SSL VPN 1.5.200

Administrator’s Guide

Virtual Private Networks

STONESOFT
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:

Third Party Licenses
The Stonesoft software includes several open source or third-party software packages. The appropriate software licensing information for those products can be found at the Stonesoft website:

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) No 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:

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

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:

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, 1231754, 1259028, 1271283, 1289183, 1289202, 1304830, 1304849, 1313290, 1326393, 1361724, 1379037, and 1379046 and US Patent Nos. 6,650,621; 6,856,621; 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; 7,325,248; 7,360,242; 7,386,525; 7,406,534; 7,461,401; 7,573,823; 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.

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 © 2013 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

Revision: SGSVAG_20130225
# TABLE OF CONTENTS

**GETTING STARTED**

**CHAPTER 1  Using Stonesoft Documentation**  
- Objectives and Audience  
- Typographical Conventions  
- Documentation Available  
- Product Documentation  
- Support Documentation  
- Contact Information  
- Licensing Issues  
- Technical Support  
- Your Comments  
- Security Related Questions and Comments  
- Other Queries  

**CHAPTER 2  What's New**  
- New Features in SSL VPN 1.5.200  
- Add Multiple CA Certificates Wizard  
- Certificate Management Tools in the Web Console  
- MSI Installer for Windows Access Client  
- Native Assessment Client for Linux  
- Stonesoft Invisible Token Authentication Method  
- SgInfo Tools in the Web Console  
- Support for 64-bit Architecture  
- Support for Metadata in Identity Federation  
- Trace Support for Windows Access Client  

**CHAPTER 3  Feature Overview**  
- Introduction  
- Assessment  
- Authentication  
- Authorization  
- Access  
- Auditing  
- Abolishment  

**CHAPTER 4  Technical Overview**  
- Introduction to System Services  
- Default Listening Ports  
- Administration Service  
- Access Point  
- Mirroring  
- Trusted Gateways  
- Cipher Suites  
- Link Translation and DNS Mapping  
- Internal Cookies  
- Policy Service  
- Resources  
- Standard Resources  
- Access Rules  
- Single Sign-On  
- Authentication Service  
- Internal Authentication  
- Directory Service and User Storage  

**CHAPTER 5  Planning**  
- Getting Started with Planning SSL VPN Deployment  
- Security Audit/Planning  
- System Architecture Review  
- Public Key Infrastructure  
- User Management Strategy  
- Analyzing Your Environment  
- Directory Service Requirements  
- Use of Special Characters  
- Resource Access  
- Access Strategies  
- Using Groups  
- Naming Conventions  
- Select Authentication Methods  
- Pre-Installation Checklist  

**CHAPTER 6  GUI Overview**  
- Getting Started with SSL VPN Graphical User Interface  
- SSL VPN Administrator  
- Online Help  
- Navigating in the SSL VPN Administrator  
- Top Menu  
- Monitor System  
- Manage Accounts and Storage  
- Manage Resource Access
<table>
<thead>
<tr>
<th>Chapter 18</th>
<th>Tunnel Resource Configuration</th>
<th>203</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Resource Configuration</td>
<td>203</td>
<td></td>
</tr>
<tr>
<td>Getting Started with Tunnel Resources</td>
<td>204</td>
<td></td>
</tr>
<tr>
<td>About the Application Portal</td>
<td>204</td>
<td></td>
</tr>
<tr>
<td>About Alternative Hosts</td>
<td>204</td>
<td></td>
</tr>
<tr>
<td>Configuration Overview</td>
<td>204</td>
<td></td>
</tr>
<tr>
<td>Creating Tunnel Resource Networks</td>
<td>205</td>
<td></td>
</tr>
<tr>
<td>Creating Tunnel Resource Hosts</td>
<td>206</td>
<td></td>
</tr>
<tr>
<td>Creating and Modifying Tunnel Sets</td>
<td>207</td>
<td></td>
</tr>
<tr>
<td>Adding a New Tunnel Set</td>
<td>207</td>
<td></td>
</tr>
<tr>
<td>Adding a Static Tunnel to a Tunnel Set</td>
<td>208</td>
<td></td>
</tr>
<tr>
<td>Adding a Dynamic Tunnel to a Tunnel Set</td>
<td>208</td>
<td></td>
</tr>
<tr>
<td>Specifying a Startup Command</td>
<td>209</td>
<td></td>
</tr>
<tr>
<td>Selecting Tunnel Resource Access Rules</td>
<td>209</td>
<td></td>
</tr>
<tr>
<td>Configuring Tunnel Resource Authorization Settings</td>
<td>210</td>
<td></td>
</tr>
<tr>
<td>Configuring IP Address Pools</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>Defining the IP Address Pool</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>Defining the Access Point Dynamic Pool IP Address</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>Enabling the Dynamic IP in the Tunnel Set</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>About the Access Client</td>
<td>212</td>
<td></td>
</tr>
<tr>
<td>Windows Native Access Client</td>
<td>212</td>
<td></td>
</tr>
<tr>
<td>Windows Vista/Windows 7-specific Configuration</td>
<td>212</td>
<td></td>
</tr>
<tr>
<td>Linux Native Access Client</td>
<td>213</td>
<td></td>
</tr>
<tr>
<td>Preparing for Linux Access Client Use on Ubuntu Linux</td>
<td>213</td>
<td></td>
</tr>
<tr>
<td>Preparing for Linux Access Client Use on Suse Linux</td>
<td>214</td>
<td></td>
</tr>
<tr>
<td>ActiveX Access Client Loader</td>
<td>214</td>
<td></td>
</tr>
<tr>
<td>Configuring Internet Explorer for the ActiveX Access Client Loader</td>
<td>214</td>
<td></td>
</tr>
<tr>
<td>Java Applet Access Client Loader</td>
<td>214</td>
<td></td>
</tr>
<tr>
<td>Pure Java Access Client</td>
<td>215</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 19</th>
<th>Client Security</th>
<th>217</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Security</td>
<td>217</td>
<td></td>
</tr>
<tr>
<td>Getting Started with Client Security</td>
<td>218</td>
<td></td>
</tr>
<tr>
<td>Configuration Overview</td>
<td>218</td>
<td></td>
</tr>
<tr>
<td>Configuring Device-Specific Controls</td>
<td>218</td>
<td></td>
</tr>
<tr>
<td>Adding Custom Device Definitions</td>
<td>218</td>
<td></td>
</tr>
<tr>
<td>Registering Device Settings</td>
<td>219</td>
<td></td>
</tr>
<tr>
<td>Configuring Device Access Restrictions</td>
<td>221</td>
<td></td>
</tr>
<tr>
<td>Configuring Assessment</td>
<td>222</td>
<td></td>
</tr>
<tr>
<td>Assessment Configuration Overview</td>
<td>222</td>
<td></td>
</tr>
<tr>
<td>Enabling Assessment</td>
<td>223</td>
<td></td>
</tr>
<tr>
<td>Defining Client Scan Paths</td>
<td>223</td>
<td></td>
</tr>
<tr>
<td>Enabling Real Time Scan</td>
<td>224</td>
<td></td>
</tr>
<tr>
<td>Hiding Resources Before Assessment Client Scan</td>
<td>224</td>
<td></td>
</tr>
<tr>
<td>Enabling Silent Assessment</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>Modifying Assessment Client Loader Order</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>Adding Assessment Plug-Ins</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>Selecting the Hardware Assessment Plug-In Configuration File</td>
<td>226</td>
<td></td>
</tr>
<tr>
<td>Configuring Abolishment</td>
<td>226</td>
<td></td>
</tr>
<tr>
<td>Abolishment Configuration Overview</td>
<td>226</td>
<td></td>
</tr>
<tr>
<td>Configuring File Removal</td>
<td>227</td>
<td></td>
</tr>
<tr>
<td>Configuring Cache Clean-Up</td>
<td>228</td>
<td></td>
</tr>
<tr>
<td>Hiding Resources Before Abolishment Client Scan</td>
<td>228</td>
<td></td>
</tr>
<tr>
<td>Enabling Silent Abolishment</td>
<td>229</td>
<td></td>
</tr>
<tr>
<td>Modifying the Abolishment Client Loader Order</td>
<td>229</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 20</th>
<th>Managing Single Sign-On and Identity Federation</th>
<th>231</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Single Sign-On and Identity Federation</td>
<td>231</td>
<td></td>
</tr>
<tr>
<td>Getting Started with Single Sign-On</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>Creating Single Sign-On (SSO) Domains</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>Adding an SSO Domain</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>Adding Domain Attributes</td>
<td>233</td>
<td></td>
</tr>
<tr>
<td>Selecting the SSO Access Rule</td>
<td>234</td>
<td></td>
</tr>
<tr>
<td>Getting Started with Identity Federation</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td>Configuration Overview</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td>Enabling Identity Federation</td>
<td>236</td>
<td></td>
</tr>
<tr>
<td>Adding a Service Provider</td>
<td>236</td>
<td></td>
</tr>
<tr>
<td>Configuring Service Provider ADFS Settings</td>
<td>237</td>
<td></td>
</tr>
<tr>
<td>Configuring Service Provider SAML 2.0 Settings</td>
<td>238</td>
<td></td>
</tr>
<tr>
<td>Adding an Identity Provider</td>
<td>240</td>
<td></td>
</tr>
<tr>
<td>Configuring Identity Provider ADFS Settings</td>
<td>240</td>
<td></td>
</tr>
<tr>
<td>Configuring Identity Provider SAML 2.0 Settings</td>
<td>241</td>
<td></td>
</tr>
<tr>
<td>Reading User Certificate Attributes</td>
<td>242</td>
<td></td>
</tr>
<tr>
<td>Exporting SAML 2.0 Metadata</td>
<td>243</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Identity Federation</td>
<td>243</td>
<td></td>
</tr>
</tbody>
</table>
GETTING STARTED

In this section:

Using Stonesoft Documentation - 11
What’s New - 15
Feature Overview - 19
Technical Overview - 25
Planning - 33
GUI Overview - 39
Working in the Web Console - 51
CHAPTER 1

USING STONESOFT DOCUMENTATION

This chapter describes how to use this guide and related documentation. It also provides directions for obtaining technical support and giving feedback on the documentation.

The following sections are included:

► Objectives and Audience (page 12)
► Documentation Available (page 13)
► Contact Information (page 14)
Objectives and Audience

The SSL VPN Administrator’s Guide covers all aspects of Stonesoft 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

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

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.
**Documentation Available**

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

**Product Documentation**


The 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

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

**Support Documentation**

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

Contact Information

For street addresses, phone numbers, and general information about Stonesoft products and Stonesoft Corporation, visit our website at http://www.stonesoft.com/.

Licensing Issues

You can view your current licenses at the License Center section of the Stonesoft website at http://www.stonesoft.com/en/customer_care/licenses/.

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 website at http://www.stonesoft.com/en/customer_care/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 the Stonesoft SSL VPN and network security to security-alert@stonesoft.com.

Other Queries

For queries regarding other matters, e-mail info@stonesoft.com.
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 the SSL VPN is configured are not listed. For a full list of changes in the software, consult the Release Notes.

The following sections are included:

► New Features in SSL VPN 1.5.200 (page 16)
New Features in SSL VPN 1.5.200

Add Multiple CA Certificates Wizard

It is now possible to add multiple CA certificates simultaneously. This makes the configuration of certificate-based authentication methods quicker and easier.

- For more information, see Adding Multiple Certificate Authority Certificates (page 154).

Certificate Management Tools in the Web Console

The Public Key Infrastructure (PKI) Management tools in the Web Console allow you to create and manage the certificates that are used in connections to the Web Console.

- For more information, see Managing Certificates in the Web Console (page 156).

MSI Installer for Windows Access Client

An MSI installer is now available for the Windows Access Client. The MSI format allows you to distribute and install the Stonesoft SSL VPN Access Client using the software distribution systems and policies in Microsoft Active Directory.

Native Assessment Client for Linux

The new native Assessment Client for Linux allows you to check the presence and/or checksums of files and directories on connecting Linux clients to apply client security requirements to Linux clients.

Stonesoft Invisible Token Authentication Method

The new Stonesoft Invisible Token authentication method is a browser-based two factor authentication method. The first time a user authenticates with a user ID and password, the user receives an SMS that contains a one-time password (OTP) for authentication. When the user selects the option to remember the browser, a shared secret is placed in the browser. The next time the user authenticates, a script automatically generates and sends an OTP.

- For more information, see Stonesoft Authentication Methods (page 128).

SgInfo Tools in the Web Console

It is now possible to collect a customized sgInfo file that contains the specified information about the SSL VPN system in the Web Console.

- For more information, see Collecting SgInfo in the Web Console (page 62).

Support for 64-bit Architecture

Both virtual and physical appliances are now available for 64-bit architecture. The 64-bit version increases performance, and improves scalability and resource utilization.
Support for Metadata in Identity Federation
You can now import and export SAML 2.0 metadata for Identity Federation configuration. This allows you to quickly configure the information about the Identity Federation configuration of Service Providers or Identity Providers, and to provide information about the Identity Federation configuration of the SSL VPN to Service Providers or Identity Providers.

• For more information, see Getting Started with Identity Federation (page 235).

Trace Support for Windows Access Client
To make troubleshooting tasks easier, the Access Client for Windows supports now traces. To configure traces, see Technical Note #7551.
CHAPTER 3

FEATURE OVERVIEW

This chapter provides an overview to the benefits you gain from the Stonesoft 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 20)
▶ Assessment (page 20)
▶ Authentication (page 21)
▶ Authorization (page 21)
▶ Access (page 22)
▶ Auditing (page 22)
▶ Abolishment (page 23)
Introduction

Stonesoft 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

Stonesoft 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 222).
Authentication

Stonesoft 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:

- **Stonesoft Challenge**: End-users receive a challenge code from the web portal and enter that along with their personal PIN code in the Stonesoft MobileID software installed, for example, on their mobile phone. MobileID then produces a one-time password for the log in.
- **Stonesoft 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.
- **Stonesoft 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.
- **Stonesoft Password**: End-users enter their password.
- **Stonesoft Synchronized**: End-users enter their personal PIN code in the Stonesoft MobileID software installed, for example, on their mobile phone. MobileID then produces a one-time password for the log in.
- **Stonesoft 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 128).

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 166).

**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 190), Getting Started with Tunnel Resources (page 204), and Getting Started with Standard Resources (page 180).

**Auditing**

The advanced auditing features in Stonesoft 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 Stonesoft SSL VPN can be further enhanced by sending the data to the Stonesoft 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 Getting Started with Monitoring the SSL VPN (page 246).

For more information on the logging and reporting features in the Stonesoft Management Center, see the main Administrator’s Guide.

**Related Tasks**

► Integrating the SSL VPN With the SMC (page 73)
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 226).
This chapter introduces the services that comprise the Stonesoft 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 26)
- Default Listening Ports (page 26)
- Administration Service (page 27)
- Access Point (page 27)
- Policy Service (page 28)
- Authentication Service (page 30)
- Directory Service and User Storage (page 31)
Introduction to System Services

The system services are illustrated below.

**Illustration 4.1  System Network**

It is recommended to locate the SSL VPN 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 Stonesoft 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 deployment network, see Default Listening Ports (page 277).

---

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

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

You publish all updates in the 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.

See Configuring Mirroring (page 79) for more information.

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.

Internal Cookies

You can define what kind of client data is sent as cookies in internal requests. Client data includes user ID, client IP, session ID and session ID cookie.

This is an example of what an internal cookie looks like in the HTTP request:

**Example** Cookie: WA_T=45; WA_UID=test; WA_WASID=0c351d862cea55cc; WA_AM=Stonesoft Password; WA_CLIP=192.168.139.1; WA_SEPO=443; WA_SSL=256; WA_INTERNAL_ID=3.0.25912196973801860.14762743034494641120710727875

To configure internal cookies, browse to Manage Resource Access → Global Resource Settings → Advanced.

Policy Service

The Policy Service is an important part of 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 Stonesoft 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

Portal Resources
- Citrix Metaframe Presentation Server
- Microsoft Sharepoint Portal Server 2003

Administration Resources
- 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 180).
Access Rules

Stonesoft 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 166), 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 232).

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 Stonesoft 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 Stonesoft 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 128) 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 Stonesoft 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 Stonesoft authentication-specific items are stored for the Stonesoft 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 75) and *Adding an External User Storage Location* (page 76).
CHAPTER 5

PLANNING

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

The following sections are included:

- Getting Started with Planning SSL VPN Deployment (page 34)
- Security Audit/Planning (page 34)
- User Management Strategy (page 35)
- Resource Access (page 37)
- Pre-Installation Checklist (page 38)
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:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital certificates</td>
<td>Electronic credentials (public keys), which are used to sign and encrypt data. Digital certificates provide the foundation of a PKI.</td>
</tr>
<tr>
<td>One or more certificate authorities (CAs)</td>
<td>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.</td>
</tr>
<tr>
<td>Certificate policy and practice statements</td>
<td>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.</td>
</tr>
<tr>
<td>Certificate repositories</td>
<td>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 Stonesoft SSL VPN Release Notes.</td>
</tr>
<tr>
<td>Certificate Revocation Lists (CRL)</td>
<td>Lists of certificates that have been revoked before reaching the scheduled expiration date.</td>
</tr>
</tbody>
</table>

**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.

Password Management

Stonesoft SSL VPN does not store passwords or encryption keys in unprotected configuration files, LDAP directories, or other system storage. The passwords are stored in the Directory Service in an 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”, “Åke”, or “Åke”. Stonesoft 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 Stonesoft 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 Stonesoft 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

<table>
<thead>
<tr>
<th>Check</th>
<th>Activity</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identify and resolve user management issues</td>
<td>Environment analyzed&lt;br&gt;Directory service secured&lt;br&gt;Password strategy in place&lt;br&gt;External user storage defined (optional)</td>
</tr>
<tr>
<td></td>
<td>Identify and resolve security issues</td>
<td>Public Key Infrastructure&lt;br&gt;Operating systems secured&lt;br&gt;File system secured&lt;br&gt;Shared resources secured&lt;br&gt;Physical environment secured&lt;br&gt;Auditing strategy in place&lt;br&gt;Backups and recovery strategies in place</td>
</tr>
<tr>
<td></td>
<td>Ensure that existing network has necessary power supplies, switches, and other network components</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perform time synchronization</td>
<td>Set the clock on the appliance through the basic Web Console (https://&lt;SSL VPN IP address&gt;:10000 if accessed directly through eth0).&lt;br&gt;If you are using a Virtual Appliance, ensure that the hosting platform does not overrule the Virtual Machine-specific time synchronization settings.</td>
</tr>
</tbody>
</table>
CHAPTER 6

GUI OVERVIEW

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

The following sections are included:

- Getting Started with SSL VPN Graphical User Interface (page 40)
- SSL VPN Administrator (page 40)
- SSL VPN Web Console (page 47)
- SSL VPN Application Portal (page 49)
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 SSL VPN Administrator is the web-based administration interface for setting up and managing SSL VPN features.

The basic features in 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. Log in 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 completing a basic working setup after the initial configuration. The section also contains instructions for getting started with the different features.

**Navigating in the SSL VPN Administrator**

The 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 42), Manage Accounts and Storage (page 43), Manage Resource Access (page 44), and Manage System (page 45). 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 system 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 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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Status</td>
<td>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 246).</td>
</tr>
<tr>
<td>User Sessions</td>
<td>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 250).</td>
</tr>
<tr>
<td>Log Viewer</td>
<td>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 251).</td>
</tr>
<tr>
<td>Diagnostics File</td>
<td>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 Support.</td>
</tr>
<tr>
<td>Logging</td>
<td>Manage settings for logging of all or specific servers in the system network. You can set log collection interval, debug mode, and which time zone to use for timestamps. For more information, see Configuring Logging (page 255).</td>
</tr>
<tr>
<td>License</td>
<td>View the contents of the current license.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Manage alerts used to notify administrators of different types of events. For more information, see Configuring Alert Notifications (page 252).</td>
</tr>
<tr>
<td>Reports</td>
<td>Generate reports containing statistics and run-time information on access, authentication, authorization, accounts, and system. For more information, see Generating Reports (page 254).</td>
</tr>
</tbody>
</table>
**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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Accounts</td>
<td>Add user accounts using the <strong>Add User Account</strong> 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 112).</td>
</tr>
<tr>
<td>User Linking</td>
<td>Create user accounts by linking from user storage. For more information on linking users, see Linking Users (page 114).</td>
</tr>
<tr>
<td>User Link Repair</td>
<td>Repair broken links used in User Linking. For more information on repairing user links, see Repairing User Links (page 115).</td>
</tr>
<tr>
<td>User Import</td>
<td>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 116).</td>
</tr>
<tr>
<td>User Groups</td>
<td>Add user groups using the <strong>Add User Group</strong> Wizard. To edit settings for a specific user group, you can search for registered user groups. For more information, see Adding User Groups (page 120).</td>
</tr>
<tr>
<td>User Storage</td>
<td>Add user storage locations using the <strong>Add User Storage Location</strong> 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 76).</td>
</tr>
<tr>
<td>Global User Account</td>
<td>Manage global default settings for all registered user accounts. The <strong>General Settings</strong> tab contain default account settings for logon to the Application Portal and Stonesoft authentication settings. Enable automatic and/or manual linking on the <strong>User Linking</strong> tab. Enable auto repair to update links to the directory service in the <strong>Auto Repair</strong> tab. For more information, see Managing Global User Account Settings (page 106).</td>
</tr>
<tr>
<td>Settings</td>
<td></td>
</tr>
<tr>
<td>Self Service</td>
<td>Self Service is used when some user administration tasks are allowed to be carried out by the end-user. Currently the following scenarios can be left to the end-user: <strong>Auto Activation</strong>, <strong>Forgotten Password</strong>, and <strong>Forgotten User Name</strong>. Self Service must be enabled and configured separately. For more information, see Managing Self Service (page 123).</td>
</tr>
</tbody>
</table>
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 Manage Resource Access: Left-side Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Resources</td>
<td>Use the <strong>Add Standard Resources</strong> Wizards to select standard resources from the list and to add standard resources. For more information, see <a href="#">Getting Started with Standard Resources</a> (page 180).</td>
</tr>
<tr>
<td>Web Resources</td>
<td>Add web resources using the <strong>Add Web Resource Host</strong> Wizard. To manage settings for a specific web resource host or path, use the + sign to display detailed resource information. For more information, see <a href="#">Creating Web Resources</a> (page 190).</td>
</tr>
<tr>
<td>Tunnel Resources</td>
<td>Add tunnel resources using the <strong>Add Tunnel Resource Host</strong> Wizard or <strong>Add Tunnel Resource Network</strong> Wizard. To manage settings for a specific tunnel resource host or path, use the + sign to display detailed resource information. For more information, see <a href="#">Creating Tunnel Resource Hosts</a> (page 206) and <a href="#">Creating Tunnel Resource Networks</a> (page 205).</td>
</tr>
<tr>
<td>Tunnel Sets</td>
<td>Add tunnel sets using the <strong>Add Tunnel Set</strong> Wizard. To edit settings for a tunnel set, select tunnel set in the list. For more information, see <a href="#">Creating and Modifying Tunnel Sets</a> (page 207).</td>
</tr>
<tr>
<td>Client Firewall</td>
<td>Add client firewalls consisting of Internet firewall configurations using the <strong>Add Internet Firewall Configuration</strong> 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.</td>
</tr>
<tr>
<td>Customized Resources</td>
<td>Add customized resources using the <strong>Add Customized Resource Host</strong> wizard. To manage settings for a specific customized resource host or, use the + sign to display detailed resource information.</td>
</tr>
<tr>
<td>Access Rules</td>
<td>Add access rules available for several resources and/or SSO domains using the <strong>Add Access Rule</strong> Wizard. To edit settings for an access rule, select access rule in the list. For more information, see <a href="#">Editing Access Rules</a> (page 168).</td>
</tr>
<tr>
<td>Application Portal</td>
<td>Add Application Portal items using the <strong>Add Application Portal Item</strong> Wizard. To edit settings for a specific item, select item in the list. For more information, see <a href="#">Getting Started with Application Portal Customizations</a> (page 90).</td>
</tr>
<tr>
<td>SSO Domains</td>
<td>Add SSO domains using the <strong>Add SSO Domain</strong> Wizard. To edit settings for a specific SSO domain, select SSO domain in the list. For more information, see <a href="#">Adding an SSO Domain</a> (page 232).</td>
</tr>
</tbody>
</table>
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 Manage System: Left-side Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Methods</td>
<td>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 132).</td>
</tr>
<tr>
<td>Certificates</td>
<td>Add, edit or delete Certificate Authorities, Server Certificates and Client Certificates. For more information, see Getting Started with Certificates (page 152).</td>
</tr>
<tr>
<td>Abolishment</td>
<td>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 226).</td>
</tr>
</tbody>
</table>
### Table 6.4 Manage System: Left-side Menu Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assessment</strong></td>
<td>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 222).</td>
</tr>
<tr>
<td><strong>RADIUS Configuration</strong></td>
<td>Add RADIUS clients using the Add RADIUS Client Wizard. To edit settings for a specific RADIUS client, select the client from 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 137).</td>
</tr>
<tr>
<td><strong>Notification Settings</strong></td>
<td>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 252).</td>
</tr>
<tr>
<td><strong>Device Definitions</strong></td>
<td>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 218).</td>
</tr>
<tr>
<td><strong>Delegated Management</strong></td>
<td>Manage administrative roles with different privileges and responsibilities. For more information, see Configuring Delegated Management (page 122).</td>
</tr>
<tr>
<td><strong>Access Points</strong></td>
<td>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 27).</td>
</tr>
<tr>
<td><strong>Policy Services</strong></td>
<td>Add Policy Services using the Add Policy Service Wizard. To edit settings for a specific Policy Service, select Policy Service from the list. Click the Manage Global Policy Service Settings link to edit default global communication settings. For more information, see Policy Service (page 28).</td>
</tr>
<tr>
<td><strong>Authentication Services</strong></td>
<td>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 144).</td>
</tr>
<tr>
<td><strong>Administration Service</strong></td>
<td>Manage internal communication settings (in the system network) and external communication settings (with the client). For more information, see Administration Service (page 27).</td>
</tr>
<tr>
<td><strong>Directory Service</strong></td>
<td>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 75).</td>
</tr>
</tbody>
</table>
The Web Console allows you to configure basic operating-system-level settings for the Stonesoft SSL VPN appliance, such as configuring network interfaces, enabling IP address pool, and configuring routing.

For more information about configuring settings in the Web Console, see Getting Started With Working in the Web Console (page 52).

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 with the SMC. For more information, see Configuring System Settings (page 60).

The following configuration options are available in the System settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Password</td>
<td>Define the new administrator password for the appliance. See Changing the Admin Password in the Web Console (page 60).</td>
</tr>
<tr>
<td>Backup Management</td>
<td>Create, restore, and delete SSL VPN backups. See Backing up the SSL VPN in the Web Console (page 266).</td>
</tr>
<tr>
<td>Initial Contact</td>
<td>Make initial contact with the Stonesoft Management Server to integrate the SSL VPN with the SMC. On this page you can also switch SSL VPN to standalone mode. See Integrating the SSL VPN With the SMC (page 73).</td>
</tr>
<tr>
<td>Mirrored Pair</td>
<td>Check the current appliance configuration, define the mode of the appliance, and download a CA certificate. See Getting Started with Configuring Mirroring (page 80).</td>
</tr>
<tr>
<td>Non-interactive SSH</td>
<td>Configure the non-interactive SSH connection between the nodes for the configuration of OpenDJ LDAP Service Mirroring. See Configuring Non-Interactive SSH (page 61).</td>
</tr>
<tr>
<td>OpenDJ LDAP Service</td>
<td>Check and configure the integrated OpenDJ LDAP directory service. See Configuring OpenDJ LDAP Service Settings (page 63).</td>
</tr>
</tbody>
</table>
Chapter 6  GUI Overview

Networking

Use the Networking settings to define network configuration and to check access logs. For more information, see Configuring Network Settings (page 53).

The following configuration options are available in the Networking settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Log</td>
<td>Check the latest access logs of the appliance.</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>View and edit the rules for the integrated appliance firewall.</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Define the network configuration of the appliance. The settings include</td>
</tr>
<tr>
<td></td>
<td>the setting of Network Interfaces, Routing and Gateways, Hostname and DNS</td>
</tr>
<tr>
<td></td>
<td>Client, Host Address, and the activation of IP address pool functionality on</td>
</tr>
<tr>
<td></td>
<td>OS level.</td>
</tr>
</tbody>
</table>

Hardware

Use the Hardware settings to set system time and change the time zone. For more information see Configuring Hardware Settings (page 52).

- Set the system time/hardware time, and change the time zone of the appliance.
SSL VPN Application Portal

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

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 Stonesoft 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.
The Web Console allows you to configure hardware settings, network settings, and other system settings for the SSL VPN appliance.

The following sections are included:

- Getting Started With Working in the Web Console (page 52)
- Configuring Hardware Settings (page 52)
- Configuring Network Settings (page 53)
- Configuring System Settings (page 60)
- Configuring OpenDJ LDAP Service Settings (page 63)
- Configuring Services (page 66)
Getting Started With Working in the Web Console

Prerequisites: None

The Web Console allows you to configure settings for the SSL VPN appliance, such as configuring network interfaces and configuring routing, managing services, and activating features.

Logging in to the Web Console

- **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 in Web Console>.

Configuring Hardware Settings

Prerequisites: None

Initially you configure the hardware settings when you install the SSL VPN as described in the SSL VPN Appliance Installation Guide. You can reconfigure the hardware settings in the Web Console.

Setting the System Time

- **To set the system time**
  1. Browse to **Hardware → System Time**.
  2. Change the time in either the System Time (operating system) or the Hardware Time (internal clock) section and click **Apply** or **Save**.
  3. Synchronize the times by clicking either **Copy from hardware time** or **Copy from system time**.
  4. Select the correct **Time Zone** and click **Save**.
Configuring Network Settings

Prerequisites: None

Initially you configure the basic network settings when you install the SSL VPN as described in the SSL VPN Appliance Installation Guide. You can add network interfaces and reconfigure the network settings in the Web Console.

Adding Network Interfaces

To add a network interface

1. Browse to Networking → Network Configuration.
2. Click Network Interfaces. The Network Interfaces page opens.
3. In the Interfaces Activated at Boot Time section, click Add a new interface or click the name of an existing interface to edit it.
4. Configure the settings in the Boot Time Interface Parameters section as described below:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Select how the IP address is assigned for the interface. If you select Static, enter the IP address.</td>
</tr>
<tr>
<td>Netmask (Static IP address only)</td>
<td>Enter the netmask address.</td>
</tr>
<tr>
<td>Broadcast (Static IP address only)</td>
<td>Enter the broadcast address for the network to which the interface belongs.</td>
</tr>
<tr>
<td>Activate at Boot</td>
<td>Select whether the interface is activated automatically when the appliance boots up.</td>
</tr>
</tbody>
</table>

5. Click Create to save the interface configuration without activating it, or click Create and Apply to save and activate the interface configuration.

Editing Network Interfaces

To edit a network interface

1. Browse to Networking → Network Configuration.
2. Click Network Interfaces. The Network Interfaces page opens.
3. In the Interfaces Activated at Boot Time section, click the name of an existing interface to edit it.
4. Configure the settings in the Boot Time Interface Parameters section as described below:

Table 7.1 Boot Time Interface Parameters

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the interface.</td>
</tr>
</tbody>
</table>
5. Click **Save** to save the interface configuration without activating it, or click **Save and Apply** to save and activate the interface configuration.

### Adding Virtual Interfaces to an Interface

Virtual interfaces allow you to add additional IP addresses to an interface.

**▼ To add virtual interfaces to an interface**

1. Click the interface name in the **Interfaces Activated at Boot Time** table. The interface opens for editing.

2. Click **Add Virtual Interface**.

3. Configure the settings in the **Boot Time Interface Parameters** section as described below:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name that is appended to the interface name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Select how the IP address is assigned for the interface. If you select <strong>Static</strong>, enter the IP address.</td>
</tr>
<tr>
<td>Netmask (Static IP address only)</td>
<td>Enter the netmask address.</td>
</tr>
<tr>
<td>Broadcast (Static IP address only)</td>
<td>Enter the broadcast address for the network to which the interface belongs.</td>
</tr>
<tr>
<td>Activate at Boot</td>
<td>Select whether the interface is activated automatically when the appliance boots up.</td>
</tr>
</tbody>
</table>
4. Click **Create** to save the interface configuration without activating it, or click **Create and Apply** to save and activate the interface configuration.

**Defining the Default Router**

The default router is the next-hop router for outgoing traffic on the selected interface.

▶ **To define the default router**

1. Browse to **Networking → Network Configuration**.
2. Click **Routing and Gateways**.
3. Define the Default Router in one of the following ways:
   - Select **None (or from DHCP)** if the IP address of the default gateway is dynamically assigned.
   - Select **Gateway** and enter the IP address of your gateway.
4. Select the interface through which the gateway **Device** is reached.
5. Click **Save**.

**What's Next?**

▶ If you want to define other routes, proceed to Defining Permanent Routes (page 55).
▶ Otherwise, click **Return to Network Configuration** to return to the Network Configuration page and click **Apply Configuration**.

**Defining Permanent Routes**

The routes that you add in the Routing Configuration Activated at Boot Time section are permanent routes that are stored in the engine's configuration files. The routes are always active, but can be deleted if they are no longer needed. You can create two types of permanent routes:

- **Static Routes**: routes to networks that are not directly connected to the engine.
- **Local Routes**: routes to directly-connected networks.

**Caution –** Activating an invalid route may make the SSL VPN inaccessible through the network and prevent access to the Web Console. Ensure that any routes you define are valid for your network environment.
To define a permanent route

1. Browse to Networking→Network Configuration.

2. Click Routing and Gateways.

3. Configure the following settings in the Routing Configuration Activated at Boot Time section as described below:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Enter the name of the interface used by the route.</td>
</tr>
<tr>
<td>Network</td>
<td>Enter the IP address of the network to which the route belongs.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Enter the netmask.</td>
</tr>
<tr>
<td>Gateway (Static route only)</td>
<td>Enter the next-hop gateway through which outgoing traffic is routed.</td>
</tr>
</tbody>
</table>

4. Click Save.

5. Repeat Step 3 to Step 4 to add any other permanent routes.

6. Click Return to Network Configuration. You are returned to the Network Configuration page.

7. Click Apply Configuration. The route is activated.

Related Tasks

▶ Deleting Active Routes (page 57)

Defining Temporary Routes

The routes that you add in the Create Active Routes section are temporary routes that are activated immediately. For example, you can create a temporary route for testing, or for temporarily creating connectivity to a particular network. Temporary routes are active until you manually delete them or until the next time you apply the network configuration or reboot the appliance.

Caution – Activating an invalid route may make the SSL VPN inaccessible through the network and prevent access to the Web Console. Ensure that any routes you define are valid for your network environment.

To define a temporary route

1. Browse to Networking→Network Configuration.

2. Click Routing and Gateways.

3. Configure the following settings in the Create Active Route section as described below:

<table>
<thead>
<tr>
<th>Table 7.2 Create Active Route Settings</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Destination</td>
<td>Select whether the route uses the Default Route for the selected interface, or enter the IP address of the network to which the route belongs.</td>
</tr>
</tbody>
</table>
Table 7.2  Create Active Route Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netmask for Destination</td>
<td>Select whether the route uses the Default Netmask for the selected interface or enter the netmask.</td>
</tr>
<tr>
<td>Route Via</td>
<td>Select the Network Interface through which outgoing traffic is routed, or select Gateway and enter the IP address of the next-hop gateway through which outgoing traffic is routed.</td>
</tr>
</tbody>
</table>

4. Click Create. The temporary route is created and activated.

Related Tasks

- Deleting Active Routes (page 57)

Deleting Active Routes

You can delete currently active permanent and temporary routes that are no longer needed. Deleting an active route deactivates the route. Deleting a permanent route also removes the route from the engine’s configuration files.

To delete active routes

1. Browse to Networking→Network Configuration.
2. Click Routing and Gateways.
3. Select the route(s) that you want to delete in the Active Routes section.
4. Click Delete Selected Routes.
   • The selected route(s) are removed from the Active Routes table.
   • Temporary routes are immediately disabled.
5. (Permanent routes only) Click Return to Network Configuration. You are returned to the Network Configuration page.
6. (Permanent routes only) Click Apply Configuration. The route(s) are permanently deleted.
Chapter 7  Working in the Web Console

Configuring the Hostname and DNS Client

The Hostname and DNS Client settings allow users to access services provided by the SSL VPN using domain names as well as IP addresses in the URL.

To configure the Hostname and DNS Client
1. Browse to Networking → Network Configuration.
2. Click Hostname and DNS Client.
3. Enter the Hostname of the SSL VPN appliance.
4. Enter the Resolution Order for DNS requests.
5. Enter the IP address(es) of the DNS Servers used by the SSL VPN appliance.
6. (Optional) Select Listed and enter the Search Domains in the text box below.
7. Click Save. You are returned to the Network Configuration page.
8. Click Apply Configuration.

Configuring Host Addresses

Host addresses statically map the specified hostnames to IP addresses. This allows the SSL VPN to resolve the specified hostnames to IP addresses without querying a DNS server.

To configure Host Addresses
1. Browse to Networking → Network Configuration.
2. Click Host Addresses.
3. Click Add a New Host Address or click the IP Address of an existing host to edit it.
4. Enter the IP Address and the Hostname.
5. Click Create after adding a new host address or click Save after editing an existing host address.
6. Click Return to Network Configuration.
7. Click Apply Configuration.
Editing User Firewall Rules

The firewall rules for the SSL VPN appliance are automatically generated based on the interface configuration of the appliance and cannot be edited. You can add and edit user firewall rules using the IPTables rule syntax. The user firewall rules are applied after the appliance firewall rules.

To edit user firewall rules

1. Browse to Networking → Firewall Configuration. The existing firewall rules and user firewall rules are displayed.

2. Edit the existing user firewall rules or enter new user firewall rules using the IPTables syntax.

   Example: `iptables -A INPUT -m state --state NEW -i eth0 -p tcp --dport 5678 -j allownlog`

3. Click Update Rules. The changes to the user firewall rules are applied.
Some of the branches of the System settings are discussed in more detail in other sections:

- For more information about working with backups, see Getting Started With Backing up and Restoring SSL VPN (page 266).
- For information about making initial contact with a Stonesoft Management Server, see Integrating the SSL VPN With the SMC (page 73).
- For information about mirrored pair configuration, see Getting Started with Configuring Mirroring (page 80).
- For more information about configuring options in the OpenDJ LDAP Service branch, see Configuring OpenDJ LDAP Service Settings (page 63).
- For information about using the Public Key Infrastructure (PKI) Management tools in the Web Console, see Managing Certificates in the Web Console (page 156).
- For more information about upgrading the SSL VPN appliance, see Getting Started With Upgrading SSL VPN (page 272).
- For more information about options in the Services branch, see Configuring Services (page 66).

**Changing the Admin Password in the Web Console**

Changing the password for the admin user in the Web Console sets the same password for both the Web Console and the SSL VPN Administrator.

Note – If you have previously set a different password for the SSL VPN Administrator, you must set the SSL VPN Administrator password again after changing the admin password in the Web Console. See Changing the Admin Password in the SSL VPN Administrator (page 72)

**To change the admin password in the Web Console**

1. Browse to System → Admin Password.
2. Enter and confirm the new password.
3. Click Change.
Configuring Non-Interactive SSH

Non-interactive SSH is used for communication between the nodes for OpenDJ LDAP Service Mirroring. To enable non-interactive SSH between the nodes, a pair of cryptographic keys must be generated and distributed to the nodes. See Technical Note #7532 for more information about configuring OpenDJ LDAP Service Mirroring.

- The SSH daemon must be enabled before you can configure non-interactive SSH. See Enabling/Disabling the SSH Daemon (page 67).
- You must be able to connect to the Web Console of both nodes from the same workstation.

To configure non-interactive SSH
1. Log in to the Web Console on the first node.
2. Browse to System → Non-Interactive SSH.
3. Click Generate Local Public Key. A public key is generated and displayed.
4. Copy the local public key to the clipboard.
5. Log in to the Web Console on the second node.
6. Browse to System → Non-Interactive SSH.
7. Click Import Remote Public Key. The Import Cryptographic Key page opens.
8. Paste the public key from the first node into the Key field and click Import.

What's Next?
- Repeat these steps on the second node.

Changing the Root User Password

The root user password is used to access the command line of the SSL VPN appliance as the root user.

To change the root password for the appliance
1. Browse to System → Root Password.
2. Enter and confirm the new password.
3. Click Change.
Collecting SgInfo in the Web Console

Collecting sgInfo creates a .zip file that contains the specified information about the SSL VPN system. Collecting sgInfo is intended for troubleshooting purposes, and is only necessary when requested by Stonesoft support.

To collect sgInfo in the Web Console
1. Browse to System → SgInfo Management.

2. (Optional) Select additional information to include in the sgInfo file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch a backup with <code>--include spool</code> and include it in sgInfo</td>
<td>Creates a backup that includes files from the /spool directory and includes the backup in the sgInfo file.</td>
</tr>
<tr>
<td>Include in sginfo.txt the list of files of other filesystems (chroot)</td>
<td>Includes file listings of duplicate mount points in the sgInfo file.</td>
</tr>
<tr>
<td>Include core dumps newer than 30 days</td>
<td>Includes any core dump files that are newer than 30 days old in the sgInfo file.</td>
</tr>
<tr>
<td>Include all core dumps</td>
<td>Includes all core dump files in the sgInfo file.</td>
</tr>
</tbody>
</table>

Note – Including a backup or core dump files may produce a very large sgInfo file.

3. Click Create sgInfo. An sgInfo file containing the selected information is created.
4. (Optional) Click Save to save the file on your workstation.

What’s Next?
► Provide the sgInfo file to Stonesoft support for troubleshooting purposes.
Configuring OpenDJ LDAP Service Settings

Prerequisites: None

The OpenDJ LDAP Service settings allow you to check and configure the integrated OpenDJ LDAP directory service. To configure OpenDJ LDAP service mirroring, see Technical Note #7532.

Monitoring the Status of the OpenDJ LDAP Service

To monitor the status of the OpenDJ LDAP service

Browse to System → OpenDJ LDAP Service. The OpenDJ Server status is displayed.

OpenDJ LDAP Service Configuration

```
--- Server Status ---
Server Run Status: Started
Open Connections: 0

--- Server Details ---
Site Name: NO-SSL_VPN
Administration Users: cn=dnslx,ou=People,dc=stonegate
Installation Path: /opt/OpenDJ
Version: OpenDJ 2.4.1
Java Version: (*)
Administration Connector: Port 4444 (LDAP)

--- Connection Handlers ---
Address:Port   Protocol: State
---------------------------------------------
-               : LDAP: Disabled
0.0.0.0:1632   : LDAP: Disabled
0.0.0.0:1638   : LDAP (allows StartTLS): Enabled
0.0.0.0:1636   : LDAPS: Enabled
0.0.0.0:1693   : JMX: Disabled

--- Data Sources ---
Base DN: dc=stonegate
Entries: (*)
Replication: Disabled
```

* Information only available if you provide valid authentication information when launching the status command.

Related Tasks

► Restarting Services in the Web Console (page 66)
► Enabling/Disabling Services in the Web Console (page 66)
Viewing the OpenDJ Log File Settings

To view the OpenDJ log file settings
1. Browse to System→OpenDJ LDAP Service.
2. Scroll down to the OpenDJ Log File Settings section.
3. Enter the LDAP Admin Password that the SSL VPN uses to connect to the OpenDJ LDAP Directory Service and click Display. The current OpenDJ log file settings are displayed.

Configuring OpenDJ Log File Settings

By default, a maximum of ten OpenDJ log files with a file size of 100 megabytes are stored.

To configure OpenDJ log file settings
1. Browse to System→OpenDJ LDAP Service.
2. Scroll down to the Change OpenDJ Log File Settings section.
3. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File Retention Count</td>
<td>Enter the maximum number of log files to store. If you do not enter a value, the previously configured value is used.</td>
</tr>
<tr>
<td>Log File Retention Size</td>
<td>Enter the maximum file size in megabytes. If you do not enter a value, the previously configured value is used.</td>
</tr>
<tr>
<td>LDAP Admin Password</td>
<td>Enter the LDAP administrator password that the SSL VPN uses to connect to the OpenDJ LDAP Directory Service. If you do not enter a password, the default LDAP administrator password is used.</td>
</tr>
</tbody>
</table>

4. Click Change.
Changing the OpenDJ LDAP Admin Password

The SSL VPN uses the OpenDJ LDAP admin password to connect to the OpenDJ LDAP Directory Service.

Note – If you have configured OpenDJ LDAP service mirroring, you must change the OpenDJ LDAP admin password on both nodes. See Technical Note #7532 for more information about configuring OpenDJ LDAP Service Mirroring.

To change the OpenDJ LDAP admin password

1. Browse to System→OpenDJ LDAP Service.
2. Scroll down to the Change Password for Superuser in OpenDJ LDAP Service section.
3. Enter the Current Password.
4. Enter and confirm the New Password.
5. (Optional) Enter the OpenDJ Port if the OpenDJ service uses a port other than the default port (1389).
6. Click Change Password.
Configuring Services

Prerequisites: None

The options on the Services page allow you to manage services in the following ways:

- Reboot the appliance. See Rebooting the SSL VPN Appliance.
- Enable, disable, and restart services separately. See Restarting Services in the Web Console and Enabling/Disabling Services in the Web Console.
- Enable or disable the SSH daemon. See Enabling/Disabling the SSH Daemon (page 67).
- Activate OATH (Open AuTHentication). See Activating OATH in the Web Console (page 139).
- Require the use of LDAPS for the internal LDAP server. See Requiring the Use of LDAPS for the Internal LDAP Server (page 67).
- Select the cryptographic operating mode. See Configuring the Cryptographic Operating Mode (page 67).
- Enable or disable syslog logging. See Enabling/Disabling Syslog Logging (page 67).
- Select the configuration file for Hardware Assessment Plugin. See Selecting the Hardware Assessment Plug-In Configuration File (page 226).

Rebooting the SSL VPN Appliance

▼ To reboot the SSL VPN appliance

2. Click Reboot. You are prompted to confirm that you want to reboot the SSL VPN appliance.
3. Click Yes. The SSL VPN appliance reboots and you are disconnected from the Web Console.
   • To continue working in the Web Console, you must log in again. See Logging in to the Web Console (page 52).

Enabling/Disabling Services in the Web Console

▼ To enable/disable services in the Web Console

2. Select the service(s) you want to enable/disable in the Manage Stonesoft SSL VPN Services section.
3. Click Enable or Disable. The selected service(s) are enabled or disabled.

Restarting Services in the Web Console

▼ To restart services in the Web Console

2. Select the service(s) you want to restart in the Manage Stonesoft SSL VPN Services section.
3. Click Restart. The selected service(s) are restarted.
Enabling/Disabling the SSH Daemon

▼ To enable/disable the SSH daemon
2. Select or deselect Enable SSH Daemon in the Access Control section.

Note – We recommend that you enable the SSH access only when needed and then disable the access again when you are done.

3. Click Apply. The SSH daemon is enabled or disabled.

Requiring the Use of LDAPS for the Internal LDAP Server

▼ To require the use of LDAPS for the internal LDAP server
2. Scroll down to the LDAP Internal Servers section.
3. Select Force LDAPS.
4. Click Apply. LDAPS is always used in communications with the internal LDAP server after the Force LDAPS setting is applied.

Configuring the Cryptographic Operating Mode

The cryptographic operating mode defines which cryptographic algorithms are available in the SSL VPN. Configuring the cryptographic operating mode is not recommended unless you are required to do so to comply with a specific regulatory standard.

▼ To configure the cryptographic operating mode
2. Scroll down to the SSL/Crypto Libraries Operating Mode section.
3. Select one of the following options:
   ▪ Normal Mode: The default mode for the SSL VPN. Leave this option selected unless you have a specific need to select one of the other options.
   ▪ FIPS: The SSL VPN uses a FIPS-compatible version of the OpenSSL cryptographic library.
   ▪ GOST: The SSL VPN uses the certified CryptoPro engine for GOST cryptographic algorithms.
4. Click Apply.

Enabling/Disabling Syslog Logging

▼ To enable/disable Syslog logging
2. Scroll down to the Log Server section.
3. Select or deselect Enable Syslog Logging.
4. Click Apply. Syslog logging is enabled or disabled.
INITIAL CONFIGURATION

In this section:

Configuring the System After Installation - 71
Configuring Mirroring - 79
Customizing the Application Portal - 89
CHAPTER 8

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 72)
- Changing the Admin Password in the SSL VPN Administrator (page 72)
- Configuring a Directory Service (page 75)
- Adding an External User Storage Location (page 76)
- Further Configuration Steps (page 78)
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 Stonesoft Management Center (SMC) to monitor the SSL VPN gateway.

---

**Configuration Overview**

1. *(Recommended)* Set a unique password for the admin user in the SSL VPN Administrator as explained in *Changing the Admin Password in the SSL VPN Administrator*.

2. *(Optional)* Configure the SMC to monitor the SSL VPN gateway as explained in *Integrating the SSL VPN With the SMC* (page 73).

3. Configure an external Directory Service to work with SSL VPN. See *Configuring a Directory Service* (page 75).

4. Add an external user storage to the SSL VPN. See *Adding an External User Storage Location* (page 76).

---

**What's Next?**

- If you want to use the SSL VPN with the SMC, begin by *Integrating the SSL VPN With the SMC* (page 73).
- Otherwise, begin by *Configuring a Directory Service* (page 75).

---

**Changing the Admin Password in the SSL VPN Administrator**

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

---

By default, the same password is used to log in to the Web Console and the SSL VPN Administrator as the admin user. We recommend changing the SSL VPN Administrator admin password to a unique password.

**▼ To change the Admin Password in the SSL VPN Administrator**

1. Log in to the SSL VPN Administrator and scroll down to the bottom of the page.

2. Click **Manage Settings**. The Settings page opens.

3. Scroll down to the Super Administrator Password section.

4. *(Optional)* Deselect **Enable Password Policy** if you do not want to require the password to meet specific security requirements.

5. Enter the **Current Password**.

6. Enter and confirm a secure **New Password**.
7. Click Save. To activate the changes, click **Publish** at the top of the page.

**Note** – If you change the password for the admin user in the Web Console after changing the password for the admin user in the SSL VPN Administrator, the same password is set for the admin user in both the Web Console and the SSL VPN Administrator. You must set the SSL VPN Administrator admin password again after changing the admin password in the Web Console.

---

**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 73).
2. Save the initial configuration information in the SMC. See *Saving the Initial Configuration* (page 74).
3. Make an initial contact between the appliance and the Management Server. See *Making Initial Contact* (page 74).
4. Import the gateway's license into the SMC. See *Importing SSL VPN License Into the SMC* (page 74).
5. Apply the configuration to the SSL VPN element you created in the SMC. See *Applying the Configuration* (page 74).

**Creating an SSL VPN Gateway Element**

**To create an SSL VPN Gateway Element**

1. Log in to the 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**.

---

*Integrating the SSL VPN With the SMC*  73
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 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 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 SSL VPN Administrator interface, browse to **Manage System → Directory Service**. The Manage Directory Service page opens.
2. Configure the following Directory Service server settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Host</td>
<td>The IP address of the primary Directory Service server.</td>
</tr>
<tr>
<td>Secondary Host</td>
<td>The IP address of the backup Directory Service server.</td>
</tr>
<tr>
<td>Port</td>
<td>The listening port of the Directory Service server.</td>
</tr>
<tr>
<td>Password</td>
<td>The administrator password of the Directory Service server</td>
</tr>
<tr>
<td>Location DN</td>
<td>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</td>
</tr>
<tr>
<td>Enable change of directory service type</td>
<td>Select this to change the Directory Service type.</td>
</tr>
<tr>
<td>Directory Service Type</td>
<td>The type of directory service used in your environment.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>*(Optional)*Use the SSL protocol for the communication with the Directory Service</td>
</tr>
</tbody>
</table>

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 one of the following options to complete the configuration:
   - **Yes**: The changes to the Directory Service settings are confirmed.
   - **Yes But Copy Contents of Current Into New One**: The contents of the current Directory Service server are copied to the new Directory Service server and the changes to the Directory Service settings are confirmed.
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.
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:

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

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:

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

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 79).
• To set up access to resources, see Daily Management (page 103).
This chapter describes how to set up mirroring between two Stonesoft SSL VPN appliances.

The following sections are included:

- Getting Started with Configuring Mirroring (page 80)
- Preparing for Mirroring (page 81)
- Configuring Basic System Services for Mirroring (page 81)
- Configuring Administrator Web Resources for Mirroring (page 84)
- Setting Up the Administrator Service for Mirroring (page 85)
- Setting Up Registered Authentication Method Servers (page 85)
- Setting Up Appliances as Primary and Secondary (page 86)
- Configuring Server Pool Monitoring Agents (page 87)
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, a Stonesoft Firewall/VPN 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 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.

When mirroring is used with Stonesoft SSL VPN, LDAP server information is not mirrored between the appliances and is stored only on the primary appliance. You must either use the internal OpenDJ user database for user storage, or configure an external User Storage. If you use the internal OpenDJ user database, configure mirroring as described in Technical Note #7532. If you use an external User Storage, OATH must be either disabled in the Web Console or configured to use an external database as described in Technical Note #5342.

Configuration Overview

1. Set up the appliances so that they are ready for mirroring. See Preparing for Mirroring (page 81).
2. Configure the Policy, Authentication, and Access Point services. See Configuring Basic System Services for Mirroring (page 81).
3. Configure remote administrator access. See Configuring Administrator Web Resources for Mirroring (page 84).
4. Complete the configuration by setting up the SSL VPN Administrator. See Setting Up the Administrator Service for Mirroring (page 85).
6. Configure the network-level settings and pair the appliances together. See Setting Up Appliances as Primary and Secondary (page 86).
Preparing for Mirroring

Note – If you use the internal OpenDJ user database, prepare for mirroring as described in Technical Note #7532.

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 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. Connect the appliances together through their dedicated interfaces.

4. 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. Browse to Manage System→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

Note – If you use an external User Storage, make sure that OATH is either disabled in the Web Console or configured to use an external database as described in Technical Note #5342 before you begin these steps.

To configure the Authentication Service for mirroring
1. Browse to Manage System—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. Browse to Manage System—Access Points in the left-hand menu.
2. Enter a Display Name for the Access Point.
3. Click the IP address 127.0.0.1 under Internal Host.
4. Enter 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:

<table>
<thead>
<tr>
<th>Example Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The dedicated interface IP address of the primary appliance.</td>
</tr>
<tr>
<td>Port</td>
<td>16972</td>
</tr>
<tr>
<td>Server Certificate</td>
<td>None Selected</td>
</tr>
<tr>
<td>Type</td>
<td>Load Balance</td>
</tr>
</tbody>
</table>

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

Note – Make sure 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. Enter a Display Name for the Access Point.

3. Enter the dedicated interface IP address of the secondary appliance in the Internal Host field.

4. Enter 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:

<table>
<thead>
<tr>
<th>Example Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The dedicated interface IP address of the secondary appliance.</td>
</tr>
<tr>
<td>Port</td>
<td>16972</td>
</tr>
<tr>
<td>Server Certificate</td>
<td>None Selected</td>
</tr>
<tr>
<td>Type</td>
<td>Load Balance</td>
</tr>
</tbody>
</table>

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. Browse to Manage System → 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 84).
- Otherwise, proceed to Setting Up the Administrator Service for Mirroring (page 85).

---

**Configuring Administrator Web Resources for Mirroring**

To use the 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**


2. Change the **Host** IP address of the resource for the 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


2. Select the authentication method for which the Authentication Method Server is set up (Stonesoft Web, Stonesoft Challenge, Stonesoft Synchronized, Stonesoft Mobile Text, or Stonesoft 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):

<table>
<thead>
<tr>
<th>Example Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>The display name of the primary/secondary appliance.</td>
</tr>
<tr>
<td>Host</td>
<td>The dedicated interface IP address of the primary/secondary appliance.</td>
</tr>
<tr>
<td>Port</td>
<td>18123</td>
</tr>
</tbody>
</table>

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 128).

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. Browse to Manage System→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 265)). 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 Stonesoft 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 Stonesoft Monitoring Agent daemon:
   ```
   msvc -d sgagentd
   ``
4. As the default permissions of sgagent.conf do not allow editing, make the file editable:
   ```
   /usr/lib/stonesoft/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 Administrator’s Guide.
7. Save your changes with command: wq
8. Restart the Stonesoft 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 Administrator’s Guide.
CHAPTER 10

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 90)
- Working with Customization Files (page 91)
- Customizing Application Portal Text (page 93)
- Customizing Application Portal Images (page 94)
- Customizing Application Portal Colors and Layout (page 95)
- Customizing HTML Templates (page 96)
- Customizing the Stonesoft Web Authentication Script (page 101)
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 Stonesoft 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 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 91).

2. Follow the general workflow outlined in Editing or Replacing Customization Files (page 92) to make the customizations. Check the task-specific file locations and names from the following sections:
   - Customizing Application Portal Text (page 93)
   - Customizing Application Portal Images (page 94)
   - Customizing Application Portal Colors and Layout (page 95)
   - Customizing HTML Templates (page 96)
   - Customizing the Stonesoft Web Authentication Script (page 101)
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 10.1 Customization Options

<table>
<thead>
<tr>
<th>What you Can Customize</th>
<th>How to do It</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Portal labels and text</td>
<td>Edit the text. See <a href="#">Customizing Application Portal Text</a> (page 93)</td>
<td>Multiple. Refer to the instructions for details.</td>
</tr>
<tr>
<td>Logon page text or buttons</td>
<td>Edit individual template files. See <a href="#">Customizing HTML Templates</a> (page 96).</td>
<td>Multiple. Refer to the instructions for details.</td>
</tr>
<tr>
<td>Logon page background</td>
<td>Replace the current background image. See <a href="#">Customizing Application Portal Images</a> (page 94).</td>
<td>ssl_vpn_title.img</td>
</tr>
<tr>
<td>Logon page colors and fonts</td>
<td>Edit the style sheet for logon pages. See <a href="#">Customizing Application Portal Colors and Layout</a> (page 95).</td>
<td>common.css</td>
</tr>
<tr>
<td>Application Portal logo</td>
<td>Replace the standard Stonesoft logo. See <a href="#">Customizing Application Portal Images</a> (page 94).</td>
<td>stonesoft_logo.png</td>
</tr>
<tr>
<td>Application Portal resource icons</td>
<td>Replace the images used. See <a href="#">Customizing Application Portal Images</a> (page 94).</td>
<td>[symbol_color].gif</td>
</tr>
<tr>
<td>Application Portal colors and fonts</td>
<td>Edit the Application Portal style sheet. See <a href="#">Customizing Application Portal Colors and Layout</a> (page 95).</td>
<td>access_portal.css</td>
</tr>
<tr>
<td>Application Portal Online Help page colors and fonts</td>
<td>Edit the Application Portal Online Help page style sheet. See <a href="#">Customizing Application Portal Colors and Layout</a> (page 95).</td>
<td>default.css</td>
</tr>
<tr>
<td>Application Portal Online Help page contents</td>
<td>Edit the Online Help HTML page. See <a href="#">Customizing Application Portal Colors and Layout</a> (page 95).</td>
<td>access_portal_help.html</td>
</tr>
<tr>
<td>Stonesoft Web authentication applet graphics</td>
<td>Replace the current skin. See <a href="#">Customizing Application Portal Images</a> (page 94).</td>
<td>WebSkin.zip</td>
</tr>
<tr>
<td>Stonesoft Web authentication applet text, layout, and behavior</td>
<td>Edit the parameters explained in <a href="#">Customizing the Stonesoft Web Authentication Script</a> (page 101).</td>
<td>Web.js</td>
</tr>
</tbody>
</table>
To edit or replace a customization file
1. Log on to the 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 10.1).
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 92).
2. Modify the text in relevant parts in the files described in the table below:

Table 10.2 Text Customization Options

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authAD.txt</td>
<td>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.</td>
</tr>
<tr>
<td>authselect.txt</td>
<td>The heading for the Select Authentication Method page.</td>
</tr>
</tbody>
</table>
Table 10.2  Text Customization Options (Continued)

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authweb.txt</td>
<td>The name of the Stonesoft Web authentication method. This is used in JavaScript dialogs that explain how to accept the Stonesoft Web ActiveX or Java applet.</td>
</tr>
<tr>
<td>company.txt</td>
<td>The name of your organization. Appears in the application portal.</td>
</tr>
<tr>
<td>company_about_url.txt</td>
<td>The link to information about your organization.</td>
</tr>
<tr>
<td>company_contact_url.txt</td>
<td>The link to your organization’s contact information.</td>
</tr>
<tr>
<td>copyright.txt</td>
<td>Copyright notice.</td>
</tr>
<tr>
<td>portal.txt</td>
<td>The name of the Application Portal. Appears on the Application Portal and on its help page.</td>
</tr>
<tr>
<td>product.txt</td>
<td>The name of the SSL VPN product. Appears on the title of each page.</td>
</tr>
<tr>
<td>tunnel.txt</td>
<td>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.</td>
</tr>
</tbody>
</table>

3. Upload the modified files as instructed in Editing or Replacing Customization Files (page 92).

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 Stonesoft 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 92).

2. Edit or replace the images as described in the table below:

Table 10.3  Images

<table>
<thead>
<tr>
<th>Directory Location</th>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-point/custom-files/</td>
<td>ssl_vpn_title.img</td>
<td>Background image for logon pages.</td>
</tr>
<tr>
<td>wwwwroot/wa/img</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>stonesoft_logo.png</td>
<td>The Stonesoft SSL VPN logo.</td>
</tr>
<tr>
<td>access-point/custom-files/</td>
<td>multiple files</td>
<td>Icons that you can select for resources (applications) in the Application Portal.</td>
</tr>
<tr>
<td>wwwwroot/wa/img/icons</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 92).
2. Edit the style definitions in the style sheets listed below.

Table 10.4 Style Sheets

<table>
<thead>
<tr>
<th>Directory Location</th>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/access-point/custom-files/</td>
<td>access_portal.css</td>
<td>Controls colors, fonts, as well as location and size of different page objects (for example, the logotype) in the Application Portal (_menu.html/wml and _welcome.html/wml).</td>
</tr>
<tr>
<td>wwwwroot/wa</td>
<td>common.css</td>
<td>The color and font definitions for logon pages.</td>
</tr>
<tr>
<td>/access-point/custom-files/</td>
<td>default.css</td>
<td>The color and font definitions for the Application Portal Online Help page.</td>
</tr>
<tr>
<td>wwwwroot/wa/help</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Upload the modified files as instructed in Editing or Replacing Customization Files (page 92).

**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 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 99).

▼ To customize HTML templates

1. (Optional) Download the default files you want to customize as instructed in Editing or Replacing Customization Files (page 92).

2. Edit the template files in the ~/wwwroot/wa/ directory as described in the table below:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
<th>Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>_auto_reauthmessage</td>
<td>Page displayed when the user must log off and re-authentication is required.</td>
<td></td>
</tr>
<tr>
<td>_chooseAuthmech</td>
<td>Page displayed when authentication method is to be selected.</td>
<td>name, displayname</td>
</tr>
<tr>
<td>_closedown_message</td>
<td>Page displayed when user is timed out from the Access Point.</td>
<td></td>
</tr>
<tr>
<td>_deleteLogonCred</td>
<td>Page displayed when password database has been cleared.</td>
<td></td>
</tr>
<tr>
<td>_error</td>
<td>Error message displayed to the user.</td>
<td>errmsg</td>
</tr>
<tr>
<td>_InternalAuthentication</td>
<td>The Internal Authentication form.</td>
<td>ihost, iuid, idom</td>
</tr>
<tr>
<td>_logoutPage</td>
<td>Page displayed when user has logged off.</td>
<td></td>
</tr>
<tr>
<td>_menu</td>
<td>The actual Application Portal page (called from welcome.html).</td>
<td></td>
</tr>
<tr>
<td>_no_session</td>
<td>Page displayed when a session has timed out.</td>
<td></td>
</tr>
<tr>
<td>_popup_msg</td>
<td>Page used to display a popup message to the user.</td>
<td>location, errmsg</td>
</tr>
<tr>
<td>_reauthmessage</td>
<td>Time-out message displayed to user.</td>
<td></td>
</tr>
<tr>
<td>File Name</td>
<td>Description</td>
<td>Variables</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>_refresh_top</td>
<td>Page displayed when a user needs to refresh the browser.</td>
<td></td>
</tr>
<tr>
<td>_securitywarning</td>
<td>Page displayed for security warnings.</td>
<td>errmsg</td>
</tr>
<tr>
<td>_TimedoutPage</td>
<td>Page displayed when a user is temporarily locked until a specific timeout occurs (currently concerns only SecurID).</td>
<td>auth_timeout</td>
</tr>
<tr>
<td>_webclient.html</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>_webclientjavaobj.html</td>
<td>Holds an instance of the Access Client Java Applet.</td>
<td></td>
</tr>
<tr>
<td>_webclientobj.html</td>
<td>Holds an instance of the Access Client ActiveX.</td>
<td></td>
</tr>
<tr>
<td>_welcome</td>
<td>Page displayed subsequent to a successful logon.</td>
<td></td>
</tr>
<tr>
<td>302</td>
<td>Page displayed to redirect the user when a page has moved.</td>
<td>location</td>
</tr>
<tr>
<td>302_top</td>
<td>Page displayed to redirect the user when a page has moved.</td>
<td>location</td>
</tr>
<tr>
<td>400</td>
<td>Page displayed subsequent to a bad request.</td>
<td></td>
</tr>
<tr>
<td>401E</td>
<td>Page displayed subsequent to external authentication failure due to mismatching credentials if the authentication method on the device is set to Basic authentication.</td>
<td>authmech</td>
</tr>
<tr>
<td>401I</td>
<td>Page displayed subsequent to an internal authentication failure due to mismatching credentials if the authentication method on the device is set to Basic authentication.</td>
<td>location</td>
</tr>
<tr>
<td>401WIL</td>
<td>Displayed when a user fails to log on using Windows Integrated Login.</td>
<td></td>
</tr>
<tr>
<td>403</td>
<td>Page displayed when a client requests a forbidden resource, that is, Access Control denies the resource to be accessed.</td>
<td>ehost</td>
</tr>
<tr>
<td>404</td>
<td>Page displayed when a requested file on the Access Point does not exist.</td>
<td>ehost</td>
</tr>
<tr>
<td>405</td>
<td>Page displayed when a HTTP-method which is not allowed has been used in a client request.</td>
<td>ehost</td>
</tr>
<tr>
<td>500</td>
<td>Page displayed when a server error occurs.</td>
<td>errmsg</td>
</tr>
<tr>
<td>pocketclient</td>
<td>Starts the installation of the Access Client for Pocket PC.</td>
<td></td>
</tr>
</tbody>
</table>
3. Edit the template files in the ~/wwwroot/wa/authmech/base directory as described in the table below:

### Table 10.5 Template files in ~/wwwroot/wa/ (Continued)

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
<th>Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestLogonLoginPage</td>
<td>Logon page for TestLogon, that is, when a user requests <a href="http://127.0.0.1:19146/wa/auth?authmech=TestLogon">http://127.0.0.1:19146/wa/auth?authmech=TestLogon</a> on the local computer where the Access Point is installed.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 10.6 Template files in ~/wwwroot/wa/authmech/base

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
<th>Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>GenericForm.&lt;file extension&gt;</td>
<td>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.</td>
<td>heading</td>
</tr>
<tr>
<td>Dialog.&lt;file extension&gt;</td>
<td>Base template used in conjunction with template specifications of type Dialog.</td>
<td>heading</td>
</tr>
</tbody>
</table>
4. Upload the modified files as instructed in Editing or Replacing Customization Files (page 92).

**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>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>Comma-separated list of allowed HTTP methods for the current host and URI.</td>
</tr>
<tr>
<td>auth_timeout</td>
<td>Number of seconds left of the period of time a user is locked from logging in (used in combination with SecurID logon).</td>
</tr>
<tr>
<td>authmech</td>
<td>The authentication method for an authenticated user.</td>
</tr>
<tr>
<td>authtimeout</td>
<td>Number of seconds remaining before an authenticated user is logged out. Used in the timeout warning page.</td>
</tr>
<tr>
<td>do</td>
<td>Used as a parameter for handling input data.</td>
</tr>
<tr>
<td>ehost</td>
<td>External host name, that is, the HTTP Host in the client request to the Access Point (for example mvpn.example.com). General variable that can be used in all templates.</td>
</tr>
<tr>
<td>eprot</td>
<td>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.</td>
</tr>
<tr>
<td>errmsg</td>
<td>Error message from the Access Point.</td>
</tr>
<tr>
<td>explanation</td>
<td>Explanatory text in Template Specification.</td>
</tr>
<tr>
<td>final_timeout</td>
<td>Number of minutes remaining before the configured maximum lifetime of the current session is reached and the session ends.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>heading</td>
<td>Main heading text in Template Specification.</td>
</tr>
<tr>
<td>idom</td>
<td>The internal domain.</td>
</tr>
<tr>
<td>ihost</td>
<td>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).</td>
</tr>
<tr>
<td>input-heading</td>
<td>Heading text for an input field in Template Specification.</td>
</tr>
<tr>
<td>iprot</td>
<td>Internal protocol currently accessed by the user: HTTP or HTTPS.</td>
</tr>
<tr>
<td>iuid</td>
<td>Internal UserID (uid filtered through NameMapper.wascr). General variable that can be used in all templates.</td>
</tr>
<tr>
<td>iuri</td>
<td>Internal URI, in requested from Access Point to host.</td>
</tr>
<tr>
<td>location</td>
<td>A URI or a URL specifying where to redirect during logon.</td>
</tr>
<tr>
<td>maxSessionTimeout</td>
<td>Maximum time in minutes for a user session. The value is specified in the configuration.</td>
</tr>
<tr>
<td>message</td>
<td>Message from the Authentication Service.</td>
</tr>
<tr>
<td>method</td>
<td>HTTP method in a GET request.</td>
</tr>
<tr>
<td>ntdomain</td>
<td>NT domain name.</td>
</tr>
<tr>
<td>pin</td>
<td>PIN for authentication.</td>
</tr>
<tr>
<td>protocol</td>
<td>An Access Client URL parameter for the protocol for the tunnel: EESSP or SSL.</td>
</tr>
<tr>
<td>reauth_uid</td>
<td>User ID used on RADIUS pages.</td>
</tr>
<tr>
<td>redirect</td>
<td>URL parameter for the Access Client.</td>
</tr>
<tr>
<td>replyMsg</td>
<td>RADIUS reply message.</td>
</tr>
<tr>
<td>servernumber</td>
<td>Logon challenge number from the Authentication Service.</td>
</tr>
<tr>
<td>title</td>
<td>Heading text.</td>
</tr>
<tr>
<td>tunnelCipherIv</td>
<td>The Base64 encoded cipher IV. Generated dynamically in the system.</td>
</tr>
<tr>
<td>tunnelCipherKey</td>
<td>The Base64 encoded cipher key. Generated dynamically in the system.</td>
</tr>
<tr>
<td>upd</td>
<td>The value of the UPD cookie used for session handling in a mirrored environment. Generated dynamically in the system.</td>
</tr>
<tr>
<td>uid</td>
<td>The UserID for an authenticated user. General variable that can be used in all templates.</td>
</tr>
<tr>
<td>uri</td>
<td>The URI that the client requested from the Access Point.</td>
</tr>
<tr>
<td>waak</td>
<td>The session handling method selected on the Advanced tab of the Global Access Point settings.</td>
</tr>
<tr>
<td>warningtimeout</td>
<td>Number of seconds remaining before a warning message or another logon page is displayed to the user.</td>
</tr>
</tbody>
</table>
Prerequisites: Finding the Root Folder for Customization Files

The Stonesoft 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.

**To customize the Stonesoft 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 92).

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

Table 10.8 Required Parameters for Stonesoft Web Authentication

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Usage</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserName</td>
<td>User ID of authenticating user.</td>
<td></td>
</tr>
<tr>
<td>Config</td>
<td>Configuration parameters.</td>
<td></td>
</tr>
<tr>
<td>Challenge</td>
<td>Challenge from the Authentication Service.</td>
<td></td>
</tr>
<tr>
<td>Modulus</td>
<td>Encryption Modulus.</td>
<td></td>
</tr>
<tr>
<td>PostURL</td>
<td>URL to which the result is posted.</td>
<td></td>
</tr>
</tbody>
</table>

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

Table 10.9 Optional Parameters for Stonesoft Web Authentication

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Usage</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShowPress</td>
<td>If set to true, the buttons are rendered in a down state when pressed.</td>
<td>true</td>
</tr>
<tr>
<td>UseFrame</td>
<td>If set to true, the applet uses a free-floating frame.</td>
<td>true</td>
</tr>
<tr>
<td>FrameName</td>
<td>Name of frame to open redirect URL in.</td>
<td></td>
</tr>
<tr>
<td>SkinFile</td>
<td>Name of the skin file.</td>
<td>WebSkin.zip</td>
</tr>
<tr>
<td>EchoChar</td>
<td>Character to echo when a character has been typed.</td>
<td>*</td>
</tr>
</tbody>
</table>
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 92).
In this section:

- Managing User Accounts - 105
- Managing Authentication Methods - 127
- Managing Authentication Services - 143
- Managing Certificates - 151
- Defining Access Rules - 165
- Standard Resource Configuration - 179
- Web Resource Configuration - 189
- Tunnel Resource Configuration - 203
- Client Security - 217
- Managing Single Sign-On and Identity Federation - 231
- Monitoring in the SSL VPN - 245
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 106)
- Managing User Storage Locations (page 112)
- Managing Global User Account Settings (page 106)
- Managing User Accounts (page 112)
- Managing User Groups (page 119)
- Getting Started with Delegated Management (page 122)
- Managing Self Service (page 123)
Getting Started with Managing User Accounts

In Stonesoft 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 Stonesoft SSL VPN user accounts. Stonesoft 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 75) and Adding an External User Storage Location (page 76).

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 106).
2. Add user and administrator accounts. See Adding Users (page 113).
3. Add user groups. See Adding User Groups (page 120).

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

2. Select one of the following tabs depending on which settings you want to configure:
   - **General Settings:** Includes default settings for user account validity, Stonesoft 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 107).
- To define settings for user linking, proceed to User Linking Settings (page 108).
- To enable/disable automatic user link repair, proceed to Auto Repair Settings (page 112).
General Settings

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

Table 11.1 Default Account Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Retries</td>
<td>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 Stonesoft authentication. Set to 10 by default.</td>
</tr>
<tr>
<td>Account Expires In</td>
<td>(Optional) 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.</td>
</tr>
</tbody>
</table>

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

Table 11.2 Required Default Account Settings for Stonesoft Authentication

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Retries</td>
<td>Maximum number of invalid login attempts allowed (1-999) before the user account is locked for Stonesoft authentication. Set to 9 by default.</td>
</tr>
</tbody>
</table>

Optional default account settings for Stonesoft authentication include:

Table 11.3 Optional Default Account Settings for Stonesoft Authentication

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use groups</td>
<td>(Optional) 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.</td>
</tr>
<tr>
<td>Use framed IP</td>
<td>(Optional) 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.</td>
</tr>
<tr>
<td>Time Lock Time-Out</td>
<td>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.</td>
</tr>
<tr>
<td>Time Lock Interval</td>
<td>Number of consecutive incorrect logon attempts allowed before the user account is time-locked. Set to 3 by default.</td>
</tr>
<tr>
<td>Change Password/PIN Notification</td>
<td>Number of days (1-19) before users are asked to change password/PIN. Set to 7 by default.</td>
</tr>
</tbody>
</table>
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 11.4 Time-Out Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Inactivity Time</td>
<td>Maximum user inactivity time in minutes (0-1440) before re-authentication is required. Set to 15 by default.</td>
</tr>
<tr>
<td>Session Time-out</td>
<td>Validity time in minutes (0-1440) for a session in the system. Set to 30 by default.</td>
</tr>
<tr>
<td>Absolute Time-out</td>
<td>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.</td>
</tr>
<tr>
<td>Time-out Warning</td>
<td>Time in seconds (0-3600) before user is warned and prompted to re-authenticate. Set to 60 by default.</td>
</tr>
<tr>
<td>Active Users Time-out</td>
<td>Time in minutes (0-1440) allowed for the user to re-authenticate after a re-authentication prompt is triggered. Set to 15 by default.</td>
</tr>
</tbody>
</table>

### 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 Stonesoft authentication method. These default settings include:

### Table 11.5 Global Settings for User Linking

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable authentication method after user linking</td>
<td>Defines whether an authentication method is enabled after user linking.</td>
</tr>
</tbody>
</table>
Managing Global User Account Settings

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

**Table 11.5  Global Settings for User Linking (Continued)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate password/PIN</td>
<td>When selected, the password/PIN is created automatically when user linking is used.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Generate Password</strong> for an automatically created password. When selected, directory mapping is not performed.</td>
</tr>
<tr>
<td>Password/PIN never expires</td>
<td>When selected, the password/PIN does not expire when user linking is used.</td>
</tr>
<tr>
<td>User cannot change password/PIN</td>
<td>When selected, users cannot change the password/PIN when user linking is used.</td>
</tr>
<tr>
<td>User must change password/PIN at next logon</td>
<td>When selected, users are required to change password/PIN at next logon when user linking is used.</td>
</tr>
<tr>
<td>Use password from directory service</td>
<td>When selected, the password used in the applicable directory service is used for authentication when user linking is used.</td>
</tr>
<tr>
<td></td>
<td>This option is only available for the following authentication methods: Stonesoft Mobile Text and Stonesoft Password.</td>
</tr>
</tbody>
</table>

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

**Table 11.6  Stonesoft Authentication Settings for User Linking**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Stonesoft Authentication When Manually Linking the User</td>
<td>Select to enable Stonesoft Authentication when manually linking the user.</td>
</tr>
<tr>
<td>Enable Stonesoft Authentication When Automatically Linking the User</td>
<td>Select to enable Stonesoft Authentication when automatically linking the user.</td>
</tr>
<tr>
<td>Notification</td>
<td>When Stonesoft authentication is enabled for automatic user linking, you are also required to select notification method. Available options are: <strong>By E-mail</strong> and <strong>By SMS</strong>.</td>
</tr>
</tbody>
</table>
Enabling Stonesoft 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 11.7 Optional Settings for Stonesoft Mobile Text**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Stonesoft Mobile Text</td>
<td>Defines whether Mobile Text Authentication is enabled after user linking.</td>
</tr>
<tr>
<td>Generate password</td>
<td>Defines whether a password is automatically created for the user.</td>
</tr>
<tr>
<td>Password never expires</td>
<td>When selected, the password is always valid.</td>
</tr>
<tr>
<td>User cannot change password</td>
<td>Defines whether the user can change the password.</td>
</tr>
<tr>
<td>User must change password on next logon</td>
<td>When selected, the user must change the password at the next logon.</td>
</tr>
<tr>
<td>Use password from directory service</td>
<td>Defines whether the password from the directory service is used.</td>
</tr>
</tbody>
</table>

**Table 11.8 Optional Settings for Stonesoft Web**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Stonesoft Web</td>
<td>Defines whether Web Authentication is enabled after user linking.</td>
</tr>
<tr>
<td>Generate password</td>
<td>Defines whether a password is automatically created for the user.</td>
</tr>
<tr>
<td>Password never expires</td>
<td>When selected, the password is always valid.</td>
</tr>
<tr>
<td>User cannot change password</td>
<td>Defines whether the user can change the password.</td>
</tr>
<tr>
<td>User must change password on next logon</td>
<td>When selected, the user must change the password at the next logon.</td>
</tr>
</tbody>
</table>

**Table 11.9 Optional Settings for Stonesoft Challenge**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Stonesoft Challenge</td>
<td>Defines whether Challenge Authentication is enabled after user linking.</td>
</tr>
<tr>
<td>Generate PIN</td>
<td>Defines whether a PIN is automatically created for the user.</td>
</tr>
<tr>
<td>PIN never expires</td>
<td>When selected, the PIN is always valid.</td>
</tr>
</tbody>
</table>
### Table 11.9  Optional Settings for Stonesoft Challenge (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User cannot change PIN</td>
<td>Defines whether the user can change the PIN.</td>
</tr>
<tr>
<td>User must change PIN on next logon</td>
<td>When selected, the user must change the PIN at the next logon.</td>
</tr>
<tr>
<td>Generate seed</td>
<td>Not editable.</td>
</tr>
</tbody>
</table>

### Table 11.10  Optional Settings for Stonesoft Password

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Stonesoft Password</td>
<td>Defines whether Password Authentication is enabled after user linking.</td>
</tr>
<tr>
<td>Generate password</td>
<td>Defines whether a password is automatically created for the user.</td>
</tr>
<tr>
<td>Password never expires</td>
<td>When selected, the password is always valid.</td>
</tr>
<tr>
<td>User cannot change password</td>
<td>Defines whether the user can change the password.</td>
</tr>
<tr>
<td>User must change password on next logon</td>
<td>When selected, the user must change the password at the next logon.</td>
</tr>
<tr>
<td>Use password from directory service</td>
<td>Defines whether the password from the directory service is used.</td>
</tr>
</tbody>
</table>

### Table 11.11  Optional Settings for Stonesoft Synchronized

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Stonesoft Synchronized</td>
<td>Defines whether Synchronized Authentication is enabled after user linking.</td>
</tr>
<tr>
<td>Generate PIN</td>
<td>Defines whether a PIN is automatically created for the user.</td>
</tr>
<tr>
<td>PIN never expires</td>
<td>When selected, the PIN is always valid.</td>
</tr>
<tr>
<td>User cannot change PIN</td>
<td>Defines whether the user can change the PIN.</td>
</tr>
<tr>
<td>User must change PIN on next logon</td>
<td>When selected, the user must change the PIN at the next logon.</td>
</tr>
<tr>
<td>Generate seed</td>
<td>Not editable.</td>
</tr>
</tbody>
</table>
**Auto Repair Settings**

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto repair user links when the users access the system</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 76).

**What's Next?**

- To add user accounts, proceed to Adding Users (page 113).
- To add user accounts by linking, proceed to Linking Users (page 114).
- To add user accounts by importing, proceed to Creating a File for Importing Users (page 116).

**Managing User Accounts** **Prerequisites:** Managing User Storage Locations

**Creating User Accounts**

There are three different ways to create user accounts in Stonesoft 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 Stonesoft SSL VPN user accounts. Stonesoft 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

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 Stonesoft 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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate password</td>
<td>A password is automatically created for the user.</td>
</tr>
<tr>
<td>Password never expires</td>
<td>The password is always valid.</td>
</tr>
<tr>
<td>User cannot change password</td>
<td>Prevents the user from changing the password.</td>
</tr>
<tr>
<td>User must change password on next logon</td>
<td>Requires the user to change the password at the next logon.</td>
</tr>
</tbody>
</table>

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 Stonesoft 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 Stonesoft authentication and no matching user account exists, a Stonesoft 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

2. Switch to the User Linking tab.
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 108).
6. Select the password/PIN properties for each authentication method.
7. Click Save.

Linking Users Manually

To link users manually

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 Stonesoft 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update user's directory link and repair all remaining users automatically</td>
<td>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.</td>
</tr>
<tr>
<td>Update user's directory link and check next user</td>
<td>Updates the user storage location and directory link information, and continues checking links one by one.</td>
</tr>
<tr>
<td>Remove user account and check next user</td>
<td>Removes the selected user account and continues checking links one by one.</td>
</tr>
<tr>
<td>Remove user account and remove all remaining users with broken links</td>
<td>Removes the selected user account and any remaining links to the user storage.</td>
</tr>
<tr>
<td>Skip repairing the user's directory link and check next user</td>
<td>Ignores the selected user account and continues checking links one by one.</td>
</tr>
</tbody>
</table>

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**

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.

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 11.13 Import File Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heading</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>String</td>
<td>A string containing any character</td>
<td></td>
</tr>
<tr>
<td>Integer</td>
<td>Non-negative numeral</td>
<td></td>
</tr>
<tr>
<td>Boolean</td>
<td>True or false</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Password in clear text or {SHA}+ [Base64-encoded SHA hashed password]</td>
<td>Make sure the date format in the file matches your browser settings</td>
</tr>
<tr>
<td>Date</td>
<td>Date format complies to your browser’s language settings</td>
<td></td>
</tr>
</tbody>
</table>

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

Table 11.14 Import File Contents

<table>
<thead>
<tr>
<th>Heading</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>String</td>
<td>Mandatory</td>
</tr>
<tr>
<td>RealName</td>
<td>String</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Comments</td>
<td></td>
<td>Comments for your reference. This column is ignored during import.</td>
</tr>
<tr>
<td>DirectoryLink</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>UserStorage</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>GroupName</td>
<td>String</td>
<td></td>
</tr>
</tbody>
</table>
Table 11.14 Import File Contents (Continued)

<table>
<thead>
<tr>
<th>Heading</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>FramedIP</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>MailAddress</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>MobileNumber</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>AccountDisabled</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>AccountValidFrom</td>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>AccountExpires</td>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>AccountNeverExpires</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>AccessMaxRetries</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>AuthenticationMaxRetries</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>ChallengeEnabled</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>ChallengePIN</td>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>ChallengePINNeverExpires</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>ChallengePINCannotChange</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>ChallengePINMustChange</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>ChallengePINGenerate</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>ChallengeSeed</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>ChallengeSeedGenerate</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>SynchronizedEnabled</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>SynchronizedPIN</td>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>SynchronizedPINNeverExpires</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>SynchronizedPINCannotChange</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>SynchronizedPINMustChange</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>SynchronizedPINGenerate</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>SynchronizedSeed</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>SynchronizedSeedGenerate</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>WebEnabled</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>WebPwd</td>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>WebPwdNeverExpires</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>WebPwdCannotChange</td>
<td>Boolean</td>
<td></td>
</tr>
</tbody>
</table>
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 116).

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 120)

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 120).

**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**

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**

4. Click Next.
5. Configure the User Group with the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Unique name used in the system to identify the user. For example, Users.</td>
</tr>
<tr>
<td>Description</td>
<td><em>(Optional)</em> A description for your own reference. For example, Group for all standard users.</td>
</tr>
<tr>
<td>Attribute Source</td>
<td>Defines whether the attribute source is a user storage location, a custom-defined attribute, or an attribute that is received from the RADIUS server on authentication.</td>
</tr>
</tbody>
</table>
Managing User Groups

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
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
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
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

Prerequisites: Adding an External User Storage Location

Delegated Management enables you to create different administrative roles with different privileges and responsibilities. Each role can be assigned to one or several users.

Note – Delegated Management requires an external User Storage Location. See Adding an External User Storage Location (page 76).

Roles are used as alert receivers in Configuring Alert Notifications (page 252). 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. The Help Desk and Super Administrator role are predefined roles. They cannot be deleted.

Configuring Delegated Management

To configure Delegated Management

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:

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

5. Click Next.
6. Select the User Group that the role manages. Click Next.
7. From Available Resources, select the resources that the role manages 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 11.15 Challenge Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal challenges</td>
<td>Defined by the system. Internal challenges cannot be changed.</td>
</tr>
<tr>
<td>System challenges</td>
<td>Defined by the Administrator. Control questions based on the information stored in an attribute in the user storage.</td>
</tr>
<tr>
<td>User challenges</td>
<td>Control questions defined by the end-user.</td>
</tr>
</tbody>
</table>

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 11.16 Forgotten Password Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send message to secondary channel when</td>
<td>Defines whether the secondary channel is used to send a requested password</td>
</tr>
<tr>
<td>Password has been issued</td>
<td></td>
</tr>
<tr>
<td>Message to secondary channel</td>
<td>Message text for the secondary channel.</td>
</tr>
</tbody>
</table>

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 11.17 Forgotten User Name Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forgotten User Name Message</td>
<td>Message text for Forgotten User Name. Use the tag {0} for inserting the user name.</td>
</tr>
</tbody>
</table>

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**


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 configure a 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 126).
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**

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.
   - **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**

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 137).
This chapter describes the creation and management of Authentication Methods.

The following sections are included:

- Getting Started with Authentication Methods (page 128)
- Stonesoft Authentication Methods (page 128)
- Additional Authentication Methods (page 131)
- Managing Authentication Methods (page 132)
- Managing RADIUS Configuration (page 137)
- Managing OATH Configuration (page 139)
Getting Started with Authentication Methods

Authentication methods are techniques used for verifying the identity of the connecting user before proceeding with the authorization process. SSL VPN supports a wide range of authentication methods and includes several proprietary methods.

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

Stonesoft Authentication Methods

The Stonesoft authentication methods are Invisible Token, Password, Web, Synchronized, OATH, Challenge, and Mobile Text.

When using the Stonesoft Synchronized or Challenge methods, users install the Stonesoft Mobile ID client application on the device being used for authentication. The following environments are supported:

- Android devices
- iOS devices
- Java devices
- Linux
- OSX
- RIM Blackberry phones
- Symbian devices
- Windows
- Windows Mobile devices

When using the Web authentication method, the installed client is either an ActiveX component or a Java applet running in a web browser.
The Stonesoft authentication methods are all based on the RADIUS protocol. Table 12.1 provides details about the RADIUS activity when using the Stonesoft authentication methods.

Table 12.1 Stonesoft Authentication RADIUS Activity

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Device Type</th>
<th>RADIUS Client Activity</th>
<th>RADIUS Server Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stonesoft Invisible Token</td>
<td>Web browser that supports Javascript</td>
<td>User ID + Password</td>
<td>Challenge: One-Time Password (OTP) by SMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User ID + Password + Browser Name</td>
<td>Challenge: One-Time Password (OTP) script in browser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User ID + Script OTP</td>
<td>Accept, Reject If Accept a new seed is returned</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User ID + SMS OTP</td>
<td>Accept, Reject</td>
</tr>
<tr>
<td>Stonesoft Web</td>
<td>Web browser that supports Java</td>
<td>User ID</td>
<td>RADIUS package: Configuration Encryption Key Challenge</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Password RADIUS package</td>
</tr>
<tr>
<td>Stonesoft Challenge</td>
<td>PC, PDA, Mobile Phone</td>
<td>User ID + OTP (OTP: Seed+PIN+Challenge)</td>
<td>Challenge</td>
</tr>
<tr>
<td>Stonesoft Synchronized</td>
<td>PC, PDA, Mobile Phone</td>
<td>User ID + OTP (OTP synchronized between client and server)</td>
<td>Accept or Reject</td>
</tr>
<tr>
<td>Stonesoft Mobile Text</td>
<td>PC, PDA, Mobile Phone</td>
<td>User ID + Password</td>
<td>Challenge: One-Time Password (OTP) by SMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User ID + OTP</td>
<td>Accept or Reject</td>
</tr>
<tr>
<td>Stonesoft Password</td>
<td>PC</td>
<td>User ID + Password</td>
<td>Accept or Reject</td>
</tr>
<tr>
<td>Stonesoft OATH</td>
<td>PC, PDA, Mobile Phone</td>
<td>User ID + OTP (OTP synchronized between client and server)</td>
<td>Accept, Reject, or resynchronize</td>
</tr>
</tbody>
</table>
About Stonesoft Invisible Token
The Stonesoft Invisible Token authentication method is a browser-based two factor authentication method. The first time a user authenticates with a user ID and password, the user receives an SMS that contains a one-time password (OTP) for authentication. When the user selects the option to remember the browser, a shared secret is placed in the browser. The next time the user authenticates, a script automatically generates and sends an OTP.

Note – The Invisible Token authentication method requires an SMS notification channel.

About Stonesoft Web
When using the Stonesoft 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 user account is registered and the Stonesoft Web authentication method is enabled, the password or PIN is created and distributed to the user.

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

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

About Stonesoft Challenge
The Stonesoft 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 Stonesoft 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 Stonesoft Synchronized
The Stonesoft 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 Stonesoft 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 Stonesoft Mobile Text
The Stonesoft 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 Stonesoft 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 Stonesoft 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 Stonesoft Password

The Stonesoft 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 Stonesoft OATH

The Stonesoft 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 Stonesoft OATH, a hardware token generates the OTP. How the OTP is achieved is vendor-dependent. See the documentation from your OATH token vendor for detailed information.

Additional Authentication Methods

The SSL VPN supports the following additional authentication methods:

Table 12.2  Additional Authentication Methods

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeWord</td>
<td>This authentication method supports Secure Computing SafeWord hardware tokens that generate an OTP.</td>
</tr>
<tr>
<td>SecurID</td>
<td>This authentication method supports RSA SecurID tokens that generate an OTP.</td>
</tr>
<tr>
<td>LDAP</td>
<td>This authentication method performs normal LDAP bind.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>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.</td>
</tr>
<tr>
<td>IBM Tivoli and IBM RACF</td>
<td>These authentication methods are LDAP bind authentication methods with the option to allow the user to change password.</td>
</tr>
<tr>
<td>Novell eDirectory</td>
<td>The Novell eDirectory authentication method is an LDAP bind authentication method with the option to allow the user to change password.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence Online</td>
<td>This authentication method supports Confidence Online clients.</td>
</tr>
<tr>
<td>User Certificate</td>
<td>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.</td>
</tr>
<tr>
<td>NTLM</td>
<td>The NTLM authentication method is used in various Microsoft network protocol implementations.</td>
</tr>
<tr>
<td>Basic</td>
<td>This authentication method performs a basic authentication according to RFC 2617, “HTTP Authentication: Basic and Digest Access Authentication”.</td>
</tr>
<tr>
<td>General RADIUS</td>
<td>The general RADIUS authentication method can be used with any RADIUS-compliant authentication server.</td>
</tr>
<tr>
<td>Extended User Bind</td>
<td>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.</td>
</tr>
<tr>
<td>Form-Based Authentication</td>
<td></td>
</tr>
<tr>
<td>Windows Integrated Login</td>
<td>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.</td>
</tr>
<tr>
<td>E-ID</td>
<td>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.</td>
</tr>
<tr>
<td>E-ID Signer</td>
<td>Using E-ID, the client can authorize an order or a document by signing.</td>
</tr>
</tbody>
</table>
To add an Authentication Method


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:

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Click Next and skip to Step 12.</td>
</tr>
<tr>
<td>User Certificate</td>
<td>Select the Certificate Authority, click Next, and skip to Step 12.</td>
</tr>
<tr>
<td>Extended User Bind</td>
<td>Select the Certificate Authority and proceed to Step 7.</td>
</tr>
</tbody>
</table>

7. (Optional) Select Return Signature if you want to display the signature.

8. (Optional) 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.

9. All other methods Proceed to Step 7.


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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The host address of the Authentication Service for the authentication method.</td>
</tr>
<tr>
<td>Port</td>
<td>The port for the Authentication Service.</td>
</tr>
<tr>
<td>Time-out</td>
<td>How long the client waits for a reply from the authentication method server before trying to connect the next one on the list.</td>
</tr>
<tr>
<td>Listen on all interfaces</td>
<td>(Stonesoft Authentication methods only) Select if you want the server to listen to all interfaces.</td>
</tr>
</tbody>
</table>
9. Define the following additional properties depending on the type of Authentication Method Server you are adding:

Table 12.3 Additional Properties

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General RADIUS</td>
<td>Shared Secret</td>
<td>The secret shared between the RADIUS client and the RADIUS server.</td>
</tr>
<tr>
<td>SecurID</td>
<td>Shared Secret</td>
<td>The secret shared between the RADIUS client and the RADIUS server.</td>
</tr>
<tr>
<td>SafeWord</td>
<td>Shared Secret</td>
<td>The secret shared between the RADIUS client and the RADIUS server.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Account</td>
<td>The Distinguished Name or Principal Name of the administrator for the Active Directory server.</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>The password used when binding to the directory server.</td>
</tr>
<tr>
<td></td>
<td>Root DN</td>
<td>The Distinguished Name of the root node.</td>
</tr>
<tr>
<td>IBM Tivoli</td>
<td>Account</td>
<td>The Distinguished Name or Principal Name of the administrator for the Active Directory server.</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>The password used when binding to the directory server.</td>
</tr>
<tr>
<td></td>
<td>Users Root DN</td>
<td>The Distinguished Name of the root domain in which to search for users.</td>
</tr>
<tr>
<td></td>
<td>Password Policy DN</td>
<td>The Distinguished Name of the domain where the password policies are located.</td>
</tr>
<tr>
<td>IBM RACF</td>
<td>Account</td>
<td>The Distinguished Name or Principal Name of the administrator for the Active Directory server.</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>The password used when binding to the directory server.</td>
</tr>
<tr>
<td></td>
<td>Users Root DN</td>
<td>The Distinguished Name of the root domain in which to search for users.</td>
</tr>
<tr>
<td></td>
<td>Password Policy DN</td>
<td>The Distinguished Name of the domain where the password policies are located.</td>
</tr>
<tr>
<td></td>
<td>Expiration message (reg-exp)</td>
<td>(Optional) The error code returned when the password is expired.</td>
</tr>
<tr>
<td>Novell eDirectory</td>
<td>Account</td>
<td>The Distinguished Name or Principal Name of the administrator for the Active Directory server.</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>The password used when binding to the directory server.</td>
</tr>
<tr>
<td></td>
<td>Users Root DN</td>
<td>The Distinguished Name of the root domain in which to search for users.</td>
</tr>
</tbody>
</table>
### Table 12.3 Additional Properties (Continued)

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Integrated Login</td>
<td>Path</td>
<td>The path to the Logon page. For example, /directory/pagename.html.</td>
</tr>
<tr>
<td></td>
<td>Enable SSL</td>
<td>Use the SSL protocol in communications with the server.</td>
</tr>
<tr>
<td></td>
<td>CA Certificate</td>
<td>The certificate of the Certificate Authority used to validate the certificates presented by other servers.</td>
</tr>
<tr>
<td>NTLM</td>
<td>Path</td>
<td>The path to the Logon page. For example, /directory/pagename.html.</td>
</tr>
<tr>
<td></td>
<td>Enable SSL</td>
<td>Use the SSL protocol in communications with the server.</td>
</tr>
<tr>
<td></td>
<td>CA Certificate</td>
<td>The certificate of the Certificate Authority used to validate the certificates presented by other servers.</td>
</tr>
<tr>
<td></td>
<td>Domain</td>
<td>The Domain to which the authentication method server belongs.</td>
</tr>
<tr>
<td>Basic</td>
<td>Path</td>
<td>The path to the Logon page. For example, /directory/pagename.html.</td>
</tr>
<tr>
<td></td>
<td>Enable SSL</td>
<td>Use the SSL protocol in communications with the server.</td>
</tr>
<tr>
<td></td>
<td>CA Certificate</td>
<td>The certificate of the Certificate Authority used to validate the certificates presented by other servers.</td>
</tr>
<tr>
<td>Extended User Bind</td>
<td>User Root DN</td>
<td>The Distinguished Name of the root domain in which to start searching for users.</td>
</tr>
<tr>
<td></td>
<td>Attribute Name</td>
<td>The name for user objects in the directory service.</td>
</tr>
<tr>
<td></td>
<td>Attribute Value</td>
<td>The object class for user objects in the directory service.</td>
</tr>
<tr>
<td></td>
<td>Search Scope</td>
<td>The range of levels at which to search when searching for objects in the directory service.</td>
</tr>
<tr>
<td></td>
<td>User DN</td>
<td>The User DN for performing the search.</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>The user password for performing the search.</td>
</tr>
<tr>
<td>E-ID</td>
<td>Service Identifier</td>
<td>The service identifier configured in the Nexus MultiID core server.</td>
</tr>
<tr>
<td></td>
<td>Server Connection Time-out</td>
<td>The maximum time for a server connection to be established.</td>
</tr>
<tr>
<td></td>
<td>Server Unavailable Interval</td>
<td>The number of connection retries for servers that are not responding.</td>
</tr>
</tbody>
</table>
10. Click Next.

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

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

13. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

### Modifying Authentication Methods

**To modify an Authentication Method**


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. To activate the changes, click Publish at the top of the page.

### Deleting Authentication Methods

**To delete an Authentication Method**


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. To activate the changes, click Publish at the top of the page.

---

Table 12.3 Additional Properties (Continued)

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-ID Signer</td>
<td>Service Identifier</td>
<td>The service identifier configured in the Nexus MultiID core server.</td>
</tr>
<tr>
<td></td>
<td>Server Connection Time-out</td>
<td>The maximum time for a server connection to be established.</td>
</tr>
<tr>
<td></td>
<td>Server Unavailable Interval</td>
<td>The number of connection retries for servers that are not responding.</td>
</tr>
<tr>
<td>Confidence Online</td>
<td>Scan check path</td>
<td>The path the Confidence Online client scans.</td>
</tr>
</tbody>
</table>
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
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
2. Switch to the User Linking tab.
3. Select Enable Stonesoft Authentication When Manually Linking the User and/or Enable Stonesoft 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

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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address for the RADIUS client.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Shared secret between the RADIUS client and the Authentication Service.</td>
</tr>
<tr>
<td>Verify Shared Secret</td>
<td>Re-enter the Shared Secret.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Unique name that identifies the server in the system.</td>
</tr>
<tr>
<td>Host</td>
<td>IP address or DNS name of the server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port for contacting the server.</td>
</tr>
<tr>
<td>Time-out</td>
<td>Time in milliseconds that the Authentication Service waits for a reply before trying to connect to the next server on the list.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Secret shared between the Authentication Service and the back-end server.</td>
</tr>
<tr>
<td>Verify Shared Secret</td>
<td>Re-enter the Shared Secret.</td>
</tr>
</tbody>
</table>

4. Click **Save**. To activate the changes, click **Publish** at the top of the page.
OATH (Open AuTHentication) is an authentication standard that is built on open standards. The configuration of OATH includes exporting users and their token status, importing tokens, backing up and restoring the OATH database, and configuring scheduled backups.

**Activating OATH in the Web Console**

To activate OATH in the Web Console

1. Log in to the Web Console.
2. Browse to **System**→**Services**.
3. Select OATH in the Features section and click **Apply**. OATH is activated on the SSL VPN appliance.

**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 check which tokens are already in the database, you can export the users and their token status as explained in Exporting Users and Token Status (page 140).

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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Name</td>
<td>Unique name that identifies the OATH token provider in the system.</td>
</tr>
<tr>
<td><strong>(Importing from existing provider only)</strong> OTP Length (digits)</td>
<td>Length of the generated One-Time Password (OTP) required by the provider (6 - 8 digits).</td>
</tr>
<tr>
<td>Delimiter</td>
<td>Symbol(s) separating fields in the token file.</td>
</tr>
<tr>
<td>TokenId Position</td>
<td>The field position of the TokenId in the token file.</td>
</tr>
<tr>
<td>Seed Position</td>
<td>The field position of the Seed in the token file.</td>
</tr>
<tr>
<td>Counter Position</td>
<td>The field position of the Counter in the token file.</td>
</tr>
<tr>
<td>Token File</td>
<td>The file that contains the OATH tokens.</td>
</tr>
</tbody>
</table>
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.

### Exporting Users and Token Status

Exporting users and their token status allows you to create a file that can be used as a backup of the users and tokens or processed in other applications. This is especially useful when you want to check which tokens are already in the database before importing new token data.

**To export users and token status**

1. Browse to **Manage System** → **OATH Configuration**. The Manage OATH Configuration page opens.
2. Click **Export Users and Their Token Status**. The User and Token Export page opens.
3. Select the **Provider Name** from which you want to export users and their token status.
4. Enter the **Delimiter** that is used to separate fields in the exported file.

**Example** To export users and their token status as a CSV (comma-separated value) file, enter a comma (,).

5. Click **Export Users Tokens**. The file is exported.
6. Click the link to view or download the exported file.

### 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 

((Stonesoft 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:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of day</td>
<td>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.</td>
</tr>
<tr>
<td>Interval in days</td>
<td>How often the backups should be done.</td>
</tr>
<tr>
<td>Backups to keep</td>
<td>The number of backups to keep before overwriting old backups. Setting the value to 0 keeps all backups.</td>
</tr>
</tbody>
</table>

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

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 the 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 the SSL VPN 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
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 the SSL VPN should log in 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.

Searching for Users by OATH Provider or OATH Token

You can search for users by OATH provider or OATH token to check which users are associated with each OATH provider or OATH token ID.

Searching for users by OATH provider or OATH token
2. Select OATH Provider Name or OATH Token ID as the Search Criteria.
3. Enter the Provider Name or Token ID you want to search for and click Search. The user list below is updated to match your search.
   • The wildcard character * is supported, and can be entered anywhere in the search string.
   • To display all users that are associated with an OATH provider or OATH token ID, enter the wildcard without any other characters (default).
CHAPTER 13

MANAGING AUTHENTICATION SERVICES

This chapter describes the creation and management of Authentication Services.

The following sections are included:

- Getting Started with Authentication Services (page 144)
- Managing Authentication Services (page 144)
- Configuring Global Authentication Service Settings (page 146)
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 144).

Managing Authentication Services
Prerequisites: None

Adding an Authentication Service

To add an Authentication Service
2. Click Add Authentication Service.
3. Enter the new Authentication Service information:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>The IP address or DNS name of the Authentication Service.</td>
</tr>
<tr>
<td>Internal Host</td>
<td>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.</td>
</tr>
<tr>
<td>Internal Communication Port</td>
<td>The port used for internal traffic (LCP) from the different services in the network (default: 8302).</td>
</tr>
<tr>
<td>Listen on all Interfaces</td>
<td>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.</td>
</tr>
<tr>
<td>Distribute key files</td>
<td>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</td>
</tr>
</tbody>
</table>
Managing Authentication Services

4. Click Add to add a new Authentication Service.

Modifying an Authentication Service

To modify an Authentication Service
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 144)).
4. Modify the information of the Authentication Service.
5. Click Save. The system confirms that the Authentication Service has been modified.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Certificate</td>
<td>The certificate used when the Authentication Service performs TLS handshaking (for example, authenticating with the PEAP-MSCHAPv2 protocol). If PEAP-MSCHAPv2 authentication protocol is used, you must assign a server certificate. If not, PEAP-MSCHAPv2 authentication will fail. All available server certificates are available for selection. Server certificates are managed in the Manage Certificates section of the SSL VPN Administrator.</td>
</tr>
<tr>
<td>Add Additional Listener</td>
<td>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.</td>
</tr>
<tr>
<td>Enable RADIUS accounting</td>
<td>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.</td>
</tr>
<tr>
<td>Host</td>
<td>The IP address or DNS name of the system that sends the accounting response message. Required when Enable RADIUS accounting is selected.</td>
</tr>
<tr>
<td>Port</td>
<td>Port for the system that sends the accounting response message. Required when Enable RADIUS accounting is selected.</td>
</tr>
<tr>
<td>Listen on all interfaces</td>
<td>Defines whether the system must listen to all interfaces for RADIUS packets.</td>
</tr>
</tbody>
</table>
Deleting an Authentication Service

To delete an Authentication Service

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 147).
- E-mail Messages: see Configuring Global E-mail Message Settings (page 149).
- SMS/Screen Messages: see Configuring Global SMS and Screen Message Settings (page 150).

Configuring Global RADIUS Authentication Settings

To configure global RADIUS authentication settings

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop unknown sessions</td>
<td>If selected, access requests by unknown RADIUS sessions are dropped. Otherwise, the server sends an Access Denied reply.</td>
</tr>
<tr>
<td>Drop unknown users</td>
<td>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.</td>
</tr>
</tbody>
</table>
Configuring Global Authentication Service Settings

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

To configure global password/PIN settings


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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy unknown users</td>
<td>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.</td>
</tr>
<tr>
<td>Reveal reject reason</td>
<td>If selected, the reason a request has been rejected is displayed to the RADIUS client.</td>
</tr>
<tr>
<td>Session Time-out</td>
<td>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.</td>
</tr>
<tr>
<td>RADIUS Encoding</td>
<td>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).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of characters in password</td>
<td>6</td>
</tr>
<tr>
<td>Maximum number of characters in password</td>
<td>16</td>
</tr>
<tr>
<td>Minimum number of letters in a password</td>
<td>2</td>
</tr>
<tr>
<td>Minimum number of numbers in a password</td>
<td>2</td>
</tr>
<tr>
<td>Password/PIN validity period in days</td>
<td>90</td>
</tr>
<tr>
<td>Setting</td>
<td>Value(s)</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Saved previous passwords/PINs not eligible for reuse</td>
<td>5</td>
</tr>
<tr>
<td>Length of OTP (characters)</td>
<td>6</td>
</tr>
<tr>
<td>Alphabet base</td>
<td>All letters and numbers.</td>
</tr>
<tr>
<td>Notification message</td>
<td>Your OTP is {0}. Enter it to login with Mobile Text)</td>
</tr>
<tr>
<td>Allow two-step authentication</td>
<td>On/Off</td>
</tr>
<tr>
<td></td>
<td>Shift</td>
</tr>
<tr>
<td></td>
<td>Random</td>
</tr>
<tr>
<td>Support value signing</td>
<td>On/Off</td>
</tr>
<tr>
<td>Number of logon attempts before user is prompted for new OTP</td>
<td></td>
</tr>
<tr>
<td>Number of logon attempts before user is denied access.</td>
<td></td>
</tr>
<tr>
<td>Look-ahead window size</td>
<td>0-1000</td>
</tr>
</tbody>
</table>
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


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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail Addresses to Notify</td>
<td>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.</td>
</tr>
<tr>
<td>E-mail Messages</td>
<td>Specify the message subject line, header, and footer.</td>
</tr>
<tr>
<td>New Password Entered/New PIN</td>
<td>The message for notifying users (and additional recipients) of new passwords or PINs to use when authenticating. Different messages can be defined for different Stonesoft authentication methods.</td>
</tr>
<tr>
<td>Entered/Entered</td>
<td></td>
</tr>
<tr>
<td>Use Directory Password</td>
<td>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.</td>
</tr>
<tr>
<td>Use Mapped Password/Use Mapped PIN</td>
<td>The message for notifying users (and additional recipients) to use their mapped password or PIN when authenticating. Different messages can be defined for different Stonesoft authentication methods.</td>
</tr>
<tr>
<td>Seed</td>
<td>The message for notifying users (and additional recipients) of new seeds to be used in the Stonesoft Mobile ID clients Synchronized and Challenge.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Password Entered/New PIN Entered</td>
<td>The message for notifying users (and additional recipients) of new passwords or PINs to use when authenticating. Different messages can be defined for different Stonesoft authentication methods.</td>
</tr>
<tr>
<td>Use Directory Password</td>
<td>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.</td>
</tr>
<tr>
<td>Use Mapped Password/Use Mapped PIN</td>
<td>The message for notifying users (and additional recipients) to use their mapped password or PIN when authenticating. Different messages can be defined for different Stonesoft authentication methods. It is strongly recommended that you change the default texts to describe which password must be used.</td>
</tr>
<tr>
<td>Seed</td>
<td>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.</td>
</tr>
</tbody>
</table>
CHAPTER 14

MANAGING CERTIFICATES

This chapter describes the creation and management of certificates.

The following sections are included:

► Getting Started with Certificates (page 152)
► Managing Certificates in the SSL VPN Administrator (page 152)
► Managing Certificates in the Web Console (page 156)
► Creating a Certificate Request (page 161)
► Unbundling Bundled Certificates (page 163)
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 end-users.

Registered Server Certificates
You manage server certificates when establishing communication with users. You can assign a server certificate to each additional listener you add to the Access Point. You can then assign specific certificates to an IP address or port.

Registered Client Certificate
When SSL is enabled, 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?
Client certificates that have been issued by a CA may sometimes be revoked, and should no longer be trusted. When this happens, the certificate is added to a Certificate Revocation List (CRL). The SSL VPN can check the trusted client certificates against a CRL and cancel any certificates that should no longer be trusted.

If you want to use a Public Key Infrastructure (PKI), you must configure each CA you use. Each CA requires a new authentication method.

Managing Certificates in the SSL VPN Administrator
Prerequisites: None

In the SSL VPN Administrator, you manage three types of certificates:

- Certificate Authorities: see Adding Certificate Authority Certificates.
- Server certificates: see Adding Server Certificates (page 155).
- Client certificates: see Adding a Client Certificate (page 155).

Related Tasks
- Creating a Certificate Request (page 161)
- Unbundling Bundled Certificates (page 163)
- Managing Certificates in the Web Console (page 156)
Adding Certificate Authority Certificates

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.

You can add Certificate Authority certificates one by one, or you can add multiple Certificate Authority certificates at the same time. Certificate Authority certificates must be in .pem format.

To create your own private Certificate Authority certificates, see Creating Private Certificate Authorities in the Web Console (page 156).

Adding Single Certificate Authority Certificates

To add a single Certificate Authority certificate

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Enter a unique name used in the system to identify the Certificate Authority.</td>
</tr>
<tr>
<td>CA Certificate</td>
<td>Click Browse and select a CA certificate.</td>
</tr>
<tr>
<td>Revocation Control</td>
<td>Select CRL, click Next.</td>
</tr>
</tbody>
</table>

3. Click Add Control Distribution Point and define the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The LDAP address (RFC2255) or HTTP address of the CDP entered as a URL.</td>
</tr>
<tr>
<td>Fetch Time Adjustment</td>
<td>Adjusted time in seconds when revocation information is retrieved, compared to the set time for revocation information fetching.</td>
</tr>
<tr>
<td>Update Time</td>
<td>Enable/disable custom update time.</td>
</tr>
<tr>
<td>Define interval for CRL retrieving</td>
<td>Interval in seconds (0 - 31536000) for CRL retrieving.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>Interval in seconds (0 - 31536000) to retry the CRL retrieving if the CRL cannot be obtained.</td>
</tr>
</tbody>
</table>

4. Click Next.
5. Select the CRL Invalid Action to define how to handle users who have already authenticated using the certificate if the requested CRL cannot be obtained.
6. Click Finish Wizard. The Certificate Authority certificate is added.
Adding Multiple Certificate Authority Certificates

You can add multiple Certificate Authority certificates as a .zip file. Each Certificate Authority certificate must be in .pem format.

Note – It is not possible to add a bundled chain of certificates using the Add Certificate Authorities wizard. You must first unbundle the certificates as instructed in Unbundling Bundled Certificates (page 163), and then compress the unbundled certificates as a .zip file.

To add multiple Certificate Authority Certificates

1. Browse to Manage System ➔ Certificates. The Manage Certificates page opens.
2. Click Add Multiple Certificate Authorities and define the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Certificate Authority</td>
<td>Select to enable the CA.</td>
</tr>
<tr>
<td>CA Certificate</td>
<td>Click Browse and select the .zip file that contains the CA certificates used to complete the entire certificate chain. The Display Name for each Certificate Authority certificate is automatically generated based on the certificate file name. You can optionally edit the Display Names of the certificates after the certificates are added.</td>
</tr>
</tbody>
</table>

3. Click Add Control Distribution Point and define the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The LDAP address (RFC2255) or HTTP address of the CDP entered as a URL.</td>
</tr>
<tr>
<td>Fetch Time Adjustment</td>
<td>Adjusted time in seconds when revocation information is retrieved, compared to the set time for revocation information fetching.</td>
</tr>
<tr>
<td>Update Time</td>
<td>Enable/disable custom update time.</td>
</tr>
<tr>
<td>Define interval for CRL retrieving</td>
<td>Interval in seconds (0 - 31536000) for CRL retrieving.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>Interval in seconds (0 - 31536000) to retry the CRL retrieving if the CRL cannot be obtained.</td>
</tr>
</tbody>
</table>

4. Click Next.

5. Select the CRL Invalid Action to define how to handle users authenticated by user certificate if the requested CRL cannot be obtained.

6. Click Finish Wizard. The Certificate Authority certificates are added.
Adding Server Certificates

Server certificates in .pem format are used when establishing communication with end-users. You can assign a server certificate to a specific IP address or port.

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 create internal server certificates for connections to the Web Console, see Creating Server Certificates in the Web Console (page 158).

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:

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

3. Click Save.

Adding a Client Certificate

Client certificates in .pem format are registered to be used in resource communication using SSL.

Note – You can only specify one client certificate for each SSL VPN installation.

To create internal client certificates for connections to the Web Console, see Creating Client Certificates in the Web Console (page 159).

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Unique name used in the system to identify the server certificate.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Certificate in .pem format.</td>
</tr>
</tbody>
</table>
Managing Certificates in the Web Console

Prerequisites: None

The Public Key Infrastructure (PKI) Management tools in the Web Console allow you to create and manage the certificates that are used in connections to the Web Console.

What’s Next?
- Creating Private Certificate Authorities in the Web Console (page 156)
- Creating Server Certificates in the Web Console (page 158)
- Creating Client Certificates in the Web Console (page 159)
- Changing the Certificate for the Web Console Credentials (page 160)

Creating Private Certificate Authorities in the Web Console

To create a local internal certificate authority

1. In the Web Console, browse to System → PKI Management. The Public Key Infrastructure Management page opens.
2. Click Create New Private Key in the Local Internal Certificate Authorities section. The Create Private Key page opens.
3. Click Create Private Key.
4. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Name</td>
<td>Enter a unique name for the key. For example, enter the name of the certificate authority, server, or client for which you are creating the key.</td>
</tr>
<tr>
<td></td>
<td><strong>Note!</strong> Do not use spaces in the name.</td>
</tr>
<tr>
<td>Key Length</td>
<td>Select the key length. The supported key lengths are 1024 bits, 2048 bits, and 4096 bits.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Enter and confirm the passphrase for the private key.</td>
</tr>
</tbody>
</table>

5. Click Create RSA Key. The key is generated and stored as a .pkcs8 file in the data/pki/local directory on the SSL VPN gateway.

7. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country [C] (Optional)</td>
<td>Enter the standard two-character country code for the country of your organization.</td>
</tr>
<tr>
<td>State or Province [S] (Optional)</td>
<td>The name of the state or province as it should appear in the certificate.</td>
</tr>
<tr>
<td>Locality [L] (Optional)</td>
<td>The name of the city as it should appear in the certificate.</td>
</tr>
<tr>
<td>Organization [O] (Optional)</td>
<td>The name of your organization as it should appear in the certificate.</td>
</tr>
<tr>
<td>Organizational Unit [OU] (Optional)</td>
<td>The name of your department or division as it should appear in the certificate.</td>
</tr>
<tr>
<td>Common Name [CN]</td>
<td>The distinguished name of the certificate. The CN is automatically entered based on the Key Name of the private key you generated.</td>
</tr>
<tr>
<td>Key Name</td>
<td>The name of the private key for the public-private key pair. The Key Name is automatically entered based on the Key Name of the private key you generated.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>The passphrase for the private key. The passphrase is automatically entered based on the Passphrase of the private key you generated.</td>
</tr>
</tbody>
</table>

8. Click **Generate Certificate Request**. The certificate request is created and stored as a .csr file in the data/pki/local directory on the SSL VPN gateway.

9. Click **Create a Private CA**. The certificate request is used to create a self-signed CA certificate. The certificate is stored as a .pem file in the data/pki/local directory on the SSL VPN gateway.
Creating Server Certificates in the Web Console

To create a server certificate

1. In the Web Console, browse to System→PKI Management. The Public Key Infrastructure Management page opens.

2. Click Create New Private Key in the Local Internal Credentials section. The Create Private Key page opens.

3. Click Create Private Key.

4. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Name</td>
<td>Enter a unique name for the key. For example, enter the name of the certificate authority, server, or client that will use the key. Note! Do not use spaces in the name.</td>
</tr>
<tr>
<td>Key Length</td>
<td>Select the key length. The supported key lengths are 1024 bits, 2048 bits, and 4096 bits.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Enter and confirm the passphrase for the private key.</td>
</tr>
<tr>
<td>Confirm Passphrase</td>
<td>Enter and confirm the passphrase for the private key.</td>
</tr>
</tbody>
</table>

5. Click Create RSA Key. The key is generated and stored as a .pkcs8 file in the data/pki/local directory on the SSL VPN gateway.


7. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country [C]</td>
<td>Enter the standard two-character country code for the country of your organization.</td>
</tr>
<tr>
<td>State or Province[S]</td>
<td>The name of the state or province as it should appear in the certificate.</td>
</tr>
<tr>
<td>Locality [L]</td>
<td>The name of the city as it should appear in the certificate.</td>
</tr>
<tr>
<td>Organization [O]</td>
<td>The name of your organization as it should appear in the certificate.</td>
</tr>
<tr>
<td>Organizational Unit [OU]</td>
<td>The name of your department or division as it should appear in the certificate.</td>
</tr>
<tr>
<td>Common Name [CN]</td>
<td>The distinguished name of the certificate. The CN is automatically entered based on the Key Name of the private key you generated.</td>
</tr>
<tr>
<td>Key Name</td>
<td>The name of the private key for the public-private key pair. The Key Name is automatically entered based on the Key Name of the private key you generated.</td>
</tr>
</tbody>
</table>
Click **Generate Certificate Request**. The certificate request is created and stored as a `.csr` file in the `data/pki/local` directory on the SSL VPN gateway.

9. Select the **Private CA** that you want to use to sign the certificate request and click **Sign Request**.

10. Enter the **Private Key Passphrase** for the Certificate Authority’s private key.

11. Deselect **Client Certificate** and click **Sign Request**.

### Creating Client Certificates in the Web Console

#### To create a client certificate

1. In the Web Console, browse to **System → PKI Management**. The Public Key Infrastructure Management page opens.

2. Click **Create New Private Key** in the Local Internal Credentials section. The Create Private Key page opens.

3. Click **Create Private Key**.

4. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Name</td>
<td>Enter a unique name for the key. For example, enter the name of the certificate authority, server, or client that will use the key. <strong>Note!</strong> Do not use spaces in the name.</td>
</tr>
<tr>
<td>Key Length</td>
<td>Select the key length. The supported key lengths are 1024 bits, 2048 bits, and 4096 bits.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Enter and confirm the passphrase for the private key.</td>
</tr>
<tr>
<td>Confirm Passphrase</td>
<td></td>
</tr>
</tbody>
</table>

5. Click **Create RSA Key**. The key is generated and stored as a `.pkcs8` file in the `data/pki/local` directory on the SSL VPN gateway.

6. Click **Create a Certificate Request**. The Generate Certificate Request page opens.

7. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country [C]</td>
<td>The two-letter ISO abbreviation for your country.</td>
</tr>
</tbody>
</table>

![](image-url)
Chapter 14  Managing Certificates

8. Click Generate Certificate Request. The certificate request is created and stored as a .csr file in the data/pki/local directory on the SSL VPN gateway.

9. Select the Private CA that you want to use to sign the certificate request and click Sign Request.

10. Enter the Private Key Passphrase for the Certificate Authority’s private key.

11. Select Client Certificate and enter the Client Name Extension.

12. Click Sign Request.

13. Enter the Private Key Passphrase and New pkcs12 Passphrase and click Create PFX.

Changing the Certificate for the Web Console Credentials

Prerequisites: Creating Server Certificates in the Web Console

The certificate for the Web Console credentials is used to establish the HTTPS connection between the administrators’ web browsers and the Web Console. The certificate is stored in a file called miniserv.pem in the /data/webmin/etc directory. Changing the certificate for the Web Console credentials overwrites the existing miniserv.pem file with the new certificate contents.

To change the certificate for the Web Console Credentials

1. Select the certificate you want to use for the Web Console credentials.

Table 14.3  Certificate Request Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State or Province [S] (Optional)</td>
<td>The name of the state or province as it should appear in the certificate.</td>
</tr>
<tr>
<td>Locality [L] (Optional)</td>
<td>The name of the city as it should appear in the certificate.</td>
</tr>
<tr>
<td>Organization [O] (Optional)</td>
<td>The name of your organization as it should appear in the certificate.</td>
</tr>
<tr>
<td>Organizational Unit [OU] (Optional)</td>
<td>The name of your department or division as it should appear in the certificate.</td>
</tr>
<tr>
<td>Common Name [CN]</td>
<td>The distinguished name of the certificate. The CN is automatically entered based on the Key Name of the private key you generated.</td>
</tr>
<tr>
<td>Key Name</td>
<td>The name of the private key for the public-private key pair. The Key Name is automatically entered based on the Key Name of the private key you generated.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>The passphrase for the private key. The passphrase is automatically entered based on the Passphrase of the private key you generated.</td>
</tr>
</tbody>
</table>
2. Enter the Passphrase associated with the certificate.

3. Click **Use**. The existing certificate contents are replaced with the new certificate contents and you are prompted to restart the Web Console.


Creating a Certificate Request

Prerequisites: None

Stonesoft SSL VPN allows you to generate a private key and a Certificate Signing Request (CSR). A CSR is a request to sign a digital certificate. When you generate a certificate, the certificate signing request is usually given to a trusted Certificate Authority (CA), such as VeriSign or Thawte. The CSR is read and a signed certificate is returned to you.

### To create a certificate request

1. Connect to the login page for the SSL VPN Administrator. Do not log in. If you are already logged in, log out and open a new connection to the login page.

2. Click either the **For Windows** or **For Linux** link according to your operating system to download certificate-related tools to your workstation. Save the archive on your local workstation.

3. Extract all files in the archive to the same location.

4. Open a command line and run the makecsr script that was extracted from the archive.

5. Enter the **Cipher Strength** for the private key.

Example 2048

6. Select whether to encrypt the private key with a password.
   - Enter `y` for yes.
   - Enter `n` for no.
7. If you entered y, enter the password. The password is shown while you type.
8. Enter the following information to create the certificate request:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country [C]</td>
<td>The two-letter ISO abbreviation for your country.</td>
</tr>
<tr>
<td>State or Province [S] (Optional)</td>
<td>The name of state or province as it should appear in the certificate.</td>
</tr>
<tr>
<td>Locality [L] (Optional)</td>
<td>The name of the city as it should appear in the certificate.</td>
</tr>
<tr>
<td>Organization [O] (Optional)</td>
<td>The name of your organization as it should appear in the certificate.</td>
</tr>
<tr>
<td>Organizational Unit [OU] (Optional)</td>
<td>The name of your department or division as it should appear in the certificate.</td>
</tr>
<tr>
<td>Common Name [CN]</td>
<td>The distinguished name of the certificate. The CN is automatically entered based on the Key Name of the private key you generated.</td>
</tr>
<tr>
<td>Key Name</td>
<td>The name of the private key for the public-private key pair. The Key Name is automatically entered based on the Key Name of the private key you generated.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>The passphrase for the private key. The passphrase is automatically entered based on the Passphrase of the private key you generated.</td>
</tr>
</tbody>
</table>

Tip – To leave an optional field empty, enter a period (.).

The following files are generated:

- server.csr: the certificate request file that is used to generate the actual certificate.
- private.pk8: the private certificate key that you must import to the SSL VPN.
- private.key: the private certificate key in an alternative format.

9. Send the server.csr certificate request for signing to the certificate authority or sign it using an internal certificate authority (CA) that you maintain.
   - If the CA is not configured as trusted in the web browsers that the end-users connect to, the users get a certificate warning that they must accept in order to access resources.
   - Many commercial certificate authorities are configured as trusted in web browsers by default.

What’s Next?

- If the signed certificate is delivered as a bundled certificate, separate the certificates as explained in Unbundling Bundled Certificates (page 163).
- Otherwise, import the signed certificate as explained in Adding Server Certificates (page 155).
Unbundling Bundled Certificates

Prerequisites: None

When acquiring a certificate from a Certificate Authority (CA), for example VeriSign or Thawte, the certificate may come in a chain of intermediate certificates. It is not possible to import bundles directly, so each certificate in the chain must be extracted and managed separately. The bundled certificate must be in .pem format.

To unbundle bundled certificates

1. Transfer the bundled certificate .pem file and the private key to the SSL VPN gateway.

2. Connect to the Linux command line on the SSL VPN gateway through the administration port or using an SSH client.
   - Log in as root. The root password is set through the Web Console.
   - See the Appliance Installation Guide for your appliance if you need information on how to access the command line or on how to change the password.

3. Enter the following command to split the certificate chain:
   ```bash
   openssl pkcs7 -in <bundle file name>.pem -print_certs -out <output file name>.pem
   ```
   Example
   ```bash
   openssl pkcs7 -in CertificateBundle.pem -print_certs -out UnbundledCertificates.pem
   ```

4. Open the <output file name>.pem file in a text editor.

5. For each certificate, copy the text starting from the -----BEGIN CERTIFICATE----- line and ending with the -----END CERTIFICATE----- line.

6. Save each certificate as a separate .pem file with a descriptive name.

What's Next?

- To add all of the unbundled certificates as Certificate Authority certificates, compress the certificate files as a .zip archive and proceed to Adding Multiple Certificate Authority Certificates (page 154).

- To add the unbundled certificates as Certificate Authority certificates one by one, proceed to Adding Single Certificate Authority Certificates (page 153).

- Otherwise, proceed to Adding Server Certificates (page 155).
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 166)
- Defining the Global Access Rule (page 167)
- Editing Access Rules (page 168)
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 167).
2. Create reusable Registered Access Rules for more specific access criteria as explained in Adding a New Registered Access Rule (page 169).
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 Stonesoft 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 221).

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 169).

To edit the Global Access Rule


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 170).

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 169).
• You can edit an existing reusable Access Rule as explained in **Modifying a Registered Access Rule** (page 169).
• 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 170).
Adding a New Registered Access Rule

▼ To add a Registered Access Rule

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
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 170).
   • 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.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>The end-user must authenticate using the method(s) you specify. If you select this type, proceed to <strong>Defining Authentication Method Access Requirements (page 171)</strong>.</td>
</tr>
<tr>
<td>User group membership</td>
<td>The end-user's account must be included in the group(s) you specify. If you select this type, proceed to <strong>Defining User Group Membership Access Requirements (page 171)</strong>.</td>
</tr>
<tr>
<td>IP Address of incoming client</td>
<td>The source IP address of the end-user's connection must be within the range you specify. If you select this type, proceed to <strong>Defining IP Address Access Requirements (page 172)</strong>.</td>
</tr>
<tr>
<td>Client Device</td>
<td>The end-user's device should meet a Device Definition that you have configured in the system (see <strong>Adding Custom Device Definitions (page 218)</strong>). If you select this type, proceed to <strong>Defining Client Device Access Requirements (page 172)</strong>.</td>
</tr>
<tr>
<td>Date, day and/or time</td>
<td>The end-user must connect within the time period(s) you define. If you select this type, proceed to <strong>Defining Time-Based Access Requirements (page 173)</strong>.</td>
</tr>
<tr>
<td>User storage</td>
<td>The end-user's account must be stored in the user storage location(s) you specify. If you select this type, proceed to <strong>Defining User Storage Access Requirements (page 174)</strong>.</td>
</tr>
<tr>
<td>Assessment</td>
<td>The end-user's device must pass the security scans you specify. If you select this type, proceed to <strong>Defining Assessment Access Requirements (page 174)</strong>.</td>
</tr>
<tr>
<td>Abolishment</td>
<td>The end-user's device must be compatible with abolishment (trace removal). If you select this type, proceed to <strong>Defining Abolishment Access Requirements (page 175)</strong>.</td>
</tr>
<tr>
<td>Access Point</td>
<td>The end-user must connect through the Access Point (SSL VPN appliance) you specify. If you select this type, proceed to <strong>Defining Access Point Access Requirements (page 176)</strong>.</td>
</tr>
</tbody>
</table>
Editing Access Rules

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 177).
- If you are editing the Global Access Rule, proceed according to the workflow in Defining the Global Access Rule (page 167).
- If you are editing an existing Access Rule, proceed according to the workflow in Modifying a Registered Access Rule (page 169).

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.
3. If you select several user groups for the Access Rule, specify how they are used:
   • Select **Combine with OR** if the user must be a member of at least one of the listed user groups.
   • Select **Combine with AND** if the user must be a member of all listed user groups.

**Defining IP Address Access Requirements**

- To create an IP address requirement
  → Enter allowed source IP addresses for the end-user’s connection. Valid inputs are as follows:
    • A single IP address (for example, 192.168.12.12).
    • Several IP addresses separated with commas (for example, 192.168.12.12,192.168.12.22,192.168.12.32).
    • The beginning and end of a range of IP addresses separated with a hyphen (for example, 192.168.12.12–192.168.12.98).

**Defining Client Device Access Requirements**

Client Device requirements in Access Rules apply a Device Definition as the access criteria. There are some default definitions, and you can also add your own as explained in Adding Custom Device Definitions (page 218). Note that you can also specify global requirements based on the Device Definitions. The restrictions you add in the Access Rules are enforced in addition to any global restrictions you define.

- To create a client device requirement
  → Specify one or several Device Definitions that the user’s device must match to access a resource protected by the Access Rule.
    • Various types of definitions are possible with various outcomes. For example, you can display a warning to users of browsers that work poorly with your internal services,
display a different Application Portal to end-users depending on the URL they use to contact the gateway, or block access from users of very old browser versions.

Note – The client device requirements are useful as guidance and enforcement for non-hostile end-users. They are not a reliable security measure against hostile access, since the information is read from the client’s HTTP request. For a more robust client security evaluation, configure Assessment. See Defining Assessment Access Requirements (page 174).

What's Next?

► If you are creating a new Access Rule, proceed to Finishing the Add Access Rule Wizard (page 177).
► If you are editing the Global Access Rule, proceed according to the workflow in Defining the Global Access Rule (page 167).
► If you are editing an existing Access Rule, proceed according to the workflow in Modifying a Registered Access Rule (page 169).

Defining Time-Based Access Requirements

You can specify a date, a date range, selected weekdays, times of day, or a combination of these criteria.

▼ To create a date, day, and/or time requirement

1. Select which type(s) of time restrictions you want to configure. You can select any combination of restrictions, which are then applied together (each added definition further restricts the access).
   • Specify date period allows you to define a date-based restriction.
   • Specify days allows you to select days of the week.
   • Specify time period allows you to define a time of day restriction.

2. Specify the period during which access to a resource is permitted for users.
   • For Date Period, you can enter either just a start date for a single date or both a start date and end date for a range of dates. Enter the year, month, and day according to the format defined by your browser’s current language setting.
     Example If the format is M/d/yy, you could enter 12/1/10 as the start date and 12/31/10 as the end date.
   • Select one or several weekdays using the corresponding options.
   • For Time Period, enter both a start time and end time. Enter the hours, minutes, and possibly the AM/PM abbreviation according to the format defined by your browser’s current language setting.
     Example If the format is h:mm a, you could enter 12:00 AM as the start time and 8:00 PM as the end time.
Defining User Storage Access Requirements

To create a user storage requirement

Select the user storage in which the user must be stored to be allowed access to a resource protected by the Access Rule. All existing registered user storage locations are available for selection.

What’s Next?

► If you are creating a new Access Rule, proceed to Finishing the Add Access Rule Wizard (page 177).
► If you are editing the Global Access Rule, proceed according to the workflow in Defining the Global Access Rule (page 167).
► If you are editing an existing Access Rule, proceed according to the workflow in Modifying a Registered Access Rule (page 169).

Defining Assessment Access Requirements

In the assessment process, an Assessment Client component on the client computer collects client configuration data, which is compared with your specified requirements.

To create an assessment requirement

1. In the Select Plug-in or Custom section, select the correct radio button:
   - Select the top button and an imported plug-in from the list. If the plug-in you would like to use is not yet available on the drop-down list, you can upload the plug-in using the controls above. For more information, see Adding Assessment Plug-Ins (page 225).
   - Select the Custom button to specify the requirements manually.

2. Specify the settings specific to the option you have chosen:
   - For plug-ins, enter the plug-in specific options.
   - For Custom, select the type of assessment and define the properties as explained in Configuring Assessment (page 222).

Note – The client scan paths you add when creating the assessment Access Rule are added to the Client Scan tab on the Manage Assessment page.
3. *(Optional)* Select **Use Default Message** and edit the message in the field below to notify the users of what has occurred when their access is denied by this assessment Access Rule. If this option is not active, the users do not see any situation-specific message.

---

### What’s Next?
- If you are creating a new Access Rule, proceed to *Finishing the Add Access Rule Wizard* (page 177).
- If you are editing the Global Access Rule, proceed according to the workflow in *Defining the Global Access Rule* (page 167).
- If you are editing an existing Access Rule, proceed according to the workflow in *Modifying a Registered Access Rule* (page 169).

### Defining Abolishment Access Requirements
Abolishment performs end-of-connection trace removal, such as clearing the client cache and browser history, as well as deleting the created, edited, or downloaded files of specified file types. You must enable and configure abolishment globally as explained in *Configuring Abolishment* (page 226) to be able to create an abolishment rule. When abolishment is enabled, it is always carried out according to the global settings whenever the client device supports this.

When you add abolishment as a requirement in an Access Rule, the gateway assesses whether carrying out the abolishment actions are possible with the connecting client, and if abolishment is not possible, the gateway denies the access.

Abolishment rules have no configurable settings.

---

### What’s Next?
- If you are creating a new Access Rule, proceed to *Finishing the Add Access Rule Wizard* (page 177).
- If you are editing the Global Access Rule, proceed according to the workflow in *Defining the Global Access Rule* (page 167).
- If you are editing an existing Access Rule, proceed according to the workflow in *Modifying a Registered Access Rule* (page 169).
Defining Access Point Access Requirements

To create an Access Point requirement

Select an Access Point to which the end-user must be connected to gain access. In most cases, each Access Point represents an SSL VPN appliance. All registered Access Points are available for selection (such as one each for the primary and the secondary appliance in a typical mirrored configuration).

Defining Identity Provider Access Requirements

To create an identity provider requirement

Select the applicable identity provider from a list of existing registered identity providers. For more information, see Getting Started with Identity Federation (page 235).

Defining Custom Access Requirements

Custom Access Rules are created as XML files outside the user interface and imported into the system. See Technical Note #2067 for more information.

To create a custom requirement

1. Select one or several custom-defined Access Rules that the end-user must fulfill to be allowed access to a resource protected by the access rule.
   • All imported custom-defined access rules are available for selection.
   • You can upload new XML files that contain Access Rules at the bottom of the currently displayed configuration page.
2. If you select several custom Access Rules for the Access Rule, specify how they are used:
   • Select **Combine with OR** if the user is allowed access if they fulfill the criteria in any one of the selected custom Access Rules. This is selected by default.
   • Select **Combine with AND** if the user must fulfill the criteria set in all of the selected custom Access Rules.

**What’s Next?**
- If you are creating a new Access Rule, proceed to Finishing the Add Access Rule Wizard (page 177).
- If you are editing the Global Access Rule, proceed according to the workflow in Defining the Global Access Rule (page 167).
- If you are editing an existing Access Rule, proceed according to the workflow in Modifying a Registered Access Rule (page 169).

**Finishing the Add Access Rule Wizard**
When you have added a rule, you return to the General Settings page of the Access Rule.

**To finish the Access Rule**
1. You can now edit the Access Rule in the following ways:
   • Add more rules, return to Selecting Criteria for Access Rules (page 170)
   • Delete rules, by clicking the rule in the **Allow user access when** table and 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.

2. When the Access Rule is complete, click **Next**. A confirmation is displayed.

3. Click **Finish Wizard** to save the Access Rule. To activate the changes, click **Publish** at the top of the page.
Chapter 16

Standard Resource Configuration

Standard Resources are partially pre-configured templates that simplify the configuration of Web and Tunnel Resources for commonly used applications.

The following sections are included:

► Getting Started with Standard Resources (page 180)
► Creating an IMAP/SMTP or POP3/SMTP Resource (page 181)
► Creating a Microsoft Outlook Web Access Resource (page 182)
► Creating a Microsoft Outlook Client Resource (page 182)
► Creating a Domino Web Access Resource (page 183)
► Creating a Microsoft Terminal Server Resource (page 184)
► Creating a Microsoft Windows File Share Resource (page 184)
► Creating an Access to Home Directory Resource (page 185)
► Creating a SalesForce Resource (page 186)
► Creating an SSL VPN Administrator Resource (page 186)
► Creating a Citrix MetaFrame Presentation Server Resource (page 187)
► Creating a Microsoft Sharepoint Portal Server Resource (page 188)
Getting Started with Standard Resources

Prerequisites: None

Standard Resources are available for several commonly used applications. You create a standard resource using a wizard. The required Tunnel or Web Resources and Tunnel Resource Networks, as well as settings are created automatically. Once a Standard Resource has been defined, it is added to the Tunnel or Web Resources and can be modified like any other Resource.

A number of commonly used applications are available as pre-configured Standard Resources to make configuration more convenient. Standard Resource templates can be used to create Tunnel Resources for the following applications:

<table>
<thead>
<tr>
<th>Category</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>IMAP/SMTP and POP3/SMTP, see Creating an IMAP/SMTP or POP3/SMTP Resource (page 181).</td>
</tr>
<tr>
<td></td>
<td>Domino Web Access 6.5, see Creating a Domino Web Access Resource (page 183).</td>
</tr>
<tr>
<td>Remote Controlling Resources</td>
<td>Microsoft Terminal Server 2000 and Microsoft Terminal Server 2003, see Creating a Microsoft Terminal Server Resource (page 184).</td>
</tr>
<tr>
<td>File Sharing Resources</td>
<td>Microsoft Windows File Share, see Creating a Microsoft Windows File Share Resource (page 184).</td>
</tr>
<tr>
<td>Other Web Resources</td>
<td>SalesForce, see Creating a SalesForce Resource (page 186).</td>
</tr>
<tr>
<td>Administration Resources</td>
<td>SSL VPN Administrator, see Creating an SSL VPN Administrator Resource (page 186).</td>
</tr>
<tr>
<td>Portal Resources</td>
<td>Citrix MetaFrame Presentation Server, see Creating a Citrix MetaFrame Presentation Server Resource (page 187).</td>
</tr>
<tr>
<td></td>
<td>Microsoft Sharepoint Portal Server 2003, see Creating a Microsoft Sharepoint Portal Server Resource (page 188).</td>
</tr>
</tbody>
</table>
About the Application Portal

When you make Resources available in the Application Portal, you specify an icon to represent the resource and enter the link text. You can select an icon from the icon library or browse to your own image file. The icon must be a .gif, .jpeg, or .png file and must not be larger than 10 kilobytes. The links in the Application Portal are displayed alphabetically.

For each resource specified to be displayed in the Application Portal, a corresponding Application Portal item is automatically created. Different users may have different Resources available to them in the Application Portal according to the Access Rules you select for the Resource. See Getting Started with Access Rules (page 166) for more information about Access Rules.

Creating an IMAP/SMTP or POP3/SMTP Resource

**Prerequisites:** Editing Access Rules

These Standard Resources provide support for IMAP or POP3 and SMTP e-mail traffic. Once the resource is defined, it is added to the Tunnel Resources.

▼ **To create an IMAP/SMTP Resource**

2. Click the + symbol to expand the **Mail** category.
3. Click **IMAP/SMTP** or **POP3/SMTP**.
4. Click **Add this Standard Resource**. The Add Standard Resource Wizard starts.
5. Enter a unique **Display Name** used to identify the resource in the system.
6. Enter the **Mail Server Address**.
7. *(Optional)* Enter the **Startup Command** used to start the local mail client on the end-user's computer.
8. Select whether the **Tunnel Type** is **Dynamic** *(Windows end-user operating system only)* or **Static** *(other end-user operating systems)*.
9. Select an icon in one of the following ways:
   • Click **Select Icon in Icon Library** and select an icon in the Select Icon window.
   • Click **Browse** and select an image file.
10. Enter the **Link Text** that is displayed below the icon in the Application Portal.
11. Select access rule(s) to restrict access to the resource from the **Available Access Rules** list and click **Add**. Click **Next**. The confirmation page is displayed.
12. Click **Next**. The confirmation page is displayed.
13. Click **Finish Wizard**. To activate the changes, click **Publish** at the top of the page.
Creating a Microsoft Outlook Web Access Resource

Prerequisites: Editing Access Rules

These Standard Resources provide web-based support for Microsoft Outlook Web Access version 5.5, 2000, 2003, or 2007. For local client support, see Creating a Microsoft Outlook Client Resource (page 182). Once the resource is defined, it is added to the Web Resources.

Note – The authentication type defined in the Exchange Server must be Basic authentication. The Exchange Server must be configured to respond to NTLM requests.

To create a Microsoft Outlook Web Access Resource

2. Click the + symbol to expand the Mail category.
3. Click the item for the version of Microsoft Outlook Web Access you use.
5. Enter a unique Display Name used to identify the resource in the system.
6. Enter the Host IP address or DNS name.
7. (Optional) Enter the HTTP Port if you want to use a port other than 80 and/or the HTTPS Port if you want to use a port other than 443. To disable HTTP or HTTPS connections, clear the HTTP/HTTPS Port.
8. Select an icon in one of the following ways:
   • Click Select Icon in Icon Library and select an icon in the Select Icon window.
   • Click Browse and select an image file.
9. Enter the Link Text that is displayed below the icon in the Application Portal.
10. Select access rule(s) to restrict access to the resource from the Available Access Rules list and click Add.
11. Click Next. The confirmation page is displayed.
12. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

Creating a Microsoft Outlook Client Resource

Prerequisites: Editing Access Rules

This Standard Resource provides support for locally installed Microsoft Outlook Client version 2000, 2003, or 2007. For web-based support, see Creating a Microsoft Outlook Web Access Resource (page 182). Once the resource is defined, it is added to the Tunnel Resources.

▼ To create a Microsoft Outlook Client Resource

2. Click the + symbol to expand the Mail category.
4. Click **Add this Standard Resource**. The Add Standard Resource Wizard starts.

5. Enter a unique **Display Name** used to identify the resource in the system.

6. Enter the **Host** IP address or DNS name of the Exchange Server.

7. Enter the **TCP Port Set** for the MAPI Exchange.

8. Enter the **UDP Port Set** for the MAPI Exchange.

9. Select an icon in one of the following ways:
   - Click **Select Icon in Icon Library** and select an icon in the Select Icon window.
   - Click **Browse** and select an image file.

10. Enter the **Link Text** that is displayed below the icon in the Application Portal.

11. Select access rule(s) to restrict access to the resource from the **Available Access Rules** list and click **Add**. Click **Next**. The confirmation page is displayed.

12. Click **Finish Wizard**. To activate the changes, click **Publish** at the top of the page.

### Creating a Domino Web Access Resource

**Prerequisites:** Editing Access Rules

This Standard Resource provides support for Domino Web Access 6.5. Once the resource is defined, it is added to the Web Resources.

**To create a Domino Web Access Resource**


2. Click the + symbol to expand the **Mail** category.

3. Click **Domino Web Access 6.5**.

4. Click **Add this Standard Resource**. The Add Standard Resource Wizard starts.

5. Enter a unique **Display Name** used to identify the resource in the system.

6. Enter the **Host** IP address or DNS name of the Domino server.

7. *(Optional)* Enter the **HTTP Port** if you want to use a port other than 80 and/or the **HTTPS Port** if you want to use a port other than 443. To disable HTTP or HTTPS connections, clear the HTTP/HTTPS Port.

**Note – You must enter either an HTTP Port or HTTPS Port.**

8. Select an icon in one of the following ways:
   - Click **Select Icon in Icon Library** and select an icon in the Select Icon window.
   - Click **Browse** and select an image file.

9. Enter the **Link Text** that is displayed below the icon in the Application Portal.

10. Select access rule(s) to restrict access to the resource from the **Available Access Rules** list and click **Add**. Click **Next**. The confirmation page is displayed.

11. Click **Finish Wizard**. To activate the changes, click **Publish** at the top of the page.
Creating a Microsoft Terminal Server Resource

Prerequisites: Editing Access Rules

These Standard Resources provide support for Microsoft Terminal Server 2000 or 2003. The TCP port is automatically set to 3389, but it can be configured according to your environment. Once the resource is defined, it is added to the Tunnel Resources.

To create a Microsoft Terminal Server Resource

2. Click the + symbol to expand the Remote Controlling Resources category.
5. Enter a unique Display Name used to identify the resource in the system.
6. Enter the Host IP address or DNS name of the Terminal Server.
7. (Optional) Enter the TCP Port for the Terminal Server.
8. Select whether the Tunnel Type is Dynamic or Static.
9. Select an icon in one of the following ways:
   • Click Select Icon in Icon Library and select an icon in the Select Icon window.
   • Click Browse and select an image file.
10. Enter the Link Text that is displayed below the icon in the Application Portal.
11. Select access rule(s) to restrict access to the resource from the Available Access Rules list and click Add. Click Next. The confirmation page is displayed.
12. Click Next. The confirmation page is displayed.
13. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

Creating a Microsoft Windows File Share Resource

Prerequisites: Editing Access Rules

This Standard Resource provides support for Microsoft Windows file sharing. Once the resource is defined, it is added to the Tunnel Resources.

To create a Microsoft Windows file share Resource

2. Click the + symbol to expand the File Sharing Resources category.
3. Click Microsoft Windows File Share.
5. Enter a unique Display Name used to identify the resource in the system.
6. Enter the Host IP address or DNS name of the file server.
7. Enter the Share to connect to on the file server.
8. (Optional) Enter the preferred Drive Letter to map on to the client
9. Select an icon in one of the following ways:
   - Click Select Icon in Icon Library and select an icon in the Select Icon window.
   - Click Browse and select an image file.

10. Enter the Link Text that is displayed below the icon in the Application Portal.

11. Select access rule(s) to restrict access to the resource from the Available Access Rules list and click Add. Click Next. The confirmation page is displayed.

12. Click Next. The confirmation page is displayed.

13. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

Creating an Access to Home Directory Resource

Prerequisites: Editing Access Rules

This Standard Resource maps a remote User Home Directory to a local drive. Once the resource is defined, it is added to the Tunnel Resources.

▼ To create an Access to Home Directory Resource


2. Click the + symbol to expand the File Sharing Resources category.


5. Enter a unique Display Name used to identify the resource in the system.

6. Enter the Host IP address or DNS name.

7. Select an icon in one of the following ways:
   - Click Select Icon in Icon Library and select an icon in the Select Icon window.
   - Click Browse and select an image file.

8. Enter the Link Text that is displayed below the icon in the Application Portal.

9. Select access rule(s) to restrict access to the resource from the Available Access Rules list and click Add. Click Next. The confirmation page is displayed.

10. Click Next. The confirmation page is displayed.

11. Click Finish Wizard. To activate the changes, click Publish at the top of the page.
Creating aSalesForce Resource

Prerequisites: Editing Access Rules

This Standard Resource provides Simplified Single Sign-On access to www.salesforce.com. This means that the SalesForce user is only prompted once for credentials. Once access had been granted, the user credentials are saved until a new login with different credentials is made. This resource is automatically configured to use the default HTTP connection to the SalesForce servers. Once the resource is defined, it is added to the Web Resources.

Note – The Access Point must be able to resolve the address to www.salesforce.com.

To create a SalesForce Resource

2. Click the + symbol to expand the Other Web Resources category.
3. Click SalesForce.
5. Enter a unique Display Name used to identify the resource in the system.
6. Select an icon in one of the following ways:
   • Click Select Icon in Icon Library and select an icon in the Select Icon window.
   • Click Browse and select an image file.
7. Enter the Link Text that is displayed below the icon in the Application Portal.
8. Select access rule(s) to restrict access to the resource from the Available Access Rules list and click Add. Click Next. The confirmation page is displayed.
9. Click Next. The confirmation page is displayed.
10. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

Creating an SSL VPN Administrator Resource

Prerequisites: Editing Access Rules

This Standard Resource provides secure remote access to the SSL VPN Administrator. The Host IP address is automatically set to 127.0.0.1 and the HTTPS port is automatically set to 8443.

Caution – The default Host and HTTPS port must not be changed.

To create an SSL VPN Administrator Resource

2. Click the + symbol to expand the Administration Resources category.
3. Click Stonesoft SSL VPN Administrator.
5. Enter a unique Display Name used to identify the resource in the system.
6. Select an icon in one of the following ways:
   • Click Select Icon in Icon Library and select an icon in the Select Icon window.
   • Click Browse and select an image file.
7. Enter the Link Text that is displayed below the icon in the Application Portal.
8. Select access rule(s) to restrict access to the resource from the Available Access Rules list and click Add. Click Next. The confirmation page is displayed.
9. Click Next. The confirmation page is displayed.
10. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

Creating a Citrix MetaFrame Presentation Server Resource

Prerequisites: Editing Access Rules

This Standard Resource provides support for Citrix MetaFrame Presentation Servers. You can configure access to the Citrix Web Server and up to three Citrix MetaFrame Servers. Once the resource is defined, it is added to the Tunnel Resources.

To create a Citrix MetaFrame Presentation Server Resource
2. Click the + symbol to expand the Portal Resources category.
3. Click Citrix MetaFrame Presentation Server.
5. Enter a unique Display Name used to identify the resource in the system.
6. Enter the Host IP address of the Citrix Web Server. When the Resource is used in tunnel sets, the Virtual IP Address is set to this address by default.
7. (Optional) Enter the HTTP Port for the Citrix WSAM Web Server traffic if you want to use a port other than 80.
   • When the Resource uses a port other than 80, the port must be added to registered alternative hosts on the General Settings tab on the Edit Resource Host page.
   • If the default port (80) is used, make sure the alternative host contains the server name without port.
8. Specify the IP address for Citrix MetaFrame Server 1.
   • Dynamic Tunnels are added to each server using ports 1494 and 2598.
9. (Optional) Specify the IP address for Citrix MetaFrame Server 2.
10. (Optional) Specify the IP address for Citrix MetaFrame Server 3.
11. Select an icon in one of the following ways:
    • Click Select Icon in Icon Library and select an icon in the Select Icon window.
    • Click Browse and select an image file.
12. Enter the Link Text that is displayed below the icon in the Application Portal.
13. Select access rule(s) to restrict access to the resource from the Available Access Rules list and click Add. Click Next. The confirmation page is displayed.
14. Click Next. The confirmation page is displayed.
15. Click Finish Wizard. To activate the changes, click Publish at the top of the page.
Creating a Microsoft Sharepoint Portal Server Resource

Prerequisites: Editing Access Rules

This Standard Resource provides support for Microsoft Sharepoint Portal Server version 2003. Once the resource is defined, it is added to the Web Resources.

To create a Microsoft Sharepoint Portal Server Resource

2. Click the + symbol to expand the Other Web Resources category.
5. Enter a unique Display Name used to identify the resource in the system.
6. Enter the Host IP address or DNS name of the Sharepoint Portal Server.
7. (Optional) Enter the HTTP Port if you want to use a port other than 80 and/or the HTTPS Port if you want to use a port other than 443. To disable HTTP or HTTPS connections, clear the HTTP/HTTPS Port.

Note - You must enter either an HTTP Port or HTTPS Port.

8. Select an icon in one of the following ways:
   - Click Select Icon in Icon Library and select an icon in the Select Icon window.
   - Click Browse and select an image file.
9. Enter the Link Text that is displayed below the icon in the Application Portal.
10. Select access rule(s) to restrict access to the resource from the Available Access Rules list and click Add. Click Next. The confirmation page is displayed.
11. Click Next. The confirmation page is displayed.
12. Click Finish Wizard. To activate the changes, click Publish at the top of the page.
CHAPTER 17

WEB RESOURCE CONFIGURATION

Web resources are applications with a web interface, or any files accessible in a web browser.

The following sections are included:

- Getting Started with Web Resources (page 190)
- Creating Web Resources (page 190)
- Defining External Sites (page 194)
- Customizing Web Resource Authorization Settings (page 194)
- Setting the Web Resource Encryption Level (page 195)
- Configuring Link Translation (page 196)
- Configuring Internal Proxies (page 199)
- Filter Scripts (page 200)
Getting Started with Web Resources

Web Resources provide secure access to web-based applications. End-users access Web resources through the Application Portal, or directly in a Web browser using bookmarks.

A Web resource is associated with a Resource Host, which defines an HTTP or HTTPS server based on a URL. A Resource Path defines a specific directory on a web server if you want to restrict end-user access to that directory only.

Configuration Overview
2. (Optional) To allow connections to the host at other addresses or on other ports, define the additional host information. See Adding Alternative Hosts (page 191).
3. (Optional) If you want to use Single Sign-On for this resource, specify the SSO settings. See Selecting Single Sign-On (SSO) Options for Web Resources (page 192).

Creating Web Resources
Prerequisites: None

To create a new Web Resource
2. Click Add Web Resource Host. The Add Web Resource Host Wizard starts.
3. Enter a unique Display Name that used in the Application Portal to identify the Web Resource.
4. Enter the Host IP address or DNS name of the server that offers the web-based application.
5. (Optional) Enter the HTTP Port that the web-based service uses if you want to use a port other than 80 and/or the HTTPS Port that the web-based service uses if you want to use a port other than 443. To disable HTTP or HTTPS connections, clear the HTTP or HTTPS Port.

Caution – Adding untrusted external resources (such as external websites) to the Application Portal is a security risk. We strongly recommend not deploying untrusted resources to the Application Portal at all. If these types of resources are needed, they must be deployed as external sites. See Defining External Sites (page 194).

Note – You must enter either an HTTP Port or HTTPS Port.
Adding Alternative Hosts

Alternative hosts allow you to specify additional server names and/or ports at which the server can be contacted. Alternative hosts are required for link translation to function properly. You can define one or several alternative hosts for the Web resource host. When the Web resource uses a non-default HTTP port (other than 80) or uses an HTTPS port other than 443, the port must be added with the alternative host.

Example www.example.com:8080
If the default port is used, the alternative host must contain the server name without a port number.

Example www.example.com

1. Add an alternative host in one of the following ways:
   • To manually define an alternative host, select Specify alternative hosts.
   • To automatically create alternative hosts, select Generate Alternative Hosts.
2. (Manual definition only) Click Add Alternative Host.
3. (Manual definition only) Enter the alternative IP address or DNS name where the server can be reached and click Add.

What's Next?
► If you want to use Single Sign-On, proceed to Selecting Single Sign-On (SSO) Options for Web Resources (page 192).
► Otherwise, proceed to Making Web Resources Available in the Application Portal (page 193)
Selecting Single Sign-On (SSO) Options for Web Resources

You can collect resources that share logon credentials in Single Sign-On (SSO) domains, allowing end-users to enter their credentials once to access several resources. Adaptive SSO does not require any existing SSO Domains to be configured. All other Single Sign-On types require existing SSO Domains. See Creating Single Sign-On (SSO) Domains (page 232) for more information.

To select SSO options for a Web Resource

2. Select the Single Sign-On Type:
   - **Text**: end-user credentials are sent as text, with different attributes defining the information needed for authentication.
   - **Cookie**: authentication information is sent in HTTP headers.
   - **Form Based**: end-user credentials are sent using a Web form.
   - **Adaptive SSO**: a form-based SSO that learns its configuration automatically and does not require separate configuration.
3. Select an existing SSO Domain or (Adaptive SSO only) select Create New Domain.
4. (Adaptive SSO only) Enter a unique New SSO Domain Name.
5. (Form Based SSO only) Click Next (new Web Resources) or switch to the Form Based SSO tab (existing Web Resources).
6. (Form Based SSO only) Configure the following additional settings for the Logon Form:
   - **Method**: Select POST (user credential data is included in the body of the request) or GET (user credential data is included in the URL).
   - Enter the **Form Action (URL)**. This is the full URL pointing to the processing script.
   - Enter the **Form Data**. This is the string that is passed to the submit action.
   - (Optional) Specify the **SSO Credentials Encoding**. By default, UTF-8 character encoding is used.
7. (Form Based SSO only) Configure the following additional settings for the Verification of Logon Response:
   - Enter the **Verification URL** to which the response from the form is sent. If it is not specified, the resulting page from the submit action is taken for validation.
   - Enter the **Form Response** message that is displayed to the end-user.
   - Select the **Form Response Interpretation** conditions under which the Form Response message is displayed:
     - **Authentication is Successful**: the message is shown when the end-user successfully authenticates.
     - **Authentication has Failed**: the message is shown when the end-user unsuccessfully attempts to authenticate.
8. (Optional, Form Based SSO only) Define a name and value for Additional Headers and Client Request Headers that are added to the HTTP request sent by the SSL VPN appliance to the internal server.

What’s Next?

- If you are configuring the SSO options as part of a Configuration Wizard, proceed to Making Web Resources Available in the Application Portal (page 193).
- Otherwise, Click Save. To activate the changes, click Publish at the top of the page.
Making Web Resources Available in the Application Portal

When you make Resources available in the Application Portal, you specify an icon to represent the resource and enter the link text. You can select an icon from the icon library or browse to your own image file. The icon must be .gif, .jpeg, or .png file and must not be larger than 10 kilobytes. The links in the Application Portal are displayed alphabetically.

For each resource specified to be displayed in the Application Portal, a corresponding Application Portal item is automatically created.

▼ To make a Web Resource available in the Application Portal

1. Select an icon in one of the following ways:
   • Click Select Icon in Icon Library and select an icon in the Select Icon window.
   • Click Browse and select an image file.
2. Enter the Link Text.

What's Next?
► If you are configuring the Application Portal settings as part of a Configuration Wizard, click Next and proceed to Selecting Resource Access Rules.
► Otherwise, click Save. To activate the changes, click Publish at the top of the page.

Selecting Resource Access Rules

Selecting Access rules allows you to define which users can access which resources and SSO Domains. If you want to create a new Access Rule, see Editing Access Rules (page 168).

▼ To configure access rules

1. Select the access rules that apply to the resource from the Available Access Rules list and click Add.
2. Click Next. The confirmation page is displayed.
3. If you are using a Configuration Wizard to create a new Resource, click Finish Wizard. Otherwise, click Save. To activate the changes, click Publish at the top of the page.

What's Next?
► The configuration is complete.
Defining External Sites

Prerequisites: None

If links to external resources are needed, the resources must be deployed as external sites so that the Application Portal gives a direct link to the site. Traffic to and from external sites is not routed through the SSL VPN and is not encrypted by the SSL VPN. Connecting to an external site through the Application Portal is the same as entering the URL directly in the end-user's browser.

Caution – Adding untrusted external resources (such as external websites) to the Application Portal is a security risk. We strongly recommend not deploying untrusted resources to the Application Portal at all.

To define external sites
2. Click Add Application Portal Item.
3. Select External Site and click Next.
4. Select an icon in one of the following ways:
   • Click Select Icon in Icon Library and select an icon in the Select Icon window.
   • Click Browse and select an image file.
5. Enter the Link Text.
6. Enter the External URL for the external site.
7. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

What's Next?
▶ The configuration is complete.

Customizing Web Resource Authorization Settings

Prerequisites: Creating Web Resources

The advanced authorization settings allow you to specify in detail how a specific Web resource is accessed.

Table 17.1 Advanced Authorization Setting

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require exact path match</td>
<td>When selected, the defined access rules for this Web resource path apply to the exact specified path only. When de-selected, the access rules apply to the specified path and all paths that contain the specified path, unless a more specific resource with its own access rules is found under the path.</td>
</tr>
<tr>
<td>Automatic access</td>
<td>You can configure the Web resource path to be accessed automatically. When Automatic Access is selected, the user session time-outs are not affected. For example, a script can automatically request a resource, but the user is still regarded as inactive according to time-out configurations.</td>
</tr>
</tbody>
</table>
Setting the Web Resource Encryption Level

**Prerequisites:** Creating Web Resources

The encryption level defines the minimum encryption strength required to access the resource. By default, 128 bit encryption is required. You can select a different encryption level or manually enter a custom encryption level.

▶ **To set the resource encryption level**

1. Open the Web Resource Host properties for editing and switch to the Advanced Settings tab.

2. Select whether to Require SSL in the traffic between the client and the system. SSL is required by default, and is recommended.

3. Select the Encryption Level required for clients to be allowed to access the Resource:
   - **Strong encryption level:** Requires at least 128 bit encryption.
   - **Weak encryption level:** Requires at least 56 bit encryption.
   - **Other encryption level:** Enter the required encryption strength in bits.

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

Prerequisites: None

Link translation ensures that all traffic to registered Web Resource Hosts is routed through the Access Point, which enables the use of SSL and a secure connection. Some Link Translation settings are configured by default, and no customizing is required to use Link Translation. You can optionally customize the Link Translation to meet your needs.

Caution – Deploy only trusted resources to the Application Portal. Resources with significantly different security zones, such as resources hosted by different companies, must be deployed using Pooled DNS Mapping or Reserved DNS Mapping.

Links contain information about the original destination server and which protocol/port it is listening to. DNS mapping translates incoming connections to the Access Point service to an internal host running in a specific port (mapped DNS name). All mapped DNS names are part of a DNS name pool. When an end-user connects to a page on another server via the Access Point, links to other servers are translated to point to the Access Point.

Example When end-users enter the URL to the registered Web resource http://www.example.com/start.asp, the Access Point recognizes the link and automatically rewrites, or translates, the URL to https://<AccessPoint>/http://www.example.com/start.asp.

A DNS name pool can be used for mapping if URL mapping is not an option. A DNS name pool can also be used when multiple DNS domains are needed, such as in multi-homing environments where SSL connectivity service is provided to several customers hosted on the same platform. One case where DNS mapping is needed is if a link is divided into subsets by protocol, host, and URL, and then dynamically put together by the browser to form a link. In that case, the Access Point cannot establish if it is a link or not and consequently cannot translate it.

In DNS mapping, a DNS name or an IP address pointing to the Access Point is mapped to an internal host and protocol. All mapped DNS names are added to a DNS name pool.

What’s Next?

- To define how link translation options are applied to a specific Resource, proceed to Configuring Global Link Translation
- To define how request and response headers must be filtered for all Resources, proceed to Configuring Global Link Translation (page 197).
- To specify DNS names that are mapped to enable link translation, proceed to Configuring Global DNS Name Pool Settings (page 198).
Configuring Resource Link Translation

Resource link translation settings define how the global link translation settings are applied to a particular resource.

▼ To configure Resource link translation settings

1. Open the Web Resource Host properties and switch to the Advanced Settings tab.

2. Select the Link Translation Type:
   - **URL Mapping**: The name of the Web Resource is added to the URL link so no additional DNS entries are needed. URL mapping is the recommended option in most cases.
   - **Pooled DNS Mapping**: Several DNS names are defined for the same service, and the SSL VPN appliance dynamically allocates, redirects, or maps a connection to one of the relative links.
   - **Reserved DNS Mapping**: An absolute or specific DNS name is defined for a Web Resource service from the DNS name pool, and the SSL VPN appliance allocates, redirects, or maps the connection to the destination. See Configuring Global DNS Name Pool Settings (page 198) for more information about DNS name pools.

3. Specify the **Reserved DNS name for HTTP** if HTTP is used and the Link Translation Type is Reserved DNS Mapping. Only mapped DNS names that are not selected by another Web resource host are displayed in the list.

4. Specify the **Reserved DNS name for HTTPS** if HTTPS is used and the Link Translation Type is Reserved DNS Mapping. Only mapped DNS names that are not selected by another Web resource host are displayed in the list.

5. *(Optional)* If the SSL VPN communicates with the internal server at a different address than the Resource Host address, enter the **Server DNS Name**. If a specific server DNS name is not defined, the Resource Host address is used.

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

Configuring Global Link Translation

▼ To configure global link translation settings


2. Define the **Request Headers** that are filtered and checked for link translation if the destination host is configured to translate request headers (set to Destination and Referrer by default).

3. Define the **Response Headers** that are filtered and checked for link translation if the host sending the response is configured to translate response headers (set to Location, Content-Base, and Content-Location by default).

4. Define the **Request Content Types** to filter (set to text/html, application/x-javascript, text/vnd.wap.wml, text/wml, and text/css by default). The string "NOT_DEFINED" can be entered to specify that the request is filtered even if no content type is sent.

5. Define the **Response Content Types** to filter (set to text/html, application/x-javascript, text/vnd.wap.wml, text/wml, and text/css by default). The string "NOT_DEFINED" can be entered to specify that the response is filtered even if no content type is sent.

6. Click **Save**. To activate the changes, click **Publish** at the top of the page.
Configuring Global DNS Name Pool Settings

You configure the DNS name pool to improve link translation, and to use multiple DNS domains. Multiple DNS domains allow several customers to be hosted on the same platform, and a single Access Point to serve multiple designs of logon pages and the Application Portal.

The registered DNS names define the pool of available DNS names. To use multiple DNS domains, you define several DNS names for the Access Point.

Note – All DNS names must also be registered in a public DNS server, or written to the hosts file on the client machine that uses the system.

When a user makes a request using a registered mapped DNS name, the Access Point looks up which server to connect to and which protocol to use and sends the request towards this server.

Three methods of DNS mapping are supported:

- URL mapping: The resource is mapped to a path instead of using a mapped DNS name.
- Pooled DNS mapping: The resource is assigned a DNS name on first Access Point request towards an internal server.
- Reserved DNS mapping: The resource is mapped to a specific DNS name.

Adding a DNS Name for the Access Point

A DNS name for the Access Point is defined by a host DNS name and relative file path towards the content of the wwwroot (the HTML interface) that must be displayed when using the corresponding DNS name.

Entries in the DNS Name Pool must end with the same string as an entry in DNS Names for Access Point. If not, the pooled DNS name is never used. For example, to add www1.example.com to the DNS Name Pool you must add a corresponding entry that ends with ".example.com" in the DNS Name for the Access Point.

Example

<table>
<thead>
<tr>
<th>vpn1.example.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn2.example.com</td>
</tr>
<tr>
<td>www1.example.com</td>
</tr>
<tr>
<td>www2.example.com</td>
</tr>
</tbody>
</table>

To add a DNS name for the Access Point


2. Select Add DNS name for the Access Point.

3. Enter the DNS Name. It is strongly recommended to define the host name as a DNS name, because the SSL VPN checks that the HTTP headers of requests sent to the host contain the domain string(s) specified in the SSL VPN license. For testing purposes the host name can also be defined as an IP address.

4. (Optional) Enter the relative file path to the WWW Root (the HTML interface) that is displayed when using the corresponding DNS name.

Example

wwwroot/wa/accesspoint1

5. Click Add.

6. Click Save. To activate the changes, click Publish at the top of the page.
Adding a DNS Name to the Pool

To add a DNS name to the pool

2. Select Add DNS Name to Pool.
3. Enter the DNS Name and click Add. It is strongly recommended that the host name is defined as a DNS name, but for testing purposes the host name can also be defined as an IP address.
4. Click Save. To activate the changes, click Publish at the top of the page.

Configuring Internal Proxies

Prerequisites: None

If you want the SSL VPN to connect to any internal resource through a cache or proxy, you must specify the settings for the internal proxy. Internal proxy configuration consists of two parts: defining the general internal proxy settings that apply to all Resources, and defining how each Resource uses the internal proxy.

Configuring Resource Internal Proxy Settings

You can select to use NTLM v2 for HTTP and HTTPS proxies. If you experience authentication problems, disabling the use of NTLM v2 may correct the problem.

To configure resource internal proxy settings

1. Open the Web Resource Host properties and switch to the Advanced Settings tab.
2. Select Connect Via Proxy to direct the connection to the Resource through a proxy server.
3. (Optional) Select Forward Cookies Between Client and Resource to allow cookies to pass from the client to the resource and back. When not selected, all cookies are stopped at the Access Point.
4. (Forwarded cookies only) Specify a list of Cookies to Check and select the Action to either Allow or Block specific cookies. You can use the wildcard character * to allow or block all cookies.
5. Select whether to Use NTLM v2. Using NTLM v2 is recommended, and the option is selected by default.
6. Click Save. To activate the changes, click Publish at the top of the page.
Configuring Global Internal Proxy Settings

Global internal proxy settings allow you to specify the relevant addresses to use when a resource is accessed through a cache or an ordinary proxy server.

To configure global internal proxy settings
2. Enter the Host IP address or DNS name and proxy Port for the Internal HTTP Proxy or cache.
3. Enter the Host IP address or DNS name and proxy Port for the Internal HTTPS Proxy or cache.
4. Enter the Host IP address or DNS name and proxy Port for Access Client traffic for the Internal TCP Proxy. The TCP proxy is used for the Access Client.
5. Select whether to Validate Server Certificate presented by the internal host. When selected, every internal host that the Access Point connects to over HTTPS must have a valid server certificate.
6. Select the CA Certificate used when validating the server certificates (required if Validate Server Certificate is enabled).
7. (Optional) Switch to the Advanced tab and specify the parameters that are added to requests that the SSL VPN makes to the internal proxy.
8. Click Save. To activate the changes, click Publish at the top of the page.

Filter Scripts
Prerequisites: None

You can use filters to change or remove content in specific pages or in requests for resources. You can apply the filter to individual Resources, or to all Resources.

There are two default directories for scripts:
- /opt/portwise/access-point/built-in-files/scripts/ for predefined scripts provided with the SSL VPN.
- /opt/portwise/files/access-point/custom-files/scripts for custom scripts you create.

Filters are written using scripts in a proprietary script language called WASCR and have the file extension .wascr. For detailed instructions on writing filter scripts, see Technical Note #2799.
Adding a Filter

To add a filter
1. (Custom filter scripts only) Copy the filter script to the directory /opt/portwise/access-point/files/custom-files/scripts/.
3. Click Add Filter.
4. Enter a unique Display Name that is used in the SSL VPN Administrator interface.
5. Enter the Script Name to use in the filter. Do not include the .wascr file extension.
6. Select whether the filter applies to the client’s Request or the server’s Response.
7. Select whether the filter applies to All Resource Hosts or a specific Resource Host.
8. Enter the Path to the web page files to be filtered. The wildcard character * can be used.
9. Select whether the filter applies to page Content or Headers.
10. (Optional, Request filters only) Specify the Content Type to filter. The wildcard character * can be used.
11. Click Add. Click Save.

What’s Next?
- Define the values for variables used in the filter as instructed in Mapping Filter Variables.
Mapping Filter Variables

For general filters, you can use variables instead of hard-coded values. You can add one or several variables, specified using name-value pairs, to each filter.

An example of how filters with variables can be used is displayed below.

Example

```xml
<APPLET code="com.function.class" archive="applet.jar">
<param name="address" value="1.2.3.4">
</APPLET>
```

In the example above, the value of the parameter “address” must be replaced with another value, depending on what path this page is downloaded from. If it is downloaded from the path `/telnet.html`, the parameter value must be replaced with “192.168.0.7”. If the page is downloaded from the path `/ftp.html`, the value must be “192.168.0.23”.

▼ To map filter variables

1. Click Add Variable. The Add Variable view opens.
2. Enter the Name of the variable.
3. Enter the Value for the variable.
4. Click Add.
5. Click Save (new filters) or Update (existing filters). To activate the changes, click Publish at the top of the page.
Tunnel resources allow end-users to access client-server applications that do not have a Web interface.

The following sections are included:

- Getting Started with Tunnel Resources (page 204)
- Creating Tunnel Resource Networks (page 205)
- Creating Tunnel Resource Hosts (page 206)
- Creating and Modifying Tunnel Sets (page 207)
- Configuring Tunnel Resource Authorization Settings (page 210)
- Configuring IP Address Pools (page 211)
- About the Access Client (page 212)
Getting Started with Tunnel Resources

Tunnel resources allow any TCP/UDP traffic between the client and the server to travel through a protected SSL connection. End-users access the resources through the Application Portal.

A tunnel is an intermediary program that acts as a blind relay between two connections. Once active, a tunnel is not considered a party to the HTTP communication, even though the tunnel may have been initiated by an HTTP request. The tunnel ceases to exist when both ends of the relayed connections are closed.

About the Application Portal

When you make Resources available in the Application Portal, you specify an icon to represent the resource and enter the name that is displayed for the resource. You can select an icon from the icon library or browse to your own image file. The icon must be a .gif, .jpeg, or .png file and must not be larger than 10 kilobytes. The links in the Application Portal are displayed alphabetically.

For each resource specified to be displayed in the Application Portal, a corresponding Application Portal item is automatically created.

About Alternative Hosts

Alternative hosts are used to map a tunnel resource to a Scripted Resource in the associated Tunnel Set. When Scripted Resource is selected, no registered resource is selected but a filter on the Access Point decides which resource to use. You must configure the filter script on the Filters tab on the Global Resource Settings page. The alternative host is specified as an IP address or a DNS name.

Configuration Overview


2. Add a tunnel resource host to the tunnel resource network, or create a tunnel resource host outside the tunnel resource network. See Creating Tunnel Resource Hosts (page 206).

3. Add a Tunnel Set to make the resource available in the Application Portal. See Creating and Modifying Tunnel Sets (page 207).
Creating Tunnel Resource Networks

Prerequisites: None

Tunnel resource networks are a collection or a range of IP addresses and ports. When you create a tunnel resource host with an IP address inside a tunnel resource network span, the tunnel resource host is automatically included in the tunnel resource network.

To create a tunnel resource network
3. Enter a unique Display Name to identify the Tunnel Resource Network.
4. Enter the first and last IP addresses in the IP Range of the Tunnel Resource Network. To use a single IP address, enter the same IP address in both fields.
5. Specify the TCP Port Set and/or the UDP Port Set to define the range of TCP and/or UDP ports on which the host accepts connections. This can be either a single port, a range of ports, or the wildcard character * for all ports (1-65535). You must specify either the TCP Port or the UDP Port.
6. (Optional) Select the type of Single Sign On to enable for the Tunnel Resource and specify the SSO options depending on the SSO type:

<table>
<thead>
<tr>
<th>SSO Type</th>
<th>SSO Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fileshare</td>
<td>Select the Fileshare SSO Domain.</td>
</tr>
<tr>
<td>Remote Desktop</td>
<td>Select the Remote Desktop SSO Domain.</td>
</tr>
<tr>
<td>Telnet</td>
<td>Select the Telnet SSO Domain.</td>
</tr>
<tr>
<td>SSH</td>
<td>Select the SSH SSO Domain and the SSH Server Certificate.</td>
</tr>
</tbody>
</table>

7. Click Next.
8. Select the access rules that apply to the resource from the Available Access Rules list and click Add.
9. Click Next. The confirmation page is displayed.
10. Click Finish Wizard. The configuration is complete. To activate the changes, click Publish at the top of the page.

What’s Next?
- If you want to use a specific server in the tunnel resource, proceed to Creating Tunnel Resource Hosts.
- Otherwise, proceed to Creating and Modifying Tunnel Sets (page 207)
Creating Tunnel Resource Hosts

Prerequisites: None

To create a tunnel resource host


2. Click Add Tunnel Resource Host. The Add Tunnel Resource Host Wizard starts.

3. Enter a unique Display Name that is used in the Application Portal to identify the Tunnel Resource.

4. Enter the IP address or DNS name of the resource Host.

5. Specify the TCP Port Set and/or the UDP Port Set to define the range of TCP and/or UDP ports on which the host accepts connections. This can be either a single port, a range of ports, or the wildcard character * for all ports (1-65535). You must specify either the TCP Port or the UDP Port.

6. (Optional) Click Add Alternative Host, enter the Alternative Host DNS name or IP address, and click Add.

7. (Optional) Select the type of Single Sign On (SSO) to enable for the Tunnel Resource and specify the SSO options depending on the SSO type:
   • Fileshare: Select the Fileshare SSO Domain.
   • Remote Desktop: Select the Remote Desktop SSO Domain.
   • Telnet: Select the Telnet SSO Domain.
   • SSH: Select the SSH SSO Domain and the SSH Server Certificate.

8. Click Next and select the access rules that apply to the resource from the Available Access Rules list and click Add.

9. Click Next. The confirmation page is displayed.

10. Click Finish Wizard. The configuration is complete. To activate the changes, click Publish at the top of the page.

What’s Next?

Create a Tunnel Set to make the resource available in the Application Portal as explained in Creating and Modifying Tunnel Sets.
Creating and Modifying Tunnel Sets

Prerequisites: See Configuration Overview

To make a tunnel resource available in the Application Portal, you must add a Tunnel Set. A Tunnel Set consists of one or several tunnels and each tunnel points to a tunnel resource. The same tunnel resource can be used in several Tunnel Sets. To make a tunnel resource accessible to end-users, you must configure a Tunnel Set to include static and/or dynamic tunnels for the resource.

Adding a New Tunnel Set

To add a Tunnel Set

2. Click Add Tunnel Set. The Tunnel Set Wizard starts.
3. Enter a unique Display Name that is used to identify the Tunnel Set in the SSL VPN Administrator.
4. Select an icon in one of the following ways:
   - Click Select Icon in Icon Library and select an icon in the Select Icon window.
   - Click Browse and select your own image file.
5. Enter the Link Text that is used for the Tunnel Set in the Application Portal.
6. Click Next.

What's Next?

► To specify fixed IP addresses for the Tunnel Set, proceed to Adding a Static Tunnel to a Tunnel Set.
► To use dynamically assigned IP addresses for the Tunnel Set, proceed to Adding a Dynamic Tunnel to a Tunnel Set (page 208).
Adding a Static Tunnel to a Tunnel Set

Static tunnels are used to tunnel resources on a local IP address on a single port. Static tunnels can be used on any platform.

To add a static tunnel to the Tunnel Set
1. (Modifying existing Tunnel Set only) Open the properties of the Tunnel Set and switch to the Tunnel Settings tab.
2. Click Add Static Tunnel to the Set. The Add Static Tunnel page opens.
3. Select the Resource that is reached through the Tunnel Set.
4. Enter the Resource Port at which the resource host can be contacted.
5. Select whether the resource is contacted using TCP or UDP.
6. Enter the Client IP Address at which the client can be contacted. The address must be in the range 127.x.x.x. By default, the Client Address is set to 127.0.0.1.
7. Enter the Client Port at which the client can be contacted. We recommend using the same port number as for the Resource Port.
8. (Optional) Select Confirm Connections to prompt users before establishing the connection.
9. If you are creating a new Tunnel Set, click Next. Otherwise click Update. You return to the Tunnel Settings page.
10. Click Next (new Tunnel Set) or Save (existing Tunnel Set).

What’s Next?
► If you want to specify a command that is executed at the start of the connection, proceed to Specifying a Startup Command (page 209).
► Otherwise, if you are creating a new Tunnel Set, proceed to Selecting Tunnel Resource Access Rules (page 209).

Adding a Dynamic Tunnel to a Tunnel Set

Dynamic tunnels are used to tunnel resources using any IP address on multiple ports. Dynamic tunnels can only be used on Windows platforms.

To add a dynamic tunnel to the Tunnel Set
1. (Modifying existing Tunnel Set only) Open the properties of the Tunnel Set and switch to the Tunnel Settings tab.
2. Click Add Dynamic Tunnel to the Set. The Add Dynamic Tunnel page opens.
3. Select the Resource that is reached through the Tunnel Set.
4. Enter the TCP Port Set and/or the UDP Port Set at which the resource host can be contacted. You can enter ports as a range and/or single ports separated by commas.
5. Select Use Virtual IP and enter the Virtual IP Address that is used to forward traffic to the resource. This can be any unused IP address.

Note – Do not use the resource host’s IP address as the Virtual IP Address.
6. If you are creating a new Tunnel Set, click **Next**. Otherwise click **Update**. You return to the Tunnel Settings page.

7. Click **Next** (new Tunnel Set) or **Save** (existing Tunnel Set).

### What’s Next?

- If you want to specify a command that is executed at the start of the connection, proceed to **Specifying a Startup Command** (page 209).
- Otherwise, if you are creating a new Tunnel Set, proceed to **Selecting Tunnel Resource Access Rules** (page 209).

## Specifying a Startup Command

The startup command is a trusted command that is executed when the tunnel is successfully started. You can define multiple commands for each Tunnel Set.

**To specify a startup command**

1. *(Modifying existing Tunnel Set only)* Open the properties of the Tunnel Set and switch to the **Startup** tab.

2. Enter the **Startup Command**. Pre-defined commands include the following:
   - **Any drive letter from A to Z**: opens the corresponding mapped drive.
   - **Explorer**: launches Windows Explorer.
   - **Outlook**: launches Microsoft Outlook.

3. *(Optional)* Enter the **Redirect URL** of the web page to open in a browser window after the tunnel has been successfully started.

4. If you are creating a new Tunnel Set, click **Next**. Otherwise, click **Save**.

### What’s Next?

- If you are creating a new Tunnel Set, proceed to **Selecting Tunnel Resource Access Rules**.

## Selecting Tunnel Resource Access Rules

**To select tunnel resource access rules**

1. *(Modifying existing Tunnel Set only)* Open the properties of the Tunnel Set and switch to the **Access Rules** tab.

2. Select one or more of the Available Access Rules and click **Add**.

3. If you are creating a new Tunnel Set, click **Next**. Otherwise, click **Save**.

4. *(New Tunnel Set only)* Review the settings and click **Finish Wizard**. The configuration is complete. To activate the changes, click **Publish** at the top of the page.
To configure tunnel resource authorization settings

1. Open the properties of the Tunnel Resource Host or Tunnel Resource Network and switch to the Advanced Settings tab.

2. (Optional) Select Connect via Proxy if there is a proxy server between the client and the SSL VPN gateway.

3. Configure the options for Automatic Access and Time-Outs as explained in the table below:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic access</td>
<td>Activating Automatic access does not override the user session time-outs when the resource is requested automatically. For example, a script can automatically request a resource, but the user is still regarded as inactive according to time-out configurations. Not selected by default.</td>
</tr>
<tr>
<td>Max Inactivity Time-Out</td>
<td>Resource-specific maximum user inactivity time in minutes (0-1440) before re-authentication is required. Set to 15 by default.</td>
</tr>
<tr>
<td>Absolute Time-out</td>
<td>Resource-specific maximum time in minutes (0-1440) since the user was last authenticated with the required authentication method. After this time has elapsed, re-authentication is required regardless of user activity. Set to 720 by default.</td>
</tr>
</tbody>
</table>

Note – The Session Time-Out option on the Global User Account Settings page ultimately controls the validity time for a session.

4. Click Save. If you are ready to transfer the changes, click Publish at the top of the page.
Configuring IP Address Pools

Prerequisites: Creating Tunnel Resource Hosts/Creating Tunnel Resource Networks

IP Address Pool is a feature that provides connecting Windows clients with a virtual IP address from a pool configured on the SSL VPN system. This IP address is used in the Tunnel Set configuration to ensure proper use of some resources, such as accessing a file share. It also allows traffic back to the connecting client from the application used.

Defining the IP Address Pool

▼ To define the IP Address Pool
1. Enable the Proxy ARP Interface in the Web Console as instructed in Configuring Network Settings (page 53).
3. Define the IP addresses in the IP Address Pool. You can enter individual IP address, or ranges of IP addresses.
4. Click Save.

Defining the Access Point Dynamic Pool IP Address

▼ To define the access point dynamic pool IP address
1. Browse to Manage System→Access Points and select the Access Point to edit.
2. Define the Dynamic Pool IP address to use for assigning client addresses. This address must be part of the same network as the addresses in the IP Address Pool.
3. Click Save.

In a mirrored configuration, repeat these steps for all Access Points.

Enabling the Dynamic IP in the Tunnel Set

▼ To enable the dynamic IP in the tunnel set
1. Browse to Manage Resource Access→Tunnel Sets and open the properties of the Tunnel Set.
2. Switch to the Advanced Settings tab.
3. Select Provide IP Address and click Save.
4. Click Publish at the top of the page.
About the Access Client

The Access Client is a software component that creates a secure encrypted network tunnel between the end-user device and a tunnel resource in the Application Portal.

The following Access Client applications are available depending on the platform:

• A Windows (Win32) application.
• A Linux application.
• A platform-independent Java application.

The Access Client is loaded either using an ActiveX Access Client loader (*Internet Explorer only*) or a Java Applet Access Client loader.

Windows Native Access Client

The Windows Native Access Client is an application installed on the end-user's computer. The first time the Access Client is used, it requires administrator rights on the client operating system. After the first use, the Access Client starts automatically and updates itself automatically, without the need for administrator rights.

The Windows Native Access Client is downloaded and installed using the ActiveX Access Client loader or the Java Applet Access Client loader. When the Access Client loader has been successfully started, the Windows Native Access Client is loaded. The checksum of the Windows Native Access Client process is verified against the application on the appliance. If the checksums match, the tunnel set is loaded.

If the checksum does not match, the user can accept the invalid application or a fresh copy of the application can be downloaded from the appliance. This requires Regular User write permissions on the disk.

Windows Vista/Windows 7-specific Configuration

The use of a single drive letter (for example, ‘F:)’ as a startup command does not work in Windows Vista/Windows 7, because all commands must be executed using “runas” to elevate to admin mode (since the mapping is done in admin mode) and ‘F:’ is not a valid executable. Use the startup command ‘explorer /root,F:’ instead. This command works on Windows XP, Windows Vista, and Windows 7.

The AES ciphers in Windows Vista/Windows 7 are not compatible with the SSL engine used in Access Point. Remove AES ciphers RSA_AES_128_CBC_SHA and RSA_AES_256_CBC_SHA from the Cipher Suites of your Access Point under Manage Global Access Point Settings.
Linux Native Access Client

The Linux Native Access Client is an application installed on the end-user's computer. The first time the Access Client is used, it requires administrator rights on the client operating system. After the first use, the Access Client starts automatically and updates itself automatically, without the need for administrator rights.

The Linux Access Client is compatible with the following Linux distributions:

- Fedora Linux 32-bit
- Ubuntu Linux 32-bit
- Suse Linux 32-bit

Only 32-bit x86 architecture is supported. To use the Linux Access Client on a 64-bit operating system, you must install the appropriate 32-bit compatibility libraries for your Linux distribution. See the documentation for your Linux distribution for more information. To enable tunnelling without requiring root privileges, you must install the following packages:

**Table 18.2 Package Dependencies**

<table>
<thead>
<tr>
<th>Distribution</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu Linux</td>
<td>libcap2-bin</td>
</tr>
<tr>
<td>Suse Linux</td>
<td>libcap-progs</td>
</tr>
</tbody>
</table>

What's Next?

- If you will use the Linux Access Client on Ubuntu Linux, begin by Preparing for Linux Access Client Use on Ubuntu Linux.
- If you will use the Linux Access Client on Suse Linux, begin by Preparing for Linux Access Client Use on Suse Linux (page 214).

Preparing for Linux Access Client Use on Ubuntu Linux

Unity, the program that manages the system tray icons in Ubuntu, only allows applications included in its whitelist to create system tray icons. To allow the Access Client icon to appear in the system tray, you must add the Access Client to the Unity application whitelist.

- **To prepare for Linux Access Client installation on Ubuntu Linux**
  1. Open a command line terminal.
  2. Enter the following command to display the Unity application whitelist: `gsettings get com.canonical.Unity.Panel systray-whitelist`.
  3. Add the following entry to the whitelist: `'sg-sslvpn-client'`.
  4. Enter the following command to activate the updated whitelist: `gsettings set com.canonical.Unity.Panel systray-whitelist "$NEWLIST"`. 
Preparing for Linux Access Client Use on Suse Linux
To allow automatic installation of the Linux Access Client, you must enable POSIX capabilities in Suse Linux. For more information, see the Suse Linux documentation.

To prepare for Linux Access Client installation on Suse
1. Open a command line terminal.
2. Edit the /boot/grub/menu.lst file and add the following parameter to the end of the kernel line in one of the boot configurations: file_caps=1.
3. Reboot the client computer and select the kernel configuration with POSIX capabilities enabled.

ActiveX Access Client Loader
The ActiveX Access Client loader can only be used with the Internet Explorer web browser. To run the ActiveX Access Client loader with Windows Vista UAC, you must add the SSL VPN appliance’s HTTPS address to the list of trusted sites in Internet Explorer. The ActiveX loader requires administrator rights on the client operating system the first time it is used. Local lookups and DNS forwarding always require administrator rights on the client operating system.

Configuring Internet Explorer for the ActiveX Access Client Loader
To configure Internet Explorer for the ActiveX Access Client Loader
1. Open Internet Explorer and browse to Tools→Internet Options.
2. Switch to the Security tab.
3. Select Internet and click Custom Level.
4. Set Download signed ActiveX controls to Enable or Prompt.
5. Set Run ActiveX controls and plug-ins to Enable or Prompt.
6. Save the changes to the Internet Options.

Java Applet Access Client Loader
The Java Applet Access Client loader is compatible with web browsers that support Java.

The Java Applet Access Client loader has the following limitations:

- (Windows only) When the Java Applet Access Client loader starts, a DLL contained in the .jar file is copied to a temporary local directory and loaded from there. This requires Restricted User write permissions.
- If the Java Applet Access Client loader fails, the end-user does not receive an error message. This is due to a lack of integration between the Java Virtual Machine and the browser.
**Pure Java Access Client**

The Pure Java Access Client is a Java applet that can be used on any platform that supports Java. The Pure Java Access Client is also used whenever the Windows Native Access Client cannot be downloaded or started.

The Pure Java Access Client first tries to connect directly to the Access Point without a proxy. If the connections do not succeed in 1000 milliseconds, proxy detection is performed. If a proxy is detected, the Pure Java Access Client connects through that proxy instead. If no proxy is detected, the Pure Java Access Client tries to connect directly to the remote server until the socket times out according to settings in the client operating system.

The Pure Java Access Client has the following limitations:

- Dynamic tunnels are not supported with the Pure Java Access Client. Only resources with static tunnels can be accessed with the Pure Java Access Client.
- Resources that request authentication cannot be accessed with the Pure Java Access Client because the Pure Java Access Client does not support authentication.
- The proxy detection function of the Pure Java Access Client requires Restricted User write permissions in the client operating system.
CHAPTER 19

CLIENT SECURITY

Client security consists of security checks and controls applied to client devices.

The following sections are included:

- Getting Started with Client Security (page 218)
- Configuring Device-Specific Controls (page 218)
- Configuring Assessment (page 222)
- Configuring Abolishment (page 226)
Client security consists of device-specific controls, assessment, and abolishment.

- Device-specific controls define whether different types of devices are allowed or denied access, and how the appearance of the interface is customized for different types of devices.
- In the assessment process, an assessment client component on the client computer collects client configuration data, which is compared with your specified requirements.
- Abolishment performs end-of-connection trace removal, such as clearing the client cache and browser history, as well as deleting the created, edited, or downloaded files of specified file types.

**Configuration Overview**

1. Specify how connections from different devices are handled as explained in Configuring Device-Specific Controls (page 218).
2. Specify which client security options are required before access to resources is granted as explained in Configuring Assessment (page 222).
3. Specify how data is cleaned up after the session is closed as explained in Configuring Abolishment (page 226).

**Configuring Device-Specific Controls**

When the client contacts the SSL VPN gateway through HTTP, the client’s request contains details about the client device in addition to the actual address that the client calls. You can use any information in the HTTP headers to profile the client devices. There are two main uses for this type of profiling:

- You can define which client devices are allowed to access resources, for example, which client browsers can be used. You can warn users to upgrade their browser, or disallow access altogether.
- You can display a different application portal and/or authentication pages for different devices. This can be done by detecting individual devices, or by URL. For example, you can display the users browsing to `mobile.example.com` a different page than the users browsing to `standard.example.com`.

**Adding Custom Device Definitions**

Device definitions match HTTP request headers in the clients’ page requests from the SSL VPN gateway. These include information on the device, operating system, and browser (type and version).

▲ To add a custom device definition

2. Click **Add Device Definition**.

3. Enter a unique **Display Name** to identify the definition in the SSL VPN Administrator.

4. Enter the browser string found in the HTTP header of requests from the device as the **Definition**.

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

### Registering Device Settings

When registering device settings, you specify which type of session handling the Access Point uses for a specific device. This can be useful for devices that, for example, cannot handle cookies. You can also direct the end-users to different versions of the Application Portal and resources based on the type of device they are identified as using or based on the URL that they use to access the SSL VPN.

If you want to create settings for devices that are not listed, you must add the device definition first as explained in Adding Custom Device Definitions (page 218).

**To register device settings**

1. Browse to **Manage Resource Access** → **Global Resource Settings** and switch to the **Client Access** tab.

2. Click **Add Device Settings**.

---

*Configuring Device-Specific Controls*
3. Select the type of **Device**. If the device is not listed, you must first add the device definition as explained in *Adding Custom Device Definitions* (page 218).

4. Select the **Session Settings** that apply to the device:
   - **The device does not support cookies**: the session is kept in the URL instead of in a cookie.
   - **The device cannot authenticate using HTML or WML forms**: the device is challenged using HTTP response 401 instead of an HTML or WML authentication form.

5. Enter the **File Extension** if the device requires a different extension than `.html`.

6. Enter the path to the **Default Page** where end-users authenticate to the SSL VPN if the device requires a different page than the global authentication page.

   **Example** Entering `https://mobile.example.com` directs handheld devices to an alternative login page.

7. Enter the path to the **Welcome Page** to which end-users are redirected after successful authentication if the device requires a different page than the global Application Portal page.

   **Example** Entering `https://mobile.example.com/welcome` directs handheld devices to an Application Portal page that is customized for mobile devices.

8. Enter the name of the **GUI Constant** that is used to customize HTML or WML pages for the device and the **GUI Constant Value** to assign to the GUI Constant.

   **Example** Entering `background-image` as the GUI Constant and `640x480` as the GUI Constant Value restricts background images to a maximum resolution of 640x480 for the device.

9. Click **Add**.

10. To confirm the changes, click **Save**. To activate the changes, click **Publish** at the top of the page.
Configuring Device Access Restrictions

Device access restrictions are used in the order they are listed. The first matching restriction takes effect.

Note – The client device controls are useful as guidance and enforcement for non-hostile end-users. They are not a reliable security measure against hostile access, since the information is read from the client’s HTTP request. For a more robust client security evaluation, configure Assessment. See Configuring Assessment (page 222) and Defining Assessment Access Requirements (page 174).

If you want to create access restrictions for devices that are not listed, you must add the device definition first as explained in Adding Custom Device Definitions (page 218).

▼ To configure client access registered device restrictions


2. Click Add Device Access Restriction.

3. Select the type of Device to which the restriction applies. If the device is not listed, you must first add the device definition as explained in Adding Custom Device Definitions (page 218).

4. Select the Permission:
   • Accept: the device is allowed to access resources through the SSL VPN.
   • Deny: the device is not allowed to access resources through the SSL VPN.
   • Warn: a warning is displayed when the device is used, but the device is allowed to access resources through the SSL VPN.

5. (Deny and Warn Permissions only) Select the HTTP Code that is sent to the device:
   • 200: OK. This is the standard response for successful HTTP requests.
   • 403: Forbidden. This indicates that the client was able to communicate with the server, but the server did not allow the client to access the requested page.
   • 404: Not Found. This indicates that the client was able to communicate with the server, but the server could not find what was requested.
   • 500: Internal Server Error. This is a general error response that does not indicate any specific error.
6. (Deny and Warn only) Enter the path to the Feedback Page or enter a Feedback Message that is displayed to the end-user. You must enter either a Feedback Page path or a Feedback Message.

7. Click Add.

8. To confirm the changes, click Save. To activate the changes, click Publish at the top of the page.

Configuring Assessment
Prerequisites: None

Assessment defines how a client must be configured to be allowed access to resources. Assessment is enforced using an Assessment Access rule for a resource or SSO domain. When an end-user attempts to access the resource, a client scan is performed and the client is allowed or denied access based on the results of the assessment. In addition to the initial client scan, you can optionally enable a real time scan to scan the client computer at regular intervals during the session.

Tip – In the dialog displayed to the end-user, the client scan is called the End-Point Integrity scan.

Assessment Configuration Overview

1. Enable the collection of information from client computers as explained in Enabling Assessment (page 223).

2. Define which information is scanned during the client scan as explained in Defining Client Scan Paths (page 223).

3. (Optional) Configure a periodic scan of the client computer during the session as explained in Enabling Real Time Scan (page 224).

4. (Optional) Configure resources to be visible in the Application Portal only after the assessment client scan as explained in Hiding Resources Before Assessment Client Scan (page 224).

5. (Optional) Configure assessment to be performed without end-user notification as explained in Enabling Silent Assessment (page 225).

6. (Optional) Specify which assessment client loaders are used in which order as explained in Modifying Assessment Client Loader Order (page 225).

7. (Optional) Upload custom Assessment Plug-in programs as explained in Adding Assessment Plug-Ins (page 225).

8. Create Assessment Access Rules for specific resources and/or SSO domains as explained in Defining Assessment Access Requirements (page 174).
Enabling Assessment
To use assessment, you must specify the types of information to collect.

- To enable assessment
  2. Select the type of client information to collect at the bottom of the page:
     - Enable collection of Windows information: the client scan collects information about the Windows domain and Windows version on the client computer.
     - Enable collection of process information: the client scan collects information about processes running on the client computer.
     - Enable collection of network information: the client scan collects information about the TCP network port, UDP network port, and network interface on the client computer.
  3. Click Save. To activate the changes, click Publish at the top of the page.

Defining Client Scan Paths
Client scan paths define which information is scanned during the client scan. Any client scan paths you add when creating Assessment Access Rules are automatically added to the Client Scan Path list.

- To define client scan paths
  2. Click Add Client Scan Path. The Add Client Scan Path page opens.
  3. Select the client Operating System to scan.
  4. Select the Type of information to scan:
     - File: scans information in the specified file.
     - Directory: scans information in the specified directory.
     - Registry Key: (Windows only) scans information in the specified registry key.
     - Registry Sub Key: (Windows only) scans information in the specified registry sub key.
  5. Enter the Path to the selected information type. Environment variables can be used.

Example Selecting Directory as the Type and entering %systemdrive%\boot.ini as the path could be used to check the boot.ini file on whichever drive letter is designated as the system drive on the client computer.

Example Selecting Registry Key as the Type and entering HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid as the Path checks the client computer's Globally Unique Identifiers (GUID) in the registry.

  6. Click Add. You return to the Manage Assessment page.
  7. Click Save. To activate the changes, click Publish at the top of the page.
Enabling Real Time Scan

The client scan is performed the first time a resource protected by an Assessment Access Rule is requested. To continue to run the client scan at regular intervals during the session, you can enable a real time scan.

▼ To enable real time scan

2. Select Enable real time scan.
3. (Optional) Specify the Interval at which the scan is performed. By default, the Interval is 120 seconds.
4. Click Save. To activate the changes, click Publish at the top of the page.

Hiding Resources Before Assessment Client Scan

By default, resources protected by an Assessment Access Rule are displayed in the Application Portal prior to the assessment client scan. You can optionally configure resources to be hidden until the assessment client scan is completed.

▼ To hide resources before assessment client scan
1. Browse to Manage System—Assessment and switch to the Advanced Settings tab.

2. Deselect Display resources in Application Portal.
3. Click Save. To activate the changes, click Publish at the top of the page.
Enabling Silent Assessment

When assessment is performed, the end-user receives a notification message by default. You can optionally configure assessment to be performed automatically without notifying the end-user.

▼ To enable silent Assessment

1. Browse to Manage System→Assessment and switch to the Advanced Settings tab.
2. Select Autosubmit Scan button.
3. Click Save. To activate the changes, click Publish at the top of the page.

Modifying Assessment Client Loader Order

By default, the ActiveX assessment client loader attempts to load the assessment client first. If this fails, the Java Applet assessment client loader attempts to load the assessment client. You can optionally modify the assessment client loader order.

▼ To modify assessment client loader order

1. Browse to Manage System→Assessment and switch to the Advanced Settings tab.
2. Select the type of Assessment Client Loader to use:
   • ActiveX - Java Applet: the loader attempts to use ActiveX, and if this fails, the loader uses the Java Applet.
   • ActiveX: the loader only uses ActiveX.
   • Java Applet: the loader only used the Java Applet.
3. Click Save. To activate the changes, click Publish at the top of the page.

Adding Assessment Plug-Ins

An alternative to registering client scan paths is to use the plug-ins available for specific client scans. The plug-ins displayed here are located in the following folder:

• When accessed through the SSL VPN Administrator file browser
  /opt/portwise/files/policy-service/ep/plugins.
• When accessed from the command line
  data/portwise/files/policy-service/ep/plugins.

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.

▼ To add assessment plug-ins

1. Browse to Manage System→Assessment and switch to the Plug-ins tab.
2. Click Browse and browse to the location of the plug-in file.
3. Click Upload Plug-in. The plug-in is uploaded.
4. Click Save when you are finished configuring Assessment settings. To activate the changes, click Publish at the top of the page.
Selecting the Hardware Assessment Plug-In Configuration File

You can select the configuration file that defines settings for the hardware assessment plug-in in the Web Console.

▼ To select the hardware assessment plug-in configuration file
1. Log in to the Web Console.
2. Browse to System→Services.
3. Scroll down to the Plugins section and click Browse.
4. Browse to the location of the serial.csv file that defines the hardware assessment plug-in configuration and click Open.
5. Click Upload. The selected file is uploaded to the SSL VPN appliance.

Configuring Abolishment

Prerequisites: None

Web browsers leave traces, such as browser history and browser cache, after a session has ended. Abolishment removes browser history, cached content on the client computer, and files that were downloaded, created, or edited during the session.

Abolishment is enforced using an Assessment Access rule for a resource or SSO domain. A resource is protected by an Abolishment Access Rule based on abolishment settings specifying what must be cleaned on the client after the session is completed. When a user attempts to access the resource, access is allowed only if the abolishment client is running, ensuring that abolishment is performed when the session is completed.

Tip – In the dialog displayed to the end-user, the Abolishment client is called the End-Point Protection client.

Abolishment Configuration Overview

1. Define what types of files are monitored and deleted at the end of the session as explained in Configuring File Removal (page 227).
2. Define what information is cleared from the browser cache at the end of the session as explained in Configuring Cache Clean-Up (page 228).
3. (Optional) Configure resources to be visible in the Application Portal only after the abolishment client scan as explained in Hiding Resources Before Abolishment Client Scan (page 228).
4. Optional) Configure abolishment to be performed without end-user notification as explained in Enabling Silent Abolishment (page 229).
5. (Optional) Specify which abolishment client loaders are used in which order as explained in Modifying the Abolishment Client Loader Order (page 229).
6. Create Abolishment Access Rules for specific resources and/or SSO domains as explained in Defining Abolishment Access Requirements (page 175).
Configuring File Removal

The monitored file types define which types of files are monitored on the client computer, and deleted at the end of the session. File removal is currently only available for Windows clients.

▼ To configure file removal

1. Browse to Manage System → Abolishment.

2. Enter the file extensions for the types of files to delete at the end of the session.

3. Select Enable delete to remove the specified types of files at the end of the session.

4. (Optional) Select Notify user and enter the Notify Message that is displayed when files are deleted at the end of the session.
   • The Abolishment dialog contains a list of files with the option to select which files to delete. The user may select not to delete any files.

Caution – If Notify User is not selected, all specified file types are deleted automatically when the session is completed.

5. Click Save. To activate the changes, click Publish at the top of the page.
Configuring Cache Clean-Up

To configure cache clean-up

1. Browse to Manage System—Abolishment and switch to the Cache Cleaner tab.

2. Select the information to clear from the cache at the end of the session:
   - Enable clean of Internet Explorer history and typed URLs clears the Internet Explorer history and visited URLs.
   - Enable clean of Internet Explorer cache entries deletes the temporary files located in the Temporary Internet Files Windows folder.

3. (Optional) Enter the URL Filter for cache entries that are deleted when Enable clean of cache entries is selected. The wildcard character * is supported. When used alone, all cache entries are deleted.

   **Note** – Entering more specific criteria removes only cache files that match the URL Filter. Other cache files are not removed.

   Example https* removes only cache entries downloaded from an HTTPS server.

   Example http://www.example.com/* removes only cache entries from the www.example.com web server.

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

Hiding Resources Before Abolishment Client Scan

By default, resources protected by an Abolishment Access Rule are displayed in the Application Portal prior to the abolishment client scan. You can optionally configure resources to be hidden until the abolishment client scan is completed.

To hide resources before Abolishment client scan

1. Browse to Manage System—Abolishment and switch to the Advanced tab.

2. Deselect Display resources in Application Portal.
3. **Click Save. To activate the changes, click Publish at the top of the page.**

**Enabling Silent Abolishment**

Normally when Abolishment is performed, the end-user receives a notification message. You can optionally configure Abolishment to be performed automatically without notifying the end-user.

**To enable silent abolishment**

1. Browse to **Manage System→Abolishment** and switch to the **Advanced** tab.

   ![Autosubmit abolish form]

2. **Select Autosubmit abolish form.**

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

**Modifying the Abolishment Client Loader Order**

By default, the ActiveX loader attempts to load the Abolishment Client first. If this fails, the Java Applet loader attempts to load the Abolishment Client. You can optionally modify the Abolishment Client loader order.

**To modify the abolishment client loader order**

1. Browse to **Manage System→Abolishment** and switch to the **Advanced** tab.

2. **Specify the type of loader to use for the Abolishment Client:**
   - **ActiveX - Java Applet:** the loader attempts to use ActiveX, and if this fails, the loader uses the Java Applet.
   - **ActiveX:** the loader only uses ActiveX.
   - **Java Applet:** the loader only used the Java Applet.

3. **Click Save. To activate the changes, click Publish at the top of the page.**
CHAPTER 20

MANAGING SINGLE SIGN-ON AND
IDENTITY FEDERATION

Single Sign-On (SSO) is a user authentication process that allowing users to enter their user credentials once to access several resources. Identity Federation enables the end-users of one security domain to access services in another security domain, without having to authenticate separately into each domain.

The following sections are included:

- Getting Started with Single Sign-On (page 232)
- Creating Single Sign-On (SSO) Domains (page 232)
- Getting Started with Identity Federation (page 235)
- Enabling Identity Federation (page 236)
- Adding a Service Provider (page 236)
- Adding an Identity Provider (page 240)
- Reading User Certificate Attributes (page 242)
- Exporting SAML 2.0 Metadata (page 243)
- Troubleshooting Identity Federation (page 243)
Getting Started with Single Sign-On

Prerequisites: None

Single Sign-On (SSO) caches user credentials for the duration of the session or longer so that end-users do not have to reauthenticate separately for each request. The SSL VPN supports two SSO methods:

Table 20.1 Supported SSO Methods

<table>
<thead>
<tr>
<th>SSO Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent SSO</td>
<td>The credentials are stored when the end-user logs out. The user credentials are stored in the SSL VPN user account in the directory service indefinitely, or until changed.</td>
</tr>
<tr>
<td>Session-based SSO</td>
<td>The credentials are stored only for the duration of the end-user session and are removed when the end-user session ends. After authentication, the end-user can access different internal applications that are part of a Single Sign-On domain without the need for re-authentication.</td>
</tr>
</tbody>
</table>

Creating Single Sign-On (SSO) Domains

Prerequisites: None

SSO domains enable Single Sign-On for resources that accept the same user credentials. An SSO domain specifies how SSO is used for the resources included in the domain. When user credentials are modified, the changes are automatically applied to all resources in the SSO domain.

Adding an SSO Domain

To add an SSO Domain

2. Click Add SSO Domain. The Add SSO Domain page opens.
3. Enter a unique Display Name.
4. Select the Domain Type:

<table>
<thead>
<tr>
<th>Domain Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>The first time an end-user accesses a resource in the SSO domain, the end-user is prompted to enter the user credentials specified for the domain. The user credential attributes are sent to the resource as text along with the end-user’s request.</td>
</tr>
<tr>
<td>Cookie</td>
<td>When an end-user accesses a resource, the system compares a cookie on the end-user’s computer to the cookie defined for the domain. If the cookies match, login is allowed without entering any user credentials.</td>
</tr>
</tbody>
</table>
5. (Optional, Text only) Select **Cache on session only** if you want the SSO credentials to be kept in memory and valid only during the user session.

Note – When Cache on session only is selected, no other Single Sign-On restrictions are available.

6. (Optional) Select **Enable inactivity check** and specify how long users can go without accessing the domain before they must provide their credentials again.

7. (Optional) Select **Enable time limit check** and specify the length of time before users must provide their credentials again, regardless of when they were last active.

8. Click **Next**.

### Adding Domain Attributes

Domain attributes specify the authentication information that is expected when users log in to the domain.

- **To add a domain attribute**
  1. Click **Add Domain Attribute**. The Add Domain Attribute page opens.
  2. Select the **Attribute Name** to add according to the Domain Type:

<table>
<thead>
<tr>
<th>Text Domain Type</th>
<th>Cookie Domain Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Name</strong>: The user name used for authentication.</td>
<td><strong>Cookie Name</strong>: The name parameter in the cookie.</td>
</tr>
<tr>
<td><strong>Password</strong>: The password used for authentication. The Ticket attribute supersedes Password attribute. If an SSO Domain is configured with both Password and Ticket attributes, Password is ignored, because the Ticket is used as the password.</td>
<td><strong>Cookie Value</strong>: The value parameter in the cookie.</td>
</tr>
<tr>
<td><strong>Domain</strong>: The domain to which the user accounts belong.</td>
<td><strong>Cookie Secure</strong>: The value of the Secure parameter in the cookie. A value of TRUE indicates that the cookie should only be used in secure connections (for example, SSL) to the server. We strongly recommend setting this parameter to TRUE.</td>
</tr>
<tr>
<td><strong>Ticket</strong>: The One Time Ticket (OTT) used by the Web services API (WS API) for SSO with Web-based applications for authentication.</td>
<td><strong>Cookie Domain</strong>: The value of the domain parameter in the cookie. The domain parameter restricts the domain(s) for which the cookie is valid. We strongly recommend using this parameter to restrict which servers the cookie is visible to.</td>
</tr>
</tbody>
</table>
3. (Optional, Text Domain Type only) Select the Attribute Restriction to define how the attributes above must be presented when the user accesses the resource for the first time.
   • **Editable**: Presented as a text field in the login form.
   • **Hidden**: Hidden in the login form (cannot be seen by the user).
   • **Locked**: Locked in the login form and cannot be edited by the user.

4. Select the Attribute the Domain is **Referenced By** to specify how the user authentication information is to be entered or retrieved.
   • **User Input**: (Text Domain Type only) The authentication information is entered by the user. Selected by default.
   • **User Attribute**: The authentication information is retrieved from the user object in the directory server.
   • **Static**: The information entered in the Attribute Value field is displayed.
   • **Session User ID**: The SSO credentials are retrieved from the user session, namely the user ID. Attribute Restriction must be set to Locked and Attribute Value must be empty.

5. Enter the **Attribute Value**.

6. Click **Next**.

7. Verify the settings and click **Next**.

### Selecting the SSO Access Rule

#### To select the access rule and finish SSO configuration

1. Select the access rule that applies to the SSO Domain and click **Add**.
2. Click **Next**.
3. Click **Finish Wizard**. To activate the changes, click **Publish** at the top of the page.

**What's Next?**

- SSO Configuration is complete.
Identity federation enables the end-users of one security domain to access services in another security domain, without having to authenticate separately into each domain. Identity federation is a collaboration between a Service Provider and the Identity Provider. The Service Provider provides access to a resource. The Identity Provider authenticates the user. The SSL VPN can operate in both roles.

The Subject is a user who uses the Service Provider’s services and is authenticated by the Identity Provider. In Stonesoft SSL VPN this is usually an end-user. However, in the SAML standard a Subject can also be a device that needs an access to a service.

The Identity Provider issues Tickets to authenticated users with the information agreed between Service Provider and Identity Provider that the Service Provider needs to fulfill its task. A Ticket is signed with the server certificate of the Identity Provider. In Stonesoft SSL VPN, a Ticket is only created when a user is authenticated.

Active Directory Federation Service (ADFS) provides support for Web SSO. ADFS supports WS-F PRP and WS-F PRIP profiles. For more information about ADFS, see the Microsoft ADFS documentation.

Security Assertion Markup Language version 2.0 (SAML 2.0) is a standard created and maintained by OASIS. For more information on SAML 2.0, see OASIS documentation. The standard is based on XML and PKI and it is built on the following four concepts:

- **Assertions**: Statements about the Subject (authentication, attribute, or authorization statement).
- **Protocols**: The types of Tickets that are created (for example, requests, responses, and artifacts).
- **Bindings**: The way a Ticket is delivered (for example, HTTP Redirect binding or HTTP Post binding).
- **Profiles**: Combinations of the above concepts and relations. For example, Web Browser SSO is a profile that combines HTTP Redirect and HTTP Post to deliver the ticket, Authentication request protocol to define the messages, and Assertions to create the actual ticket to provide SSO in web browsers.

**Configuration Overview**

1. Install server certificates. See Adding Server Certificates (page 155).
2. Install CA certificates. See Adding Certificate Authority Certificates (page 153).
4. Enable Identify Federation and configure the global Identity Federation settings. See Enabling Identity Federation (page 236).
5. If the SSL VPN acts as an Identity Provider, add the Service Provider(s) that trust the SSL VPN. See Adding a Service Provider (page 236).
6. If the SSL VPN acts as a Service Provider, add the Identity Provider(s) that the SSL VPN trusts. See Adding an Identity Provider (page 240).
Enabling Identity Federation

Prerequisites: Configuration Overview

To enable Identity Federation


2. Select Enable Identity Federation and select the Server Certificate that is used to sign and validate certificates.

3. Enter the Entity ID that the SSL VPN uses when it acts as the Identity Provider in communications with Service Providers as a URL.
   - Valid protocols are HTTP and HTTPS (strongly recommended).
   - The slash ('/') at the end of the URL must be included when a Stonesoft SSL VPN Identity Provider is used.

   Example https://id.example.com/wa/auth/saml/

4. Enter the Entity ID that the SSL VPN uses when it acts as the Service Provider in communications with Identity Providers as a URL.

   Example https://service.example.com/wa/auth/saml/

5. Click Save.

What’s Next?

► If the SSL VPN acts as the Identity Provider, continue by Adding a Service Provider.
► If the SSL VPN acts as the Service Provider, continue by Adding an Identity Provider (page 240).

Adding a Service Provider

Prerequisites: Enabling Identity Federation

When the SSL VPN acts as the Identity Provider, you must configure the Service Providers that trust the SSL VPN.

To add a Service Provider


2. Click Add Service Provider. The Add Service Provider page opens.

3. Select ADFS Compliant or SAML 2.0 Compliant according to the standard that the Service Provider uses.

4. (Optional, SAML 2.0 only) Click Browse and select the file that contains the SAML 2.0 metadata for the Service Provider.

5. Click Next. The General Settings page opens. If you imported SAML 2.0 metadata, the information from the metadata is already entered.

What’s Next?

► Configuring Service Provider ADFS Settings (page 237)
► Configuring Service Provider SAML 2.0 Settings (page 238)
# Configuring Service Provider ADFS Settings

## To configure Service Provider ADFS settings

1. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Unique name to identify the Service Provider in the SSL VPN Administrator. Example: service.example.com</td>
</tr>
<tr>
<td>Stonesoft Realm</td>
<td>The URI that identifies the Stonesoft SSL VPN. Used to create trust between Stonesoft SSL VPN Identity Federation and the Service Provider. Example: urn:federation:identity</td>
</tr>
<tr>
<td>Service Provider Realm</td>
<td>The URI that identifies the Service Provider. Used to create trust between Stonesoft SSL VPN Identity Federation and the Service Provider. Example: urn:federation:service</td>
</tr>
<tr>
<td>Service Provider URL</td>
<td>Enter the URL of the Service Provider. Valid protocols are HTTP and HTTPS (<em>strongly recommended</em>). The slash ('/') at the end of the URL must be included when a Stonesoft SSL VPN Identity Provider is used. Example: <a href="https://service.example.com/wa/auth/adfs/IdPdisplayname/">https://service.example.com/wa/auth/adfs/IdPdisplayname/</a></td>
</tr>
</tbody>
</table>

2. Click Next. The Add Service Provider - Assertion Settings page opens.

3. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validity</td>
<td>The length of time (in minutes) the assertion is considered valid. The validity time is limited by the Session Time-out time specified in the Global User Account settings. Do not configure the Validity time too low. If there is a time mismatch between Identity Provider and Service Provider, the ticket is not valid.</td>
</tr>
<tr>
<td>Subject</td>
<td>Select a type and enter a user storage attribute to map to it. If several types are selected, they are prioritized from the top. After the first match, types are added as assertions.</td>
</tr>
</tbody>
</table>

4. *(Optional)* Click Add Attribute Statement and define any additional attributes the Identity Provider sends to the Service Provider in the ticket as described in the table below:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Type</td>
<td>Select one of the predefined types: NameValue, UPN, EmailAddress, CommonName, or Group.</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Attribute name is set automatically for all attribute types, except for NameValue.</td>
</tr>
<tr>
<td>User Attribute</td>
<td>Directory service attribute name for the user that is to be added as the ADFS attribute statement value.</td>
</tr>
</tbody>
</table>
Tip – Attribute statements contain specific details about the user. Groups and Roles are typical attributes, but financial data or any other property can formally be carried in an Attribute Statement.

6. Configure the Access Rules requirements for creating an ADFS response.
   • The most common Access Rules used in this context are Authentication Methods.
   • The Identity Provider only federates identities for users authenticated with the authentication requirements specified here.
   • See Getting Started with Access Rules (page 166) for more information.
7. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

What's Next?
► The Service Provider configuration is complete.

Configuring Service Provider SAML 2.0 Settings

To configure SAML 2.0 settings
1. Check the automatically entered information or manually configure the following settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Unique name to identify the Service Provider in the SSL VPN Administrator.</td>
</tr>
<tr>
<td></td>
<td>Example: service.example.com</td>
</tr>
<tr>
<td>EntityID</td>
<td>Valid protocols are HTTP and HTTPS <em>(strongly recommended).</em> The slash ('/')</td>
</tr>
<tr>
<td></td>
<td>at the end of the URL must be included when a Stonesoft SSL VPN Identity</td>
</tr>
<tr>
<td></td>
<td>Provider is used.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="https://service.example.com/wa/auth/saml/">https://service.example.com/wa/auth/saml/</a></td>
</tr>
<tr>
<td>Service Provider URL</td>
<td>Enter the URL of the Service Provider. Valid protocols are HTTP and HTTPS</td>
</tr>
<tr>
<td></td>
<td><em>(strongly recommended).</em> The slash ('/') at the end of the URL must be</td>
</tr>
<tr>
<td></td>
<td>included when a Stonesoft SSL VPN Identity Provider is used.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="https://service.example.com/wa/auth/adfs/IdPdisplayname/">https://service.example.com/wa/auth/adfs/IdPdisplayname/</a></td>
</tr>
<tr>
<td>Service Provider Audience</td>
<td>Enter the URL to which replies should be sent if it is different from the</td>
</tr>
<tr>
<td><em>(Optional)</em></td>
<td>requesting URL of the Service Provider. Valid protocols are HTTP and HTTPS</td>
</tr>
<tr>
<td></td>
<td><em>(strongly recommended).</em> The slash ('/') at the end of the URL must be</td>
</tr>
<tr>
<td></td>
<td>included when a Stonesoft SSL VPN Identity Provider is used.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="https://sp.example.com/SAML2">https://sp.example.com/SAML2</a></td>
</tr>
<tr>
<td>Select CA Certificate</td>
<td>The CA Certificate used to validate requests from this Service Provider. If</td>
</tr>
<tr>
<td></td>
<td>none is selected then both signed and unsigned requests are accepted. If a</td>
</tr>
<tr>
<td></td>
<td>CA Certificate is selected, the request must be signed.</td>
</tr>
</tbody>
</table>

2. Click Next.
3. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validity</td>
<td>The length of time (in minutes) the assertion is considered valid. The validity time is limited by the Session Time-out time specified in the Global User Account settings. Do not configure the Validity time too low. If there is a time mismatch between Identity Provider and Service Provider, the ticket is not valid.</td>
</tr>
<tr>
<td>Subject</td>
<td>Select how to identify the user associated with the identity information.</td>
</tr>
</tbody>
</table>

Note – When selecting the Subject source E-mail or Mobile phone, the system fetches the value from the SSL VPN user account. If no value is defined, the system queries the user in User Storage (using Directory Mapping on the User Storage settings). If no value is found, the SAML ticket is not created.

4. (Optional) Click **Add Attribute Statement** and define any additional attributes the Identity Provider sends to the Service Provider in the ticket as described in the table below:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 2.0 Attribute</td>
<td>Name of the SAML 2.0 attribute statement.</td>
</tr>
<tr>
<td>User Attribute</td>
<td>Directory service attribute name for the user that is to be added as the SAML 2.0 attribute statement value.</td>
</tr>
</tbody>
</table>

5. (Optional) Select **Add Client IP** to attach the client IP as an attribute to the SAML 2.0 response sent to the Service Provider.

6. (Optional) Select **Add Certificate Information** to attach certificate information from the session to the SAML 2.0 response sent to the Service Provider. See Reading User Certificate Attributes (page 242) for more information.

Note – Certificate information is attached only when the user is authenticated with a certificate authentication method.


8. Configure the **Access Rules** requirements for creating a SAML response.
   - The most common Access Rules used in this context are Authentication Methods.
   - The Identity Provider only federates identities for users authenticated with the authentication requirements specified here.
   - See Getting Started with Access Rules (page 166) for more information.

9. Click **Finish Wizard**. To activate the changes, click **Publish** at the top of the page.

**What’s Next?**

- The Service Provider configuration is complete.

**Related Tasks**

- Exporting SAML 2.0 Metadata (page 243)
Adding an Identity Provider

**Prerequisites:** Enabling Identity Federation

- **To add an Identity Provider**
  1. Browse to **Manage Resource Access** → **Identity Federation**.
  2. Click **Add Identity Provider**. The Add Identity Provider page opens.
  3. Select **ADFS Compliant** or **SAML 2.0 Compliant** according to the standard that the Identity Provider uses.
  4. (Optional, SAML 2.0 only) Click **Browse** and select the file that contains the SAML 2.0 metadata for the Identity Provider.
  5. Click **Next**. The General Settings page opens. If you imported SAML 2.0 metadata, the information from the metadata is already entered

**What’s Next?**
- Configuring Identity Provider ADFS Settings
- Configuring Identity Provider SAML 2.0 Settings (page 241)

### Configuring Identity Provider ADFS Settings

- **To configure ADFS settings**
  1. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Unique name to identify the Service Provider in the SSL VPN Administrator. Example: identity.example.com</td>
</tr>
<tr>
<td>Stonesoft Realm</td>
<td>The URI that identifies Stonesoft SSL VPN Identity Federation. Used to create trust between Stonesoft SSL VPN Identity Federation and the Service Provider. Example: urn:federation:service</td>
</tr>
<tr>
<td>Identity Provider Realm</td>
<td>The URI that identifies the Identity Provider. Used to create trust between Stonesoft SSL VPN Identity Federation and the Identity Provider. Example: urn:federation:identity</td>
</tr>
<tr>
<td>Identity Provider URL</td>
<td>URL to the Identity Provider’s WS-Federation Passive Requestor Interoperability Profile service. The use of HTTPS is strongly recommended. Example: <a href="https://identity.example.com/wa/auth/adfs/">https://identity.example.com/wa/auth/adfs/</a></td>
</tr>
<tr>
<td>Select CA Certificate</td>
<td>The CA Certificate provided by the Identity Provider used to verify the integrity of the replies from this Identity Provider. You must select a CA Certificate.</td>
</tr>
</tbody>
</table>

2. Click **Next**.
3. Select which **Authentication Statements** are expected from the Identity Provider and which **User Attribute** to use when mapping the assertion to a user.
4. Select the attributes that are expected in the ticket.
5. (Optional) Select the following additional settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Users Not Listed in Any User Storage</td>
<td>Allow users that not listed in any user storage to authenticate. Usually the sharing of user information between directories is not allowed. When this option is selected, the Service Provider must trust the information provided by the ticket from the Identity Provider.</td>
</tr>
<tr>
<td>Not Yet Valid Identity</td>
<td>Accept tickets that are not yet valid. This is to prevent problems when the Service Provider and the Identity Provider do not have synchronized clocks.</td>
</tr>
</tbody>
</table>

6. Click **Finish Wizard**. To activate the changes, click **Publish** at the top of the page.

### Configuring Identity Provider SAML 2.0 Settings

1. (Optional) Deselect **Visible in Authentication Menu** if you do not want to allow the Identity Provider initiate Federated Authentication processes.

2. Check the automatically entered information or manually configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Unique name to identify the Service Provider in the SSL VPN Administrator. Example: identity.example.com</td>
</tr>
<tr>
<td>Entity ID</td>
<td>Valid protocols are HTTP and HTTPS <em>(strongly recommended)</em>. The slash (‘/’) at the end of the URL must be included when a Stonesoft SSL VPN Identity Provider is used. Example: <a href="https://identity.example.com/wa/auth/saml/">https://identity.example.com/wa/auth/saml/</a></td>
</tr>
<tr>
<td>Identity Provider URL</td>
<td>URL to the Identity Provider’s WS-Federation Passive Requestor Interoperability Profile service. The use of HTTPS is strongly recommended. Example: <a href="https://identity.example.com/wa/auth/saml/">https://identity.example.com/wa/auth/saml/</a></td>
</tr>
<tr>
<td>CA Certificate</td>
<td>Select the CA Certificate provided by the Identity Provider used to verify the integrity of the replies from this Identity Provider. You must select a CA Certificate.</td>
</tr>
</tbody>
</table>

3. Click **Next**.
4. Define the following Attribute Settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Users Not Found in Any User Storage</td>
<td>Allow users that not listed in any user storage to authenticate. Usually the sharing of user information between directories is not allowed. When this option is selected, the Service Provider must trust the information provided by the ticket from the Identity Provider.</td>
</tr>
<tr>
<td>User Storage Attribute Name</td>
<td>The directory service attribute name the SAML subject is mapped against to find a local user for the session. If no local user is found, the access is denied unless unknown users are allowed.</td>
</tr>
<tr>
<td>Response Attribute Name</td>
<td>The SAML Attribute name in the SAML 2.0 response that is used as a user name. If empty, the value of the SAML Subject Name Identifier is used as a user name.</td>
</tr>
<tr>
<td>Response Attribute is Base 64 Encoded (Optional)</td>
<td>Select this option if the SAML 2.0 response is bas 64 encoded.</td>
</tr>
</tbody>
</table>

5. Click Finish Wizard. To activate the changes, click Publish at the top of the page.

What’s Next?
- The Identity Provider configuration is complete.

Related Tasks
- Exporting SAML 2.0 Metadata (page 243)

Reading User Certificate Attributes

It is possible to add information from a user certificate to the SAML ticket if the user is authenticated with a certificate authentication method. This information can be read by the Service Provider from the SAML session to create groups depending on it. For example, you can create a group of users that have authenticated with a certificate from the same issuer. To be able to read this data, you must know the names of the attributes stored in the ticket.

Note – The serial number values (CA.Certificate.SerialNumber and Certificate.SerialNumber) are presented in hex format without white spaces.

The following attributes are stored in the ticket:
- CA.Certificate.SerialNumber
- Certificate.SerialNumber
- Certificate.Issuer
- Certificate.Issuer.CommonName
- Certificate.Issuer.GivenName
- Certificate.Issuer.Surname
- Certificate.Issuer.OrganizationName
Exporting SAML 2.0 Metadata

Prerequisites: Adding a Service Provider / Adding an Identity Provider

Exporting SAML 2.0 metadata allows you to provide information about the Identify Federation configuration of the SSL VPN as an XML file to Service Providers or Identity Providers.

To export SAML 2.0 metadata
2. If the SSL VPN acts as an Identity Provider, click Download IDP Metadata and save the XML file.
3. If the SSL VPN acts as a Service Provider, click Download SP Metadata and save the XML file.

What's Next?
提供更多 XML metadata file to the Service Provider or the Identity Provider.

Troubleshooting Identity Federation

Prerequisites: None

Check the following sources for additional information when troubleshooting identity federation problems:

Table 20.2 Identify Federation Troubleshooting Tools

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Service debug log</td>
<td>The Policy Service debug log contains information about how the Service Provider has handled a ticket or why the ticket was not accepted.</td>
</tr>
<tr>
<td>Access Point raw external log</td>
<td>The Access Point raw external log for the Identity Provider shows what has been sent to the user’s browser. The Access Point raw external log for the Service Provider shows the delivered ticket before it is passed to the Policy Service and validated. Note that the ticket is Base64 encoded in the raw external log.</td>
</tr>
</tbody>
</table>
The signer certificate is sent in the request/response, and verified using the corresponding CA certificate. Ensure that the CA certificate uploaded to the SSL VPN is the one that issued the signer certificate.

Make sure that the URLs have been entered correctly and that they end with a `/`

Make sure that the system time on the Service Provider and Identity Provider is synchronized.

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates</td>
<td>The signer certificate is sent in the request/response, and verified using the corresponding CA certificate. Ensure that the CA certificate uploaded to the SSL VPN is the one that issued the signer certificate.</td>
</tr>
<tr>
<td>Identity Provider URL/Service Provider URL</td>
<td>Make sure that the URLs have been entered correctly and that they end with a <code>/</code>.</td>
</tr>
<tr>
<td>Server time</td>
<td>Make sure that the system time on the Service Provider and Identity Provider is synchronized.</td>
</tr>
</tbody>
</table>
CHAPTER 21

MONITORING IN THE SSL VPN

The monitoring of the SSL VPN consists of logging and alerting, reporting, and auditing.

The following sections are included:

► Getting Started with Monitoring the SSL VPN (page 246)
► Monitoring System Status (page 246)
► Monitoring Current User Sessions (page 250)
► Viewing Logs in the SSL VPN Administrator (page 251)
► Configuring Alert Notifications (page 252)
► Generating Reports (page 254)
► Configuring Logging (page 255)
Getting Started with Monitoring the SSL VPN

Prerequisites: None

You can monitor the SSL VPN either through the SSL VPN Administrator, or through the Stonesoft Management Client. Detailed instructions for monitoring the SSL VPN through the Management Client can be found in the Online Help of the Management Client and the Administrator's Guide PDF.

Limitations

Status and event information is only displayed if the license includes the applicable services or features.

Monitoring System Status

Prerequisites: None

Status Overview

The Status Overview displays information about the current status of the system.

The Status Overview consists of the following sections:

- **Users**: displays the registered number of concurrent users and user accounts.
- **Resources**: lists the resource hosts and Single Sign-On (SSO) domains.
- **System information**: displays information about the software version, the license version, and the license type.
- **Administrators**: lists the display name of the current administrator and the total number of administrators currently logged in.
Event Overview
The Event Overview provides a snapshot of the status of the different services. It is updated every 15 seconds.

<table>
<thead>
<tr>
<th>Event Overview</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/18/10 11:58 AM</td>
<td>Debug logging: disabled</td>
</tr>
<tr>
<td>3/18/10 11:58 AM</td>
<td>User storage Internal LDAP: connected</td>
</tr>
<tr>
<td>3/18/10 11:58 AM</td>
<td>Directory Service: connected</td>
</tr>
<tr>
<td>3/18/10 11:58 AM</td>
<td>Access Point: connected</td>
</tr>
<tr>
<td>3/18/10 11:58 AM</td>
<td>Administration Service: started</td>
</tr>
<tr>
<td>3/18/10 11:58 AM</td>
<td>Policy Service: connected</td>
</tr>
<tr>
<td>3/18/10 11:58 AM</td>
<td>Authentication Service: connected</td>
</tr>
</tbody>
</table>

Listed events include:
- Failed or restored connections to the directory service or any of the configured user storage locations.
- Failed or restored connections to any of the services included in the system network.
- Activated or deactivated debug logging.

Monitoring General Status
General status is shown at Monitor System → System Status on the General Status tab.

The Display Name and Host DNS name or IP address are listed for all registered Services in Stonesoft Network, Directory Services, User Storage Locations, and RADIUS Clients.
1. Details of the *Administration Service* include information about the *Host*, the *Current Server Time*, and the software *Version*.
2. The status of the configured notification channels is also displayed.

### Access Points

Access Point status is shown at **Monitor System**→**System Status** on the Access Points tab.

1. Details of the *Access Point* include information about the *Host*, the *Current Server Time*, and the software *Version*.
2. Information about the current connections, the hardware status, and SSL status is also displayed.
**Policy Services**

Policy Service status is shown at **Monitor System ➔ System Status** on the Policy Services tab.

![Policy Service Status](image)

All registered Policy Services are listed. Details of the Policy Services include information about the **Host**, the **Current Server Time**, and the software **Version**.

**Authentication Services**

Authentication Service status is shown at **Monitor System ➔ System Status** on the Authentication Services tab.

![Authentication Service Status](image)

All registered Authentication Services are listed. Details of the Authentication Services always include information about the **Host**, and may also include information about the **Current Server Time**, and the software **Version**.
Monitoring Current User Sessions

Prerequisites: None

On the User Sessions page, you can search for user sessions, view ongoing user sessions, and close current user sessions.

Viewing Current User Sessions

To view current user sessions


2. Enter the search criteria:
   • User ID: enter a complete User ID, or part of a User ID and the wildcard character *.
   • Authentication Method: select the authentication method used when the end-user logged in.

3. Click Search. A list of all current user sessions that match your search criteria is displayed.

Closing Current User Sessions

To close current user sessions

Select Delete next to the user session in the list and click Delete. The user session is closed, and the end-user must log in again.

Note – Deleting a user session only closes the active session. It does not delete the user account.
Log messages can be viewed in the SSL VPN Administrator’s Log Viewer. When you view logs, you select Filter settings to select which logs are displayed. You can use Search Criteria to trace specific log events, such as user activity through selected servers. You can select multiple registered servers in the Log Viewer. The messages displayed in the Log Viewer are restricted to selected servers.

**To view logs in the SSL VPN Administrator**

1. Browse to **Monitor System→Log Viewer**. The Log Viewer opens.
2. Select the **Log Type** to display:

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Information about the functioning of the SSL VPN and run-time events.</td>
</tr>
<tr>
<td>Audit</td>
<td>Information about user activity, such as log on, log out, and session events. All SSL VPN Administrator user activities are also logged here.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Information about RADIUS authentication events. RADIUS logs are available for Administration Services.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Information about HTTP server requests. HTTP logs are available for Access Points and Administration Services.</td>
</tr>
</tbody>
</table>

3. Select the **Services** for which to show logs. You can select individual services, or Ctrl-click to select multiple services.
4. Enter additional **Search Criteria**. The searches are not case-sensitive and the search criteria can consist of several words.
   - For an exact match, all entered words must exist.
   - For an OR search, use the special word ‘or’. OR operations have precedence over AND operations: “a or b and c or d” is equal to “(a or b) and (c or d)”.
   - Negations can be obtained using the minus sign ‘-’.
   - The wildcard characters ‘*’ and ‘?’ are allowed.
   - * signifies any number of characters, and ? signifies exactly one character.
   - Regular expressions are allowed: ‘[’, ’]’, ‘{’, ’}’, ‘^’, and ‘$’.
   - To search for the special characters ‘?’’, ‘*’, ‘[’, ’]’, ‘{’, ’}’, and ‘^’; use quoted searches.
5. Specify the **Time Range** during which the logs were created.
6. Click **View Log**. The logs matching your search criteria open in a new tab.
Configuring Alert Notifications

**Prerequisites:** Alert channels must be configured in the Notification Settings

Alert notifications are messages sent to selected receivers when specified events occur in the system. Alert notification messages are distributed by e-mail and/or SMS. You must configure the appropriate channels for each service separately in the Manage System section on the Notification Settings pages.

**Adding Alerts**

- **To add an alert**
  1. Browse to **Monitor System**→**Alerts**. The Manage Alerts page opens.
  2. Click **Add Alert**. The Add Alert Wizard starts.
  3. Enter a unique **Display Name** to represent the alert in the SSL VPN Administrator.
  4. Select at least one **Notification Channel**.
  5. Click **Next**.

**What’s Next?**
- Proceed to Specifying Alert Event Types.

**Specifying Alert Event Types**

You can select and combine a number of predefined alert events. Alert events include lost and restored connections to the Directory Service or services in the system network, or user activity, such as exceeded number of access requests.

- **To specify the alert event types**
  1. *(Modifying an existing alert only)* Open the properties of the Alert and switch to the **Alert Events** tab.
  2. Select the alert event(s) for which you want an alert to be sent:

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Accounts</td>
<td>Alerts are triggered when accounts are locked or unlocked for access, when users authenticate, and for time-locks. See the Online Help for detailed descriptions of alert events for User Accounts.</td>
</tr>
<tr>
<td>Resource Host</td>
<td>Alerts are triggered when resources go offline or online. See the Online Help for detailed descriptions of alert events for Resource Hosts.</td>
</tr>
<tr>
<td>Services in Stonesoft Network</td>
<td>Alerts are triggered when the connection to services in the system network are lost or restored. See the Online Help for detailed descriptions of alert events for services in system Network.</td>
</tr>
<tr>
<td>Directory Service</td>
<td>Alerts are triggered when the connection to the Directory Service is lost or restored. See the Online Help for detailed descriptions of alert events for Directory Services.</td>
</tr>
</tbody>
</table>
3. If you are adding a new alert, click **Next**. Otherwise click **Save**.

### What’s Next?
- If you want to change the alert receivers for an existing alert, or if you are adding a new alert, proceed to **Specifying Alert Receivers**.

### Specifying Alert Receivers

> **To specify alert receivers**
> 1. *(Modifying an existing alert only)* Open the properties of the Alert and switch to the **Alert Receivers** tab.
> 2. Select one or more of the **Available Roles** for receiving the alert and click **Add**.
> 3. Click **Next**.
> 4. *(Optional)* Click **Add E-mail Address** and enter the e-mail address. Click **Next** *(new alert)* or **Add E-mail Address** *(existing alert)*.
> 5. *(Optional)* Click **Add Cell Phone Number** and enter the mobile phone number to which SMS notifications are sent. Click **Next** *(new alert)* or **Add Cell Phone Number** *(existing alert)*.

**Note – You must enter either an e-mail address or a mobile phone number.**

6. Click **Finish Wizard** *(new alert)* or **Save** *(existing alert)*. To activate the changes, click **Publish** at the top of the page.
Generating Reports
Prerequisites: None

In addition to viewing logs in the Log Viewer, you can also generate reports. Reports include real-time and historical statistical data. Related reports are organized in report groups.

▼ To generate a report
2. Select the report group by clicking the report name under Generate Report.
3. (Optional) Select Complete Report to generate a report containing statistics from all available report types.
4. Specify the Time Range:
   • Last allows you to specify a time period in hours, days, weeks, months, or years.
   • From - to allows you to enter specific start and end dates and times.
   • All Available specifies a time range that begins from the time when the log database was created.
5. Select Filter to restrict which data is included in the report. For detailed descriptions of the report filters, see the Online Help.
6. Select the Chart Type and graphics Style. Each type of report includes default Chart Types and Styles, but you can freely customize and combine Chart Types and Styles.
7. Click Generate Report. You are prompted to save the report.
8. Select the Download settings for the report:
   • PDF: the report is downloaded in PDF format.
   • Data: report data is downloaded as a tab-delimited text file.
   • Images: images are scaled to the specified resolution and downloaded.
9. Click Download. Depending on the download settings, a .zip or .pdf file with the specified contents is created, and can be downloaded by clicking the link.
Configuring Logging

Prerequisites: None

Configuring the logging settings allows you to customize what logging information is collected and how the information is collected. You can adjust the types of logs that the system generates and set a filter for the severity level of logs that are collected. When adjusting logging, keep in mind that both Reports and Alerts are affected by the log collecting settings.

Configuring Logging for a Registered Server

To configure logging for a registered server

2. Click the Registered Server for which you want to configure logging.
3. Select the Log Type you want to collect for the server:
   - System Logs: Collects information about the functioning of the SSL VPN and run-time events.
   - Audit Logs: Collects information about user activity, such as log on, log out, and session events. All SSL VPN Administrator user activities are also logged here.
   - HTTP Logs: Collects information about HTTP server requests. HTTP logs are available for Access Points and Administration Services.
   - RADIUS Logs: Collects information about RADIUS authentication events. RADIUS logs are available for Administration Services.
4. Select the Log Level for each log type:
   - Off: no logs are collected.
   - Fatal: only logs about fatal errors are collected.
   - Warning: logs about warnings and fatal errors are collected.
   - Info: logs about info messages, warnings, and fatal errors are collected.
5. Select the Log File Rotation to define how log files are stored:
   - New log file is created every day: a new log file is created each day, and events are logged in the daily file.
   - Log file rotation is disabled: all events are logged in the same file.
   - Rotation is based on file size: a new log file is created when the log file reaches the maximum size.
6. (Only for rotation based on size) Specify the Max File Size in kilobytes.
7. (Optional) Specify the number of Max Files in Rotation after which the system deletes the oldest log file and creates a new log file.
8. If you are configuring HTTP Logging or Audit Logging for an Access Point, configure the Additional Options for HTTP Logs on Access Points (page 256) or Additional Options for Audit Logs on Access Points (page 257).
9. Click Save. To activate the changes, click Publish at the top of the page.
Additional Options for HTTP Logs on Access Points

If the log type is HTTP log for an Access Point, the following additional settings are also available:

**Table 21.1  Settings for HTTP Logs on Access Points**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP Address</td>
<td>The Client IP Address that must be used when the Raw External Log and Raw Internal Log are enabled when debug mode is selected. The logs only register events coming from the entered IP Address. By default all IP addresses are logged. Wildcards are allowed in the Client IP Address. Examples: 192.168.* - Log all IP addresses in the 192.168 subnet. 127.* - Log all IP addresses in the 127 subnet. * - Log all IP addresses.</td>
</tr>
<tr>
<td>Information to be registered in the log file</td>
<td>The authentication method used by the client.</td>
</tr>
<tr>
<td>Authentication method used by the client</td>
<td>Defines whether the client browser allows the response to be cached.</td>
</tr>
<tr>
<td>Client browser is allowed to cache response</td>
<td>The IP address of the client that accessed the Access Point.</td>
</tr>
<tr>
<td>Client IP address</td>
<td>The session id (WASID) of the client (cs-session).</td>
</tr>
<tr>
<td>Client session</td>
<td>The user name used by the client.</td>
</tr>
<tr>
<td>Client user name</td>
<td>The client's cookie headers.</td>
</tr>
<tr>
<td>Cookies</td>
<td>The size of the response (sc-bytes, cs-bytes).</td>
</tr>
<tr>
<td>Data transferred from client</td>
<td>The query that is sent from the client to the Access Point. If the path is followed by a '?' the query is what comes after the '?' (cs-uri-query).</td>
</tr>
<tr>
<td>Query</td>
<td>The device used by the client (defined in the Device Definition section).</td>
</tr>
<tr>
<td>Device</td>
<td>The DNS name the client uses for the Access Point (cs-host).</td>
</tr>
<tr>
<td>Host header</td>
<td>The version of the HTTP protocol used by the client.</td>
</tr>
<tr>
<td>HTTP version</td>
<td>The session ID of the Policy Service session (cs-internal-session).</td>
</tr>
<tr>
<td>Internal client session</td>
<td>The requested path on the internal server (sr-uri-stem).</td>
</tr>
<tr>
<td>Internal path</td>
<td>The protocol used between the Access Point and the resource host (sr-protocol).</td>
</tr>
</tbody>
</table>

---
If the log type is Audit Log for Access Point, the following additional settings are also available:

**Table 21.2 Settings for Audit Logs on Access Points**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information to be registered in the log file</td>
<td></td>
</tr>
<tr>
<td>Client authentication method</td>
<td>The authentication method used by the client.</td>
</tr>
<tr>
<td>Client IP address</td>
<td>The IP address of the client that accessed the Access Point.</td>
</tr>
<tr>
<td>Client session</td>
<td>The session ID (WASID) of the client.</td>
</tr>
<tr>
<td>Client user name</td>
<td>The user name used by the client.</td>
</tr>
<tr>
<td>Query</td>
<td>The query that is sent from the client to the Access Point. If the path is followed by a '?' (cs-uri-query).</td>
</tr>
<tr>
<td>Device</td>
<td>The device used by the client (defined in the Device Definition section).</td>
</tr>
</tbody>
</table>
### Table 21.2 Settings for Audit Logs on Access Points (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event code</td>
<td>The event code of the message.</td>
</tr>
<tr>
<td>Event text</td>
<td>The message text.</td>
</tr>
<tr>
<td>Host header</td>
<td>The DNS name the client uses for the Access Point (cs-host).</td>
</tr>
<tr>
<td>Internal client session</td>
<td>The session ID of the Policy Service session (cs-internal-session).</td>
</tr>
<tr>
<td>Method</td>
<td>The method used between the client and the Access Point. This is usually GET or POST.</td>
</tr>
<tr>
<td>Path</td>
<td>The requested path (cs-uri-stem)</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol used between the client and the Access Point. This is usually HTTP or HTTPS.</td>
</tr>
<tr>
<td>Referrer</td>
<td>The client’s referrer header, that is, the previous site that linked the user to the Access Point.</td>
</tr>
<tr>
<td>Resource host</td>
<td>The DNS name or the IP address of the resource host (r-host).</td>
</tr>
<tr>
<td>Response code</td>
<td>The status code from the Access Point (sc-status).</td>
</tr>
<tr>
<td>Time taken</td>
<td>The duration of the event, in seconds.</td>
</tr>
<tr>
<td>User agent</td>
<td>The client’s user agent header.</td>
</tr>
<tr>
<td>Error codes to suppress</td>
<td>Defines which error codes to exclude from the log files. You can enter multiple error codes separated with a comma.</td>
</tr>
<tr>
<td></td>
<td>The following error codes are registered in the log files by default: 1022300, 1022301, 1022302, 1022303, 1022304, 1022305, 1022306, 1022307, 1022308, 1022309, 1022310, 1022312, 1022313, 1022314, 1022315, 1022316, 1022317, 1022319, 1022320, 1022321, 1022322, 1022323, 1022330, 1022331, 1022332, 1022500, 1022501, 1022600, 1022601, 1022602 and 1022603.</td>
</tr>
</tbody>
</table>
Configuring Global Logging Settings

The global logging settings affect all logs collected from all registered servers.

▼ To configure global logging settings
2. Click Manage Global Logging Settings.
3. Configure the settings as needed:
   • Log Directory: Enter the path to the location where log files are stored.
   • Time Zone: Select the time zone for log timestamps. Local time uses the appliance’s system time.
   • Log Collection Interval: Enter the interval in seconds for how frequently logs are collected from the network servers. Setting the Log Collection Interval too high can prevent the ability to view real-time reports. Alerts are not sent until the related logs are collected.
4. Click Save. To activate the changes, click Publish at the top of the page.

Enabling Debug Logging

Debug logging enables the following types of additional Access Point log collection:
   • Raw External Log
   • Raw Internal Log
   • Raw Proxy Interchange Log
   • Hyperlinks Log
   • Form-based Log

▼ To enable debug logging
2. Click Manage Global Logging Settings. The Manage Global Logging Settings page opens.
3. Select Enable debug logging.
4. Click Save. To activate the changes, click Publish at the top of the page.
MAINTENANCE

In this section:

- Licenses - 263
- Working With Backups - 265
- Upgrading - 271
A license verifies that you are entitled to use the SSL VPN, and defines which features are enabled.

The following sections are included:

- Getting Started with Licenses (page 264)
- Installing and Updating Licenses Through SSL VPN Administrator (page 264)
- Installing and Updating Licenses Through SMC (page 264)
Getting Started with Licenses

Licenses are issued when you purchase a product and you can upgrade them to new supported versions as part of each component’s support and maintenance contract.

The licenses for SSL VPN appliances can be installed either in the SSL VPN Administrator or in the Stonesoft Management Center (SMC) if the SSL VPN has been integrated with the SMC.

When managing licenses through the SMC, the SSL VPN licensing information is not communicated from the SSL VPN to the SMC. You must first import the SSL VPN license to the SMC, and transfer the license information from the SMC to the SSL VPN in a policy upload.

Initial installation of licenses is described in the SSL VPN Appliance Installation Guide. When you receive the Stonesoft SSL VPN appliance, it comes with a temporary license that you must replace with a permanent license after initial configuration.

New licenses can be downloaded from the Stonesoft License Center at http://www.stonesoft.com/en/customer_care/licenses/.

Limitations

Only features that are included in the license are shown in the SSL VPN Administrator.

You must upload a new license file if you have purchased additional features, if your license file has expired, or if it is corrupt.

Installing and Updating Licenses Through SSL VPN Administrator

To import and install a license through SSL VPN Administrator

2. In the SSL VPN Administrator, browse to Monitor System→License.
3. Scroll down to Upload New License at the bottom of the page.
4. Click Browse and browse to the location of the license file.
5. Click Upload License. To activate the changes, click Publish at the top of the page.

Installing and Updating Licenses Through SMC

To import and install a license through SMC

2. In the Management Client, select Administration→Licenses→SSL VPN.
3. Right-click SSL VPN and select Install Licenses.
4. Browse to the license file and click Install.
5. Apply the configuration to transfer the license to the SSL VPN engine.
Backups allow you to save and restore configuration information.

The following sections are included:

- Getting Started With Backing up and Restoring SSL VPN (page 266)
- Backing up and Restoring the SSL VPN in the Web Console (page 266)
- Backing up and Restoring the SSL VPN on the Command Line (page 267)
Getting Started With Backing up and Restoring SSL VPN

The backing up and restoring of SSL VPN can be done either in the SSL VPN Web Console (recommended) or on the appliance command line.

Limitations
A backup can be restored safely only on the same version it was created on.

What Do I Need to Know Before I Begin?
In a mirrored configuration, only the primary appliance needs to be backed up.

Backing up and Restoring the SSL VPN in the Web Console

Back up the SSL VPN in the Web Console

To back up SSL VPN in the Web Console
2. (Optional) Enter a Comment to identify the backup.
3. Click Create Backup. The backup process starts. When the backup is finished the following message is displayed: “Backup creation finished. You can save it to your browser’s host.”
4. Download the created backup by clicking Save.

Restoring a Backup in the Web Console

To restore a backup in the Web Console
1. Browse to System→Backup Management.
2. Click the Restore button next to the backup file you want to restore. The restoring of the backup starts. When the process is finished, a confirmation message is displayed.
Backing up and Restoring the SSL VPN on the Command Line

Accessing the Command Line Interface

▼ To access the command line interface

1. Connect to the appliance in one of the following ways:
   • Connect a keyboard and display to the appliance.
   • Connect a serial cable between the appliance and a computer. Make a terminal
   connection from the computer with settings 9600bps, 8 databits, 1 stopbit, no parity.
   • Open an SSH connection to the appliance. SSH access to the command line can be
   enabled and disabled through the Web Console (System→Services). When SSH is
   enabled, it can be used through any interface (unless TCP port 22 is reserved by some
   other service).

2. Log in with the following credentials:
   • Username: root.
   • Password: the password set for the appliance during the initial configuration.

   Tip – You can change the password through the Web Console (System→Root Password), in the
   configuration script (sg-reconfigure), or through the SMC.

3. (Optional) Change the keyboard layout by running the command
   `sg-reconfigure --no-shutdown`.
   • The default keyboard layout is US English. In this layout, the dash character (required for
   running the command) is located next to the backspace key.

What’s Next?

► To backup SSL VPN in the command line interface, proceed to Backing up the SSL VPN
   on the Command Line (page 268).

► To restore SSL VPN in the command line interface, proceed to Restoring a Backup on
   the Command Line (page 269).
Chapter 23  Working With Backups

Back up SSL VPN configurations on the command line

**Prerequisites:** Accessing the Command Line Interface

The backup script backs up all necessary files on the appliance, including all configuration files, customizations made to the look of the portal pages, and the user database.

**Note** — The backup script shuts down all services for the duration of the backup process (this takes typically under one minute). Run the backup during a scheduled maintenance break if you need to avoid this short interruption of service to your end-users.

**To back up SSL VPN configuration in the command line interface**

1. Run the `sg-backup` command (for additional options, run the command with the option `--help`).
2. Wait for the backup to finish. The backup is created in a new directory in the `/spool/backups` directory. The name and location of the backup file are displayed in your console.
3. Copy the backup file to a safe location using SSH file transfer or by copying the files to a location that you can access through the SSL VPN Administrator.

**Example** To make the files accessible through the SSL VPN Administrator:

Give the command: `cp /spool/backups/<backup file>.tar.gz /data/portwise/administration-service/files/`

In the SSL VPN Administrator, click **Browse** at the top of the page and download the file to your computer.

Change the file ownership using the command: `chown pwuser:pwuser <backup-file-name>.tar.gz`. If the ownership is not changed, some operations (such as deleting the file) are not possible from the Administrator interface.

4. **(Optional)** Run the command `rm /spool/backups/<backup file>` to delete the backup from the temporary folder.
   - When you back up the system, the configurations are stored in memory, and are cleared when the appliance boots up the next time.
   - We recommend that you delete the temporary files manually to clear the memory used if you run the backup script more than once without rebooting.
Restoring a Backup on the Command Line

Prerequisites: Accessing the Command Line Interface

Note – The backup restoration shuts down all services for the duration of the process (this takes typically under one minute). Run the backup during a scheduled maintenance break if you need to avoid this short interruption of service to your end-users.

To restore SSL VPN from a backup in the command line interface

1. Copy the backup archive file to the appliance using SSH file transfer or by copying the files through the SSL VPN Administrator.

Example To make the files accessible through the SSL VPN Administrator:
In the SSL VPN Administrator, click Browse at the top of the page and upload the file to the appliance.
On the appliance command line, run the command cd /data/portwise/administration-service/files/ to access this folder.
Change the file ownership using the command: chown pwuser:pwuser <backup-file-name>.tar.gz. If the ownership is not changed, some operations (such as deleting the file) are not possible from the Administrator interface.

2. Run the sg-restore command line in the directory where the backup file is stored (for additional options, run the command with the option --help).

3. Wait for the backup restoration to finish.

4. Reboot the appliance by entering the command reboot.
CHAPTER 24

UPGRADING

This section provides step-by-step instructions for upgrading SSL VPN appliances to a new software version.

The following sections are included:

► Getting Started With Upgrading SSL VPN (page 272)
► Upgrading Stand-Alone SSL VPN (page 272)
► Upgrading SSL VPN With SMC (page 273)
Getting Started With Upgrading SSL VPN

The upgrading of SSL VPN can be done through the SSL VPN Web Console, or through the Management Client (if applicable).

What Do I Need to Know Before I Begin?
Upgrading a mirrored SSL VPN is similar to upgrading a single SSL VPN. However, when upgrading a mirrored system, you must first finalize the upgrade of the Primary node, and then upgrade the Secondary node.

To upgrade the SSL VPN through the Management Client, you must have configured the SSL VPN to work with the SMC as described in Integrating the SSL VPN With the SMC (page 73).


Upgrading Stand-Alone SSL VPN
Prerequisites: None

The upgrade requires a .zip file for the new software version. You can download the file from the Stonesoft website. Transfer the file to the computer you use to connect to the SSL VPN Web Console on the appliance.

▼ To upgrade the SSL VPN through the Web Console
1. Open the Web Console and browse to System→Remote Upgrade.

2. Click Browse and select the .zip file for the new software version.
3. Click Upgrade.
4. Browse to System→Services and click Reboot.

What’s Next?
 ► The upgrade is complete and the SSL VPN gateway reboots.
**Upgrading SSL VPN With SMC**

**Prerequisites:** SMC must be installed and configured, Making Initial Contact

If you have the Stonesoft Management Center installed and you have established initial contact between the Management Server and the SSL VPN, you can upgrade the SSL VPN through the SMC.

▼ **To upgrade SSL VPN with SMC**

1. Log in to the Management Client and select **File**→**Import**→**Import Engine Upgrades** from the menu. The Import Engine Upgrade dialog opens.

2. Select the engine upgrade (**sslgw_engine_version_platform.zip** file) and click **Import**. The import takes a while. You can see the related messages in the status bar at the bottom of the Management Client window.

3. In the System Status view, browse to **SSL VPN Gateways**.

4. Right-click the SSL VPN gateway and select **Configuration**→**Upgrade Software**. The Remote Upgrade Task Properties dialog opens.

5. Select **Remote Upgrade (transfer + activate)** as the upgrade **Operation**.

6. Select the SSL VPN gateway as the **Target** to upgrade.

7. **Select** the Engine Upgrade **.zip** file you imported.

8. Click **OK**. The SSL VPN is upgraded.

**What’s Next?**

► The upgrade is complete and the SSL VPN gateway reboots.
APPENDICES

In this section:

Default Listening Ports - 277
Glossary - 281
Index - 291
This Appendix lists the default listening ports used for traffic to and from the services running on the SSL VPN gateway. The most important ports are shown in the illustration below. For a complete listing, refer to the table that follows.

**Illustration A.1  Default Ports for System Services**
<table>
<thead>
<tr>
<th>Firewall Interface</th>
<th>From</th>
<th>To</th>
<th>Listening Port</th>
<th>Protocol and Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Interface</td>
<td>All</td>
<td>Access Point</td>
<td>TCP 80</td>
<td>HTTP (for redirection to HTTPS)</td>
</tr>
<tr>
<td>External Interface</td>
<td>All</td>
<td>Access Point</td>
<td>TCP 443</td>
<td>HTTPS (SSL)</td>
</tr>
<tr>
<td>N/A</td>
<td>Access Point</td>
<td>Access Point</td>
<td>TCP 16972</td>
<td>Internal Communication for load-balancing between appliances (on physical interface eth1)</td>
</tr>
<tr>
<td>Internal Interface</td>
<td>Access Point</td>
<td>Any internal application</td>
<td>Port used by internal application</td>
<td>Communication between Access Point and internal applications</td>
</tr>
<tr>
<td>Internal Interface</td>
<td>Access Point</td>
<td>Administration Service</td>
<td>TCP 8300</td>
<td>Internal communication between the Access Point and the Administration Service</td>
</tr>
<tr>
<td>N/A</td>
<td>Policy Service</td>
<td>LDAP Server</td>
<td>TCP 389</td>
<td>LDAP communication with external user storage</td>
</tr>
<tr>
<td>N/A</td>
<td>Policy Service</td>
<td>LDAP Server</td>
<td>TCP 636</td>
<td>LDAPS communication with external user storage</td>
</tr>
<tr>
<td>N/A</td>
<td>External RADIUS client</td>
<td>Authentication Service</td>
<td>UDP 18120</td>
<td>RADIUS communication for Stonesoft Mobile Text</td>
</tr>
<tr>
<td>N/A</td>
<td>External RADIUS client</td>
<td>Authentication Service</td>
<td>UDP 18121</td>
<td>RADIUS communication for Stonesoft Web</td>
</tr>
<tr>
<td>N/A</td>
<td>External RADIUS client</td>
<td>Authentication Service</td>
<td>UDP 18122</td>
<td>RADIUS communication for Stonesoft Challenge</td>
</tr>
<tr>
<td>N/A</td>
<td>External RADIUS client</td>
<td>Authentication Service</td>
<td>UDP 18123</td>
<td>RADIUS communication for Stonesoft Password</td>
</tr>
<tr>
<td>N/A</td>
<td>External RADIUS client</td>
<td>Authentication Service</td>
<td>UDP 18124</td>
<td>RADIUS communication for Stonesoft Synchronized</td>
</tr>
<tr>
<td>N/A</td>
<td>External RADIUS client</td>
<td>Authentication Service</td>
<td>UDP 18125</td>
<td>RADIUS communication for Stonesoft OATH</td>
</tr>
<tr>
<td>Internal Interface</td>
<td>Access Point</td>
<td>Administration Service</td>
<td>TCP 8300</td>
<td>Internal communication between the Access Point and the Administration Service</td>
</tr>
<tr>
<td>N/A</td>
<td>Authentication Service</td>
<td>LDAP Server</td>
<td>TCP 389</td>
<td>LDAP communication with external user storage</td>
</tr>
<tr>
<td>N/A</td>
<td>Authentication Service</td>
<td>LDAP Server</td>
<td>TCP 636</td>
<td>LDAPS communication with external user storage</td>
</tr>
<tr>
<td>Firewall Interface</td>
<td>From</td>
<td>To</td>
<td>Listening Port</td>
<td>Protocol and Comment</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------</td>
<td>------------------------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N/A</td>
<td>Administrator client</td>
<td>Administration Service</td>
<td>TCP 8443</td>
<td>HTTPS for administration (through management interface eth0 only).</td>
</tr>
<tr>
<td>N/A</td>
<td>Web Console client</td>
<td>Administration Service</td>
<td>TCP 10000</td>
<td>HTTPS for administration (through management interface eth0 only).</td>
</tr>
<tr>
<td>Internal, external or none</td>
<td>External RADIUS client</td>
<td>Authentication Service</td>
<td>UDP 18119</td>
<td>RADIUS communication for accounting</td>
</tr>
</tbody>
</table>
Glossary

A

Access Rules
Define specific requirements for access to resources and SSO domains. The access rules can be used in combination for more detailed access control. Example: (access rule A AND access rule B) AND (Access rule C OR access rule D).

ASCII
American Standard Code for Information Interchange. Standard 8 bit code used in data communications. Many files interchanged from one software program to another and from IBM to Mac formats go through translation into ASCII.

ASN.1
Abbreviation for Abstract Syntax Notation one, a standard notation describing data structures for representing, encoding, transmitting, and decoding data. ASN.1 provides a set of formal rules for describing the structure of objects that are independent of machine-specific encoding techniques.

Authentication
The process of verifying the identity of an individual connecting to a system. Identities are verified through different authentication methods. See also: Authentication Method, Access Rules.

Authentication Method
A procedure used to perform authentication. Different authentication methods provide different levels of proof when identifying a user connecting to a system: from verifying basic static passwords to handling complex combinations of challenges, encryption keys, and passwords. See also: Authentication.

Authentication Server
A server used in application access control. For access to specific network resources, the server may itself store user permissions and company policies or provide access to directories that contain the information. Examples of authentication servers are Stonesoft SSL VPN Authentication Service, SecurID and SafeWord. See also: Authentication.

Authorization
The process of granting or denying access to a system resource. See also: Authentication Method, Access Rules.
**BankID**  
See E-ID.

**Base64**  
A method of encoding binary data sent as an attachment through e-mail. Base64 encoding divides three bytes of data into four bytes of ASCII text, making the resulting file size approximately 33% larger.

**Base DN**  
Identifies the root node of the LDAP data store pointing to the directory containing user data.

**CA**  
Abbreviation for Certificate Authority, a trusted third-party organization or company that issues digital certificates. The role of the CA is to validate the identity of the individual holding the certificate and to sign the certificate so that it cannot be forged.

**CA Certificate**  
Abbreviation for Certificate Authority Certificate, a certificate that identifies a certification authority. CA certificates are used to decide whether to trust certificates issued by the CA, for example when a web browser validates a server certificate.

**Cipher**  
A cryptographic algorithm used to encrypt and decrypt files and messages.

**Client Certificate**  
An attachment to an electronic message used for security purposes. The client certificates are associated with user accounts to authenticate users and give access to protected resources.

**CDP**  
Abbreviation for Control Distribution Point.

**Client Device**  
The software of a client that communicates with the server. The client device may include operating system, plug-ins, specific configurations and the proxies/gateways that the client communicates through. Examples of client devices are: Netscape 7, Windows, Macintosh, Internet Explorer and WAP-phone. A client device may be combination of entities. For example, this combination may be present for a single device: Windows, Internet Explorer and Internet Explorer 6.

**CRC**  
Abbreviation for Certificate Revocation Control. A control performed by the system to make sure that the user certificate is not revoked.

**CRL**  
Abbreviation for Certificate Revocation List. A document maintained and published by a certification authority that lists certificates that have been revoked.
CVC
Abbreviation for Certificate Authority Validity Control, a control performed by the system on the user certificate to verify that a trusted CA has issued the User Certificate.

Delegated Management
A feature used to delegate administration of user accounts and resources to multiple administrators with different privileges and responsibilities.

DER
Abbreviation for Distinguished Encoding Rules, used to encode ASN.1 objects for a consistent encoding using a binary format. Microsoft Internet Explorer understands certificates downloaded in this format. See also: ASN.1

Device
See Client Device.

Digital Certificate
Digital certificates are used to identify people and resources over networks such as the Internet. Digital certificates enable secure communication between two parties. A trusted third-party organization or company, Certificate Authority, issues certificates. The certificate contains the public key and the name of its owner. The user certificate also carries the digital signature of a Certification Authority to verify its integrity. See also: CA.

Directory Service
A directory of names, profile information and machine addresses of every user and resource on the network. It is used to manage user accounts and network permissions. When sent a user name, it returns the attributes of that individual, which may include a telephone number as well as an e-mail address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

Directory Service User Group
A user group containing all users belonging to a certain user group defined in an existing directory service.

Display Name
Defines the unique name used in the system to identify an object.

Distribution Channel
The media channel through which information is sent. For example, Mobile ID can send information via SMS or SMTP.

DMZ
Abbreviation for Demilitarized Zone, a middle ground between an organization’s trusted internal network and an untrusted, external network such as the Internet. It is recommended that the Access Point is placed in the DMZ.
DN
Abbreviation for Distinguished Name, used as primary key to entries in directory services. For example, a DN for where users reside in the directory service could be cn=users,dc=mycompany,dc=com.

DNS
Abbreviation for Domain Name System, a name resolution system that allows users locate computers on a Unix network or the Internet (TCP/IP network) by domain name. The DNS server maintains a database of domain names (host names) and their corresponding IP addresses. For example, if www.mycompany.com was presented to a DNS server, the IP address 204.0.8.51 would be returned.

E
E-ID
E-ID (formerly BankID) is a service that offers secure electronic identification and signature on the Internet, which is now legally binding in the EU. The service has been developed by a number of large banks for use by members of the public, authorities, companies, and other organizations.

Encryption
Any procedure used in cryptography to convert plaintext into ciphertext in order to prevent anyone except the intended recipient from reading that data.

F
Firewall
A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. The firewall is normally installed at the point where network connections enter a site, normally named DMZ.

FTP
Abbreviation for File Transfer Protocol, a protocol used to transmit files between computers on the Internet. See also: TCP

H
Host
A computer, for example a server, that acts as a source of information or signals. It is connected to a TCP/IP network, including the Internet. A host has a specific local or host number that, together with the network number, forms its unique IP address.

HTTP
Abbreviation for HyperText Transfer Protocol, a protocol used to transmit files over the World Wide Web.

HTTPS
Abbreviation for HTTP with SSL encryption for security. See also: HTTP, SSL.
I

Identity Provider
In Identity Federation, the Identity Provider handles the authentication of the user, that is, it makes sure that the user is the one he claims to be. In Stonesoft SSL VPN this could mean requiring a Mobile Text login or some other sort of authentication.

L

LDAP

Log Levels
Indicate the severity of a message stored in a log: fatal, warning, info, or debug.

M

MIME
Abbreviation for Multipurpose Internet Mail Extensions. A protocol for Internet e-mail that enables the transmission of non-text data such as graphics, audio, video and other binary types of files.

N

NTLM
Abbreviation for NT LAN Manager, a protocol used for authentication.

O

OATH
OATH (Open AuTHentication) is an authentication method that uses OTPs for authentication. OTPs are generated from a seed and a counter.

OpenSSL
An open source implementation of the SSL and TLS protocols. See also: SSL, TLS.

OU
Abbreviation for Organizational Unit, a standard naming attribute used in LDAP. See also: LDAP.

P

PEM
Acronym for Privacy Enhanced Mail, a standard for secure e-mail on the Internet. It supports encryption, digital signatures and digital certificates as well as both private and public key methods.

PIN
Acronym for Personal Identification Number. A private code used for identification of an individual.
PKI
Abbreviation for Public Key Infrastructure, a framework for creating a secure method for exchanging information based on public key cryptography.

Port
A port is usually an interface through which data are sent and received.

Proxy
A server that is placed between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

RADIUS
Acronym for Remote Authentication Dial-In User Service, the de facto standard protocol for authentication servers. RADIUS uses a challenge/response method for authentication.

Registered
A registered entity (for example, service, host, or domain) is an entity, that has been defined, saved and published to be used in the system.

Resource
A corporate application users can access from a remote location. Available resource types are Web resources, tunnel resources, file share resources and customized resources.

Resource Host
Defines the computer where the resource is deployed. A resource host is identified through its unique IP address. A Web resource host or customized resource host can have one or several paths connected to it.

Resource Path
Defines the route to a specific part of the web resource host or customized resource host, for example http://www.resourcehost.com/path/, where the resource path defines a subset of the resource host. Resource paths are defined when user access is restricted to that specific subset only.

SAML
Acronym for Security Assertion Markup Language, an XML standard for exchanging authentication and authorization data between an identity provider and a service provider. Stonesoft SSL VPN supports SAML 2.0.

Seed
An initial value used to generate pseudorandom numbers. Used when authenticating with Stonesoft Challenge for example.
**Server Certificate**
Server certificates ensure that communication between clients and application servers is secure and private. The clients use the server certificate to authenticate the identity of the server and to encrypt information for the server, using SSL.

**Server Pool Monitoring Agent**
Server Pool Monitoring Agents are software components that are used for sending SSL VPN appliance data to the Stonesoft Firewall. The firewall uses this data for load balancing.

**Service Provider**
In Identity Federation, the Service Provider provides services. In the SSL VPN, service is access to a resource, a tunnel set or a Web resource, to which the Service Provider provides access.

**Shared Secret**
A shared secret is used, for example, between the Authentication Service and a RADIUS client to mask passwords used in authentication. The shared secret is set manually by the Administrator.

**SMS**
Abbreviation for Short Message Service, a service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to cell phones that use Global System for Mobile (GSM) communication.

**SMPP**
Abbreviation for Short Message Peer-to-Peer protocol. SMPP is a telecommunications industry protocol for exchanging SMS messages between SMS peer entities such as short message service centres.

**SSL**
Acronym for Secure Sockets Layer, a commonly used protocol for managing the security of a message transmission on the internet. SSL uses the public- and private-key encryption system, which includes the use of a digital certificate.

**SSO**
Abbreviation for Single Sign-On, the ability for users to log on once to a network and be able to access all authorized resources. A Single Sign-On program accepts the user’s name and password and automatically logs on to all appropriate servers.

**SSO Domain**
A collection of resources that share the same logon credentials. A user can have logon credentials for several SSO domains.
TCP
Abbreviation for Transport Control Protocol, a transport layer protocol that moves multiple packet data between applications. See also: FTP.

TLS
Abbreviation for Transport Layer Security, a protocol intended to secure and authenticate communications across a public networks by using data encryption. See also: SSL.

Tunneling
A technology that enables a network to send its data via another network’s connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. Tunnels are often used to transmit non-IP protocols across IP networks.

UDP
Abbreviation for User Datagram Protocol, a transport layer protocol for the Internet. It is a datagram protocol which adds a level of reliability and multiplexing to IP datagrams. It is defined in RFC 768.

URI
Abbreviation for Uniform Resource Identifier, a formatted string that serves as an identifier for a resource, typically on the Internet. URIs are used in HTML to identify the anchors of hyperlinks. URIs in common practice include URLs. See also: URL.

URL
Abbreviation for Uniform Resource Locator, a unique, identifying address of any particular page on the web. See also: URI.

User Certificate
See Client Certificate.

User Group
A collection of users which share the same properties regarding access rights. There are three types of user groups: User Location Group, User Property Group and Directory Service User Group.

User Location Group
A user group which contains all users located under a specific node in the directory tree.

User Property Group
A user group which contains all users with a specific user attribute.

User Storage
A directory service containing information about users, user groups, and user certificates.
**WAP**
Acronym for Wireless Application Protocol. A set of communication protocol standards to enable access of online services from a cell phone.

**X.509**
A specification for digital certificates published by the ITU-T (International Telecommunications Union - Telecommunication). It specifies information and attributes required for the identification of a person or system.
INDEX

A
abolishment, 23, 226–229
  in access rules, 175
accented characters, 36
access, 22
access client, 212
  activeX loader, 214
    for linux, 212
  java applet loader, 214
  pure java access client, 215
  windows 7 configuration, 212
  windows native access client, 212
  windows vista configuration, 212
access point, 27
access rules, 30, 165
  access point, 176
    adding, 169
    criteria in, 170
    for web resources, 193
access to home directory, 180, 185
active directory, 131
activeX access client loader, 214
administration resources, 180, 186
administration service, 27
alert notifications, 252
  adding, 252
  alert event types, 252
  alert receivers, 253
alternative hosts, 191, 204
application portal, 181
  colors, 95
  customizing, 89, 92
  external sites, 194
  graphical elements, 94
  layout, 95
  page templates, 96
  texts, 93
  web resources, 193
applying the configuration, 74
assessment, 20, 222–226
  client scan paths, 223
  enabling, 223
  in access rules, 174
  plug-ins, 225
  real time scan, 224
  silent assessment, 225
auditing, 22
authentication, 21
  stonesoft, 31
authentication method access rules, 171
authentication methods
  adding, 132
  deleting, 136
  managing, 127, 151
  modifying, 136
  stonesoft challenge, 130
  stonesoft invisible token, 130
  stonesoft mobile text, 130
  stonesoft OATH, 131
  stonesoft password, 131
  stonesoft synchronized, 130
  stonesoft web, 130
authentication service
  adding, 144
authentication services, 30, 143
authorization, 21, 165
authorization settings, 210
back-end servers for RADIUS, 138
backups, 15, 265, 277
  in web console, 266
  on command line, 268
basic authentication, 132
basic system settings, configuring, 51
certificate authentication, 132
certificate authorities, 152
certificate revocation list (CRL), 152
checklist for installation, 38
cipher suites, 28
citrix metaframe, 180, 187
client certificates, 152
client device access rules, 172
client scan paths, 223
client security, 217–229
clock, see time settings
colors in application portal, 92, 95
colors in application portal, 92, 95
command line access, 267
certificate revocaiton list (CRL), 152
certificate revocation list (CRL), 152
contact information, 14
content filters, 200
creating SSL VPN element in SMC, 73
custom access rules, 176
customer support, 14
date, see time settings
default ports for system services, 26
default resources, 179
delegated management, 122
device-specific controls, 218–222
device access restrictions, 221
Index
device definitions, 218
device settings, 219
DNS
  mapping, 28
  pooled DNS mapping, 197
  reserved DNS mapping, 197
DNS name pool, 198
domino, 180, 183
dynamic pool IP, 211
dynamic tunnels, 208
E
edirectory, 131
e-ID, 132
e-ID signer, 132
e-mail messages, 149
extended user bind, 132
external directory service, configuring, 75
external sites, 194
external user storage, adding, 76
external user storage, updating, 77
F
file sharing resources, 180, 184, 185
filters for content, 200
firmware upgrade, 271
fonts in application portal, 92
foreign characters, 36
form-based authentication, 132
G
general RADIUS, 132
global access rule, 166, 167
global assessment settings, 223
global user account settings, 106
graphics, replacing, 94
groups
  user group in Directory Service, 120
  user location group, 119
  user property group, 119
H
help desk role, 122
host address, configuring, 58
host name, configuring, 58
HTML templates, 96
I
IBM, 131
icons, replacing, 94
identity federation, 231
identity provider access rules, 176
images, replacing, 94
IMAP, 180, 181
importing SSL VPN license to SMC, 74
importing users, 118
internal authentication, 21
internal proxies, 199
IP address access rules, 172
IP address pools, 211
dynamic pool IP, 211
IP addressing, configuring, 53
J
java applet access client loader, 214
L
layout in application portal, 92, 95, 96
LDAP, 131
licenses, 263
  installing through Administrator, 264
  installing through SMC, 264
link translation, 28, 196
  DNS name pool, 198
  pooled DNS mapping, 197
  reserved DNS mapping, 197
  URL mapping, 197
linking users, 114
linux, 267
linux access client, 212
load-balancing, 27
logo in application portal, 92
logon page customization, 92
logs, 251
  configuring logging, 255
M
mail resources, 180, 181, 182, 183
making initial contact, 74
mapping links, 196
microsoft active directory, 131
mirroring, 27
  administration service IP, 85
  administrator web resources, 84
  basic system services, 81
  configuring, 79
  configuring appliances as primary and secondary, 86
  preparing for mirroring, 81
monitoring, 245
  alert notifications, 252
  logs, 251, 255
  reports, 254
system status, 246
user sessions, 250
N
new features, 15
novell, 131
NTLM, 132

O
OATH, 131, 139
online help, 41
open authentication, 139
operating system, 267
operating system upgrade, 271
outlook, 180, 182

P
page templates for application portal, 96
passwords, 36, 147
patches, 271
PIN, 147
planning, 33
policy service, 28
access rules, 30
resources, 29
standard resources, 29
pooled DNS mapping, 197
POP3, 180, 181
portal resources, 180, 187, 188
pre-configured resources, 179
product overview, 20
proxies, 199
pure jave access client, 215

R
RACF, 131
RADIUS, 132, 137
real time scan, 224
registered access rules, 166, 169
registered authentication method servers, 85
remote controlling resources, terminal server, 180, 184
remote upgrade support, 273
reports, 254
reserved DNS mapping, 197
resources, 29
restoring backups
  in web console, 266
  on command line, 269
roles, 122
root CA, 152
routing, configuring, 55

S
SafeWord, 131
safeword, 132
salesforce, 180, 186
saving the initial configuration, 74
screen messages, 150
scripted resources, 204
securID, 131
self service, 123
  activation, 125
  challenge, 123
  enabling authentication methods for, 137
  internal challenge, 123
  management, 126
  system challenge, 123
  user challenge, 123
server certificates, 152
server pool monitoring agents, 87
services, 29
  access point, 27
  administration, 27
  authentication, 30
  default ports, 26
  policy, 28
sharepoint, 180, 188
silent assessment, 225
single sign-on (SSO), 30, 192, 231
  adding a domain, 232
  domains, 232
SMS messages, 150
SMTP, 180, 181
software upgrade, 271
SSL VPN administrator, 180, 186
standard resources, 29, 179–188
  access to home directory, 180, 185
  administration, 180, 186
  citrix metaframe, 180, 187
  domino, 180, 183
  file sharing, 180, 184, 185
  IMAP, 180, 181
  other, 180, 186
  outlook, 180, 182
  POP3, 180, 181
  portal resources, 180, 187, 188
  salesforce, 180, 186
  sharepoint, 180, 188
  SMTP, 180, 181
SSL VPN administrator, 186
Stonesoft SSL VPN administrator, 180
terminal server, 180, 184
windows fileshare, 180, 184
startup command, 209
static tunnels, 208
stonesoft authentication, 21
  introduction to, 31
  settings, 128
stonesoft challenge authentication, 130
stonesoft invisible token authentication, 130
stonesoft mobile text authentication, 130
stonesoft OATH authentication, 131
stonesoft password authentication, 131
stonesoft synchronized authentication, 130
stonesoft web authentication, 101, 130
super administrator, 122
support services, 14
system
  host address, 58
  host name, 58
  IP addressing, 53
  routing, 55
time, 52
system status, 246

T
technical support, 14
terminal server, 180, 184
texts, modifying in application portal, 93
time settings, configuring, 52
time-based access rules, 173
tivoli, 131
translating links, 196
trusted gateways, 27
tunnel resources, 203–215
  access client, 212
  access rules, 209
  access to home directory, 185
  alternative hosts, 204
  authorization settings, 210
citrix metaframe, 187
IMAP, 181
IP address pools, 211
outlook, 182
POP3, 181
pre-configured resources, 179
scripted resources, 204
SMTP, 181
terminal server, 184
tunnel resource hosts, 206
tunnel resource networks, 205
tunnel sets, 207
dynamic tunnels, 208
startup command, 209
static tunnels, 208
windows fileshare, 184
types of access rules, 170

U
Unknown Host Header, 49
updating external user storage, 77
upgrading, 271
URL mapping, 197
user accounts, 105
user group membership access rules, 171
user groups, 119
deleting, 121
managing, 121
searching, 121
user location group, 119
user property group, 119
user sessions
  closing, 250
  monitoring, 250
user storage access rules, 174
users
  adding, 113
  deleting, 119
  importing, 118
  linking, 114
  modifying, 119

V
variables in page templates, 99
viewing logs, 251

W
WASCR, 200
web resources, 189
  access rules for, 193
  alternative hosts, 191
  application portal options, 193
  authorization, 194
  creating, 190
domino, 183
encryption level, 195
filters, 200
internal proxies, 199
link translation, 196
outlook, 182
pre-configured resources, 179
salesforce, 186
sharepoint, 188
single sign-on (SSO), 192
SSL VPN administrator, 186
webmail, 180, 181, 182, 183
windows
  fileshare, 180, 184
  integrated login, 132
windows native access client, 212
  windows 7 configuration, 212
  windows vista configuration, 212
WML templates, 96

X
X.509, 153
Stonesoft Guides

Administrator’s Guides - step-by-step instructions for configuring and managing the system.

Installation Guides - step-by-step instructions for installing and upgrading the system.

Reference Guides - system and feature descriptions with overviews to configuration tasks.


For more documentation, visit
www.stonesoft.com/support/

Stonesoft Corporation
Itälahdenkatu 22 A
FI-00210 Helsinki
Finland
Tel. +358 9 476 711
Fax +358 9 4767 1349

Stonesoft Inc.
1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA
Tel. +1 770 668 1125
Fax +1 770 668 1131

Copyright 2013 Stonesoft Corporation. All rights reserved. All specifications are subject to change.