

Compliance Guardian Online 3 Quick Start User Guide

Service Pack 2

**Revision A
Issued April 2014**

Table of Contents

- About Compliance Guardian Online 3
- Getting a Quick Start with Compliance Guardian Online 4
 - Registering an Compliance Guardian Online Account 4
 - Logging into Compliance Guardian Online 4
 - Assigning Roles to People 4
- Configuring Settings Before Scanning Websites or SharePoint Online Sites..... 6
 - Configuring Profiles or Policies 6
 - Configuring Test Suite or Check in Test Suite Manager or Check Manager 6
 - Configuring Authentication Profile for Scanning SharePoint Online Sites..... 7
- Scanning Websites or SharePoint Online Sites 7
- Viewing Job Information in Job Monitor 7
- Viewing Scanned Report 7
- Other Settings 7
 - Configuring Preference Settings 7
 - Compliance Guardian Online Auditor 7
- Extending License..... 8
- Notices and Copyright Information 9

About Compliance Guardian Online

Compliance Guardian Online is an online version of Compliance Guardian used to scan websites or SharePoint Online sites for accessibility, privacy, site quality, and security.

Compliance Guardian is designed to ensure that information is available and accessible to the people who should have it and protected from the people who should not. Compliance Guardian helps Chief Privacy Officers, Chief Information Security Officers, Compliance Managers, Records Managers, SharePoint Administrators, and Company Executives proactively protect their IT environments from harmful information leaks, contamination, or misuse while simultaneously ensuring that all activities and content residing in their environments are compliant, accessible, and manageable.

Compliance Guardian is designed to empower organizations to comply with regulatory, statutory, or organization specific requirements to manage and oversee access to sensitive data.

Compliance Guardian works with AvePoint's extended Compliance Solutions to provide a "heat map" that provides additional actionable context about the document including: how old is the document, who authored it, how many times has it been accessed, who can access it, who has accessed it, and what have they done with it. In this way, organizations can take specific steps to protect and mitigate their risk.

By identifying, classifying, and taking action on compliance risks, and presenting this information in easily digestible formats for various stakeholders, organizations can more effectively build and maintain a compliant framework.

For full details about all of the modules and settings in Compliance Guardian Online, refer to the [Compliance Guardian Online User Guide](#).

Getting a Quick Start with Compliance Guardian Online

To quickly start using Compliance Guardian Online, the user can begin by using the features described in the following sections.

Registering an Compliance Guardian Online Account

Before using the unified Compliance Guardian Online login page URL for all users, each Compliance Guardian Online Manager verifies the user's credentials by itself.

Register an Compliance Guardian Online account by selecting **Create an account?** in the Compliance Guardian Online **Sign In** interface. Enter the corresponding registration information, and specify the domains you want to scan. Then, select **Submit** to submit the registration information.

The registered user will have 14 free days to use Compliance Guardian Online after the registration. The user can extend the license to use more Compliance Guardian Online features. For more information on extending license, refer to [Extending License](#).

Logging into Compliance Guardian Online

To log into Compliance Guardian Online, complete the following steps:

1. Open Compliance Guardian Online.
2. On the Compliance Guardian **Sign In** page, enter the following information:
 - **Login ID** – Enter the registered e-mail address.
 - **Password** – Enter the password.
 - **Stay signed in** – Select whether or not to keep signing in Compliance Guardian Online.
3. Select **Login** to log into Compliance Guardian Online.

Assigning Roles to People

After registering Compliance Guardian Online, navigate to **Compliance Guardian Online > Settings > Account Manager** to add users and assign roles to these users to define their permissions to use the product in Compliance Guardian Online.

There are two default groups:

- **Power Administrator Group** – The Power Administrator Group is the default group in Compliance Guardian Online. It cannot be deleted. The registered user can add users to the group. Users in the Power Administrator Group have Full Control permissions to use Compliance Guardian Online.

***Note:** Full Control permission means you can perform all available functions in Compliance Guardian Online.

- **Standard User Group** – The Standard User Group is another default group in Compliance Guardian Online. It also cannot be deleted. The registered user must first edit this group to assign permissions to the group, and add users to this group.

***Note:** The users in the Standard User Group cannot extend a license, use Account Manager, use Auditor Settings, use Test Suite Manager, or use Check Manager in Compliance Guardian Online although the group has the Settings permission.

The permission roles include:

- **Compliance** – Compliance includes **Compliance Scanner**, **Compliance Reports**, and **Human Auditor**.
 - **Compliance Scanner** – Permission to use Compliance Scanner in Compliance Guardian Online.
 - **Compliance Reports** – Permission to use Compliance Reports in Compliance Guardian Online. Group users cannot use **Compliance Reports > Human Auditor** if only this checkbox is selected.
 - **Human Auditor** – Permission to use **Compliance Reports > Human Auditor**. Group users can also change the file's status in the **Compliance Reports > Scan Result > View Detailed Report**.
- **Common** – **Common** includes **Settings** and **Create Shared Policies, Profiles and Scans**.
 - **Settings** – Permission to use Settings in Compliance Guardian Online.

***Note:** The users in the created group cannot extend a license, cannot use **Account Manager**, **Auditor Settings**, **Test Suite Manager** and **Check Manager** although you have selected **Settings** for the group.
 - **Create Shared Policies, Profiles and Scans** – Permission to set their scans and profiles to **Public** as the **Share Mode** (all users can see the scans or profiles the user created if the **Share Mode** of the scans or profiles is **Public**).

Configuring Settings Before Scanning Websites or SharePoint Online Sites

Before scanning the websites or SharePoint Online sites, navigate to **Compliance Guardian Online > Settings > Application Profiles** to configure the following settings.

Configuring Profiles or Policies

Configure the spider profile, filter policy, user agent profile, authentication profile, alert profile, and e-mail template according to your own requirement. You can also use the default profiles or policies for a scan without configuring them.

Configuring Test Suite or Check in Test Suite Manager or Check Manager

In order to provide a flexible and customizable compliance solution, AvePoint developed the AvePoint Testing Language (ATL) to provide organizations with the ability to rapidly respond to new compliance threats and requirements. ATL is an XML structured language that is used to validate and classify content related to compliance to standards or guidelines, including but not limited to security, privacy, accessibility, and content classification. Because it is open and modifiable, ATL allows for coverage to specifically match an organization's needs. ATL uses test definition files (checks) to match your environment and standards, test your framework and repair issues, validate that your content complies with organizational standards, and identify all content that requires user review and distribute a list of items to the appropriate parties.

- **Test Suite** – A test suite is a logical grouping of test definition files, or a set of checks, that define how to present the scanned data. Test suites allow you to build scan plans for your specific regulations and requirements. These collections are the basis of Compliance Guardian Online scans. A test suite contains one or more checks and a configuration file that is used to define how to combine these checks and set risk levels for scan results.
- **Check** – A check is an XML file that defines the logic that Compliance Guardian Online uses to check files. Checks identify the purpose (the type of check to run, such as a pattern of characters), the condition (such as social security number pattern), and the possible result (true or false). Users can change the values in the checks to determine the check conditions, but the elements' specific format defined by Compliance Guardian Online in the checks must stay the same.

In **Test Suite Manager** and **Check Manager**, you can view, edit, upload or download a test suite or check for the flexible and customizable compliance scan.

***Note:** If you have a trial license, you can only edit the following four built-in test suites: **Section 508**, **WCAG 2.0**, **Site Quality Report** and **Privacy Basics**, but you cannot edit any checks. You must purchase the corresponding test suite groups as part of your license for editing, uploading or downloading test suites or checks. For more information, refer to the [Compliance Guardian Online User Guide](#).

Configuring Authentication Profile for Scanning SharePoint Online Sites

You must configure an authentication profile in **Authentication Profile** to connect to Office 365 admin center before scanning the SharePoint Online Sites.

Scanning Websites or SharePoint Online Sites

Use **Compliance Scanner** to define the scan rules and then create a scan for scanning websites or SharePoint Online sites.

Viewing Job Information in Job Monitor

Use **Job Monitor** to view the detailed information of a scan job. You can download the job details, stop or delete a job in Job Monitor.

Viewing Scanned Report

After the scans, the related scan reports are recorded in **Compliance Reports**. Navigate to **Compliance Guardian Online > Compliance Reports** to view or manage the scan results or the reports including Risk Report, Data Table Report, File Errors Report, File Type Report, PDF Exception Report, Violation Report, Link Validation Report, and Page Title Report. You can also export the report to a datasheet or HTML file for your reference.

Other Settings

You can change the **Preference** settings and use **Compliance Guardian Online Auditor** to view the activities in Compliance Guardian Online.

Configuring Preference Settings

Navigate to **Compliance Guardian Online > Settings > Preference** to define the Compliance Guardian Online home page and time zone.

Compliance Guardian Online Auditor

Navigate to **Compliance Guardian Online > Settings**, and then use **Compliance Guardian Online Auditor** to view the auditor data report. You can also export the desired auditor data report. Use **Auditor Settings** to configure the related settings.

Extending License

You can extend your license to an enterprise one for using more functionalities, or you must extend your license if you want to continue use Compliance Guardian Online after your trial license is expired. In **License Manager**, select **Extend License**, fill out the request form, and then select **Submit** to send the request to Compliance Guardian Online for extending the license.

Notices and Copyright Information

Notice

The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright

Copyright ©2013-2014 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

Trademarks

AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Microsoft Office SharePoint Servers 2007/2010/2013, SharePoint Portal Server 2003, Windows SharePoint Services, Windows SQL server, and Windows are either registered trademarks or trademarks of Microsoft Corporation.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes

The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311
USA