ONE IDENTITY™

Cloud Access Manager 8.1.4

Advanced Customization

Copyright 2018 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

⊗ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

⚠ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⓘ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Cloud Access Manager Advanced Customization
Updated - November 2018
Version - 8.1.4

Contents

Introduction

This guide describes how you can customize the appearance of Cloud Access Manager to meet the needs of your users and to match your corporate branding.

Overview

You can easily change common aspects of the look and feel of Cloud Access Manager using the **Customize Appearance** options in the Cloud Access Manager Administration User Interface (UI). For example, you can change the colors, company name and logo in the Admin UI. For more extensive changes, you can manually edit the Cascading Style Sheet (CSS) file that is used to style Cloud Access Manager from the Admin UI.

If you cannot achieve the look you require by editing the CSS file, you can also edit the HTML of the Login and Home Realm Discovery (HRD) pages. You will find the customization settings in the Admin UI under **Settings | Customize Appearance**.

- To manually edit the CSS file, select **Enable advanced customization mode**. You will then be able to download the CSS file and upload a modified version. This CSS file is called theme.css.

  If you want to reference additional images and fonts in the CSS file, you can copy the images/fonts to the customization directory on each Security Token Service (STS) host:

  C:\Program Files\One Identity\Cloud Access Manager\Customization\

  You can then reference these files using the path /CloudAccessManager/Customization/`<filename>` in the CSS file.

- To manually edit the HTML for the Login and HRD pages, you need to log into each of the STS hosts and manually edit the following files:

  C:\Program Files\One Identity\Cloud Access Manager\Customization\Login.htm

  C:\Program Files\One Identity\Cloud Access Manager\Customization\UserIdentity.html

  When you edit these HTML files, you must ensure the changes are applied to each STS host. If you need to include JavaScript or image files, you can place these files in the same directory and reference them using a relative path.

Upgrading

Files that you have edited manually will not be updated when Cloud Access Manager is upgraded to the latest version.

It is important that you keep track of the changes that you have made to the default files, so that you can re-apply those changes to the latest default files after upgrade.

We recommend that you keep your own backup of the original versions of the files that you edit so that you can compare the original default file with the upgraded default file to see the changes that have been made.

Updated default files can be found in the following locations:

- For any files uploaded using the Cloud Access Manager Admin User Interface (UI):
  - Go to the page where you uploaded the file (such as the **Customize Appearance** settings page or the **Customize** page for any authenticators that you have customized)
  - Download the default files using the buttons provided
- For the login and Home Realm Discovery (HRD) HTML files, you can find the updated default files in the backup folders in the following locations:
- C:\Program Files\One Identity\Cloud Access Manager\Customization\Login\backup\Login.htm
- C:\Program Files\One Identity\Cloud Access Manager\Customization\HRD\backup\UserIdentity.html

Changing text

To change any existing text in Cloud Access Manager you will need to update the language definition files. Please refer to the *One Identity Cloud Access Manager How to Support Multiple Languages* guide for information on how to do this.

If you add any new text into the login or Home Realm Discovery (HRD) pages and also want to support multiple languages, then you will need to add this text to all of your language definition files and reference the key within the HTML file.

- For new text in the login page, you will need:
  - update the login_`<language code>`.json files
  - reference the key using the HTML attribute: data-localize="`<key>`"
- For new text in the HRD page:
  - update the cam_`<language code>`.json file
  - reference the key using one of the following methods:
    - enter where you want the text to be displayed: {{ '`<key>`' | translate }}
    - using the HTML attribute: translate=”`<key>`”

Changing the company logo

To change the company logo on all user facing pages, perform the following steps. The logo displayed in the **Administration Console** is not changed.

To change the company logo on user facing pages

1. From the Cloud Access Manager **Administration Console**, click **Settings | Customize Appearance** and upload your company logo.

   > ⓘ NOTE: The logo should be at least 160x160px in size to ensure there is no loss of image quality.

2. If you have selected **Enable advanced customization mode** you need to complete steps 3 to 6 to update your customized theme.css file with the size of the logo.
3. Click **Download Current Customization CSS** to download the current theme.css file.
4. To update the logo size used on the login page, locate the following rule in the theme.css file and update the width declarations to the required width for your logo.

   ```
   loginLogo {
    background-image: url("/_WTStatic/public/customization/companylogo.png");
    background-repeat: no-repeat;
    height: 160px;
    width: 160px;
    margin: 60px auto 50px auto;
   }
   ```

   > ⓘ NOTE: The logo is automatically resized to a height of 160 pixels when uploaded.

5. To update the logo size used in the header bar on the portal pages, locate the following rule in the theme.css file and update the width declaration to the required width for your logo.

   ```
   #custom .cui-application-frame .oi-logo {
    width: 30px;
    background-image:url("/_WTStatic/public/customization/companylogo.png");
    height: 30px;
    background-size: auto 30px;
    background-repeat: no-repeat;
   }
   ```

6. Finally upload the modified theme.css file and clock **Save**.

Using an alternative cascading style sheet for a single authenticator

By default all users will see the same colors and styling regardless of which authenticator they have used to authenticate. These steps describe how to configure an authenticator to use an alternative cascading style sheet.

To change the CSS for a single authenticator

1. From the Cloud Access Manager **Administration Console**, click **Settings | Customize Appearance**.
2. Select **Enable advanced customization mode** and click Save.
3. Click **Authenticators** and then click **Edit** on the authenticator that will use the alternative CSS.
4. Click the **Customization** tab and select **Customize this authenticator**.
5. Click **Download Current Customization CSS** to download the current theme.css file.
6. Amend the CSS file with your changes and then upload it.
7. Click **Finish** to save your changes.

Using an alternative company logo for a single authenticator

By default all users will see the same company logo regardless of which authenticator they have used to authenticate. These steps describe how to configure an authenticator to use an alternative company logo.

To change the company logo for a single authenticator

1. From the Cloud Access Manager **Administration Console**, click **Settings | Customize Appearance**.
2. Select **Enable advanced customization mode** and click **Save**.
3. Click **Authenticators** and then click **Edit** on the authenticator that will use the alternative company logo.
4. Click the **Customization** tab and select **Customize this authenticator**.
5. Click **Download Current Customization CSS** to download the current theme.css file.
6. Upload the logo to use for this authenticator.

   NOTE: The logo should be at least 160x160px in size to ensure there is no loss of image quality.

7. In the CSS, locate the following rule used to display the logo on the login page:

   ```
   loginLogo {
    background-image: url("/_WTStatic/public/customization/companylogo.png");
    background-repeat: no-repeat;
    height: 160px;
    width: 160px;
    margin: 60px auto 50px auto;
   }
   ```

8. Update the background-image declaration to reference the logo path for the authenticator. The logo path can be found in the help text on the **Customize Authenticator** page and is in the following format where `<id>` is the **Authenticator ID**:

   /_WTStatic/public/customization/auth-`<id>`/companylogo.png

9. Update the width declaration to the required width for your logo on the login page.

10. Locate the following rule used to display the logo in the **Header bar** on the portal pages:

    ```
    #custom .cui-application-frame .oi-logo {
     width: 30px;
     background-image:url("/_WTStatic/public/customization/companylogo.png");
     height: 30px;
     background-size: auto 30px;
     background-repeat: no-repeat;
    }
    ```

11. Update the background-image declaration to reference the logo path for the authenticator. The logo path can be found in the help text on the **Customize Authenticator** page and is in the following format where `<id>` is the **Authenticator ID**:

    /_WTStatic/public/customization/auth-`<id>`/companylogo.png

12. Update the width declaration to the required width for your logo in the header bar.

13. To support users of Internet Explorer 8, locate the following rule and update the logo path in the filter declaration to reference the logo path for the authenticator.

    ```
    #custom .cui-application-frame .oi-logo {
     filter: progid:DXImageTransform.Microsoft.AlphaImageLoader(src='/_
    WTStatic/public/customization/companylogo.png', sizingMethod='scale');
     background-image: none;
    }
    ```

14. Finally upload the modified theme.css file and click **Finish**.

Using an alternative company name for a single authenticator

By default all users will see the same company name regardless of which authenticator they have used to authenticate. These steps describe how to configure an authenticator to use an alternative company name.

To change the company name for a single authenticator

1. From the Cloud Access Manager **Administration Console**, click **Settings | Customize Appearance**.
2. Select **Enable advanced customization mode** and click **Save**.
3. Click **Authenticators** and then click **Edit** on the authenticator that will use the alternative company name.
4. Click the **Customization** tab and verify that **Customize this authenticator** is selected.
5. Click **Download Current Customization CSS** to download the current theme.css file.
6. Locate the following two rules in the theme.css file to change the name displayed in the **Header bar** and on the login page:

   ```
   #custom .cui-application-title:before {
    content: "One Identity Cloud Access Manager";
   }
    .loginTitle:before {
   content: "One Identity Cloud Access Manager";
   }
   ```
7. Update both content declarations to contain the required company name.
8. Finally upload the modified theme.css file and click **Finish**.

Stacking the username and password fields

To stack the username and password fields

1. From the Cloud Access Manager **Administration Console**, click **Settings | Customize Appearance**.
2. Verify that **Enable advanced customization mode** is selected.
3. Click **Download Current Customization CSS** to download the current theme.css file.
4. Append the following rule to the end of the theme.css file:

```
#loginForm {
 width: 300px;
 margin: 0 auto;
 padding-top: 30px;
}
```

5. Upload the modified theme.css file and click **Save**.

Changing the font

To change to your web font

1. Copy your web font into the following directory on each of your STS hosts:

   C:\Program Files\One Identity\Cloud Access Manager\Customization\
2. From the Cloud Access Manager **Administration Console**, click **Settings | Customize Appearance**.
3. Verify that **Enable advanced customization mode** is selected.
4. Click **Download Current Customization CSS** to download the current theme.css file.
5. Append the following rules to the end of the theme.css file:

   ```
   @font-face {
    font-family: yourfont;
    src: url('/CloudAccessManager/Customization/yourfont-webfont.woff') format
   ('woff');
    font-weight: normal;
    font-style: normal;
   }
   #custom,
   #custom .cui-masthead .cui-application-title,
   #custom .cui-masthead,
   #custom .section-title,
   #custom .loginTitle,
   #custom h2,
   #custom h3 {
    font-family: 'yourfont';
   }
   ```
6. Change the src declaration to reference your font filename.

7. Change the two font-family declarations to your font name.
8. Upload the modified theme.css file and click **Save**.

Changing the application sub-name

By default the application sub-name displayed in the header bar is **Application Portal**.

To change the application sub-name

1. From the Cloud Access Manager **Administration Console**, click **Settings | Customize Appearance**.
2. Verify that **Enable advanced customization mode** is selected.
3. Click **Download Current Customization CSS** to download the current theme.css file.
4. Append the following rules to the end of the theme.css file:

   ```
   .cui-application-subname {
    display: none;
   }
   .cui-application-title:after {
    content: 'Employee Portal';
   }
   ```

5. Update the content declaration to contain the required name.
6. Upload the modified theme.css file and click **Save**.

Removing the company name

If you want to remove your company name text from your company logo, perform the following steps.

To remove your company name text from your company logo

1. From the Cloud Access Manager **Administration Console**, click **Settings | Customize Appearance**.
2. Select **Enable advanced customization mode** and click Save.
3. Click **Authenticators** and then click **Edit** on the authenticator that will use the alternative company logo.
4. Click the **Customization** tab and verify that **Customize this authenticator** is selected.
5. Click **Download Current Customization CSS** to download the current theme.css

file.

6. Remove or comment the following rules:

```
#custom .cui-application-title:before {
 content: "One Identity Cloud Access Manager";
}
.loginTitle:before {
 content: "One Identity Cloud Access Manager";
}
```

7. Upload the modified theme.css file and click **Save**.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product