

EMS Platform Services
Installation & Configuration Guide
April 2019

Accruent Confidential and Proprietary, copyright 2019. All rights reserved.

This material contains confidential information that is proprietary to, and the property of, Accruent, LLC. Any unauthorized use, duplication, or disclosure of this material, in whole or in part, is prohibited.

No part of this publication may be reproduced, recorded, or stored in a retrieval system or transmitted in any form or by any means—whether electronic, mechanical, photographic, or otherwise—without the written permission of Accruent, LLC.

The information contained in this document is subject to change without notice. Accruent makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Accruent, or any of its subsidiaries, shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Table of Contents

CHAPTER 1: EMS Platform Services	1
Contact Customer Support	1
CHAPTER 2: Introduction to EMS Platform Services	2
Overview	2
What is EMS Platform Services?	2
Get Started with Integrations	2
Begin the Integration Process	3
API Documentation	4
Base URL for All API Requests	4
Date/Time Standards	4
Common Response Codes	4
HTTP Request Methods	5
CHAPTER 3: Architecture	6
CHAPTER 4: System Prerequisites and Requirements for EMS Platform Services	8
EMS Platform Services Prerequisites and Requirements	8
Install the ASP.NET Core	9
CHAPTER 5: Licensing Requirements for EMS Platform Services	10
Licensed Integrations	10
Non-Licensed Integrations	10
CHAPTER 6: Install EMS Platform Services	11
Install Platform Services	11
Install a Multiple Instance of EMS Platform Services in the IIS	13
Verify Installation Status	14
Verify NTLM Authentication	15
Upgrade EMS Platform Services Software	17
CHAPTER 7: EMS Platform Services Configuration Guide	19
Contact Customer Support	19
CHAPTER 8: EMS Authentication Methods	20
CHAPTER 9: Configure Platform Services in the Admin Portal	23

Home	24
Clear the Cache	24
Integrations	24
Create a New Integration Client	25
Reset the Client Secret	27
Booking Rules	27
Connect EMS Web App to EMS Platform Services	30
Roles	31
Create New Roles	32
Edit Existing Role Routes	32
Logs	32
Edit Log Level Details	32
Header, OpenID, and SAML (Authentication Options)	33
Auth Keys	36
Calendaring	37
Enable G Suite Integration	37
Conferencing	40

CHAPTER 1: EMS Platform Services

EMS Platform Services is the new add-on, middle-tier component that provides a modern, scalable way for partners and customers to integrate with the EMS Platform. Platform Services enables the development of multi-platform applications that can be customized, cloud-based, scalable, and easily integrated.

- [Introduction to EMS Platform Services](#)
- [Architecture](#)
- [Prerequisites and Requirements](#)
- [Licensing Requirements for Platform Services](#)
- [Install EMS Platform Services](#)

See Also: [Configuring Platform Services in the Admin Portal](#).

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available at [Accruent Access](#).
- **Option 2:** Submit a case directly via [Accruent Access](#).
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.

**Important!**

If you do not have a customer login, register [here](#).

CHAPTER 2: Introduction to EMS Platform Services

This topic contains introductory information regarding EMS Platform Services:

- [Overview](#)
- [Get Started with Integrations](#)
- [API Documentation](#)

See Also: [Architecture](#) and [Prerequisites and Requirements](#)

Overview

What is EMS Platform Services?

EMS Platform Services is a Platform as a Service (PaaS) solution offering modern, RESTful APIs. Platform Services enables the development of multi-platform applications that can be customized, cloud-based, scalable, and easily integrated. It is a true middle tier, providing a business and resource layer that enables the central development of applications, reducing complexity and development time. Platform Services fosters innovation by ensuring easy maintenance and efficient management of an application's life cycle.

In the current EMS architecture, databases exchange business logic directly with applications in the business tier. The Platform Services architecture creates an intermediary layer of business logic and resources that provides a buffer between the applications and EMS databases. Fixes, enhancements, and/or new features can now be dispersed simultaneously to all products through Platform Services.

See Also: [EMS Platform Services Architecture](#)

Get Started with Integrations

Platform Services provides RESTful APIs that empower customers and partners to build custom, multi-platform applications connected to EMS. Any client/device accessing EMS Platform Services must be a registered Integration Client. The one exception is that anyone can access the public (open) API requests (/status, /health, /clientauthentication).

There are two types of Integrations:

- Custom—Customer applications
- Partner—Third-party EMS partner applications (e.g., 7PointsSolutions, Pepperdash, control concepts, etc.)

Partner and Custom types can be classified as either of the following two client sub-categories:

1. User-based: User-based clients (EMS Mobile, EMS for Outlook) need to authenticate as a user to perform any actions. These clients need an integration client role with minimal access to the following API resources (above and beyond public resources):
 - /authentication
 - /logging
2. Non-user Based: Non-user Based clients (EMS Kiosk, EMS Room Sign App) provide functionality independent of users but also support user-like functionality (such as Check-In and on-the-fly room reservations). These clients need a role with wider access.

Begin the Integration Process

To start the integration process, follow these steps:

1. Verify if you have a license for adding Integrations. EMS Licensing manages a numeric count of both Custom and Partner Integration Types. Contact your EMS Sales Representative for a license for EMS Platform Services. View Licensing Requirements (see [Licensing Requirements for Platform Services](#)).
2. Access Platform Services documentation (e.g., <https://Yourcompany.com/EmsPlatform/swagger>).
3. Access admin portal for Platform Services (e.g., <https://Yourcompany.com/EmsPlatform/admin>) to create a new Integration Client. See [Configuring Platform Services in the Admin Portal](#) for more information.

**Note:**

Creating a new Integration Client will generate a Client ID and Secret pair.

4. Platform Services requires a valid JWT Authentication token to call any of the API resources with the exception of /public, /status and /clientauthentication. Before making any API request, you must first call /clientauthentication with a Client ID and Secret pair generated in the previous step.
 - The Client token returned from calling /clientauthentication should be applied to the x-ems-api-token header for subsequent API requests.

**Note:**

There can be multiple active instances of a particular client interacting with the Platform. All devices that share a client/secret will share a common authentication token. If the token expires, all devices will need to authenticate again to get a new shared token.

5. For API resources that require an authenticated web user, your integration client will need to request a web user authentication token for that user. To acquire an authentication token, call the /authentication requests.
6. The Web token returned from calling /authentication should also be applied to the x-ems-api-token header; thus, replacing the client token with a user token.

**Note:**

Refer to the [API documentation](#) to determine the appropriate token (i.e., client token or web token) for the header field.

API Documentation

Navigate to Platform Services URL (e.g. <https://Yourcompany.com/EmsPlatform/swagger>) to view the API documentation. You can also manually type in the URL (<https://Yourcompany.com/EmsPlatform/swagger>).

Base URL for All API Requests

All requests should be made to URL for EMS Platform Services (e.g., <https://Yourcompany.com/EmsPlatform>).

Date/Time Standards

All dates and times passed to the API requests follow RFC 3339 Standard and must be in UTC.

All DateTimes follow the standard (e.g., 2008-09-08T22:47:31-07:00)

Common Response Codes

Response Code	Title	Meaning
200	Success	Successful data call/pull
400	Bad Request	Server could not understand the request due to invalid syntax
401	Invalid/Missing Client Credential	User credentials are incorrect; invalid login info
500	Server Error	General status code that indicates the server encountered an unexpected condition and could not fulfill the request

Response Code	Title	Meaning
503	Service Unavailable	Application pools are not currently enabled
519	Server Internal Error	System requirements are not met

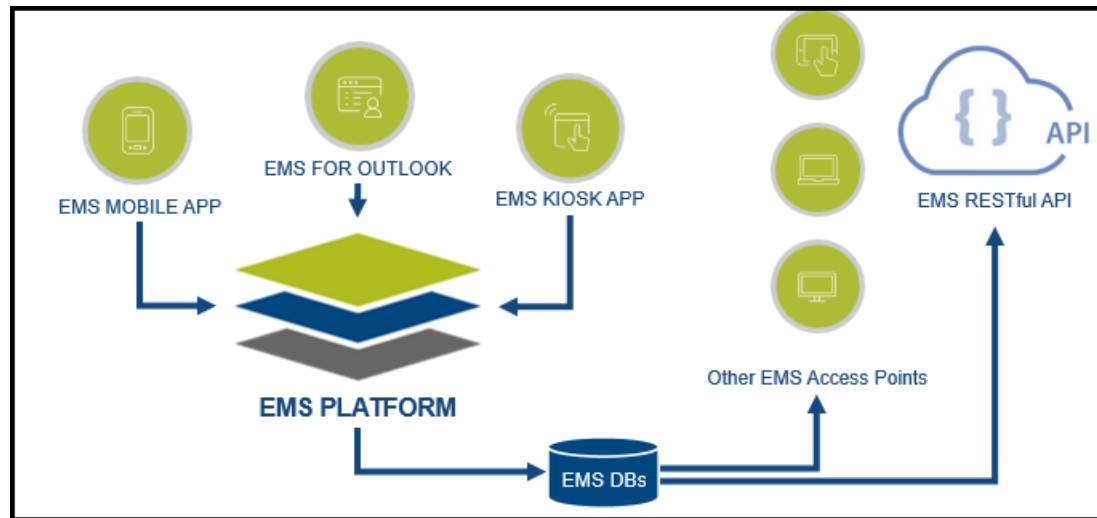
HTTP Request Methods

Method	Description
GET	Requests data from a specified source.
POST	Sends data to the API server to create or update a resource; data sent to the server is stored in the request body of the HTTP request.
PUT	Sends data to the API server to create or update a resource (similar to POST). However, PUT requests are idempotent and calling the same PUT request multiple times will always produce the same result. Calling a POST request repeatedly might have the side effect of creating the same resource multiple times.
DELETE	Deletes the specified resource.
PATCH	Applies partial modifications to a resource.

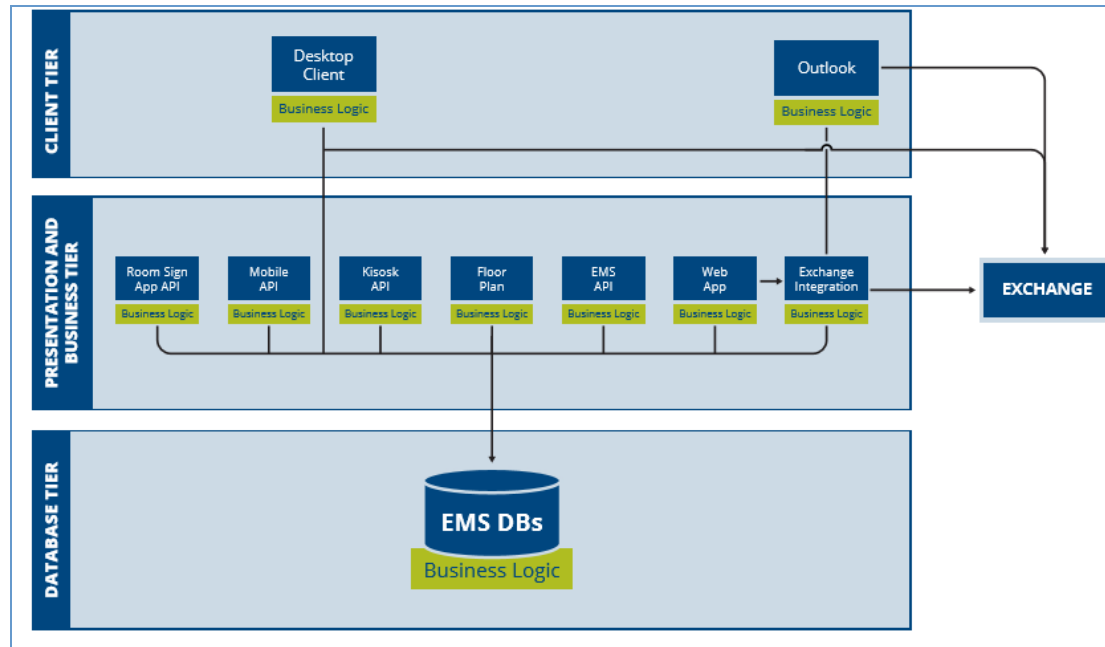
CHAPTER 3: Architecture

In June 2017, the EMS Mobile App was implemented with EMS Platform Services. As of January 2018, the EMS Kiosk App and EMS for Outlook have both been placed on the EMS Platform Services layer. In the future, all EMS applications will consume the Platform Services layer.

For our clients and partners, EMS Platform Services provides a platform for faster, more straightforward custom integrations. Clients will experience a more valuable, consistent user experience across all EMS products. In addition, features and enhancements across all access points will experience faster turnaround times. Platform Services has empowered EMS to be a true enterprise solution.



Current EMS Platform Services Architecture (As of January 2018)



Legacy EMS Architecture (Prior to January 2018)

See Also: [Connect with EMS Platform Services.](#)

CHAPTER 4: System Prerequisites and Requirements for EMS Platform Services

The following information is necessary to successfully [install EMS Platform Services](#). See Also: [Licensing Requirements](#).



Important!

As of [Update 28](#), users are required to deploy EMS Platform Services with [ASP.NET Core](#), rather than the HTTP Platform Handler.

EMS Platform Services Prerequisites and Requirements

Operating System	IIS
Windows Server 2012	8
Windows Server 2012 R2	8.5
.NET Framework	4.6.1
Application Pool	4.0

Prerequisites (Prior to Update 28)

HTTPPlatformHandler IIS Module	Download Version 1.2 here OR download the installer here .
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development: <ul style="list-style-type: none"> • ISAPI Extensions • ISAPI Filters • .NET Extensibility 4.6

Prerequisites (Update 28 and Later)

ASP.NET Core	See Also: Installing ASP.NET Core .
------------------------------	---

Operating System	IIS
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development: <ul style="list-style-type: none">• ISAPI Extensions• ISAPI Filters• .NET Extensibility 4.6

Install the ASP.NET Core



Important!

As of [Update 28](#), users are required to deploy EMS Platform Services with [ASP.NET Core](#), rather than the HTTP Platform Handler.

1. [Download the .NET files](#).
2. Choose .NET Core version 2.1.
3. In the right-hand “Runtime” column, select **ASP.NET Core/.NET Core: Runtime & Hosting Bundle**.



Note:

ASP.Net handler is a part of the Runtime & Hosting Bundle.

CHAPTER 5: Licensing Requirements for EMS Platform Services

Licensed Integrations

EMS offers the following LICENSED integrations for Platform Services:

1. **Custom Integrations:** Used when writing applications/services connecting to EMS.
2. **Partner Integrations:** Used when purchasing integrations built by EMS partners (e.g. 7 Points Solutions, PepperDash and Control Concepts).

**Note:**

The EMS Platform Services License includes a numeric count of custom and partner-type integrations. Please contact your EMS Sales Representative for more information.

Non-Licensed Integrations

EMS offers the following NON-LICENSED integrations for Platform Services:

1. **EMS Front end applications:** Necessary to support standard functionality (e.g., EMS Mobile App).
2. **EMS packaged integration access:** Used to support standard EMS pre-packaged integrations (e.g., Skype for Business Integration, Exchange Room Integration).

CHAPTER 6: Install EMS Platform Services



Important!

As of [Update 28](#), users are required to deploy EMS Platform Services with [ASP.NET Handler](#), rather than the HTTP Platform Handler.

This topic provides information on the following:

- [Install EMS Platform Services](#)
 - [Install multiple instances of EMS Platform Services in the IIS](#)
- [Verify Installation Status](#)
- [Verify NTLM Authentication](#)
- [Upgrade EMS Platform Services Software](#)

Install Platform Services



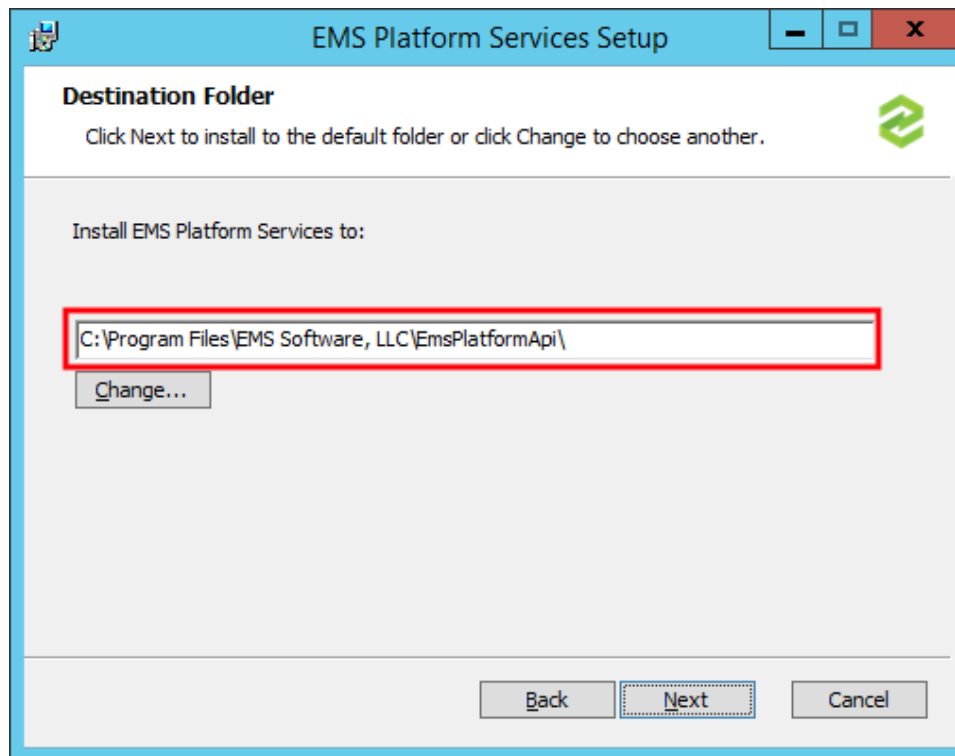
Important!

Verify the [System Requirements](#) and install the [Prerequisites](#) prior to installing EMS Platform Services.

1. Log into [Accruent Access](#).
2. Click **My Products**.
3. Under **EMS**, click **Downloads**.

The downloads page opens in a new browser tab.
4. In the **Software Downloads** area, click the link for your version of software, for example, **V44.1 Releases & Patches**.

A new page opens listing the downloads available based on your license.
5. Download **EMSPlatformServices.msi**. (Required for all installations.)
6. The EMS Platform Services Setup Wizard will appear. Click **Next** to begin installation.



EMS Platform Services Setup Wizard

7. Choose a default folder for installing EMS Platform Services. The Platform installer by default will try to install in the Programs folder. You can change the path to wwwroot folder. The typical install path is C:\Program Files\EMS Software, LLC\EmsPlatformApi\. Click **Next**.
8. You will need to enter the SQL server and EMS database, configured to allow external connections. Make a note of the database name.

Select the **Use Windows Authentication for Database Connection** checkbox to use an Active Directory account instead of the EMS User for database authentication.

**Note:**

If you are unsure of the SQL server and EMS database name, you can find the SQL server and EMS database name in the EMS Web App (**Admin Functions > Connection String values** under the version number heading) or EMS Desktop Client (**File > Change Database > Provide Server Parameters** dialog). You can also contact your company's IT group to locate the information.

9. Enter a Virtual Directory Name.
10. To enable NTLM authentication for Everyday User Authentication for the Platform Services Admin

Portal and Integration Clients, click the **Enable NTLM For EMS Everyday User Authentication** box.



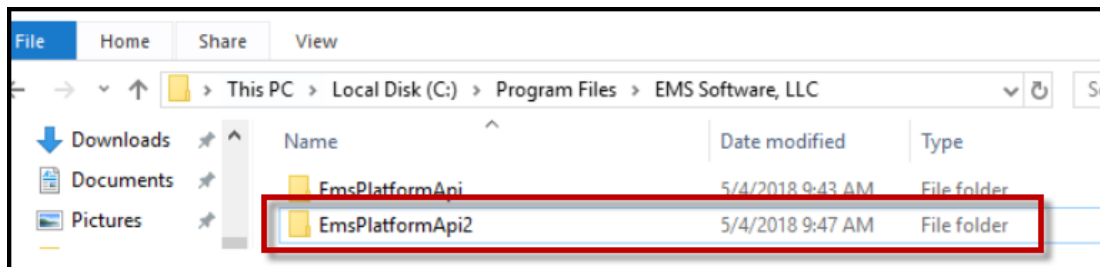
Important!

To use NTLM authentication when logging into the EMS Platform Services Admin Portal, you must select the **Enable NTLM For EMS Everyday User Authentication** box. If you complete the installation process without selecting the **Enable NTLM For EMS Everyday User Authentication** box and you want to use NTLM authentication, you will need to re-install the EMS Platform Services software and select the checkbox during install.

11. Click the **Install** button to complete the installation. You will receive a prompt from the Wizard that installation is complete. EMS Platform Services is now installed on your Web server.
12. Click **Finish**.
13. If you enabled NTLM authentication through the **Enable NTLM For EMS Everyday User Authentication** box during installation, [verify the NTLM authentication](#).

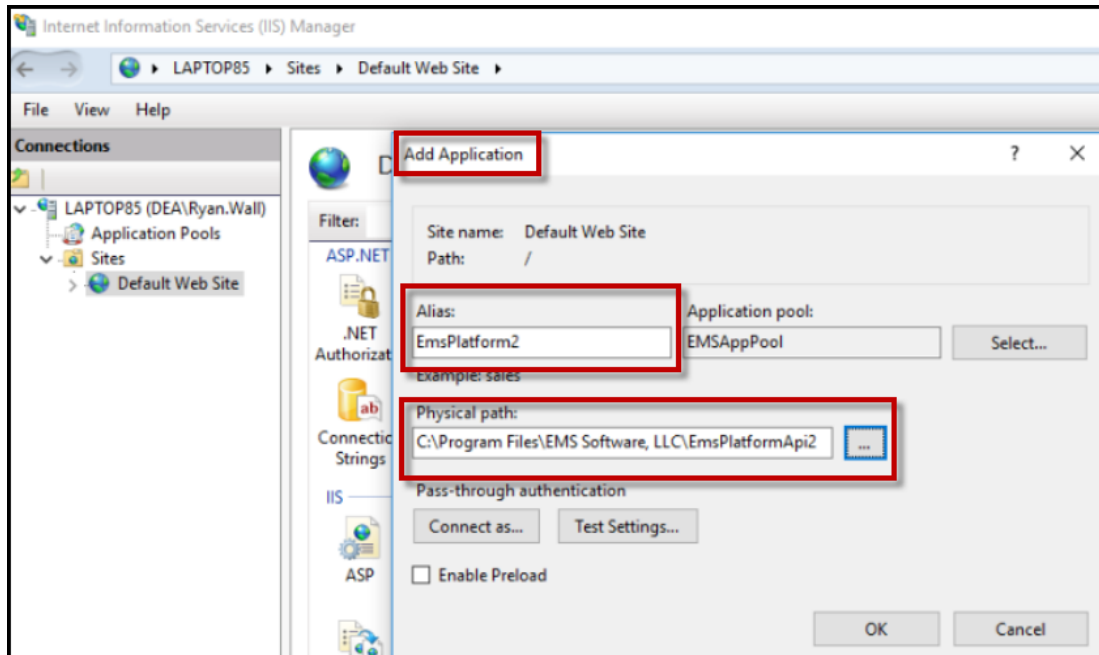
Install a Multiple Instance of EMS Platform Services in the IIS

1. After [installing EMS Platform Services](#), copy the installed directory for each additional instance of EMS Platform Services.



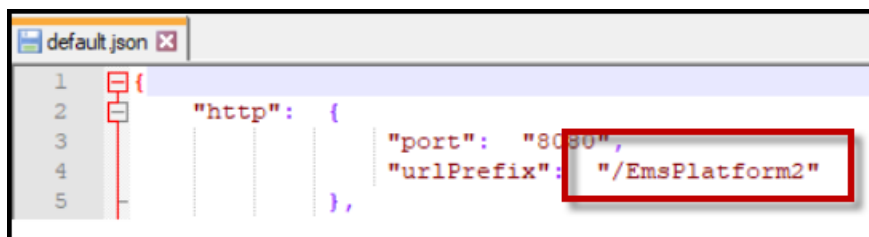
Copy of Installed Directory of EMS Platform Services

2. From your Internet Information Services (IIS) Manager, right click and select **Add Application**. In the Add Application dialog box, choose a unique name in the **Alias** field. In the **Physical Path** field, include the path of the copied folder above.



Adding a Multiple Instance of EMS Platform Services in IIS

3. Click **OK**.
4. Navigate to your **default.json** file (or **web.config** override file). Edit the `urlPrefix` setting to match the unique name of the instance in the IIS.

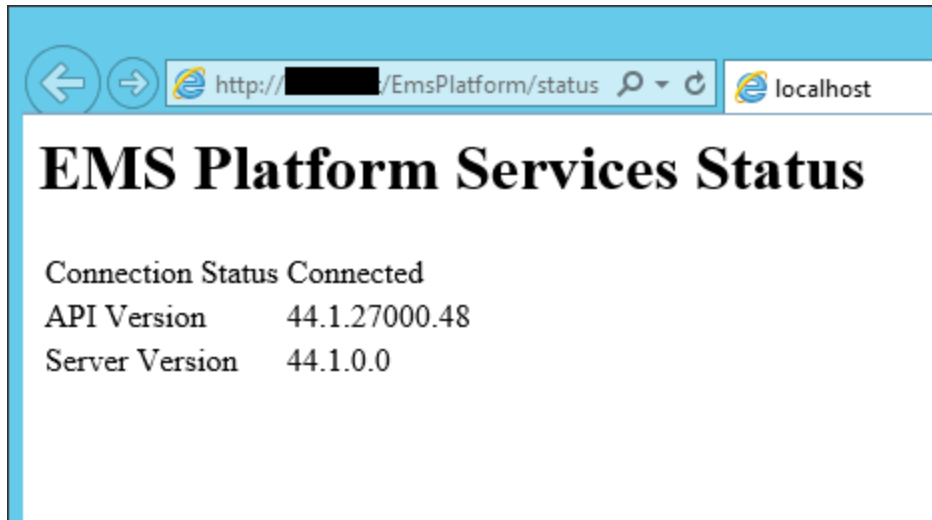


Editing the urlPrefix in the default.json File of the Multiple Instance

5. Reset the IIS.

Verify Installation Status

1. Access your URL for Platform Services (e.g., <https://yourcompany.com/EMSPlatform>).
2. Verify the status of your installation by navigating to <https://yourcompany.com/EMSPlatform/status>.



Status Screen for EMS Platform Services

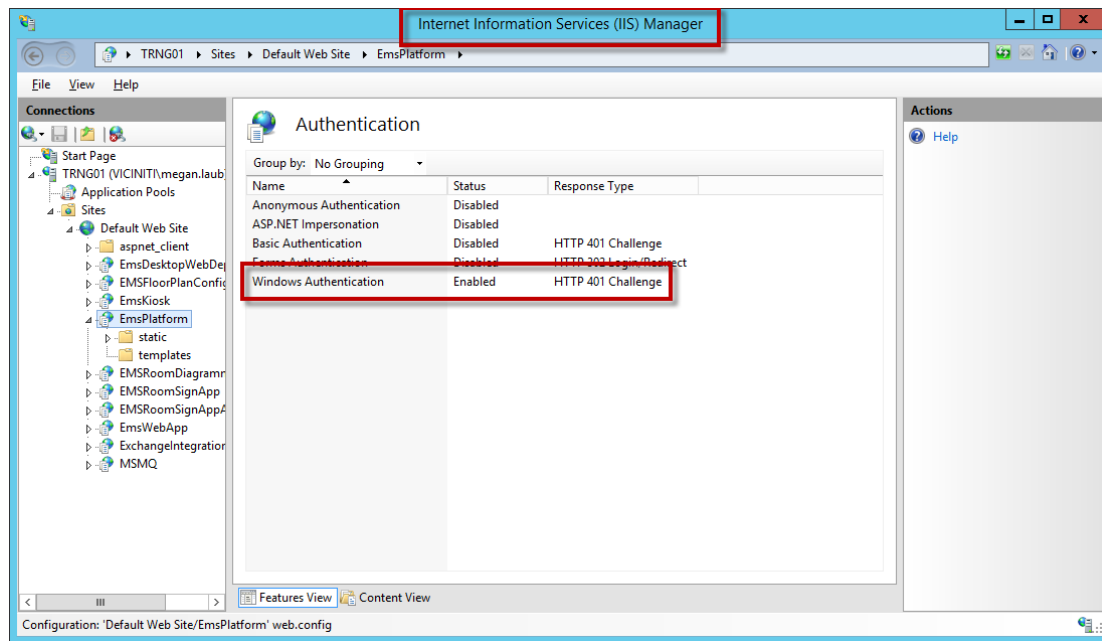
Verify NTLM Authentication



Important!

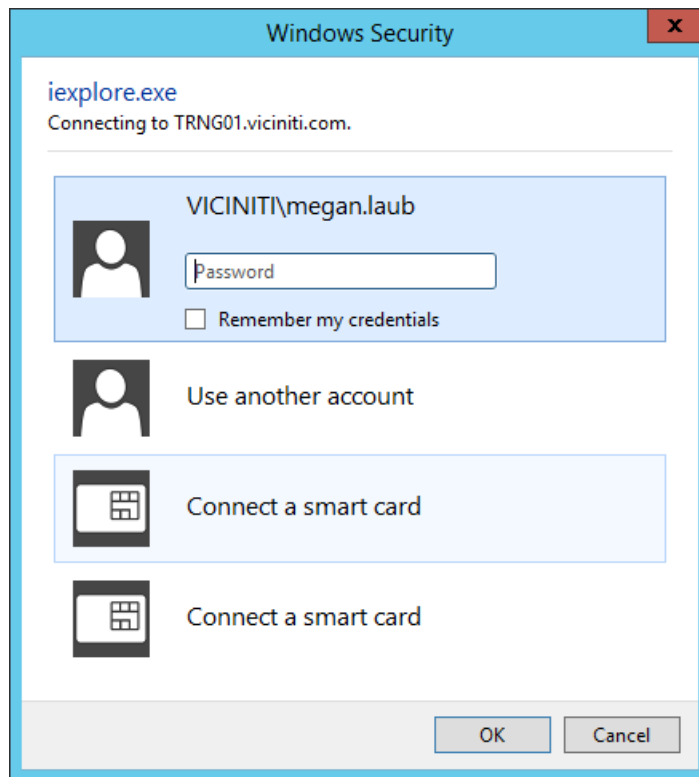
To use NTLM authentication when logging into the EMS Platform Services Admin Portal, you need to have selected the **Enable NTLM For EMS Everyday User Authentication** checkbox during the [installation process](#). If you completed the installation process without selecting the **Enable NTLM For EMS Everyday User Authentication** box and you want to use NTLM authentication, you will need to re-install the EMS Platform Services software and select the checkbox during install.

1. Verify that Windows Authentication is enabled from your Internet Information Services (IIS) Manager.



Windows Authentication Enabled in IIS Manager

2. Navigate to the EMS Platform Services Admin Portal (e.g., <https://yourcompany.com/EMSPlatform/admin>).
3. Verify that the Windows Security dialog box appears.



Verifying Windows Security Screen When Logging into the Admin Portal

4. Enter the Everyday User's **username** and **password**.

Upgrade EMS Platform Services Software

To upgrade EMS Platform Services to the current version of the software, you will need to do the following:

1. Uninstall the EMS Platform Services software through **Windows Control Panel > Programs > Uninstall a Program**.
2. Obtain the current release of EMS Platform Services from the Downloads area in Accruent Access.

To view the Downloads area, log into [Accruent Access](#) and click **My Products > EMS Downloads** (opens a new tab) > **V44.1 Releases & Patches** (in Software Downloads area).



Note:

For more information on obtaining the latest version of the EMS Platform Services software and on enhancements and fixes to the software, see also: [Updating to the Latest Version of EMS \(Patches and Builds\)](#) and [Release Notes](#).

3. Re-install the EMS Platform services by completing the steps in the [Install Platform Services](#) section.

**Note:**

If multiple instances of the EMS Platform Services software exist in IIS, you will need to delete the instances from the Windows directory and from IIS, and then install the multiple instances again once you have finished upgrading the EMS Platform Services software. See Also: [Install a Multiple Instance of EMS Platform Services in the IIS](#).

CHAPTER 7: EMS Platform Services Configuration Guide

From the EMS Platform Services Admin Portal, you can clear the cache, view license and application information, configure authentication methods, manage integration clients, and view logs. You can configure settings for EMS Platform Services from the following tabs:

- [Home—Perform Admin Functions](#)
- [Integrations—Manage EMS Integrations](#)
- [Roles—Create New Roles or Edit Existing Ones](#)
- [Logs—View Global and Integration Logs](#)
- [Header](#)
- [OpenID](#)
- [SAML](#)
- [Auth Keys—Create New Keys](#)
- [Calendar—Enable GSuite Integration](#)
- [Conferencing—Skype for Business](#)

See Also: [EMS Authentication Methods](#)

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available at [Accruent Access](#).
- **Option 2:** Submit a case directly via [Accruent Access](#).
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.

**Important!**

If you do not have a customer login, register [here](#).

CHAPTER 8: EMS Authentication Methods

Authentication is the process of identifying an individual or entity that is attempting to log into a secure domain. EMS Software supports multiple authentication methods that are suited to different applications and use cases.

The following table provides information on the various authentication methods for each EMS product.

EMS Product	Authentication Options	Available on EMS Platform Services	Available to EMS Cloud Services Customers	Best Practices
EMS Desktop Client	<ul style="list-style-type: none"> • EMS Native Authentication • LDAP • Windows Authentication 	NO	YES. However, not available in Citrix (LDAP and Windows Authentication).	
EMS Web App	<ul style="list-style-type: none"> • Windows Authentication • LDAP • EMS Native Authentication • SAML 2.0 (ADFS) • CAS • Portal Authentication 	NO	YES (LDAP, EMS Authentication, and SAML 2.0 ADFS) NO (Windows Authentication and Portal Authentication)	
EMS Kiosk App	Primary Authentication: <ul style="list-style-type: none"> • Standard • Exact Match • LDAP • Badge Second Authentication: <ul style="list-style-type: none"> • Exact Match • LDAP • Standard 	YES	YES	
EMS Kiosk App (Legacy)	Primary Authentication: <ul style="list-style-type: none"> • Standard 	NO	YES	

EMS Product	Authentication Options	Available on EMS Platform Services	Available to EMS Cloud Services Customers	Best Practices
	<ul style="list-style-type: none"> Exact Match LDAP Badge <p>Secondary Authentication:</p> <ul style="list-style-type: none"> Security Type Badge 			
EMS Room Sign App	<ul style="list-style-type: none"> Group Authentication: <ul style="list-style-type: none"> Badge External Reference Group/Contact Email Network ID Other ID Personnel Number Contact Authentication Secondary Authentication 	NO	YES	Best Practices
EMS Mobile App	<ul style="list-style-type: none"> SAML NTLM Windows Authentication LDAP OpenID Persistent Authentication EMS Native Authentication 	YES	<p>YES (SAML, LDAP, OpenID, EMS Native Authentication)</p> <p>NO (NTLM Windows Authentication and Header Authentication)</p>	
Master Calendar	<ul style="list-style-type: none"> NTLM Windows Authentication LDAP Portal Authentication Native Authentication 	NO	<p>YES (LDAP and EMS Native Authentication)</p> <p>NO (Portal and NTLM Windows Authentication)</p>	

EMS Product	Authentication Options	Available on EMS Platform Services	Available to EMS Cloud Services Customers	Best Practices
Campus Planning Interface	<ul style="list-style-type: none"> • EMS Native Authentication • Windows Authentication • LDAP Authentication • Portal Authentication 	NO	YES (EMS Authentication and LDAP) NO (Windows Authentication and Portal)	
EMS for Outlook	<ul style="list-style-type: none"> • Exchange Authentication 	YES	N/A	
EMS Floor Plan	<ul style="list-style-type: none"> • EMS Native Authentication 	NO	YES	

See Also:

- [Authentication Options for EMS Web App](#)
- [Authentication Options for EMS Mobile App](#)
- [Authentication Options for EMS Master Calendar](#)
- [Authentication Options for EMS Regics](#)
- [Integrated Authentication Considerations](#)
- [Integrated Windows Authentication](#)
- [Manage Everyday Users For Integrated Authentication](#)
- [LDAP Authentication](#)
- [Portal or Federated Authentication](#)
- [Portal Authentication Methods](#)
- [SAML Authentication](#)

CHAPTER 9: Configure Platform Services in the Admin Portal

To begin configuration of EMS Platform Services, navigate to the EMS Platform Services Admin Portal using the Platform Services admin URL (e.g., <https://yourcompany.com/EMSPlatform/admin>). From the EMS Platform Services Admin Portal, you can clear the cache, view license and application information, configure authentication methods, manage integration clients, and view logs.

EMS Platform Services Admin Portal consists of the following tabs:

- [Home—Perform Admin Functions](#)
- [Integrations—Manage EMS Integrations](#)
- [Connect EMS Web App to EMS Platform Services](#)
- [Roles—Create New Roles or Edit Existing Ones](#)
- [Logs—View Global and Integration Logs](#)
- [Header](#)
- [OpenID](#)
- [SAML](#)
- [Auth Keys—Create New Keys](#)
- [Calendaring—Enable G Suite Integration](#)
- [Conferencing—Skype for Business](#)

EMS Platform Services

44.1.24000.220

EMS Platform Services

Admin Functions

[Clear Cache](#)

Empty the cache of parameters on this server

License & Application Information

Platform API Version	44.1.24000.220
Expiration Date	Fri, Feb 15, 2019 5:00 PM
Allowed Web Users	9999999
Custom Integration Limit	9999
Partner Integration Limit	9999

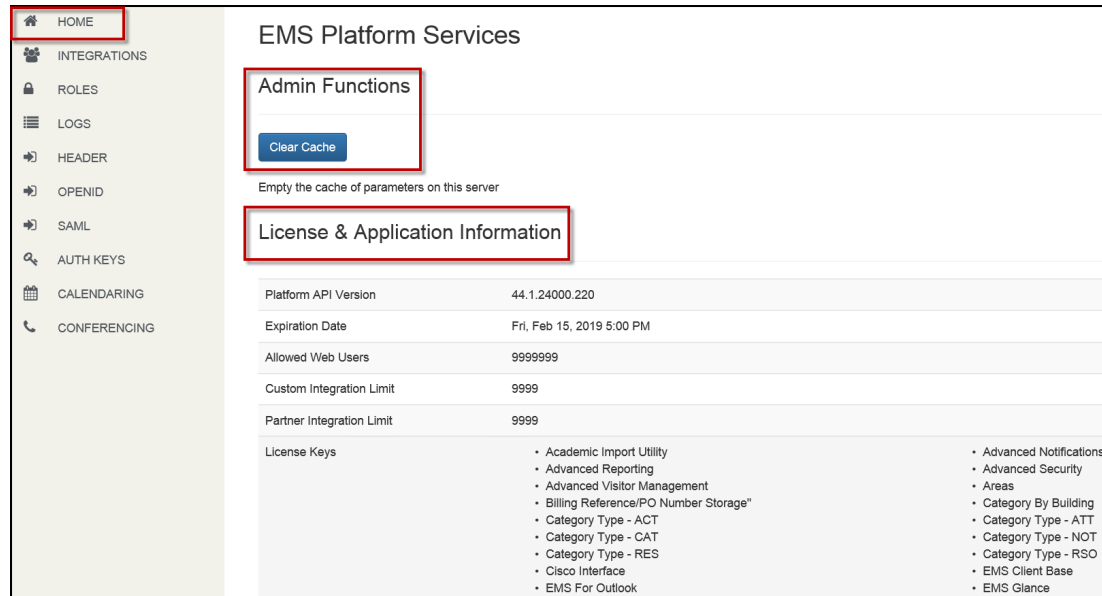
License Keys

- Academic Import Utility
- Advanced Reporting
- Advanced Visitor Management
- Billing Reference/PO Number Storage
- Category Type - ACT
- Category Type - CAT
- Category Type - RES
- Cisco Interface
- EMS For Outlook
- Advanced Notifications
- Advanced Security
- Areas
- Category By Building
- Category Type - ATT
- Category Type - NOT
- Category Type - RSO
- EMS Client Base
- EMS Glance

EMS Platform Services Admin Portal

Home

When logged into EMS Platform Services Admin Portal from an EMS Everyday User account with a Web Admin security role, you can perform Administrative Functions, such as [Clearing the Cache](#) and viewing License and Application Information.



Home Tab of EMS Platform Services Admin Portal

Clear the Cache



Important!

The cache must be cleared in EMS Platform Services and the EMS Web App whenever parameter changes are made in the EMS Desktop Client.

To clear your cache and have EMS Platform Services re-read the database parameters:

1. From the **Home** tab, click the **Clear Cache** button.
2. You will receive a notification that the cache has been cleared successfully.

Integrations

You can manage your EMS Integrations from the **Integrations** tab. From here, you can [create](#), edit status, delete integration clients, or [reset the Client Secret](#).

Create a New Integration Client

1. Navigate to the **Integrations** tab on the EMS Platform Services Admin Portal. From this screen, you can view a list of integrations and their statuses.
2. To create a new integration client, click the **New Integration Client** button.

Integrations Tab of EMS Platform Services Admin Portal

3. Create a client **Name**.
4. From the **Type** drop-down, choose either **Custom** or **Partner**.
5. Choose a **Role** from the drop-down.

Note:

The **Active** box is checked by default. This indicates that your integration is active.

6. Click **Enable Logging** to view the logs for this integration through the Log section of the Admin Portal.
7. Configure **User Authentication**.
 - a. To designate the Client as an Everyday User, check the **Everyday User Authentication Required** box. If this box is not checked, all other options for everyday user authentication will be inaccessible. [Header](#), [OpenID](#), and [SAML](#) are configured from the EMS Platform Services Admin

Portal.

- b. Check the **User Authentication is Persistent** box to allow users to remain logged in.
- c. The default for **Token Duration** is one day (1440 minutes). Customize this duration by entering a number of minutes in the field.
- d. Choose an authentication method from the **Everyday User Authentication Method** drop-down. Your choices include:
 - **EMS Native**—Authenticates users via Everyday Application User (webuser) credentials stored in the EMS database. No additional authentication configuration is required.
 - **Header**—If this authentication is chosen, you must navigate to the **Header** tab. Enter the **Header Variable** and click **Save Changes**. See Also: [Portal Authentication Methods](#).
 - **LDAP**—This authentication provides single-sign-on capability using your organization's LDAP environment and can be used in both intranet and internet deployments of EMS Everyday applications. See Also: [LDAP Authentication](#).
 - **NTLM**—To configure NTLM authentication, click the **Enable NTLM For EMS Everyday User Authentication** box during installation. See [Verifying NTLM Authentication](#) to complete this authentication.
 - **OpenID**—If this authentication is chosen, navigate to the **OpenID** tab and complete the required fields. See Also: [OpenID Connect Authentication](#).
 - **SAML**—If this authentication is chosen, navigate to the **SAML** tab and complete the required fields. See Also: [SAML Authentication](#).



Note:

The Header, OpenID, and SAML authentication settings are applied globally. All Integration Clients with these authentication types selected will default to these settings.

8. Based on client type, EMS Platform Services checks against license count, and current number of "active" integration clients. If license count is 0 or equal to the current number of "active" clients, then EMS Platform Services denies the request to add an additional client. You must set the existing client to inactive or increase your license count via normal licensing processes. Please refer to [Licensing Requirements](#) for more details.
9. Click **Save Client**. A Client ID and Secret pair is generated once the Integration Client is successfully saved. Copy and save the Client Secret in a secure location. You will NOT be able to retrieve the Client Secret. To obtain a new Client Secret, you will need to reset it. See Also: [Reset Client Secret](#).

**Important!**

Partner and Custom types can be classified as either of the following client sub-categories: **User-based** and **Non-user based**.

User-based: User-based clients (EMS Mobile, EMS for Outlook) need to authenticate as a user to perform any actions. These clients need an integration client role with minimal access to the following API resources (above and beyond public resources):

/authentication

/logging

Non-user based: Non-user based clients (EMS Kiosk, EMS Room Sign App) provide functionality independent of users but also support user-like functionality (such as Check-In or on-the-fly room reservations). These clients need a role with wider access.

Reset the Client Secret

1. Navigate to the **Integrations** tab on the EMS Platform Services Admin Portal.
2. Select the **Integration Client**.
3. Click the **Reset Secret** button.

Booking Rules

The following booking rules are validated by each of these calls.

Call	BOOKING RULES
Create Reservation	Web template must exist (for user)
	Web template must be associated with the proper rooms
	Max bookings
	Date limit
	Max bookings per date range
	Max bookings per date
	Max minutes
	Twenty four hour max

Call	BOOKING RULES
	Booking cutoffs
	If VC—must have host/host group
	Event Type ID must be valid
	If Exchange, Exchange ID must be valid (reaches out to Exchange)
	PROC: Handle setting conflict status if necessary
Availability	User has template
	Template is active
	Must have time zone record for the room
	24 Hour max
	Max minutes
	No bookings in past
	Inventory (e.g., projector)
	Cutoffs
	Last allowed date
	Max bookings per date
	Max bookings before last date
	Building Hours
	Blocking bookings
Add Booking	Reservation must exist
	Template must exist for user
	Max bookings

Call	BOOKING RULES
	Max minutes
	Twenty four hour max
	Booking cutoffs
Edit Booking	License
	Web template / user
	Template access ("template mode")
	Room access (must be in template, and not be the calendaring TBD room)
	Not crosslisted
	Status must allow edits
	Must not be invoiced
	Must not have a service order in progress
	Must not have setup/teardown and be in progress
	Must not be managed space event in progress
	Must not be a VC in progress
	Cutoff rules
	Last Date rules
	Category cutoff rules
	Must not be invited (in calendaring) and be in progress
	Max bookings
	Date limit
	Max bookings per date range

Call	BOOKING RULES
	Max bookings per date
	Max minutes
	Twenty four hour max
	Booking cutoffs
	Timezone must exist
	PROC: Cutoff rules
	PROC: Last Date rules
	PROC: Max Minutes
	PROC: MaxBookings per day
	PROC: Categories (Allow weekends, category cutoff rules)
	PROC: Setup & Capacity Validation
	PROC: 24 Hours Max
	PROC: Building Hours
	PROC: Conflict check

Connect EMS Web App to EMS Platform Services



Important!

Beginning with [Update 31](#), EMS Platform Services is a prerequisite for installing and using the EMS Web App. If EMS Platform Services has not yet been [installed](#) in your environment, validate the [hardware and software requirements for EMS Platform Services](#).

If your organization uses the EMS Mobile App, EMS Kiosk App, Google Integration, EMS for Outlook, or SAML authentication, then EMS Platform Services is already running in your environment.

To connect EMS Web App to EMS Platform Services, follow these steps;

1. Navigate to the EMS Platform Services Admin Portal.
2. Select **Integrations**. Under Clients, click on the EMS Web App link.
3. Click the **Reset Secret** button and copy the generated Secret.
4. In the web.config file located in the designated folder for your current version of EMS, insert the copied Secret ID into the value field.

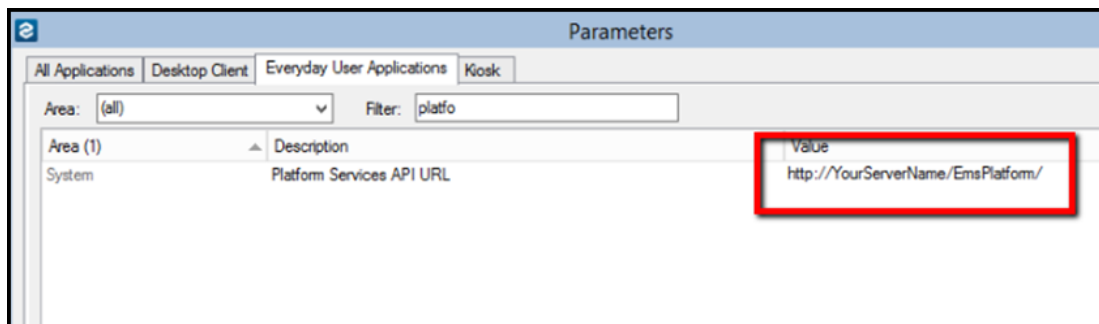
```
<add key="platformServicesSecret" value="YourSecretID" />
```



Important!

EMS Cloud Services customers do not need to generate a Secret or insert it into the web.config file (Steps 3 and 4).

5. [Clear the cache in EMS Platform Services.](#)
6. In the EMS Desktop Client, navigate to **System Administration > Settings > Parameters > Everyday User Applications**. Configure the **Platform Services API URL** parameter and then click **Close**.



Everyday User Applications Tab, Platform Services API URL

Roles

Roles are separate entities responsible for capturing the rules associated with authorizing clients and users. These authentication roles allow users to access specific rest API routes. Roles are applied to clients, both [user-based](#) and [non-user based](#).

From the **Roles** tab, you can [create new roles](#) or [edit existing roles](#).

Create New Roles

1. Navigate to the **Roles** tab on the EMS Platform Services Admin Portal.
2. Click the **New Role** button.
3. Provide a unique Role Name in the **Name** field.
4. From the **Available Routes** list, move the routes you want associated to this role to the **Selected** list by using the Move (>) arrow.

Edit Existing Role Routes

1. Navigate to the **Roles** tab on the EMS Platform Services Admin Portal.
2. Click on the role route you want to edit. A list of routes associated with the role appears.
3. From the **Available Routes** list, move the routes you want associated to this role to the **Selected** list by using the Move (>) arrow.

Logs

You can view logs from the EMS Platform Services Admin Portal. You can [edit log level details](#) through the default.json file.

There are two types of logs in EMS Platform Services:

- **Global logs:** Includes logs only for EMS Platform Services.
- **Integration logs:** Includes logs for a selected integration client. Enable logging for any integration client you want to view logs for by choosing a Client from the dropdown.

Edit Log Level Details

1. Navigate to the [Default](#) folder that was created during [installation](#).
2. Open the default.json file for editing.
3. Under **Logging**, set the **logLevel** field to **Debug**.

```
{
  "http": {
    "port": "8080",
    "urlPrefix": "/"
  },
  "logging": {
    "logLevel": "INFO",
    "formatter": "text",
    "fileLogging": {
      "logToFile": true,
      "logFileFolder": ".\\LogFiles",
      "logFilename": "api.log",
      "maxSizeMB": 10,
      "maxBackups": 20,
      "maxAgeDays": 0
    }
  }
}
```

Default.json File

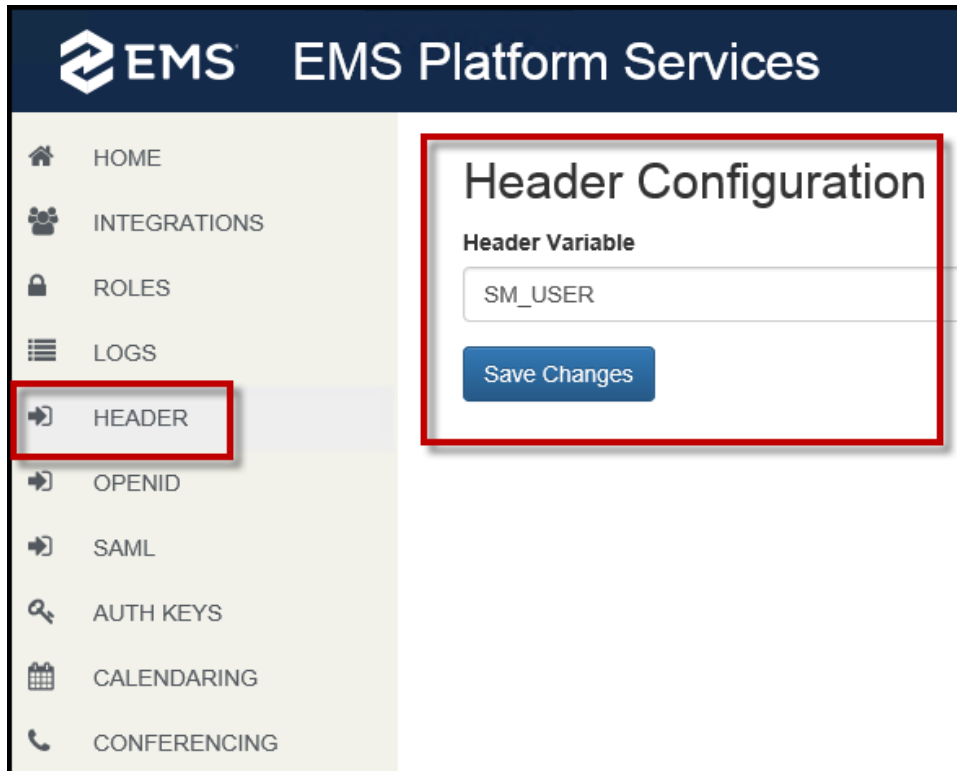
Header, OpenID, and SAML (Authentication Options)

EMS supports two authentication types for the EMS Platform Services Admin Portal:

1. **EMS Native authentication**—An Everyday User with Everyday User Admin Security Template credentials can log into the EMS Platform Services Admin Portal. Verify license information is correctly reflected on the admin home page.
2. **NTLM authentication**—During installation of EMS Platform Services, click the **Enable NTLM For EMS Everyday User Authentication** box.

The following authentication methods are EMS Desktop Client-integration specific:

- **Header authentication.** See Also: [Portal Authentication Methods](#).



Header Tab of EMS Platform Services Admin Portal

- **LDAP authentication**—The LDAP Authentication method provides single-sign-on capability using your organization's LDAP environment and can be used in both intranet and internet deployments of EMS applications (e.g., EMS Web App and EMS Mobile App). See Also: [LDAP Authentication](#).
- **Open ID authentication**—Authentication with Open ID requires configuration in EMS Mobile App before users can authenticate. See Also: [Open ID Connect Authentication](#).

The screenshot displays the EMS Platform Services Admin Portal. The left sidebar contains a menu with the following items: HOME, INTEGRATIONS, ROLES, LOGS, HEADER, OPENID (highlighted with a red box), SAML, AUTH KEYS, CALENDARING, and CONFERENCING. The main content area is titled 'Open ID Configuration' and contains two input fields: 'User Info Endpoint' with the value 'https://example.com/userinfo' and 'User Info Request Method' with the value 'GET'. A blue 'Save Changes' button is located at the bottom of the configuration area. A red box highlights the entire configuration section.

OpenID Tab of EMS Platform Services Admin Portal

- **SAML authentication**—Authentication with SAML requires configuring set up for EMS Mobile App and EMS Web App prior to beginning the authentication flow. See Also: [SAML Authentication](#).

HOME

INTEGRATIONS

ROLES

LOGS

HEADER

OPENID

SAML

AUTH KEYS

CALENDARING

CONFERENCING

SAML Configuration

Request And Response Properties

Form Post Field Name

SAMLResponse

User Identity Field

Name ID

Identity Attribute Name

e.g., emailAddress

Identity Provider Issuer

e.g., some-issuer

Service Provider Issuer

http://localhost/EmsPlatform

HTTP Binding Type

Redirect

URLs

Identity Provider URL for Service Provider Redirect

https://idp.example.com/auth/saml

Service Provider Base URL for IdP Callback

http://localhost/EmsPlatform

Certificate Paths

SAML Certificates are now Auth Keys

Path to Identity Provider Public Certificate

e.g., C:\secrets\certs\idp.cer

Path to Service Provider Public Certificate

e.g., C:\secrets\certs\sp-public.cer

Path to Service Provider Private Certificate

e.g., C:\secrets\certs\sp-private.cer

Save Changes

SAML Tab of EMS Platform Services Admin Portal

Auth Keys

Auth Keys are used for SAML certificates. See Also: [SAML Authentication](#).

To create a new Auth Key:

1. Navigate to the **Auth Keys** tab in the EMS Platform Services Admin Portal.
2. Click **New Auth Key**.
3. Provide a **Purpose**.
4. Provide a date range for when the Auth Key will be valid by entering dates in the **Not Before** and **Not After** fields.
5. Enter a Public Key (PEM).

6. Enter a Private Key (PEM).
7. Click **Save Auth Key**.

Calendaring

Google Calendar Integration will allow access to G Suite users' Google Calendars to provide their free/busy statuses within EMS for scheduling meetings. Everyday Users can see attendee availability directly within the EMS Web App or Mobile App alongside space availability information from the EMS database.

Enable G Suite Integration



Important!

A license must be imported prior to Enabling G Suite in the EMS Platform Services Admin Portal. See Also: [Configure G Suite Integration](#).

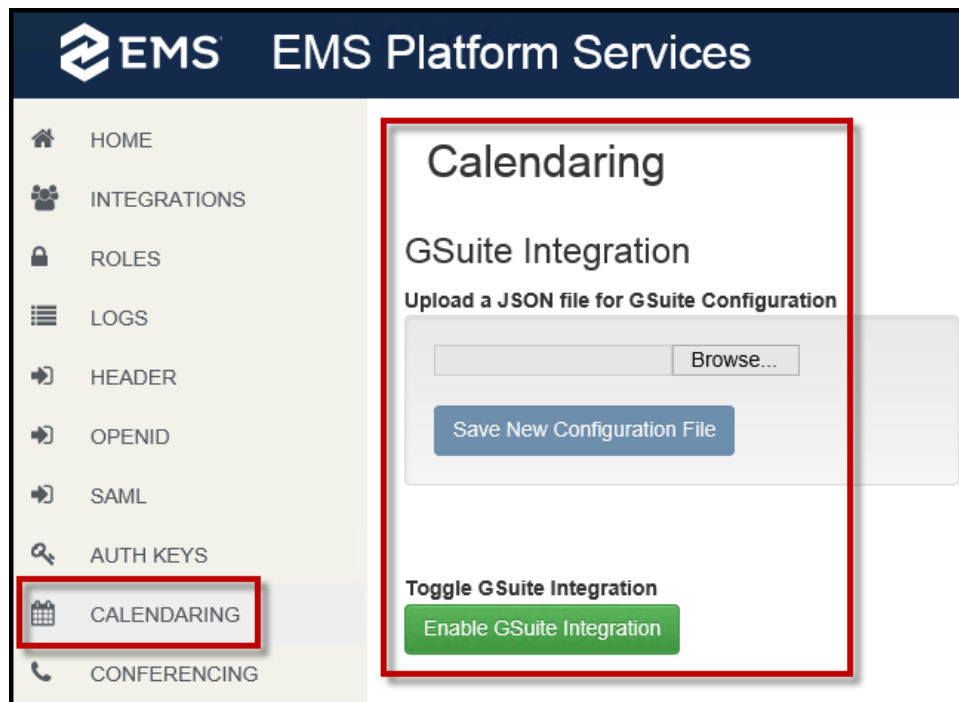
1. Navigate to the **Calendaring** tab in the EMS Platform Services Admin Portal.
2. Upload the JSON file created for your [G Suite project](#). Click **Browse** to navigate to the file and click **Save New Configuration File**.
3. In the **Service Account Mailbox** field, enter the mailbox address and then click the **Update** button.



Note:

As of [Update 31](#), a Service Account Mailbox is required for the G Suite Integration. The Service Account Mailbox can be any mailbox within your domain (or your organizational unit if you are not integrating the entire domain). The mailbox does not require special permissions.

4. Toggle between **Enabling** and **Disabling** G Suite Integration by using the Enable G Suite Integration button.



Calendaring Tab of EMS Platform Services Admin Portal

**Important!**

Known Issue for Update 32—Clicking the G Suite Integration enable/disable button AFTER the first time the integration is enabled will break the integration.

After the first time the G Suite Integration is enabled, if you click the enable/disable toggle button again (EMS Platform Services Admin Portal > **Calendaring** tab), the G Suite Integration will no longer work.

If your G Suite Integration is no longer functioning because the enable/disable button was clicked after the integration was initially enabled, complete these steps to repair the integration:

- a. From the **Calendaring** tab of the EMS Platform Services Admin Portal, ensure the enable/disable toggle button is set to enabled.

If the toggle button is currently set to disabled, toggle to enabled, and then refresh the page.

**Note:**

The button is *enabled* when it is red and displays the words **Disable GSuite Integration**.

The button is *disabled* when it is green and displays the words **Enable GSuite Integration**.

- b. [Re-upload the JSON file](#).

**Note:**

Do not click the enable/disable toggle button after re-uploading the JSON file.

- c. Once the JSON file has been uploaded, restart the app pool used by EMS Platform Services.

**Note:**

EMS Cloud Services Customers—EMS Cloud Operations must restart the app pool for EMS Platform Services. To request a restart, [contact EMS Support](#).

Conferencing

EMS integration of Skype for Business allows users to easily integrate instant messaging and audio/video conferencing to their meetings without the need for A/V support. Users can add, join, or modify/cancel Skype for Business meetings added to bookings. See Also: [Configure Skype for Business](#).

To configure Skype for Business in the EMS Platform Services Admin Portal:

1. Navigate to the **Conferencing** tab.
2. Provide a **Client Name** in the **Azure Active Directory Client ID** field. This determines the ID of the registered application.
3. Provide the **Azure Active Directory Tenant**. This determines the name of the AAD tenant.
4. Provide the **Skype for Business AutoDiscover URL**. This performs autodiscovery to find the appropriate server to communicate with. Multiple URLs must be separated by commas and cannot contain any spaces. The client machine and the Web server should have access to the Autodiscover URL.
5. Choose a **Skype for Business Server Authentication Method** from the drop-down. This determines the authentication type that is used to generate a token. You can choose from the following authentication methods:
 - **NTLM**
 - **ADFS**
 - **Username/Password**
 - **Oauth (Online)**
6. In the Skype Meeting Options area, select an option from the **These people don't have to wait in the lobby** drop-down list. This field determines which participants do not need to wait before joining the meeting. The following options are available:
 - **Only me, the meeting organizer**
 - **People I invite from my company**
 - **Anyone from my organization**
 - **Anyone (no restrictions)**

The screenshot shows the 'EMS Platform Services' admin portal. On the left is a navigation menu with icons and labels: HOME, INTEGRATIONS, ROLES, LOGS, HEADER, OPENID, SAML, AUTH KEYS, CALENDARING, and CONFERENCING (which is highlighted with an orange border). The main content area is titled 'Conferencing Configuration'. It contains several form fields: 'Azure Active Directory Client ID' with a sub-label 'Client Name', 'Azure Active Directory Tenant', 'Skype For Business AutoDiscover URL' with a placeholder 'e.g., emailAddress', and 'Skype Meeting options' with a sub-label 'These people don't have to wait in the lobby' and a dropdown menu currently set to 'Anyone from my organization'. A 'Save Changes' button is at the bottom.

EMS Platform Services

Conferencing Configuration

Azure Active Directory Client ID

Client Name

Azure Active Directory Tenant

Skype For Business AutoDiscover URL

e.g., emailAddress

Skype Meeting options

Other Skype configuration can be controlled via Skype for Business PowerShell or Skype for Business Server 2015 Control Panel

These people don't have to wait in the lobby

Anyone from my organization

Save Changes

Conferencing Tab of EMS Platform Services Admin Portal

EMS Platform Services - April 2019

Accruent, LLC

11500 Alterra Parkway

Suite 110

Austin, TX 78758

www.accruent.com