detailed information, see [User Linking Settings](#) (page 88).
6. Select the password/PIN properties for each authentication method.
7. Click **Save**.

Linking Users Manually

▼ To link users manually

1. Browse to **Manage Accounts and Storage**→**User Linking**. The Manage User Linking page opens.
2. Enter the **User ID** to link.
3. Select the **Notification** method for sending the new password/PIN/seed to the user.
4. Select the authentication **Message Set** for the user.
5. Click **Link User**.
6. Select the presentation format for new password/PIN/seed messages.
7. Click **Next**. The user is linked to a user account.
8. Click **Save**.

Repairing User Links

If users are moved or deleted from the user storage location, established links between StoneGate SSL VPN user accounts and the directory service are broken. When this occurs, these users cannot authenticate.

To repair broken links, missing users are searched from the user storage location. When missing users are found, the links are re-established.

Link repair can be performed using two methods:

- Use the User Link Repair wizard to check directory links, and repair or delete user accounts with broken links.
- Use the default global setting Auto Repair to repair user links automatically when users access the system.

Repairing User Links Manually

▼ To repair user links manually

1. Browse to **Manage Accounts and Storage**→**User Link Repair**.
2. Click **User Link Repair**. The User Link Repair wizard starts.
3. Select one of the following link repair options:

Option	Description
Update user's directory link and repair all remaining users automatically	The system checks any remaining links to the user storage and tries to repair them. If the user has been moved or modified, the user storage location and directory link information are updated.
Update user's directory link and check next user	Updates the user storage location and directory link information, and continues checking links one by one.
Remove user account and check next user	Removes the selected user account and continues checking links one by one.
Remove user account and remove all remaining users with broken links	Removes the selected user account and any remaining links to the user storage.
Skip repairing the user's directory link and check next user	Ignores the selected user account and continues checking links one by one.

When all broken user links have been repaired, a summary is displayed.

4. Click **Save**.

Enabling Automatic User Link Repair

▼ To enable automatic user link repair

1. Browse to **Manage Accounts and Storage**→**Global User Account Settings**.
2. Switch to the **Auto Repair** tab. The Auto Repair Users page opens.
3. Select **Auto Repair User Links When the Users Access the System**.

4. Click **Save**.

Creating a File for Importing Users

You can create multiple user accounts simultaneously by importing a file containing user information separated by commas, semi-colons, or tabs.



Note – Authentication methods enabled on the User Linking tab in Manage Global User Account Settings and their corresponding settings are not retrieved when creating user accounts through user import.

The file used for import must be formatted according to the following formatting rules:

- The first row in the import file must contain the column headings that specify the fields in the import file.
- The headings cannot contain any spaces
- The headings are not case-sensitive.
- Each row must contain data for only one user.
- Empty rows and rows beginning with a comment sign (#) are ignored during import.

The formatting rules are applied to the following import file items:

Table 10.13 Import File Items

Item	Description	Comment
Heading	Description	
String	A string containing any character	
Integer	Non-negative numeral	
Boolean	True or false	
Password	Password in clear text or {SHA}+ [base64-encoded SHA hashed password]	Make sure the date format in the file matches your browser settings
Date	Date format complies to your browser's language settings	

The content of each entry in the import file is the following:

Table 10.14 Import File Contents

Heading	Value	Comment
UID	String	Mandatory
RealName	String	Mandatory
Comments		Comments for your reference. This column is ignored during import.
DirectoryLink	String	

Table 10.14 Import File Contents (Continued)

Heading	Value	Comment
UserStorage	String	
GroupName	String	
FramedIP	String	
MailAddress	String	
MobileNumber	String	
AccountDisabled	Boolean	
AccountValidFrom	Date	
AccountExpires	Date	
AccountNeverExpires	Boolean	
AccessMaxRetries	Integer	
AuthenticationMaxRetries	Integer	
ChallengeEnabled	Boolean	
ChallengePIN	Password	
ChallengePINNeverExpires	Boolean	
ChallengePINCannotChange	Boolean	
ChallengePINMustChange	Boolean	
ChallengePINGenerate	Boolean	
ChallengeSeed	String	
ChallengeSeedGenerate	Boolean	
SynchronizedEnabled	Boolean	
SynchronizedPIN	Password	
SynchronizedPINNeverExpires	Boolean	
SynchronizedPINCannotChange	Boolean	
SynchronizedPINMustChange	Boolean	
SynchronizedPINGenerate	Boolean	
SynchronizedSeed	String	
SynchronizedSeedGenerate	Boolean	
WebEnabled	Boolean	
WebPwd	Password	

Table 10.14 Import File Contents (Continued)

Heading	Value	Comment
WebPwdNeverExpires	Boolean	
WebPwdCannotChange	Boolean	
WebPwdMustChange	Boolean	
WebPwdGenerate	Boolean	
PasswordEnabled	Boolean	
PasswordPwd	Password	
PasswordPwdNeverExpires	Boolean	
PasswordPwdCannotChange	Boolean	
PasswordPwdMustChange	Boolean	
PasswordPwdGenerate	Boolean	
PasswordPwdUseDirectory	Boolean	
MobileTextEnabled	Boolean	
MobileTextPwd	Password	
MobileTextPwdNeverExpires	Boolean	
MobileTextPwdCannotChange	Boolean	
MobileTextPwdMustChange	Boolean	
MobileTextPwdGenerate	Boolean	
MobileTextPwdUseDirectory	Boolean	
NotifyByMail	Boolean	
NotifyBySMS	Boolean	
NotifyToAddress	E-mail address	

Importing Users

▼ To import users in a file

1. Format the file of users to be imported as instructed in [Creating a File for Importing Users](#) (page 96).
2. Browse to **Manage Accounts and Storage**→**User Import**. The Manage User Import page opens.
3. Select the **Separator in File** according to which separator is used.
4. **Browse** for the users file to be imported.
5. Click **Import Users**.

6. Click **Save**.

Modifying Users

▼ To modify user information

1. Browse to **Manage Accounts and Storage**→**User Accounts**. The Manage User Accounts page is displayed.
2. Enter the search criteria in the **User ID** field and click **Search**. The system displays a list of all the users that match the search criteria.
3. In the Search Result list, click the User ID of the user whose information you want to modify.
4. Update the user account information and click **Save**.

Deleting Users

▼ To delete a user

1. Browse to **Manage Accounts and Storage**→**User Accounts**. The Manage User Accounts page is displayed.
2. Enter the search criteria in the **User ID** field and click **Search**. The system displays a list of all the users that match the search criteria.
3. In the Search Result list, click the User ID of the user you want to delete.
4. Click **Delete** at the bottom of the page. You are prompted to confirm the deletion of the user account.
5. Click **Yes** to delete the user account.

Managing User Groups

Prerequisites: [Adding Users](#)

User groups categorize users. This categorization controls what a user can access, or what actions the users must perform to enable certain access rights. There are three types of user groups: User Location Groups, User Property Groups, and User Groups in Directory Service.

User Location Groups

User location groups contain all users stored under a specific node in the User Storage structure. This type must be used when the users are stored in a location with structural significance. [Adding a User Location Group](#) (page 100)

User Property Groups

User property groups contain user accounts with special properties. Use this type of group when users have common properties that can be used for categorization, such as job function. These properties are managed as attributes. Each attribute contains a source, name, and value, and together they constitute a property.

The attribute source values for User Property Groups are:

- User storage location
- Custom-defined (user attributes specified on the General Settings page of User Accounts)
- RADIUS sessions

- SAML sessions

See [Adding a User Property Group](#) (page 100).

User Groups in Directory Service

Directory Service groups contain all users that belong to a certain user group defined in your user storage. Use this type to integrate existing local user groups.



Note – This type of user group cannot be added or modified.

Adding User Groups

Adding a User Location Group

▼ To add a user location group

1. Browse to **Manage Accounts and Storage**→**User Groups**. The Manage User Groups page opens.
2. Click **Add User Group**. The Add User Group page opens.
3. Select **User Location Group**.
4. Click **Next**.
5. Select the user storage location to connect the user group to and click **Next**.
6. Enter a unique **Display Name** that identifies the user group in the system.
7. Click **Show Tree** and browse to the branch where the users in this group are stored. Click **OK**.
8. Click **Finish Wizard**. The User Group is created. To activate the changes, click **Publish** at the top of the page.

Adding a User Property Group

▼ To add a user property group

1. Browse to **Manage Accounts and Storage**→**User Groups**. The Manage User Groups page opens.
2. Click **Add User Group**. The Add User Group page opens.
3. Select **User Property Group**.
4. Click **Next**.
5. Configure the User Group with the following properties:

Property	Description
Display Name	Unique name used in the system to identify the user. For example, <i>Users</i> .
Description	<i>(Optional)</i> A description for your own reference. For example, <i>Group for all standard users</i> .
Attribute Source	Defines whether the attribute source is a user storage location, a custom-defined attribute, or an attribute included in the RADIUS session.

Property	Description
Attribute Name	Defines the attribute name defined in the LDAP schema (for example, <i>groupID</i>).
Attribute Value	Defines the user attribute value. All users of this group must have the same attribute value.

6. Click **Finish Wizard**. The User Group is created. To activate the changes, click **Publish** at the top of the page.

Searching User Groups

▼ To search for a User Group

1. Browse to **Manage Accounts and Storage**→**User Groups**. The **Manage User Groups** page opens.
2. Enter the user group **Display Name**, select the **User Group Type**.
3. Click **Search**. The system displays a list of all the user groups that match the search criteria.

Editing User Groups

▼ To edit a User Group

1. Browse to **Manage Accounts and Storage**→**User Groups**. The **Manage User Groups** page opens.
2. Enter the user group **Display Name**. The user group properties are shown.
3. Change the properties of the user group as needed and click **OK**. To activate the changes, click **Publish** at the top of the page.

Deleting User Groups

▼ To delete a User Group

1. Browse to **Manage Accounts and Storage**→**User Groups**. The **Manage User Groups** page opens.
2. Click **User Groups**. The **Manage User Groups** page opens.
3. Search for the user group to delete and select **Delete User Group**. You are prompted to confirm the deletion of the user account.
4. Click **OK** to delete the user group. To activate the changes, click **Publish** at the top of the page.

Getting Started with Delegated Management

Delegated Management enables you to create different administrative roles with different privileges and responsibilities. Each role can be assigned to one or several users stored in the registered user storage location.



Note – The roles **Help Desk** and **Super Administrator** are predefined roles. They cannot be deleted.

Roles are used as alert receivers in [Configuring Alert Notifications](#) (page 218). Selected roles receive notification messages about selected alert events. If you plan to use the new role for alerts, you must ensure that e-mail addresses and/or cell phone numbers are entered in the user properties for the selected users.

Configuring Delegated Management

▼ To configure Delegated Management

1. Browse to **Manage System**→**Delegated Management**. The Delegated Management page opens.
2. Click **Add Role**. The Add Role page opens.
3. Enter a unique **Display Name** that identifies the role in the system.
4. Select the privileges for the role:

Privilege	Description
Help desk administration	Entitles the role to add, edit, and delete all settings saved for a user account.
User account management	Entitles the role access to all functionality available in the Manage Accounts and Storage section.
Resource management	Entitles the role to add, edit, and delete both resource hosts and resource paths.
Resource path management	Entitles the role to add, edit, and delete resource paths for selected resource hosts.
View logs	Entitles the role to view logs for all servers using the Log Viewer.
Publish	Entitles the role to publish updated configurations.

5. Click **Next**.
6. Select the **User Group** that the role manages. Click **Next**.
7. Select the resources that the role manages from Available Resources, and click **Add**.
8. Click **Next**.
9. Enter the **User ID** of the administrators to whom this role is assigned.
10. Click **Finish Wizard**.

Managing Self Service

Prerequisites: None

Self Service delegates part of the user maintenance to the end-users. End-users can automatically activate their user account, request a forgotten password, or request a forgotten user ID.

To manage self service settings in a secure way, the system requests a number of control answers from the end-user to verify the end-user's identity. The control questions are referred to as Challenges. Challenges are divided into three categories:

Table 10.15 Challenge Categories

Category	Description
Internal challenges	Defined by the system. Internal challenges cannot be changed.
System challenges	Defined by the Administrator. Control questions based on the information stored in an attribute in the user storage.
User challenges	Control questions defined by the end-user.

Task-specific Self Service Challenges

Auto Activate Challenges

The Auto Activate task has the following challenges defined by default:

- System e-mail
- System control challenge

The Challenges are issued in the following order:

1. The end-user is prompted to enter the e-mail address registered for their account in the User Storage.
2. The end-user is challenged with the defined system control challenge, for example, the end-user's ID number.

If a user can be found in the system using the e-mail address and with the corresponding answer to the system control challenge, the Auto Activation sequence is initiated.

Request Forgotten Password Challenges

The Request Forgotten Password task has the following challenges defined by default:

- User Name
- System control challenge
- User challenge
- System e-mail

The Challenges are issued in the following order:

1. The end-user is prompted to enter the User Name as defined in the Auto Activate process.
2. The end-user is challenged with the defined system control challenge, for example, the end-user's ID number.
3. The end-user is prompted to answer the user challenge control question defined in the Auto Activation process.
4. The end-user is prompted to enter the e-mail address defined in the system.

As a control mechanism, the administrator can select to send a message using an alternative channel when a new password has been requested and generated. For example, if the user selects to receive the password by e-mail, a message is sent by SMS. The administrator can also select what message is delivered.

Table 10.16 Forgotten Password Settings

Setting	Description
Send message to secondary channel when Password has been issued	Defines whether the secondary channel is used to send a requested password
Message to secondary channel	Message text for the secondary channel.

If a user can be found in the system using the User Name and the corresponding answers to the system control challenge, the user defined challenge, and the system e-mail, the Request Forgotten Password sequence is initiated.

Request Forgotten User Name Challenges

The Request Forgotten User Name task has the following challenges defined by default:

- User Name
- System control challenge
- User Challenge
- System e-mail

The Challenges are issued in the following order:

1. The end-user is prompted to enter the User Name as defined in the Auto Activate process.
2. The end-user is challenged with the defined system control challenge, for example, the end-user's ID number.
3. The end-user is prompted to answer the user challenge control question defined in the Auto Activation process.
4. The end-user is prompted to enter the e-mail address as defined in the system.

As a control mechanism, the administrator can select to send a message using an alternative channel when a forgotten user name has been requested and generated. For example, if the user selects to receive the user name by e-mail, a message is sent by SMS. The administrator can also select what message is delivered.

Table 10.17 Forgotten User Name Settings

Setting	Description
Forgotten User Name Message	Message text for Forgotten User Name. Use the tag {0} for inserting the user name.

If a user can be found in the system using the User Name and the corresponding answers to the system control challenge, the user challenge, and the system e-mail, the Request Forgotten User Name sequence is initiated.

Activating Self Service

▼ To activate Self Service

1. Browse to **Manage Accounts and Storage**→**Self Service**. The Manage Self Service page opens.
2. Select one of the following options:
 - **Yes - help me with the settings:** The system automatically configures default settings that work for the most common setups.
 - **No - I will do the configuration myself:** The system automatically configures the basic settings and leaves the rest of the configuration to be done manually.

What's Next?

- ▶ If you selected Yes - help me with the settings, the most common settings are configured and the configuration of Self Service is complete.
- ▶ If you selected No - I will do the configuration myself, proceed to [Managing System Challenges](#) (page 105).

Managing System Challenges

The Manage System Challenges page shows all pre-configured System Challenges that are defined automatically. The challenges marked with the **Update this** label must be modified before the configuration is complete.

▼ To manage Self Service challenges

1. Browse to **Manage Accounts and Storage**→**Self Service**. The Manage Self Service page opens.
2. Click **Modify System Challenges**. The Manage System Challenges page opens.
3. Click **Add System Challenge** to add a new challenge, or click a system challenge name under Registered System Challenges to modify it.

4. Select one of the challenges by clicking the link. The Edit System Challenge page opens. There are three settings on the page:
 - **Display Name:** Name of the challenge.
 - **Challenge Question:** The question to be presented to the user.
 - **Attribute Name:** The name of the User Storage attribute that holds the challenge information (for example, birthdate or cn).

Always remove the Update This label once you have edited the challenge. This provides a visual cue that the challenge has been updated.



Note – For internal challenges and User Challenge, the Attribute Name cannot be changed.

Adding Challenges to Self Service Tasks

When you have finished updating the challenges, you must add these challenges to the self service tasks.

▼ To add challenges to self service tasks

1. Browse to **Manage Accounts and Storage**→**Self Service**. The Manage Self Service Settings page opens.
2. Select one of the following options according to the challenge you are adding:
 - **Add Auto Activate Challenge**
 - **Add Forgotten Password Challenge**
 - **Add Forgotten User Name Challenge**

The Select Challenge for this Configuration page opens.

3. Select the **System Challenge** and click **Add this Challenge**. Repeat these steps to add any additional challenges.
4. Click **Previous** to return to the Manage Self Service Settings page.

Tip – You can change the order of the challenges in each section using the **Up and **Down** links, or use the **Remove** link to remove an unwanted challenge.**

5. Click **Save**. To activate the changes, click **Publish** at the top of the page.

What's Next?

- ▶ To complete the Self Service configuration, enable the authentication methods as instructed in [Enabling Authentication Methods for Self Service](#) (page 116).

CHAPTER 11

MANAGING AUTHENTICATION METHODS

This chapter describes the creation and management of Authentication Methods.

The following sections are included:

- ▶ [Getting Started with Authentication Methods](#) (page 108)
- ▶ [StoneGate Authentication Methods](#) (page 108)
- ▶ [Additional Authentication Methods](#) (page 111)
- ▶ [Managing Authentication Methods](#) (page 112)
- ▶ [Managing RADIUS Configuration](#) (page 117)
- ▶ [Managing OATH Configuration](#) (page 118)
- ▶ [Managing Certificates](#) (page 122)

Getting Started with Authentication Methods

Authentication methods are techniques used for verifying the identity of the connecting user before proceeding with the authorization process.

What Authentication Methods do

Authentication methods are used as requirements in access rules. An access rule can combine several authentication methods and other requirements.

What Do I Need to Know Before I Begin?

Different authentication methods provide various levels of security. Which authentication method to choose depends on your users' needs. Consider the importance of mobility, device flexibility, and level of security. Refer to each authentication method for more detailed information

Configuration Overview

1. Add an Authentication Method. See [Managing Authentication Methods](#) (page 112).
2. Add an Authentication Method Server. See [Managing Authentication Methods](#) (page 112).

Authentication Methods

SSL VPN supports a wide range of authentication methods and includes several proprietary methods.

StoneGate Authentication Methods

The StoneGate authentication methods are Password, Web, Synchronized, OATH, Challenge, and Mobile Text.

When using the StoneGate Synchronized or Challenge methods, users install the StoneGate Mobile ID client application on the device being used for authentication. Supported environments are Linux, Windows, Windows Mobile, MacOS, Android smartphones, Java smartphones, RIM Blackberry phones, Apple iPhone, and Symbian phones. When using the Web authentication method, the installed client is either an ActiveX component or a Java applet running in a web browser.

The StoneGate authentication methods are all based on the RADIUS protocol. [Table 11.1](#) provides details about the RADIUS activity when using the StoneGate authentication methods.

Table 11.1 StoneGate Authentication RADIUS Activity

Authentication Method	Device Type	RADIUS Client Activity	RADIUS Server Activity
StoneGate Mobile Text	PC PDA Mobile Phone	User ID + Password	Challenge: One-Time Password (OTP) by SMS
		User ID + OTP	Accept or Reject
StoneGate Password	PC	User ID + Password	Accept or Reject

Table 11.1 StoneGate Authentication RADIUS Activity (Continued)

Authentication Method	Device Type	RADIUS Client Activity	RADIUS Server Activity
StoneGate Challenge	PC	User ID	Challenge
	PDA Mobile Phone	User ID + OTP (OTP: Seed+PIN+Challenge)	Accept or Reject
StoneGate Synchronized	PC PDA Mobile Phone	User ID + OTP (OTP synchronized between client and server)	Accept or Reject
StoneGate OATH	PC PDA Mobile Phone	User ID + OTP (OTP synchronized between client and server)	Accept, Reject, or resynchronize
StoneGate Web	PC	User ID	RADIUS package: Configuration Encryption Key Challenge
		Password RADIUS package	Accept or Reject

About StoneGate Mobile Text

The StoneGate Mobile Text authentication method is based on a combination of a PIN and one-time password (OTP) distributed by SMS. The user enters the PIN on the logon page, and an OTP is generated and distributed to the user’s mobile phone.

The StoneGate Mobile Text authentication method can be used on mobile devices, such as a handheld PC or a mobile phone, as well as on a desktop computer.

Mobile Text supports the following distribution protocols/channels:

- SMTP
- CIMD
- SMPP
- HTTP

You can configure a primary and secondary channel. We recommend configuring the secondary SMS channel to be used if the primary fails.

All authentication and notification messages are sent by mobile text to the mobile phone number or e-mail address specified for the user account on the StoneGate Authentication Settings page of the User Account properties.

When **Allow Two-step Authentication** is selected, the authentication is distributed over two sessions. In the first session, the server sends the OTP to the mobile phone. In the second session, the user logs on with the OTP.

About StoneGate Web

When using the StoneGate Web authentication method, users enter their user ID, and a Java applet or ActiveX component is launched, prompting the users to enter a password or PIN. The password or PIN is then hashed and encrypted before it is returned to the server.

When a new StoneGate user account is registered and the StoneGate Web authentication method is enabled, the password or PIN is created and distributed to the user.



Note – StoneGate Web authentication method can be used only with the Access Point.

StoneGate Web can be used for authentication on a laptop or desktop computer.

About StoneGate Challenge

The StoneGate Challenge authentication method can be used for authentication in a Web browser, WAP client, or with a PDA. Users enter their user ID, and are prompted with a challenge to provide the correct response to be allowed access.

The StoneGate Mobile ID client software generates the response. Users enter their PIN in the Mobile ID client, and the one-time password (OTP) is created. Mobile ID clients can be installed on mobile devices, such as a handheld PC or a mobile phone, as well as on a laptop or desktop computer.

About StoneGate Password

The StoneGate Password authentication method is based on static password authentication. A static password is created and maintained for authenticating remote access with a RADIUS client.

About StoneGate Synchronized

The StoneGate Synchronized authentication method can be used for authentication in a Web browser, WAP client, or with a PDA. Users enter their user ID and are prompted to enter a one-time password (OTP) to be allowed access.

The StoneGate Mobile ID client software generates the OTP. Users enter their PIN in the Mobile ID client and the OTP is created. Mobile ID clients can be installed on mobile devices, such as a handheld PC or a mobile phone, as well as on a laptop or desktop computer.

About StoneGate OATH

The StoneGate OATH authentication method can be used for authentication in a Web browser, WAP client, or with a PDA. Users enter their user ID and are prompted to enter a one-time password (OTP) to be allowed access.

In StoneGate OATH, a hardware token generates the OTP. How the OTP is achieved is vendor-dependant. See the documentation from your OATH token vendor for detailed information.

Additional Authentication Methods

StoneGate SSL VPN supports the following additional authentication methods:

Table 11.2 Additional Authentication Methods

Authentication Method	Description
SafeWord	This authentication method supports Secure Computing SafeWord hardware tokens that generate an OTP.
SecurID	This authentication method supports RSA SecurID tokens that generate an OTP.
LDAP	This authentication method performs normal LDAP bind.
Active Directory	The Active Directory authentication method is an LDAP bind authentication method with the option to allow the user to change the password. This functionality is only supported with Microsoft Active Directory (AD) servers. The directory service must be configured for SSL communication.
IBM Tivoli and IBM RACF	These authentication methods are LDAP bind authentication methods with the option to allow the user to change password.
Novell eDirectory	The Novell eDirectory authentication method is an LDAP bind authentication method with the option to allow the user to change password.
Confidence Online	This authentication method supports Confidence Online clients.
User Certificate	The User Certificate authentication method is based on user/certificate attribute mapping. The user is authenticated only if there is an exact, unique match between the configured certificate attribute and the user attribute.
NTLM	The NTLM authentication method is used in various Microsoft network protocol implementations.
Basic	This authentication method performs a basic authentication according to RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication".
General RADIUS	The general RADIUS authentication method can be used with any RADIUS-compliant authentication server.
Extended User Bind	The Extended User Bind authentication method adds an extended form of user data retrieval, parsing, and matching with user-presented certificates and the LDAP user object.
Form-Based Authentication	
Windows Integrated Login	Windows Integrated Login authentication enables the use of Windows domain credentials for authentication. User credentials are retrieved from the client, and do not have to be entered by the user.
E-ID	A consortium of Scandinavian banks has agreed on a standard service for electronic authorization and signing over the Internet. The E-ID software is Java-based, and no client installations are required.

Table 11.2 Additional Authentication Methods (Continued)

Authentication Method	Description
E-ID Signer	Using E-ID, the client can authorize an order or a document by signing.

Managing Authentication Methods

Prerequisites: None

Adding Authentication Methods

You add authentication methods using the Add Authentication Method wizard. Each step of the wizard is represented by a tab when editing a specific authentication method.

The steps and tabs are:

- General settings
- RADIUS replies (*displayed only if the authentication method is RADIUS-based*)
- Extended properties

▼ To add an Authentication Method

1. Browse to **Manage System**→**Authentication Methods**. The Manage Authentication Methods page opens.
2. Click **Add Authentication Method**. The Add Authentication Method wizard starts.
3. Select the authentication method to be added and click **Next**.
4. (*Optional*) To make prevent the authentication method from appearing in the authentication menu, deselect **Visible in the Authentication Menu**.
5. Enter a **Display Name** for the authentication method and specify the authentication method logon **Template Name**.
6. Proceed according to the authentication method you are configuring:

Authentication Method	Configuration
LDAP	Click Next and skip to Step 12 .
User Certificate	Select the Certificate Authority , click Next , and skip to Step 12 .
Extended User Bind	Select the Certificate Authority and proceed to Step 7 .
E-ID Signer	(<i>Optional</i>) Select Return Signature if you want to display the signature. (<i>Optional</i>) If you want to copy the extended properties from another authentication method, select Inherit Extended Properties and select the authentication method to Use Settings From . Proceed to Step 7 .
All other methods	Proceed to Step 7 .

7. Click **Add Authentication Method Server**. The Add Authentication Method Server page opens.

8. Define the following general properties for the Authentication Method Server:

Property	Description
Host	The host address of the Authentication Service for the authentication method.
Port	The port for the Authentication Service.
Time-out	How long the client waits for a reply from the authentication method server before trying to connect the next one on the list.
Listen on all interfaces	(<i>StoneGate Authentication methods only</i>) Select if you want the server to listen to all interfaces.

9. Define the following additional properties depending on the type of Authentication Method Server you are adding:

Authentication Method	Property	Description
General RADIUS	Shared Secret	The secret shared between the RADIUS client and the RADIUS server.
SecurID	Shared Secret	The secret shared between the RADIUS client and the RADIUS server.
SafeWord	Shared Secret	The secret shared between the RADIUS client and the RADIUS server.
Active Directory	Account	The Distinguished Name or Principal Name of the administrator for the Active Directory server.
	Password	The password used when binding to the directory server.
	Root DN	The Distinguished Name of the root node.
IBM Tivoli	Account	The Distinguished Name or Principal Name of the administrator for the Active Directory server.
	Password	The password used when binding to the directory server.
	Users Root DN	The Distinguished Name of the root domain in which to search for users.
	Password Policy DN	The Distinguished Name of the domain where the password policies are located.

Authentication Method	Property	Description
IBM RACF	Account	The Distinguished Name or Principal Name of the administrator for the Active Directory server.
	Password	The password used when binding to the directory server.
	Users Root DN	The Distinguished Name of the root domain in which to search for users.
	Password Policy DN	The Distinguished Name of the domain where the password policies are located.
	Expiration message (reg-exp)	(Optional) The error code returned when the password is expired.
Novell eDirectory	Account	The Distinguished Name or Principal Name of the administrator for the Active Directory server.
	Password	The password used when binding to the directory server.
	Users Root DN	The Distinguished Name of the root domain in which to search for users.
Windows Integrated Login	Path	The path to the Logon page. For example, /directory/pagename.html.
	Enable SSL	Use the SSL protocol in communications with the server.
	CA Certificate	The certificate of the Certificate Authority used to validate the certificates presented by other servers.
NTLM	Path	The path to the Logon page. For example, /directory/pagename.html.
	Enable SSL	Use the SSL protocol in communications with the server.
	CA Certificate	The certificate of the Certificate Authority used to validate the certificates presented by other servers.
	Domain	The Domain to which the authentication method server belongs.
Basic	Path	The path to the Logon page. For example, /directory/pagename.html.
	Enable SSL	Use the SSL protocol in communications with the server.
	CA Certificate	The certificate of the Certificate Authority used to validate the certificates presented by other servers.

Authentication Method	Property	Description
Extended User Bind	User Root DN	The Distinguished Name of the root domain in which to start searching for users.
	Attribute Name	The name for user objects in the directory service.
	Attribute Value	The object class for user objects in the directory service.
	Search Scope	The range of levels at which to search when searching for objects in the directory service.
	User DN	The User DN for performing the search.
	Password	The user password for performing the search.
E-ID	Service Identifier	The service identifier configured in the Nexus MultiID core server.
	Server Connection Time-out	The maximum time for a server connection to be established.
	Server Unavailable Interval	The number of connection retries for servers that are not responding.
E-ID Signer	Service Identifier	The service identifier configured in the Nexus MultiID core server.
	Server Connection Time-out	The maximum time for a server connection to be established.
	Server Unavailable Interval	The number of connection retries for servers that are not responding.
Confidence Online	Scan check path	The path the Confidence Online client scans.

10. Click **Next**.

11. (*RADIUS-based authentication methods only*) Click **Next**. The RADIUS Replies page opens. Add RADIUS replies if necessary, and click **Next**.

12. If necessary, add **Extended Properties** to customize how the authentication is handled.

13. Click **Finish Wizard**.

Modifying Authentication Methods

▼ To modify an Authentication Method

1. Browse to **Manage System** → **Authentication Methods**. The Manage Authentication Methods page opens.
2. Select the authentication method to be modified. The General Settings tab of the Edit Authentication Method page opens.
3. (*Optional*) Change the general settings (**Display Name** and **Template Name**) of the authentication method.

4. (Optional, RADIUS-based authentication methods only) Switch to the **RADIUS Replies** tab to change the registered RADIUS replies or to add a new RADIUS Reply.
5. (Optional) Switch to the **Extended Properties** tab to customize how the authentication is handled and to add and delete extended properties.
6. Click **Save**.

Deleting Authentication Methods

▼ To delete an Authentication Method

1. Browse to **Manage System**→**Authentication Methods**. The Manage Authentication Methods page opens.
2. Select the authentication method to be deleted. The system displays the Edit Authentication Method page.
3. Click **Delete** to delete the authentication method. You are prompted to confirm the deletion of the authentication method.
4. Click **Yes** to delete the selected authentication method.

Enabling Authentication Methods for Self Service

You must enable authentication methods before end-users can use the Self Service functions.

▼ To enable authentication method for Self Service

1. Browse to **Manage System**→**Authentication Methods**. The Manage Authentication Methods page opens.
2. Select the authentication method to be modified. The General Settings tab of the Edit Authentication Method page opens.
3. Select **Manage Default Template Specification** and change the template specification from **GenericForm** to **SelfServiceForm** if you are using a password-based authentication method, or to **SelfServiceFormPIN** if you are using a PIN-based authentication method.

▼ To define the authentication method settings for Self Service

1. Browse to **Manage Accounts and Storage**→**Global User Account Settings**.
2. Switch to the **User Linking** tab.
3. Select **Enable StoneGate Authentication When Manually Linking the User** and/or **Enable Stonegate Authentication When Automatically Linking the User**.
4. Select the **Notification** method.
5. Enable authentication methods and define the authentication method-specific password/PIN/seed options.
6. Click **Save**. To activate the changes, click **Publish** at the top of the page.

Managing RADIUS Configuration

Prerequisites: None

Adding RADIUS Clients

A RADIUS client connects to a RADIUS server for authentication. A RADIUS client can be the Policy Service, a firewall, or the RADIUS plug-in for the Policy Service.

User groups are sent as a RADIUS attribute. Based on user group membership Access Rules, the RADIUS client performs the access control.

▼ To add RADIUS clients

1. Browse to **Manage System**→**RADIUS Configuration**.
2. Click **Add RADIUS Client**.
3. Configure the properties as described below:

Property	Description
IP Address	IP address for the RADIUS client.
Shared Secret	Shared secret between the RADIUS client and the Authentication Service.
Verify Shared Secret	Re-enter the Shared Secret.
Accept Attributes/ Challenge Attributes/ Reject Attributes	Attributes sent to the RADIUS client as a response together with Accept/Challenge/Reject. Accept/Challenge/Reject attributes must be specified in key-value pairs connected with an equal sign (=).

4. Click **Save**. To activate the changes, click **Publish** at the top of the page.

Adding RADIUS Back-End Servers

RADIUS back-end servers handle third-party authentication methods. Usually, the RADIUS server is the Authentication Service, but it can proxy the access request to another authentication server, depending on the authentication method being used. A back-end server can be, for example, an RSA SecurID Server.

▼ To add RADIUS Back-end servers

1. Browse to **Manage System**→**RADIUS Configuration**.
2. Click **Add RADIUS Back-End Server**.
3. Configure the properties as described below:

Property	Description
Display Name	Unique name that identifies the server in the system.
Host	IP address or DNS name of the server.
Port	Port for contacting the server.

Property	Description
Time-out	Time in milliseconds that the Authentication Service waits for a reply before trying to connect to the next server on the list.
Shared Secret	Secret shared between the Authentication Service and the back-end server.
Verify Shared Secret	Re-enter the Shared Secret.

4. Click **Save**. To activate the changes, click **Publish** at the top of the page.

Managing OATH Configuration

Prerequisites: None

Importing Tokens

Before you start importing new token data, you should have received import parameters from the token provider. These parameters include the information about the delimiter separating the attribute fields, and the position of the token ID, seed, and counter in the file. The OATH token file must contain one token for each row and have fields separated with the delimiter symbol(s). New tokens must have token IDs that do not conflict with those already in the database.

▼ To import tokens

1. Browse to **Manage System**→**OATH Configuration**.
2. Select one of the following options:
 - **Import tokens to new provider:** a new provider is added to the database and the tokens are added to the new provider's list.
 - **Import tokens to existing provider:** the tokens are appended to the list of the selected provider.
3. Configure the properties as described below:

Property	Description
Provider Name	Unique name that identifies the OATH token provider in the system.
OTP Length (digits)	(<i>Importing from existing provider only</i>) Length of the generated One-Time Password (OTP) required by the provider (6 - 8 digits).
Delimiter	Symbol(s) separating fields in the token file.
TokenId Position	The field position of the TokenId in the token file.
Seed Position	The field position of the Seed in the token file.
Counter Position	The field position of the Counter in the token file.
Token File	The file that contains the OATH tokens.
Seed and counter are base 64 encoded	Select if the seed and counter are base64 encoded.

4. Click **Continue**.

5. Click **Import**. To activate the changes, click **Publish** at the top of the page.



Caution – If you navigate away from the token import web page during the import, the import task will not be completed, and the performance of Administrator and Authentication Services may be negatively impacted.

Backing Up the OATH Token Database

OATH database backups are automatically scheduled, but you can also perform them manually. The manual backup is mainly intended to be used when migrating from the internal database to an external one.



Note – Because the OATH database changes every time a user successfully logs in, manual backups may not contain the most current information.

▼ To backup the OATH token database

1. Browse to **Manage System**→**OATH Configuration**.
2. Click **Backup OATH token database**.
3. (Optional) Enter the **Backup reason** for your own reference.
4. Click **Start Backup**.

Scheduling Automatic OATH Backups

Automatic OATH backups are enabled by default. Disabling the backups is not recommended. However, you can disable this feature if you are using an external database and the backups are handled by the external database management system.

To guarantee backups in the event of a system failure, include the backup directory (`{StoneGate Administrator}/plugins/root/download/oath/backup/scheduled`) in system backups.

▼ To configure OATH backup scheduling

1. Browse to **Manage System**→**OATH Configuration**.
2. Click **Configure backup scheduling**.
3. Configure the properties as described below:

Property	Description
Time of day	The time (in 24 hour format) when backups start. Taking backups is resource-consuming. It is recommended to schedule them when there is the least load on the system.
Interval in days	How often the backups should be done.
Backups to keep	The number of backups to keep before overwriting old backups. Setting the value to 0 keeps all backups.

4. Click **Save**. To activate the changes, click **Publish** at the top of the page.

Restoring an OATH Token Database Backup

▼ To restore an OATH token database backup

1. Browse to **Manage System**→**OATH Configuration**. The Manage OATH Configuration page opens.
2. Click **Restore OATH token database**. The Restore OATH Database page opens, showing a list of scheduled backups, manual backups, and field for browsing for a backup file to be imported from an external location.
3. Select the backup to be restored and click **Continue**. The Confirm Data page opens.
4. Click **Start Restore**.

Defining OATH Database Connection

There are scenarios in which the built-in default database used by StoneGate SSL VPN may be insufficient. This may happen, for example, when storage requirements exceed the capacity of the built-in database, or if several Authentication Services are used for load balancing/high availability.

It is possible to change the database that StoneGate uses for storing its OATH-related data. After the changes to the database connectivity settings have been published, you must restart the Authentication Service, because the Authentication Service only reads its database settings during startup.

▼ To define an OATH database connection

1. Browse to **Manage System**→**OATH Configuration**. The Manage OATH Configuration page opens.
2. Under Database Connectivity, click **Configure Database Connection**.
3. Define the following attributes:
 - **Dialect**: The hibernate database dialect.
 - **URL**: The URL to the database.
 - **Driver**: The driver used for the database, for example, a jdbc-driver.
 - **User**: The user that StoneGate should login to the database as.
 - **Password**: The password associated to the User-parameter above (the password can be an empty string).
 - **Confirm Password**: The confirmation field of the password.
4. Click **Save**.

Getting Started with Certificates

What are Certificate Authorities?

A Certificate Authority (CA) issues client certificates used in authentication. The CA certificate is needed to authenticate an end-user.

Registered Server Certificates

You manage server certificates when establishing communication with users. It is possible to specify a server certificate for each additional listener for the Access Point, which enables you to have specific certificates for each IP address or port.

Registered Client Certificate

When SSL is selected, the client certificate is used when communicating with the resources. Only one client certificate can be specified.

What do I need to know before I begin?

Some client certificates issued by a CA may be falsified, or in some other way be subject to unintended usage. To cancel an already issued client certificate, the client certificate validation routine checks the certificate against Certificate Revocation List (CRL). The CRL is distributed through a CRL Distribution Point (CDP). Supported CDP Protocols are HTTP and LDAP.

If you want to use Public Key Infrastructure, you must configure each CA you wish to use. After that you can use the configured CA, when adding user certificate authentication methods.

Each CA requires a new authentication method. This is a feature, which makes it possible to have several CAs configured and enabled and then be able to configure which CAs that are valid for a specific resource. This is a powerful feature since the trustworthiness of a CA can vary.

Limitations

There are two prerequisites for managing Certificate Authorities:

- A X.509 v3 certificate must be stored in some persistent form on the application host.
- A CA Root must be stored in your user storage in order to create CA objects.

Managing Certificates

Prerequisites: None

In StoneGate SSL VPN, you manage three types of certificates:

- Certificate authorities: see [Adding a Certificate Authority](#).
- Server certificates: see [Adding Server Certificates](#) (page 123).
- Client certificates: see [Adding a Client Certificate](#) (page 123).

Adding a Certificate Authority

▼ To add a Certificate Authority

1. Browse to **Manage System**→**Certificates**. The Manage Certificates page opens.
2. Click **Add Certificate Authority** and define the following settings:

Setting	Description
Enable Certificate Authority	Select to enable the CA.
Display Name	Unique name used in the system to identify Certificate Authority.
CA Certificate	Select one or more CA certificates used to complete the entire certificate chain.
Revocation Control	Select CRL , click Next and continue to Step 3 , or select OCSP and proceed to Step 4 .



Note – Use OCSP certification revocation control when possible. If you specify both CRL and OCSP, the CRL check is done first, and OCSP only if the certificate is not found.

3. Define the following settings for CRL Revocation Control:

Setting	Description
CRL Invalid Action	Defines how to handle users authenticated by user certificate if the requested CRL cannot be obtained.
Address	The LDAP address (RFC2255) or HTTP address of the CDP, entered as a URL.
Fetch Time Adjustment	Adjusted time in seconds when revocation information is retrieved, compared to the set time for revocation information fetching.
Update Time	Enable/disable custom update time.
Define interval for CRL retrieving	Interval in seconds (0 - 31536000) for CRL retrieving.
Retry Interval	Interval in seconds (0 - 31536000) to retry the CRL retrieving if the CRL cannot be obtained.

4. Click **Save**. The Certificate Authority is added.

Adding Server Certificates

PEM formatted server certificates are registered to be used when establishing communication with end-users. You can specify server certificates for specific IP addresses and ports, which is useful when managing additional listeners.

A CA is required to complete the entire certificate chain. A specific CA certificate for the server certificate can be selected if the browser does not have the root or intermediate CA used to verify the server certificate.

▼ To add a Server Certificate

1. Browse to **Manage System**→**Certificates**. The Manage Certificates page opens.
2. Click **Add Server Certificate** and define the following settings:

Setting	Description
Display Name	Unique name used in the system to identify the server certificate.
Certificate	PEM formatted certificate.
Key	Private key for the certificate (PKCS#8 key in either DER or PEM format).
Password	Password to use if the information is encrypted.
Using Hardware Security Module	Enable/disable the use of the hardware security module.

3. Click **Save**.

Adding a Client Certificate

PEM formatted client certificates are registered to be used in resource communication using SSL.



Note - You can only specify one client certificate per StoneGate SSL VPN installation.

▼ To add a Client Certificate

1. Browse to **Manage System**→**Certificates**. The Manage Certificates page opens.
2. Click **Manage Client Certificate Settings**, and define the following settings:

Setting	Description
Display Name	Unique name used in the system to identify the server certificate.
Certificate	PEM formatted certificate.
Key	Private key for the certificate (PKCS#8 key in either DER or PEM format).
Password	Password to use if the information is encrypted.

3. Click **Save**.

CHAPTER 12

MANAGING AUTHENTICATION SERVICES

This chapter describes the creation and management of Authentication Services.

The following sections are included:

- ▶ [Getting Started with Authentication Services](#) (page 126)
- ▶ [Managing Authentication Services](#) (page 126)
- ▶ [Configuring Global Authentication Service Settings](#) (page 128)

Getting Started with Authentication Services

Authentication Services authenticate users accessing resources.

Authentication Services support the following RADIUS-based authentication methods: Mobile Text, Web, Challenge, Password, OATH, and Synchronized.

A number of settings can be specified globally to apply to all Authentication Services. The global settings include RADIUS authentication and password/PIN settings.

Registered Authentication Services are listed on the Manage Authentication Services page.

What Do I Need to Know Before I Begin?

Usually there is no need to make changes to Authentication Services. You only need to manage Authentication Services if the system is a part of a mirrored configuration.

Configuration Overview

1. (Optional) Add an Authentication Service. See [Managing Authentication Services](#) (page 126).
2. (Optional) Configure Global Access Point Service settings. See [Configuring Global Authentication Service Settings](#) (page 128).

Managing Authentication Services

Prerequisites: None

Adding an Authentication Service

▼ To add an Authentication Service

1. Browse to **Manage System**→**Authentication Services**. The Manage Authentication Services page opens.
2. Click **Add Authentication Service**.
3. Enter the new Authentication Service information:

Label	Description
Display Name	The IP address or DNS name of the Authentication Service.
Internal Host	IP address or DNS name of the Authentication Service. avoid using the IP address 0.0.0.0 to listen to all local IP addresses. Instead, use the Listen on all interfaces option that specifies the interfaces that the service listens to.
Internal Communication Port	The port used for internal traffic (LCP) from the different services in the network (default: 8302).
Listen on all Interfaces	When selected, the service listens to all specified IP addresses. When not selected, the services only listen to the IP address specified as internal host.
Distribute key files automatically	Selecting this option automatically distributes key files from the Administration Service to the Authentication Service after the Authentication Service has been installed. If you do not select this option, you must copy the key files manually

Label	Description
Server Certificate	<p>The certificate used when the Authentication Service performs TLS handshaking (for example, authenticating with the PEAP-MSCHAPv2 protocol). If PEAPMSCHAPv2 authentication protocol is used, you must assign a server certificate. If not, PEAPMSCHAPv2 authentication will fail.</p> <p>All available server certificates are available for selection. Server certificates are managed in the Manage Certificates section of the StoneGate SSL VPN Administrator.</p>
Add Additional Listener	<p>Enter the additional IP addresses or DNS names that the Authentication Service listens to. The listeners are added to the list of hosts available in the RADIUS Accounting section.</p>
Enable RADIUS accounting	<p>When selected, the system responds to RADIUS accounting packets sent from RADIUS clients. The system logs the incoming RADIUS packet and replies with an accounting response packet. Accounting packets can also contain information about when a user logs in and out of a system.</p>
Host	<p>The IP address or DNS name of the system that sends the accounting response message. Required when Enable RADIUS accounting is selected.</p>
Port	<p>Port for the system that sends the accounting response message. Required when Enable RADIUS accounting is selected.</p>
Listen on all interfaces	<p>Defines whether the system must listen to all interfaces for RADIUS packets.</p>

4. Click **Add** to add a new Authentication Service.

Modifying an Authentication Service

▼ To modify an Authentication Service

1. Browse to **Manage System**→**Authentication Services**. The Manage Authentication Services page opens.
2. Under Registered Authentication Services, click the Service ID of the Authentication Service that you want to modify. The Edit Authentication Service page opens.
3. Select an Authentication Service to modify. The system displays the previously entered information for the Authentication Service (see [Step 3 in Adding an Authentication Service](#) (page 126)).
4. Modify the information of the Authentication Service.
5. Click **Save**. The system confirms that the Authentication Service has been modified.

Deleting an Authentication Service

▼ To delete an Authentication Service

1. Browse to **Manage System**→**Authentication Services**. The Manage Authentication Services page opens.
2. Under Registered Authentication Services, click the Service ID of the Authentication Service you want to delete. The Edit Authentication Service page opens.
3. Click **Delete**. You are prompted to confirm the deletion of the Authentication Service.
4. Click **Yes** to delete the service.

Configuring Global Authentication Service Settings

Prerequisites: None

The Global Authentication Service Settings define, for example, how the passwords must be formatted and how the notification messages are delivered to the end-users.

Global Authentication Service Settings are configured on the following tabs:

- RADIUS Authentication: see [Configuring Global RADIUS Authentication Settings](#).
- Password/PIN Settings: see [Configuring Global Password/PIN Settings](#) (page 129).
- E-mail Messages: see [Configuring Global E-mail Message Settings](#) (page 131).
- SMS/Screen Messages: see [Configuring Global SMS and Screen Message Settings](#) (page 132).

Configuring Global RADIUS Authentication Settings

▼ To configure global RADIUS authentication settings

1. Browse to **Manage System**→**Authentication Services**. The Manage Authentication Services page opens.
2. Click **Manage Global Authentication Service Settings**. The Manage Global Authentication Service Settings page opens.
3. Select the **RADIUS Authentication** tab and configure the relevant settings as described below:

Setting	Description
Drop unknown sessions	If selected, access requests by unknown RADIUS sessions are dropped. Otherwise, the server sends an Access Denied reply.
Drop unknown users	If selected, access requests by unknown users are dropped and the Authentication Service ignores the requests without reply. Otherwise, the Authentication Service accepts the request, but the authentication fails with an access reject message. Leaving Drop Unknown Users unselected can be useful for chained authentication.

Setting	Description
Proxy unknown users	This setting is applied before the Drop Unknown Users setting if both are selected. If selected, unknown users are authenticated using another RADIUS server. The Authentication Service tries to proxy the request to the configured RADIUS back-end server. If the request is not serviced, the Authentication Service handles the request according to the Drop Unknown Users setting.
Reveal reject reason	If selected, the reason a request has been rejected is displayed to the RADIUS client.
Session Time-out	The length of time (in seconds, 180 by default) the state attribute is valid. The RADIUS session times out after this time limit. The server discards the RADIUS session after this time span.
RADIUS Encoding	When the system receives a RADIUS package, it normally transforms the data to strings according to the UTF-8 standard. Some RADIUS clients do not support the UTF-8 standard, in which case another standard must be specified (by default, UTF-8).

Configuring Global Password/PIN Settings

The settings on the Password/PIN Settings tab define global password and PIN restrictions for StoneGate Authentication Services.

▼ To configure global password/PIN settings

1. Browse to **Manage System**→**Authentication Services**. The Manage Authentication Services page opens.
2. Click **Manage Global Authentication Service Settings**. The Manage Global Authentication Service Settings page opens.
3. Select the **Password/PIN Settings** tab and configure the relevant settings as described below:

Setting	Value(s)	Valid for
Minimum number of characters in password	6	StoneGate Mobile Text, StoneGate Web, StoneGate Password, StoneGate Synchronized, StoneGate OATH.
Maximum number of characters in password	16	StoneGate Mobile Text, StoneGate Web, StoneGate Password, StoneGate Synchronized, StoneGate OATH.
Minimum number of letters in a password	2	StoneGate Mobile Text, StoneGate Web, StoneGate Password.
Minimum number of numbers in a password	2	StoneGate Mobile Text, StoneGate Web, StoneGate Password.
Password/PIN validity period in days	90	StoneGate Mobile Text, StoneGate Web, StoneGate Challenge, StoneGate Password, StoneGate Synchronized, StoneGate OATH. When set to 0, the password/PIN does not expire.

Setting	Value(s)	Valid for
Saved previous passwords/PINs not eligible for reuse	5	StoneGate Mobile Text, StoneGate Web, StoneGate Challenge, StoneGate Password, StoneGate Synchronized, StoneGate OATH. The user cannot use any of the 5 previous passwords/PINs saved in password history.
Length of OTP (characters)	6	StoneGate Mobile Text.
Alphabet base	All letters and numbers.	StoneGate Mobile Text. Note: Exclude characters and numbers that can be easily confused, such as, for example, 0/o/0.
Notification message	Your OTP is {0}. Enter it to login with Mobile Text)	StoneGate Mobile Text.
Allow two-step authentication	On/Off	StoneGate Mobile Text. Authentication is split into two sessions: one to make the server send the OTP to the cell phone, and one to login with the OTP. Default value: Off.
Keyboard appearance	Fixed Shift Random	StoneGate Web. Default: Random.
Allow the use of desktop keyboard for numbers	On/Off	StoneGate Web. Default: Off.
Support value signing	On/Off	StoneGate Challenge Default: Off.
Number of logon attempts before user is prompted for new OTP		StoneGate Synchronized Default: 3.
Number of logon attempts before user is denied access.		StoneGate Synchronized Default: 10.
Look-ahead window size	0-1000	StoneGate OATH Default: 50. When set to 0, the look-ahead window is disabled.

Configuring Global E-mail Message Settings

The settings on the E-mail Messages tab define the e-mail messages sent to users to notify them of new or changed passwords, PINs, or seeds.

▼ To configure global e-mail message settings

1. Browse to **Manage System**→**Authentication Services**. The Manage Authentication Services page opens.
2. Click **Manage Global Authentication Service Settings**. The Manage Global Authentication Service Settings page opens.
3. Select the **E-mail Messages** tab and configure the relevant settings as described below:

Setting	Description
E-mail Addresses to Notify	One or more e-mail addresses (separated by a semicolon) to which e-mail notifications for new or changed passwords, PINs, or seeds are sent.
E-mail Messages	Specify the message subject line, header, and footer.
New Password Entered/New PIN Entered	The message for notifying users (and additional recipients) of new passwords or PINs to use when authenticating. Different messages can be defined for different StoneGate authentication methods.
Use Directory Password	The message for notifying users (and additional recipients) to use the password specified in the directory service when authenticating. It is strongly recommended that you change the default texts to describe which password must be used.
Use Mapped Password/Use Mapped PIN	The message for notifying users (and additional recipients) to use their mapped password or PIN when authenticating. Different messages can be defined for different StoneGate authentication methods.
Seed	The message for notifying users (and additional recipients) of new seeds to be used in the StoneGate Mobile ID clients Synchronized and Challenge.

Configuring Global SMS and Screen Message Settings

The settings on the SMS/Screen Messages tab define the messages sent by SMS and displayed to users on screen to notify them of new or changed passwords, PINs, or seeds for each authentication method.

▼ To configure global SMS/screen message settings

1. Browse to **Manage System**→**Authentication Services**. The Manage Authentication Services page opens.
2. Click **Manage Global Authentication Service Settings**. The Manage Global Authentication Service Settings page opens.
3. Select the **SMS/Screen Messages** tab and configure the relevant settings as described below:

Setting	Description
New Password Entered/New PIN Entered	The message for notifying users (and additional recipients) of new passwords or PINs to use when authenticating. Different messages can be defined for different StoneGate authentication methods.
Use Directory Password	The message for notifying users (and additional recipients) to use the password specified in the directory service when authenticating. It is strongly recommended that you change the default texts to describe which password must be used.
Use Mapped Password/Use Mapped PIN	The message for notifying users (and additional recipients) to use their mapped password or PIN when authenticating. Different messages can be defined for different StoneGate authentication methods. It is strongly recommended that you change the default texts to describe which password must be used.
Seed	The message for notifying users (and additional recipients) of new seeds to use in the Mobile ID clients Synchronized and Challenge. It is possible to distribute the mode Challenge or Synchronized together with the seed, resulting in a pre-configured Mobile ID Challenge or Synchronized client with injected seed.

CHAPTER 13

DEFINING ACCESS RULES

Access rules define sets of access criteria for granting end-users permission to use resources. Many different types of criteria are available for combining into detailed sets of conditions.

The following sections are included:

- ▶ [Getting Started with Access Rules](#) (page 134)
- ▶ [Defining the Global Access Rule](#) (page 135)
- ▶ [Editing Access Rules](#) (page 136)

Getting Started with Access Rules

Access Rules determine the criteria for authorizing end-users.

What Access Rules Do

Access Rules define one or more conditions that must be met for a particular end-user to be allowed access to a resource or SSO domain. When you create a resource or SSO domain, you can apply any combination of Access Rules.

Example An Access Rule can require that the end-users use a particular authentication method, that their user account is part of a certain user group, and that their connection is made from a computer that meets your organization's minimum security requirements.

In most cases, the conditions determine access to individual resources and select which resources are shown to the end-user in the Application Portal. With some types of conditions, you can grant access with a warning message to the end-user.

There are three ways to define Access Rules:

- You can define one *Global Access Rule* that is always applied to all resource access. If the Global Access Rule is defined, any resource-specific Access rules you create are considered as additional criteria to the Global Access Rule.
- You can define *registered Access Rules*, which are reusable rules that you save under a display name and select in any place you want to apply those particular access criteria. You must create the registered Access Rules before you configure the resources that will use them.
- You can define Access Rule conditions individually in each instance of use (usually in a particular resource) without creating a reusable Registered Access Rule. This approach is useful in rare cases when a resource has truly unique conditions for access.

The way you create the Access rules does not directly affect their content; the same definitions are available in all cases.

What Do I Need to Know Before I Begin?

Each Access Rule can contain several different conditions for access. An individual condition in an Access Rule is called a *Rule*.



Note – The system does not require you to add any Access Rules at any stage of the configuration. If no Access Rules are applied, all users can access the resource using any authentication method that is configured for them. To define a more stringent baseline in your system, define the Global Access Rule (see below).

Configuration Overview

The following is the recommended configuration order:

1. Define the general access criteria that you want to apply globally to all resource access through the SSL VPN gateway as explained in [Defining the Global Access Rule](#) (page 135).
2. Create reusable Registered Access Rules for more specific access criteria as explained in [Adding a New Registered Access Rule](#) (page 137).
3. (If applicable) Define resource-specific Access Rule instances as part of creating resources that have unique access requirements.

Defining the Global Access Rule

Prerequisites: None

The Global Access Rule is applied to all resources and SSO domains. Conditions set by both the Global Access Rule and any specific rules you define for the resource must be met for the end-user to gain access.

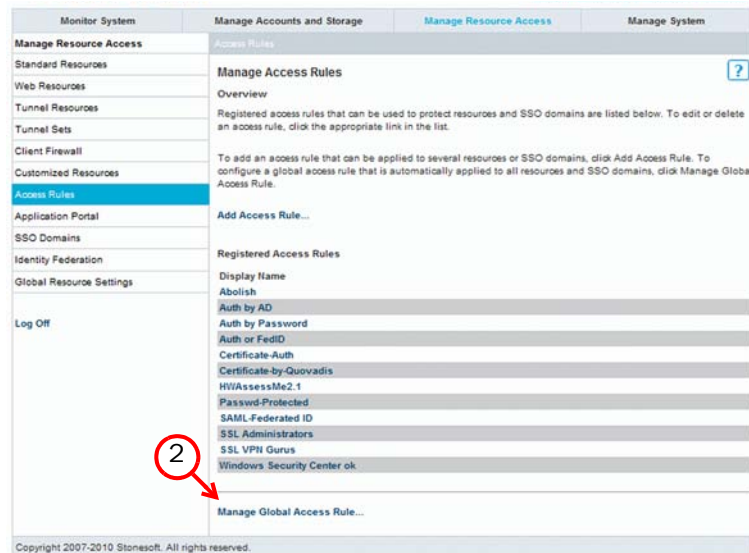
Example A Global Access Rule could define that all end-users must authenticate using StoneGate MobileID authentication and be a member of the user group “remote access users”. All users must always meet these basic requirements, removing the need for specific configuration in each new resource. This way, a Web Resource for Intranet access needs no additional Access Rule configuration. Further access criteria is only added to resources that differ from the Global Access Rule criteria, such as an additional Access Rule that requires membership in user group “sales” or “management” for access to a customer database.

The Global Access rule can contain client device restrictions, but device-specific global restrictions can also be configured separately as explained in [Configuring Device Access Restrictions](#) (page 189).

If you have previously created Registered Access Rules, you can optionally use those to define the Global Access Rule. Since any further changes to the Registered Access Rule are applied globally, carefully consider which Access Rules you can select without risking configuration mistakes. To create reusable Access Rules, see [Adding a New Registered Access Rule](#) (page 137).

▼ To edit the Global Access Rule

1. Browse to **Manage Resource Access**→**Access Rules**. The Manage Access Rules page opens.



2. Click **Manage Global Access Rule**. The Manage Global Access Rule page opens.

3. (Optional) Select existing registered Access Rules that are applied as criteria in the Global Access Rule in the **Select Access Rules** section.
 - If you add several Access Rules in this section, the user must meet the criteria in all of the Access Rules at the same time for access to be granted (logical AND).
 - The Access Rules are applied from the top to bottom in the order that they are listed in **Selected Access Rules**. To change the order, remove and re-add the rules in the correct order.
 - Be careful when editing the registered Access Rules you add here. If you later change the selected registered Access Rules, also the changes are applied globally.
4. (Optional) Add instance-specific Access Rules to be applied as criteria in the Global Access Rule in the **Add Access Rules** section.
 - These rules only exist in the Global Access Rule, and they only change if you specifically edit them in the Global Access Rule.
 - If you add several Access Rules in this section, they are considered as alternatives to each other by default, so the user must only meet the criteria in one of the rules you add to gain access (logical OR). To change to logical AND for some Access Rules, select them and use the **Combine** action. A **Split** action becomes available to reverse this change.
 - For instructions on how to create the Access Rule, proceed to [Selecting Criteria for Access Rules](#) (page 138).
5. Click **Save** when you are finished. To activate the changes, click **Publish** at the top of the page.

The Global Access Rule is shown for your reference whenever you create resources and SSO Domains, but cannot be deactivated.

Editing Access Rules

Prerequisites: None

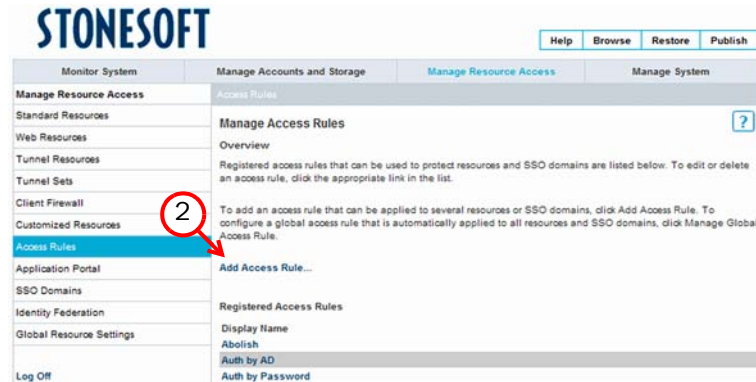
You edit Access Rules in the following ways:

- You can add a new reusable Access Rule as explained in [Adding a New Registered Access Rule](#) (page 137).
- You can edit an existing reusable Access Rule as explained in [Modifying a Registered Access Rule](#) (page 137).
- You can add or modify resource-specific non-reusable access rules when you are editing the resource, proceed as explained in [Selecting Criteria for Access Rules](#) (page 138).

Adding a New Registered Access Rule

▼ To add a Registered Access Rule

1. Browse to **Manage Resource Access**→**Access Rules**. The Manage Access Rules page opens.



2. Click **Add Access Rule**. The Add Access Rule page opens.
3. Enter the **Display Name** you want to use.

What's Next?

- ▶ Continue as explained in [Selecting Criteria for Access Rules](#).

Modifying a Registered Access Rule

▼ To modify an existing registered Access Rule

1. Browse to **Manage Resource Access**→**Access Rules**. The Manage Access Rules page opens.
2. Click the access rule to be edited from the list of the **Registered Access Rules**. The Edit Access Rule page opens.
3. You can now edit the Access Rule in the following ways:
 - Add and edit rules as explained in [Selecting Criteria for Access Rules](#) (page 138).
 - Delete rules by clicking the rule in the **Allow user access when** table and then clicking **Delete** on the page that opens.
 - Define how several added rules interact with each other.
 - By default, they are considered as alternatives, so the user must only meet the criteria in one of the rules you add (logical OR).
 - You can change to logical AND for some Access Rules if you select the rules and then click **Combine**.
 - A **Split** action becomes available to separate previously combined rules.
4. Click **Save** when you are finished. To activate the changes, click **Publish** at the top of the page.

Selecting Criteria for Access Rules

▼ To add an access requirement for a Rule

1. Click **Add Rule**, or click an existing rule you want to modify under **Allow user access when**.



2. Select the type for the rule (if creating a new rule) and proceed to the correct section as indicated below.

Type	Description
Authentication method	The end-user must authenticate using the method(s) you specify. If you select this type, proceed to Defining Authentication Method Access Requirements (page 139).
User group membership	The end-user's account must be included in the group(s) you specify. If you select this type, proceed to Defining User Group Membership Access Requirements (page 139).
IP Address of incoming client	The source IP address of the end-user's connection must be within the range you specify. If you select this type, proceed to Defining IP Address Access Requirements (page 140).
Client Device	The end-user's device should meet a Device Definition that you have configured in the system (see Adding Custom Device Definitions (page 186)). If you select this type, proceed to Defining Client Device Access Requirements (page 140).
Date, day and/or time	The end-user must connect within the time period(s) you define. If you select this type, proceed to Defining Time-Based Access Requirements (page 141).
User storage	The end-user's account must be stored in the user storage location(s) you specify. If you select this type, proceed to Defining User Storage Access Requirements (page 142).
Assessment	The end-user's device must pass the security scans you specify. If you select this type, proceed to Defining Assessment Access Requirements (page 142).
Abolishment	The end-user's device must be compatible with abolishment (trace removal). If you select this type, proceed to Defining Abolishment Access Requirements (page 143).
Access Point	The end-user must connect through the Access Point (SSL VPN appliance) you specify. If you select this type, proceed to Defining Access Point Access Requirements (page 144).

Type	Description
Identity Provider	The end-user must connect through the Identity Provider you specify. If you select this type, proceed to Defining Identity Provider Access Requirements (page 144).
Custom-defined	Allows you to define information paths and client data requirements yourself instead of using a plug-in. You can define requirements for Windows and Mac OS X clients. If you select this type, proceed to Defining Custom Access Requirements (page 144).

Defining Authentication Method Access Requirements

▼ To specify an authentication method requirement

1. Select one or more authentication methods that the end-user must use to access a resource protected by the access rule. All registered and enabled authentication methods are available for selection.
2. If you select several authentication methods for the Access Rule, specify how they are used:
 - Select **Combine with OR** if the user can authenticate with one of the selected authentication methods. This is selected by default.
 - Select **Combine with AND** if the user must use all listed authentication methods. The order in which you select the methods determines the order in which the authentication methods are used.

What's Next?

- ▶ If you are creating a new Access Rule, proceed to [Finishing the Add Access Rule Wizard](#) (page 146).
- ▶ If you are editing the Global Access Rule, proceed according to the workflow in [Defining the Global Access Rule](#) (page 135).
- ▶ If you are editing an existing Access Rule, proceed according to the workflow in [Modifying a Registered Access Rule](#) (page 137).

Defining User Group Membership Access Requirements

▼ To specify a user group membership requirement

1. (Optional) To find a specific group, enter its name and click **Search**. The user group listing below is updated to match your search.
 - The wildcard character * is supported, and can be entered anywhere in the search string.
 - To display all groups, enter the wildcard without any other characters (default).
2. Add one or more user groups to the **Selected user groups** list.

