Federated Authentication Release Notes

Volte Build 52xx on CMS released Wednesday 4.16.2014

Overview

CrownPeak now offers Federated Authentication to users of the CMS and the Web Hosting environments. Employees, partners, and vendors can authenticate to these environments through a local account profile or via a company-hosted identity provider.
With Federated Authentication enabled, users:

- No longer need a separate user name and password for the CrownPeak CMS
- No longer need to log in to the pre-production Websites to review or approve content when accessing the server from their company network

Once authenticated, users are authorized to the correct level of access within the CMS through the assigned group roles, in exactly the same way authorization is managed today.

CrownPeak Federated Authentication supports the SAML 2.0 standard and is available as an add-on option for an incremental subscription fee. Please contact a CrownPeak sales representative or CrownPeak Customer Support for more details.

Summary of Features

CMS Instance Administration (CMS-1746)
Federated Authentication is enabled at the CMS instance level. This is one of the first steps in the process. It requires that a **claims trust relationship be in place between CrownPeak and your company's identity provider**.

CMS User/Group Administration (CMS-3179)
The existing CMS user and group administration features have been enhanced to support Federated Authentication. Individual users can be enabled one at a time or in small groups to support a staged migration process within an organization.

CMS Auditing Reports (CMS-3162)
All transactions related to Federated Authentication have been added to the CMS System Audit report. Look for this report by navigating to **[Reports][Audit][System]**.

CMS Volte Installation (CMS-3175)

Web Hosting Administration (CMS-3571)
Federation Authentication also allows authorized CMS administrators to update the list of reviewers that approve content on a company's stage and other pre-production Websites. This eliminates the need for password resets and the traditional login screen for these Websites.

Web Hosting User Administration (CMS-3574)
Each web site has its own user administration template that allows users to create permission lists at each stage of a company's workflow cycle including: Development, Stage, and more.

Web Hosting Auditing Reports (CMS-3162)
The Website administration templates also log all of the user changes to the CMS System Audit report. This includes users added, removed, or updated at each stage of the CMS workflow.

CMS Classic Installation Update (CMS-3120)

CMS Volte is moving to a new location as part of this feature enhancement. The instance will move from cms.crownpeak.**com**/[Company]/UI/ to cms.crownpeak.**net**/[Company]/UI/. As a result, users will need to remove and reinstall the Volte desktop application. See below for more details.

CDC for MS Visual Studio Update (CMS-3119)
The CrownPeak Desktop Connector (CDC) for MS Visual Studio has been updated to support Federated Authentication. Select an identity provider and press the **[Connect]** button.

CMS Classic also has a new URL for Federated Authentication. The instance will move from cms.crownpeak.**com**/[Company]/ to cms.crownpeak.**net**/[Company]/. There will be an automatic redirect setup for those users who have not updated their browser links.

CDC for Eclipse Update (CMS-3128)
The CrownPeak Desktop Connector (CDC) for Eclipse is still in development. Look for this version of the desktop tool to be updated in early summer 2014.

CMS Administration: Setting up the Environment in Volte

Contact CrownPeak Support to request the Federated Authentication feature. CrownPeak will perform the following tasks to enable the feature:

1. *Setup up a claims trust relationship between CrownPeak and the customer's identity provider*
2. *Enable Federated Authentication in the CMS instance and Web Hosting environment(s)*
3. *Setup user and group access in the CMS instance and Web Hosting environment(s)*

Setup up a claims trust with CrownPeak
The CrownPeak Professional Service team will coordinate a meeting with a company's IT security group and request a claims trust relationship between CrownPeak and a company's identity provider. This process may take between a few days and a few weeks to establish, depending on a company's internal security approval process. Once this step is completed the process can move forward.

Enable Federated Authentication in Volte
1. *Login as a CMS administrator.*
2. *Navigate to the **[Settings/Configuration/Authentication Settings]** page.*
3. *Click the **[Yes]** radio button to enable the **[Fed-Auth Enabled**] setting.*
4. *The CMS is now set up to use the Federated Authentication service.*
5. *Select a **[Default Identity Provider]** and disable local user/password access[1].*
   Note:
   a. *CrownPeak recommends that the disable password option is set once all users have been switched to Federated Authentication.*
   b. *The CMS System Audit report will log all federated authentication changes to the pages above.*

[1] Local user/password access allows users to authenticate with a local CMS user ID and password if set.

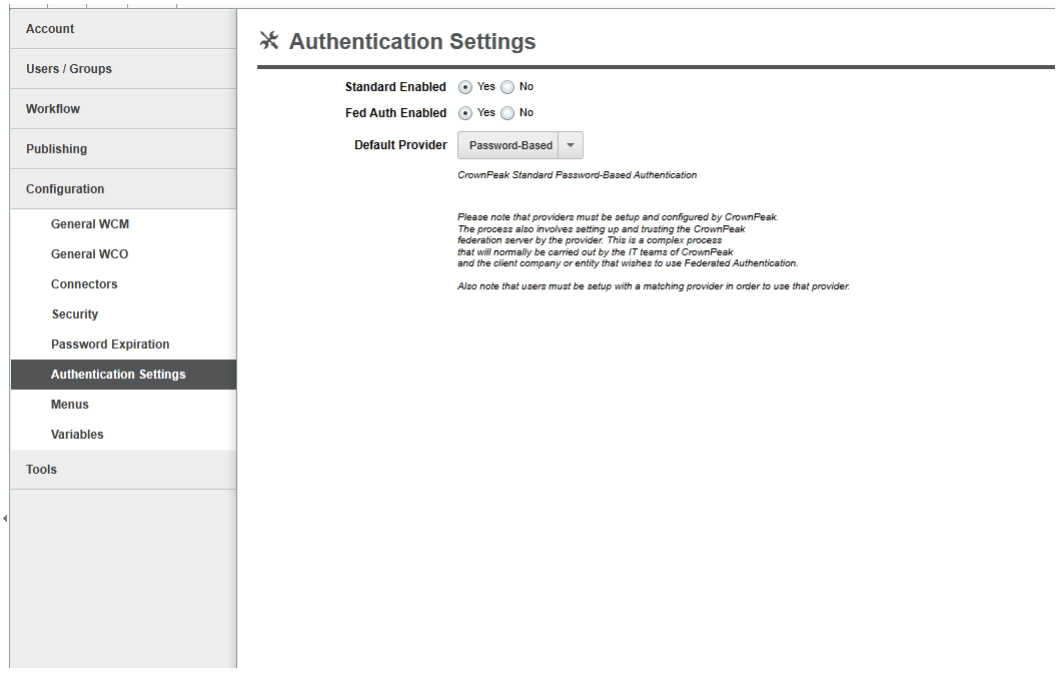

Figure 1. Volte Authentication Settings Screen

Enable users and group access:

1. *Navigate to the **Settings/Users Groups/Groups** page.*
2. *Update each Security group to disable 'Users can **change Identity Provider Settings**'.*

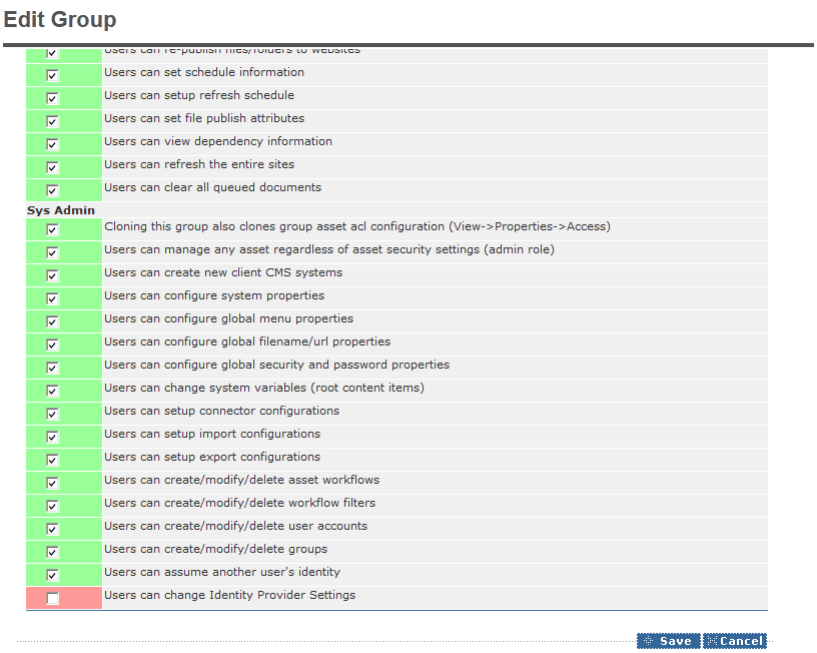

Figure 2. Group Access Settings Screen

3. *Navigate to the **[Settings/User/Group/Edit User]** page.*
4. *Create or update the user's CMS profile.*

5. *Update the **[Username]** field with the value of the user's SAML ID[2]*
6. *Update the **[Identity Provider]** field from '**Password Based**' to '**Company Name**'*

Note:

a. *This disables the local CMS user/password access for the user profile and identifies that the user is now configured to leverage Federated Authentication services.*

b. *The CMS System Audit report will log all user security profile changes to the pages above.*

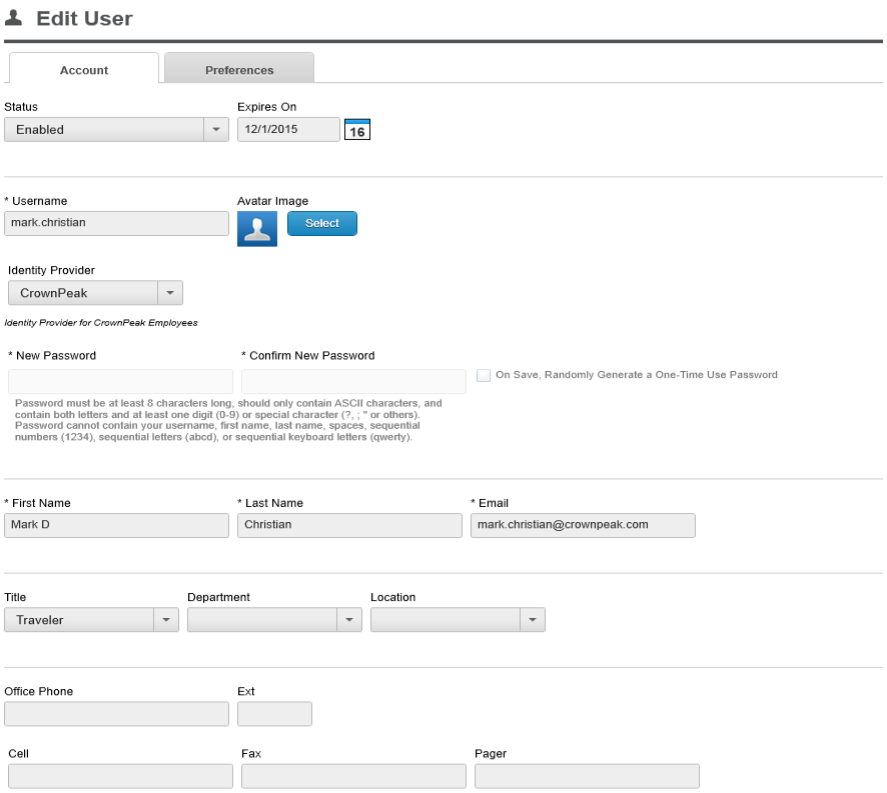

Figure 3. Volte User Settings Screen

[2] Your company's information security group can provide this value.

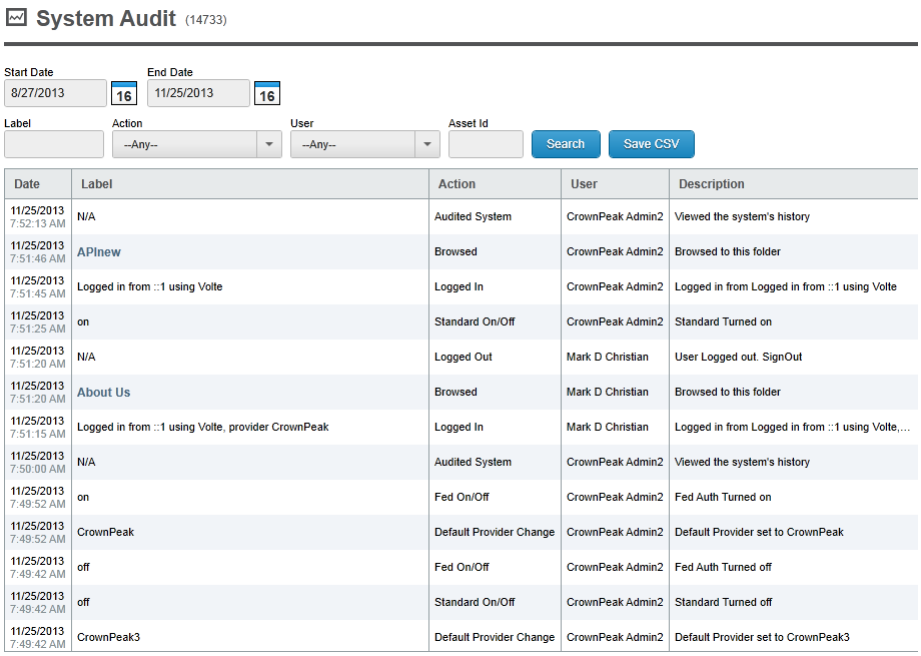

Figure 4. Volte System Audit Report

Enable Federated Authentication in Classic

1. *Login as a CMS administrator*
2. *Navigate to the **[System/Configuration/Authentication Settings]** page.*
3. *Click the **[Yes]** radio button to enable the **[Fed-Auth Enabled**] setting.*
4. *The CMS is now set up to use the Federated Authentication service.*
5. *Select a **[Default Identity Provider]** and disable local user/password access[3].*

   Note:
   a. *CrownPeak recommends that the disable password option is set once all users have been switched to Federated Authentication.*
   b. *The CMS System Audit Report will log all federated authentication changes to the pages above.*

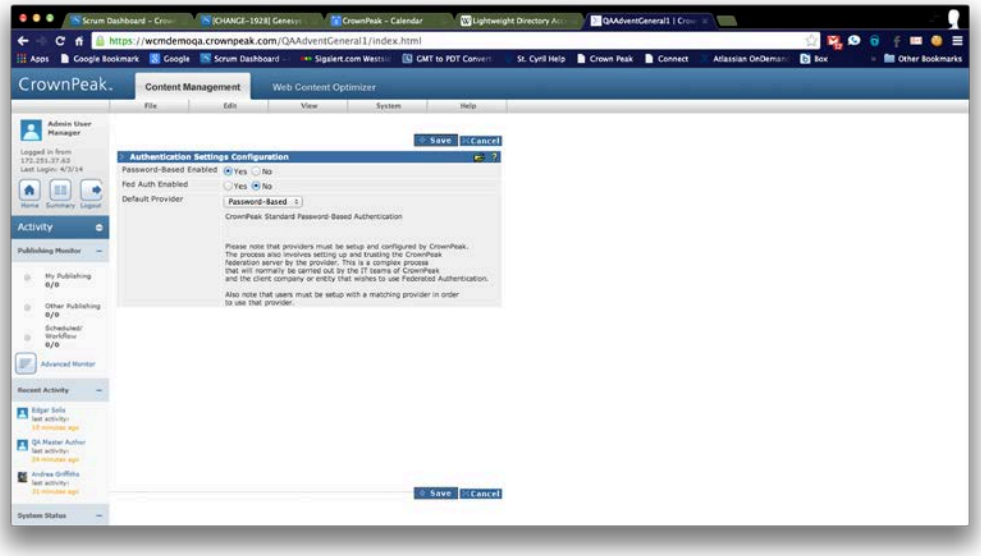

Figure 5. Classic Authentication Settings Screen

Enable users and group access:

1. *Navigate to the **[System/Configure/Groups]** page.*
2. *Update each Security group to disable 'Users can **change Identity Provider Settings**'.*

[3] Local user/password access allows users to authenticate with a local CMS user ID and password if set.

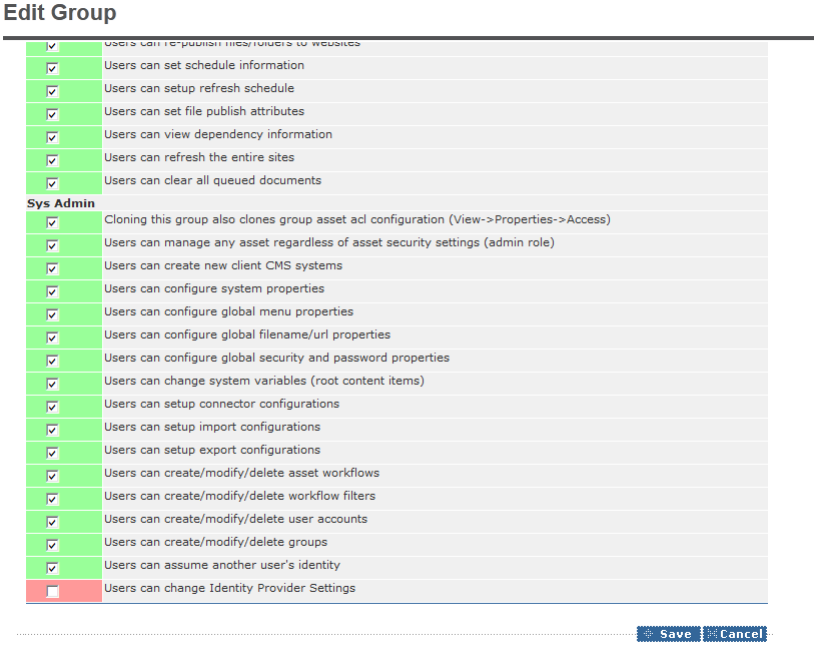

Figure 2. Classic Group Access Settings Screen

3. *Navigate to the **[System/Configure/User/Edit User]** page.*
4. *Create or update the user's CMS profile.*
5. *Update the **[Username]** field with the value of the user's SAML ID[4]*
6. *Update the **[Identity Provider]** field from '**Password Based**' to '**Company Name**'*

   Note:

   a. *This disables the local CMS user/password access for the user profile and identifies that the user is now configured to leverage Federated Authentication services.*
   b. *The CMS System Audit Report will log all user security profile changes to the pages above.*

[4] Your company's information security group can provide this value.

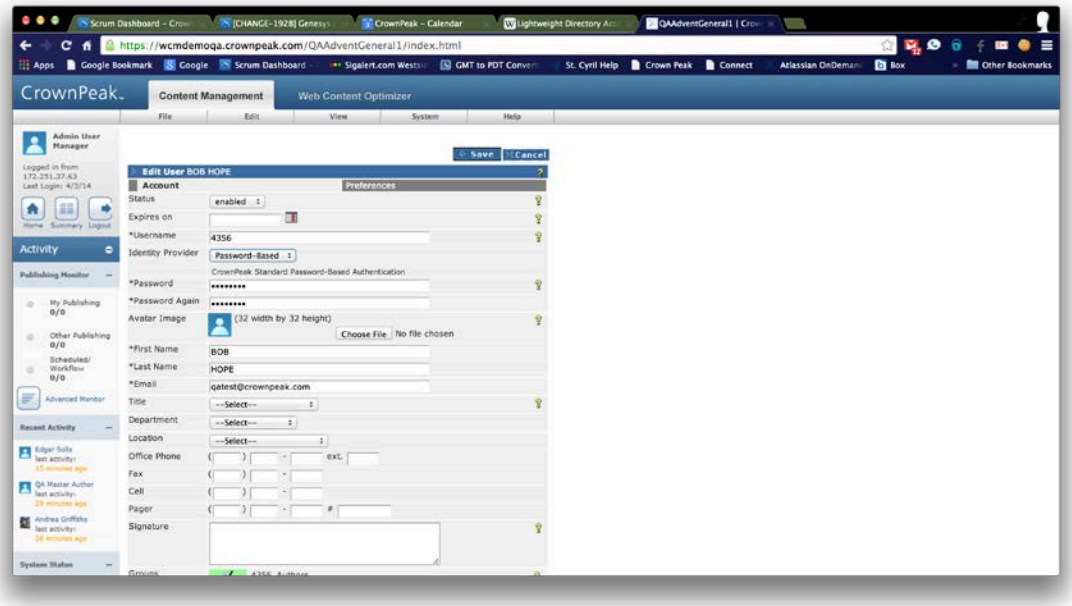

Figure 6. Classic User Settings Screen

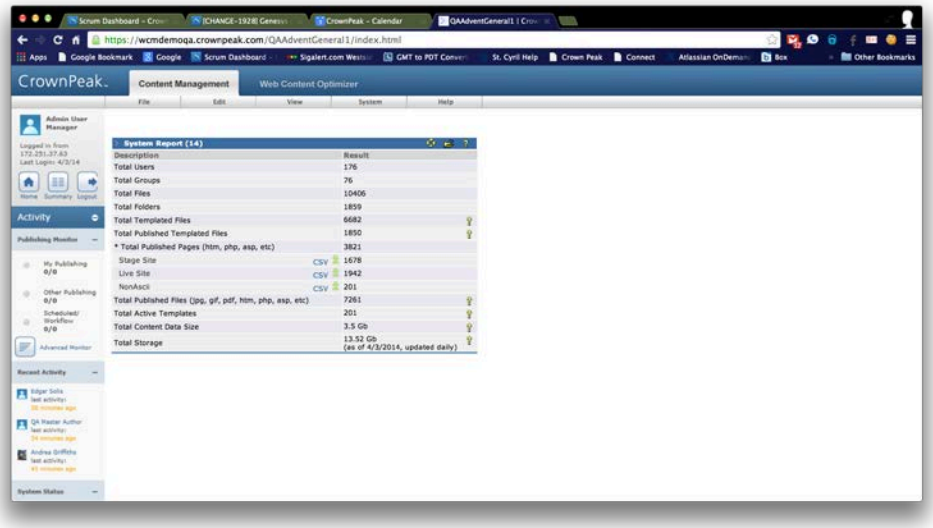

Figure 7. Classic System Audit Report

CMS Users: Installing and Logging into Volte

Once the administration steps are completed, all CMS users must reinstall the Volte application.

Install CMS Volte with Federated Authentication:

1. *Copy the Volte URL provided by CrownPeak into an approved Internet browser.*
   i.e.: https://cms.crownpeak.net/[Company]/UI/?providerName=[ProviderName]
2. *The Volte application installs itself on the user's local desktop*
   Note: This process will setup a cookie on the end user's desktop that contains the Default Identity provider.
3. *A Volte CMS icon will appear on the end user's desktop at the end of the process.*
4. *Network Authentication*
   a. *If currently connected to a customer's network then the end user will be able to click on the Volte CMS icon and launch the CMS Volte application without requiring a login.*
   b. *If NOT connected to a customer's network then users will be will be required to first login to a company network prior to gaining access to the CMS.*

Logging into the CMS with Volte

1. *Click on the Volte CMS icon.*
2. *The CMS will present an identity provider selection screen to the user the first time if the user's identity provider has not been previously set[5]. This entry screen replaces the traditional user name/password login screen.*

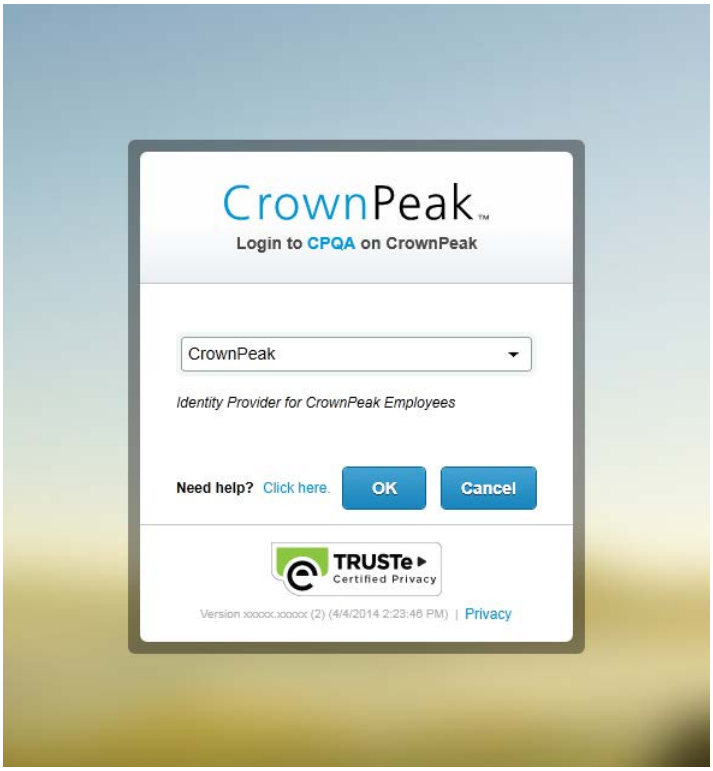

Figure 8. Provider Selection Screen

[5] Once selected, Volte will remember the selection and will not prompt again.

3. *Click the 'Connect' button.*

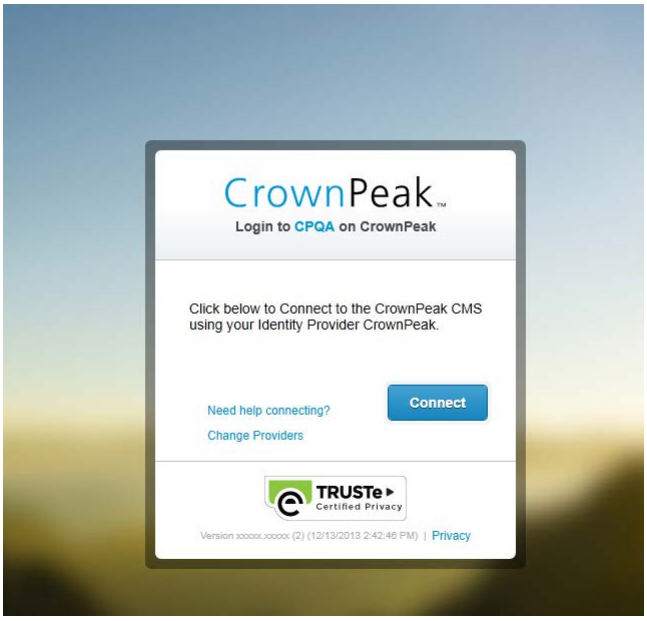

Figure 9. Provider Connect Screen

4. *The CMS initiates communication with a customer's network and confirms the user's access rights via a SAML 2.0 authentication request.*

CMS Users: Logging into Classic

Once the administration steps are completed, all CMS users must log into CMS Classic with the new URL.

Log into CMS Classic with Federated Authentication:

1. *Copy the Volte URL provided by CrownPeak into an approved Internet browser.*
   *i.e.: https://cms.crownpeak.**net**/[Company]/index.html/?providerName=[ProviderName]*
2. *Network Authentication*
   a. *If currently connected to a customer's network then the end user will be able to click on the Volte CMS icon and launch the CMS Volte application without requiring a login.*
   b. *If NOT connected to a customer's network then users will be will be required to first login to a company network prior to gaining access to the CMS.*
3. *The CMS will present an identity provider selection screen to the user the first time if the user's identity provider has not been previously set[6]. This entry screen replaces the traditional user name/password login screen.*

[6] Once selected, Volte will remember the selection and will not prompt again.

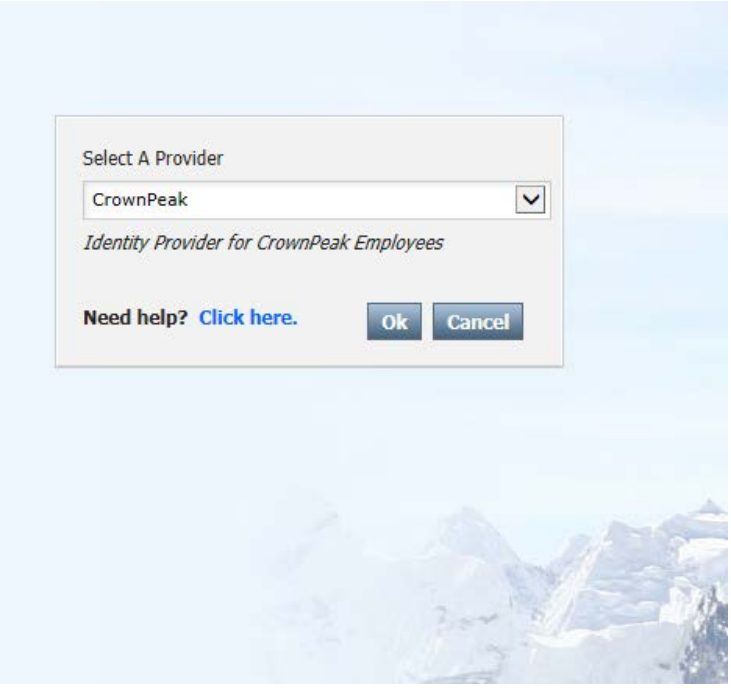

Figure 10. Provider Selection Screen

4. *Click the 'Connect' button.*

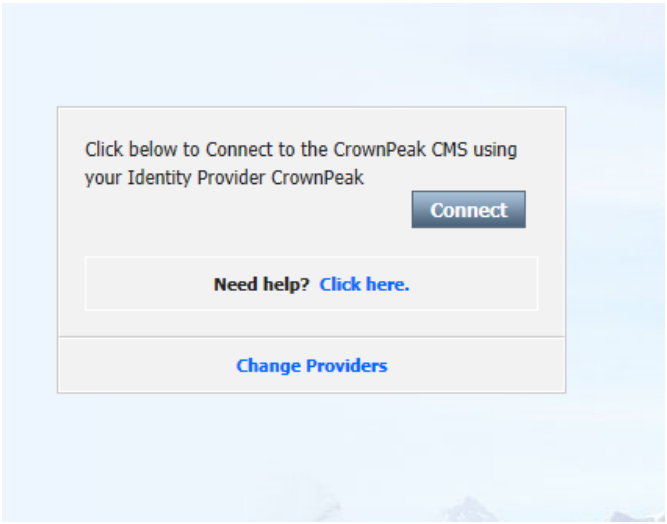

Figure 11. Provider Connect Screen

5. *The CMS initiates communication with a customer's network and confirms the user's access rights via a SAML 2.0 authentication request.*

Install CrownPeak Desktop Connector (CDC) for Visual Studio

Users can also connect to the CMS via the Visual Studio Desktop Connector.

Install CMS CDC with Federated Authentication

1. *Copy the new CrownPeak Desktop Connector (CDC) URL into an approved Internet browser.*
   Sample login URL: ***http://desktop.crownpeak.com/dc/standalone/fedalpha/publish.htm***
2. *The CDC is installed on the local desktop.*
3. *A CrownPeak Desktop Connector icon will appear on the desktop at the end of the process.*
4. *Double-clicking on the icon will launch the CMS CDC application without requiring a login (when currently authenticated to the company network).*

Setup Web Hosting Platform in Volte

A CrownPeak administrator or a company administrator with the appropriate privileges can configure Federated Authentication services for the Web Hosting environments.

Setup a Website in Volte

1. *Navigate to the* ***Settings/Configuration/Authentication/Settings*** *page.*
2. *Click the* ***[Yes]*** *radio button to enable the [****Fed-Auth Hosting Enabled****] setting.*
3. *The Web Hosting environment is now set up to use the Federated Authentication service.*
4. *The CMS System Audit Report will log all federated authentication changes to the pages above.*

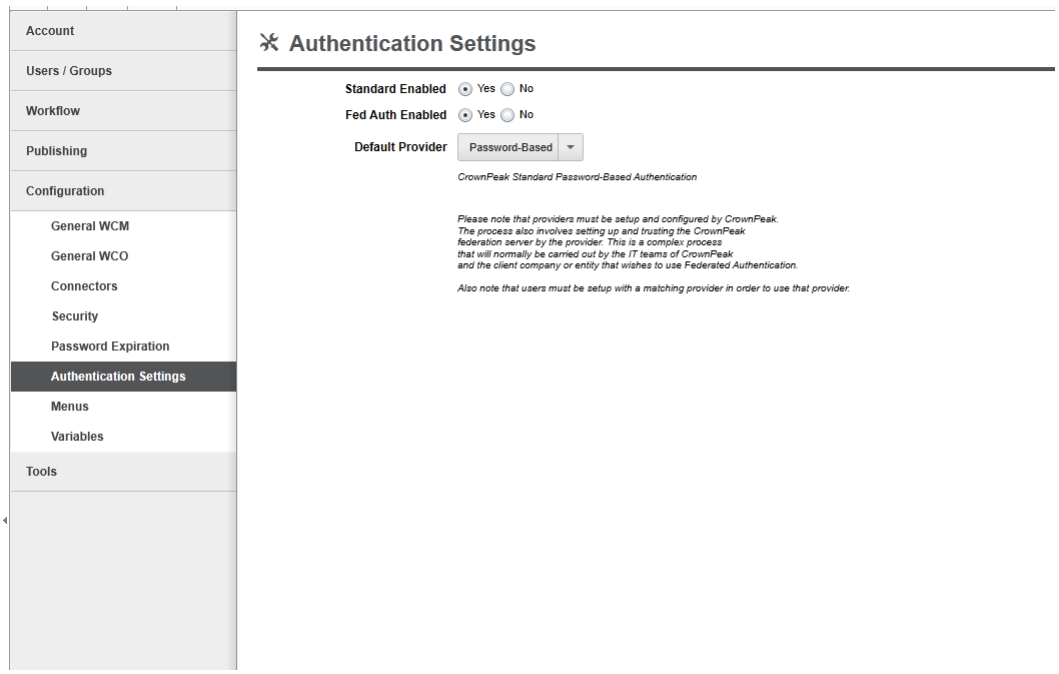

Figure 7. Volte Authentication Settings Screen

Federation Site Web Hosting Setup

1. *Navigate to the **Settings/Publishing/Fed Auth Configuration** page.*
2. *Change the [**Fed Auth Enabled**] drop down box to "On" next to each of the Web Hosting environments that require federated authentication.*
3. *Click the **[Save]** button at the bottom of the Publishing Packages page.*
4. *This will create a new [**User Access Control List]** asset in the root directory of the Website folder.*
5. *The CMS System Audit Report will log all federated authentication changes to the pages above.*

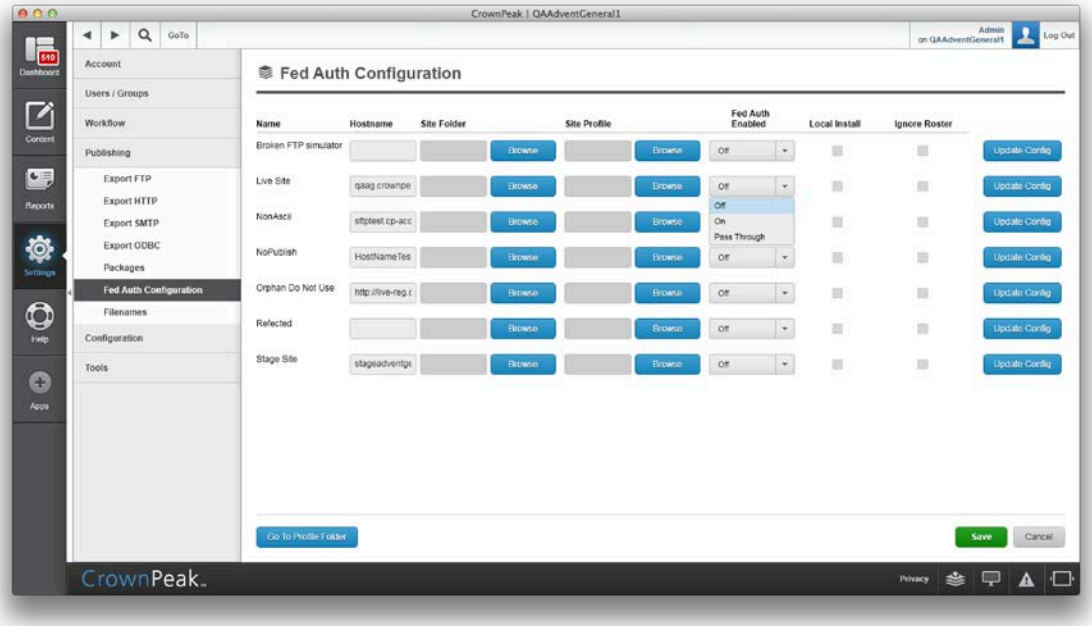

Figure 8. Volte Package Configuration Screen

Configuring Access Rights for Web Hosting in Volte

1. *Navigate and select the [**User Access Control List**] asset in the root directory of the Website folder.*
2. *Select the menu option [Action][Edit Form].*
3. *The CMS will present the user with the input template asset screen organized into a company's workflow stages.*
4. *Add, edit or delete the list of users in the text area control located in each of the stage sections. A valid user entry will consist of the user's [Display Name], [Email Address], [UserID] separated by commas. Users must be listed on separate lines in the text area control.*
5. *Click the [Save] button at the bottom of the Publishing Packages page.*
6. *The asset will be saved in the site's root directory within the CMS and will be transferred to all federated authentication configured Web Hosting environments as part of the publishing process.*
7. *Additional values can be added to the end of each line separated by commas. These additional values are passed along and made available to the Web Hosting environment as web server global variables.*
8. *The CMS System Audit report will log all federated authentication changes to the pages above.*

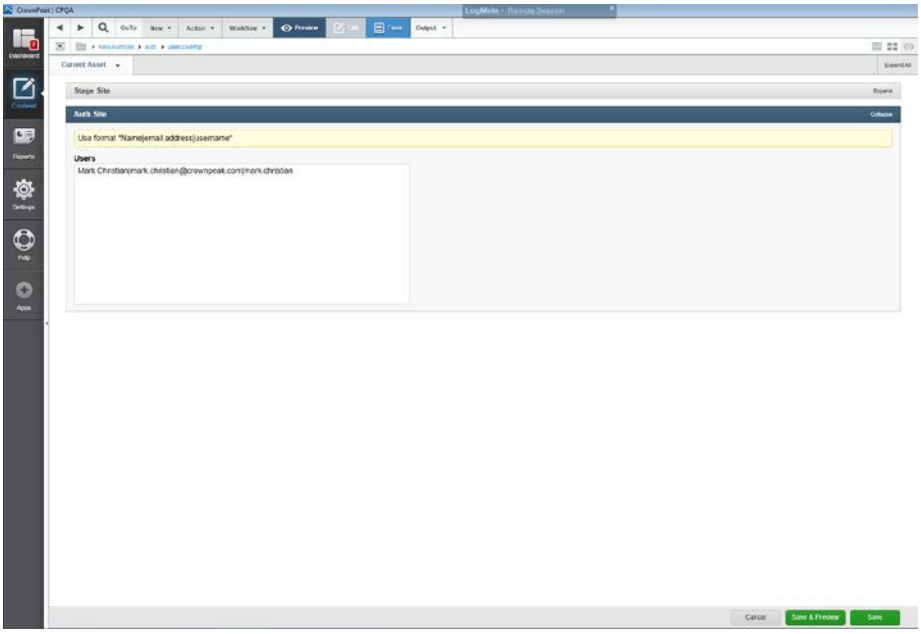

Figure 9. User Access Control List asset

Setup Web Hosting Platform in Classic

A CrownPeak administrator or a company administrator with the appropriate privileges can configure Federated Authentication services for the Web Hosting environments.

Setup a Website

1. *Navigate to the **System/Configure/Authentication Settings** page.*
2. *Click the **[Yes]** radio button to enable the [**Fed-Auth Hosting Enabled**] setting.*
3. *The Web Hosting environment is now set up to use the Federated Authentication service.*
4. *The CMS System Audit report will log all federated authentication changes to the pages above.*

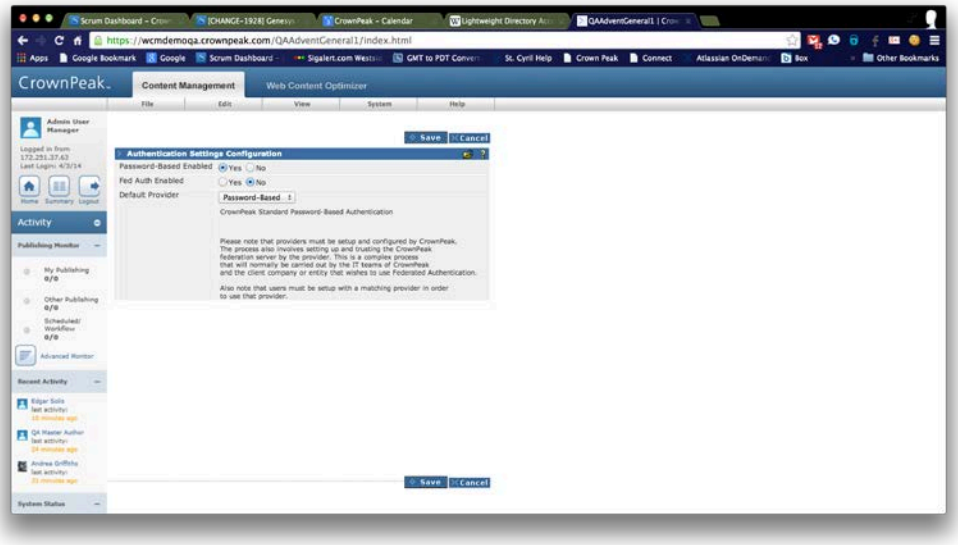

Figure 12. Classic Authentication Settings Screen

Federation Site Web Hosting Setup

1. *Navigate to the **Settings/Publishing/Fed Auth Configuration** page.*
2. *Change the [**Fed Auth Enabled**] drop down box to "On" next to each of the Web Hosting environments that require federated authentication.*
3. *Click the **[Save]** button at the bottom of the Publishing Packages page.*
4. *This will create a new [**User Access Control List]** asset in the root directory of the website folder.*
5. *The CMS System Audit report will log all federated authentication changes to the pages above.*

Configuring Access Rights for Web Hosting in Classic

1. *Navigate and select the [**User Access Control List**] asset in the root directory of the website folder.*
2. *Select the menu option [Action][Edit Form].*
3. *The CMS will present the user with the input template asset screen organized into a company's workflow stages.*
4. *Add, edit or delete the list of users in the text area control located in each of the stage sections. A valid user entry will consist of the user's [Display Name], [Email Address], [UserID] separated by commas. Users must be listed on separate lines in the text area control.*
5. *Click the [Save] button at the bottom of the Publishing Packages page.*
6. *The asset will be saved in the site's root directory within the CMS and will be transferred to all federated authentication configured Web Hosting environments as part of the publishing process.*
7. *Additional values can be added to the end of each line separated by commas. These additional values are passed along and made available to the Web Hosting environment as web server global variables.*
8. *The CMS System Audit report will log all federated authentication changes to the pages above.*

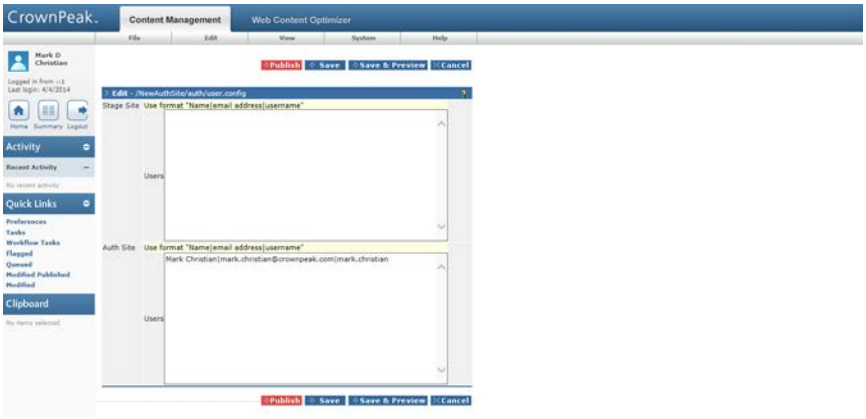

Figure 14. User Access Control List asset

Federation Authentication Terminology

The CrownPeak Federated Authentication feature supports the SAML 2.0 standard specification to establish an identity federation. SAML 2.0 is used for exchanging authentication and claims data (also known as authorizations or entitlements) between organizations. SAML 2.0 is an XML-based protocol that uses assertions to pass information about principals (users) between a SAML identity provider, and a SAML consumer, that is, a service provider. Below is a list of common terms associated with Federated Identity Management, Federated Authentication, and SAML 2.0.

Term	*Definition*
ACL	*Access Control List*
CMS	*The CrownPeak Content Management System (CMS)*
Volte	*The CrownPeak Content Management System Silverlight Out-of-Browser application called "Volte".*
Classic	*The CrownPeak Content Management System prior version web client called "Classic".*
Claim	*A statement about a subject. For example, "User A belongs to security group B." Claims can be used to grant permissions.*
CDC for Visual Studio	*The CrownPeak Desktop Connector (CDC) for Visual Studio on the PC platform*
CDC for Eclipse	*The CrownPeak Desktop Connector (CDC) for Eclipse on the Mac platform*

Term	*Definition*
Authentication	*The process of confirming the identity of a user. ("Is this person who they say they are?")*
Authorization	*The process whereby security privileges are assigned to a user. ("What is this person allowed to do?")*
CMS	*Content Management System*
FIdM	*Federated identity management (FIdM) is a common set of policies, practices and protocols in place to manage the identity and trust of users and devices across organizations.*
FTP	*File Transfer Protocol*
Identity Provider (IdP)	*A service that authenticates a user's identity.*
Relying party (RP)	*A service (Application) that grants or denies access, based on the assertion of a trusted identity provider.*
Relying party trust	*The relationship that establishes trust between a RP and an IdP.*
Rule group	*Rules that define which claims are passed from the identity provider to the relying party application (Service Bus). A rule group also defines mappings, so that claims from the identity provider translate into claims that are meaningful to the relying party application.*
SaaS	*Software as a Service*
SAML	*Security Assertion Markup Language (SAML). An XML-based open standard data format for exchanging authentication and authorization data between parties.*
SFTP	*Secure File Transfer Protocol*
URL	*Uniform Resource Locator*

Frequently Asked Questions

Question: What standards does CrownPeak Federated Authentication support?
Answer: **CrownPeak Federated Authentication feature supports the SAML 2.0 standard specification to establish an identity federation. SAML 2.0 is used for exchanging authentication and claims data (also known as authorizations or entitlements) between organizations.**

Question: What identity providers does CrownPeak Federated Authentication support?
Answer: CrownPeak supports any SAML 2.0-compliant identity provider.

Question: What SAML authentication profiles does CrownPeak Federated Authentication support?
Answer: CrownPeak supports both Identity Provider Initiated (IdP-Initiated) SSO and Service Provider Initiated (SP-Initiated) SSO.

- ***IdP-Initiated SSO - The Federation process is initiated by the Identity Provider (IdP) sending an unsolicited SAML Response to the Service Provider (SP)***
- ***SP-Initiated SSO – The Service Provider (SP) generates an AuthnRequest that is sent to the Identity Provider (IdP) as the first step in the Federation process and the IdP then sends a SAML Response.***

Question: Does CrownPeak Federated Authentication support LDAP authentication?
Answer: No. Lightweight Directory Access Protocol (LDAP) is not a SAML 2.0 protocol

Question: Does CrownPeak Federated Authentication support Windows Integrated Authentication?
Answer: No. Windows Integrated Authentication is not a SAML 2.0 protocol

Question: Does CrownPeak Federated Authentication support: a) multifactor authentication or b) support biometric authentication?
Answer: Yes, but not directly. SAML 2.0 does not prescribe or support any particular authentication method directly. Companies are free to use any authentication method for authenticating their end users. As long as the ultimate assertion token is passed to CrownPeak Federated Authentication using valid SAML 2.0 protocol, CrownPeak Federated Authentication will accept it.

CrownPeak™