EMS MOBILE APP Configuration Guide

V44.1

Last Updated: August 2018

Table of Contents

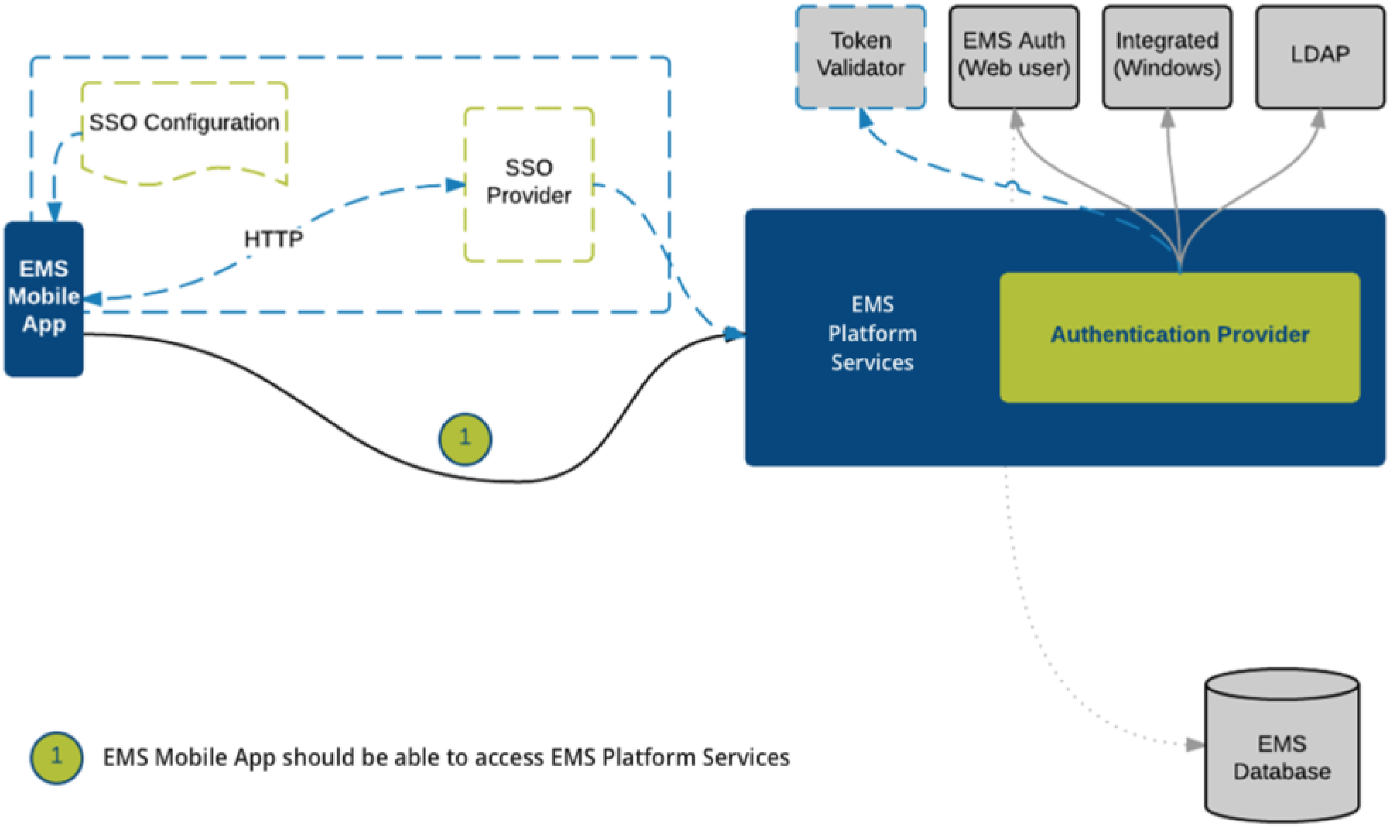
CHAPTER 1: EMS Mobile App Configuration Guide

EMS Mobile App, available on iOS and Android smartphones, is designed primarily for everyday users "on the go." It allows users to make simple reservations in unmanaged spaces (i.e., spaces without services and approvals), such as workspaces and open conference rooms.

This guide provides the following information for configuring the EMS Mobile App:

CHAPTER 2: Configure EMS Mobile Authentication

This section provides the following information about configuring EMS Mobile Authentication.



© 2016 EMS Software, LLC

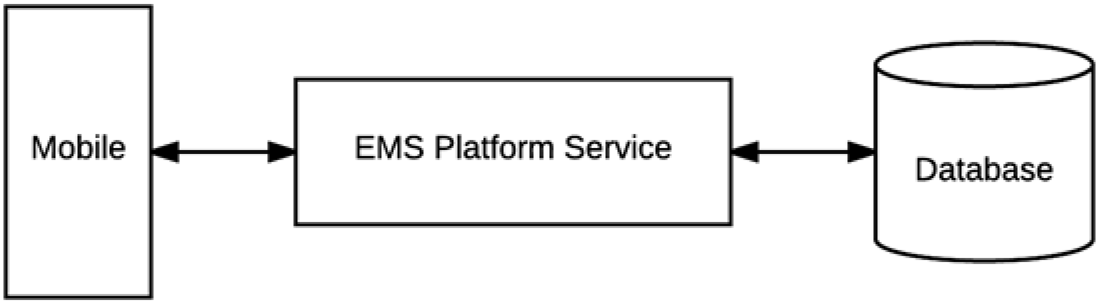
Authentication options for the EMS Mobile App include:

- EMS Native Authentication
- LDAP Authentication
- Open ID Connect Authentication
    - Open ID Connect Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App
- Persistent Authentication
- SAML Authentication
    - SAML Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App
- Windows Authentication (NTLM) for EMS Mobile

CHAPTER 3: EMS Native Authentication

Authenticate your users via Everyday Application User (emsuser) credentials stored in the EMS database. The following example shows the default configuration that ships with EMS Mobile App.

Example EMS Native Authentication in the EMS Mobile App



After successful connection to EMS Platform Services, the user will:

1. Enter his or her credentials on the Sign In screen.
2. Tap **Sign In**.

3. User will be taken to the Home screen.

If the credentials are missing or invalid when the user taps **Sign In**, an error message will appear indicating invalid credentials or that the fields are required.

TEST YOUR EMS NATIVE AUTHENTICATION

Assuming you have installed the EMS Platform Services (at https://yourcompany.com/ems-platform-api), you can test the authentication with a curl command:

```
curl -X POST -H 'x-ems-consumer: MobileApp' -H 'Content-Type: application/json' -d '{"username":"your_username", "password":"your_password"}' https://ems.yourcompany.com/endpoint...authentication
```

...where your_*username* and your_*password* are your credentials.

> **NOTE: api/v1/authentication** is the endpoint within the API where your request must be sent.

CHAPTER 4: LDAP Authentication

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory information. 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 Everyday applications such as EMS Web App and EMS Mobile App.

For example, when a user logs into EMS Web App or EMS Mobile App with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the Network ID and/or External Reference fields of your EMS Everyday User records. If a match exists, the Everyday User will be logged in to the application, inheriting any Everyday User Process Template rights to which their LDAP Group has been assigned.

NOTE: The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.

NOTE: The Field Used to Authenticate Everyday User parameter (within System Administration > Settings > Parameters (Everyday User Applications tab) is used by the applications to determine which value should be used for authentication.

Follow the steps in this section to authenticate your users via LDAP. After successful connection to the platform API, the user will log in following the scenario below:

- The user will enter credentials on the Sign In screen and tap **Sign In**.
- EMS Mobile App will send credentials to the EMS Platform Services.
- EMS Platform Services will verify credentials against the configured LDAP provider.
- EMS Platform Services will respond to the EMS Mobile App.
- User will be taken to the Home screen.

If the credentials are missing when the user taps **Sign In**, an error message will display stating that fields are required. If the platform API is unable to verify the credentials, the mobile app will inform the user based on that response.

To use LDAP authentication, you will need to:

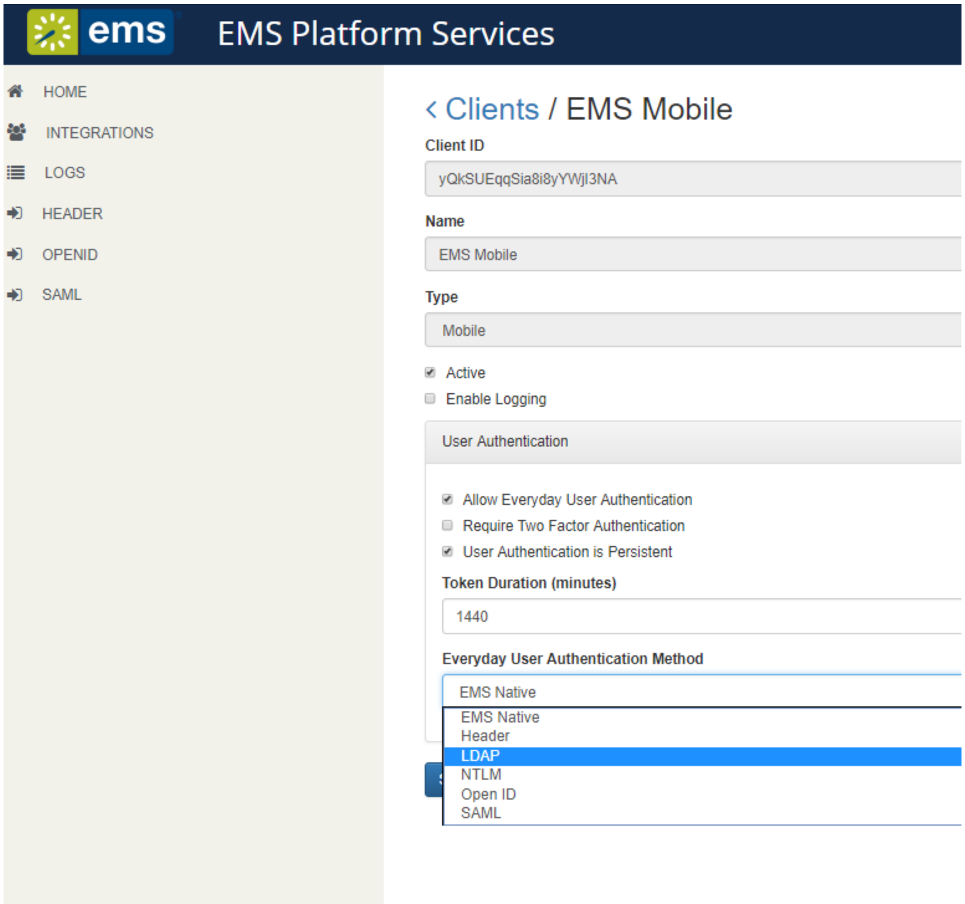
1. Configure your LDAP Provider.
2. Test your LDAP Configuration.
3. Test your LDAP Authentication.

This topic covers the following topics related to LDAP configuration:

- Configure EMS Web App to Use LDAP Authentication
- Configure EMS Web App Security
- Configure Communication Options
- Core Properties
- Non-AD Config
- LDAP Queries
- Save Your Configuration
- Test Your Configuration
- Configure Authentication for EMS Mobile App

CONFIGURE YOUR LDAP PROVIDER

1. Navigate to Platform Services admin portal (https://yourcompany.com/ems-platform-api) and select Integrations from the sidebar.
2. Select EMS Mobile and choose LDAP from everyday user authentication method dropdown.



‹ Clients / EMS Mobile

Client ID
yQkSUEqqSia8i8yYWjl3NA

Name
EMS Mobile

Type
Mobile

☑ Active
☐ Enable Logging

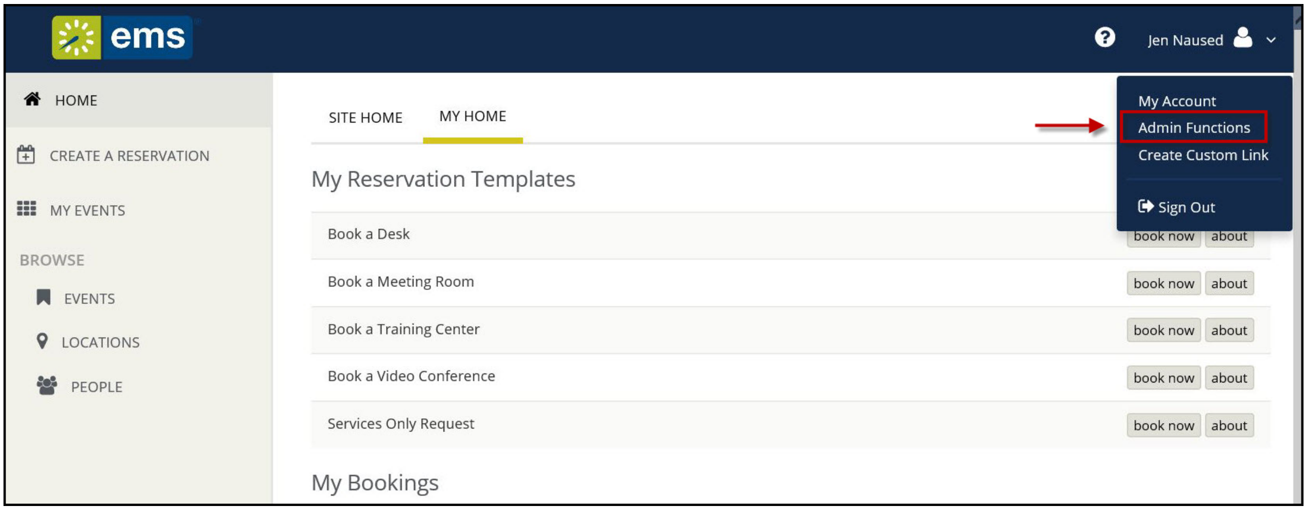
User Authentication

☑ Allow Everyday User Authentication
☐ Require Two Factor Authentication
☑ User Authentication is Persistent

Token Duration (minutes)
1440

Everyday User Authentication Method
EMS Native

3. Navigate to the **EMS Web App** > **Admin Functions** page, listed under your name in the upper right corner of the application.

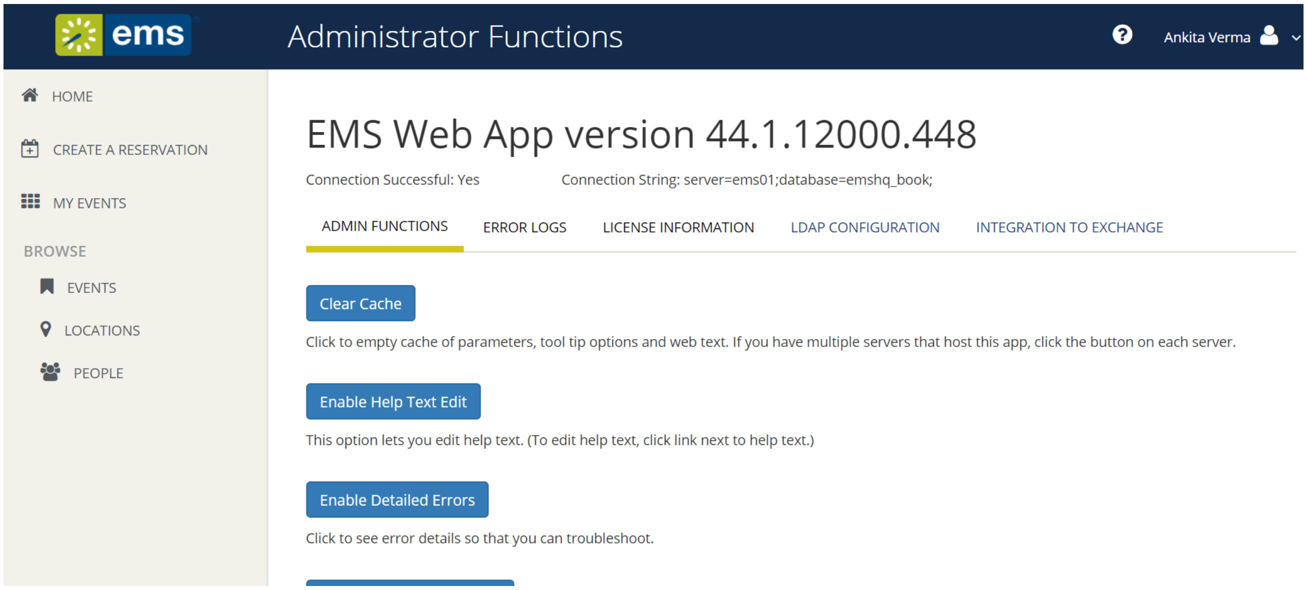


My Reservation Templates

Book a Desk	book now	about
Book a Meeting Room	book now	about
Book a Training Center	book now	about
Book a Video Conference	book now	about
Services Only Request	book now	about

My Bookings

4. Tap the **LDAP Configuration** tab and complete all required LDAP information, and then Test Your LDAP Configuration.



EMS Web App version 44.1.12000.448

Connection Successful: Yes   Connection String: server=ems01;database=emshq_book;

Click to empty cache of parameters, tool tip options and web text. If you have multiple servers that host this app, click the button on each server.

This option lets you edit help text. (To edit help text, click link next to help text.)

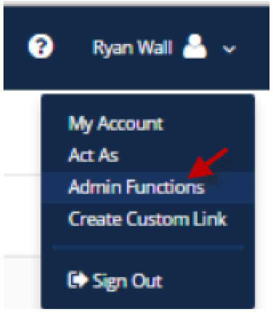
Click to see error details so that you can troubleshoot.

TIP: This is the same process you use for LDAP Authentication. The EMS Platform Services API uses the same configuration information.

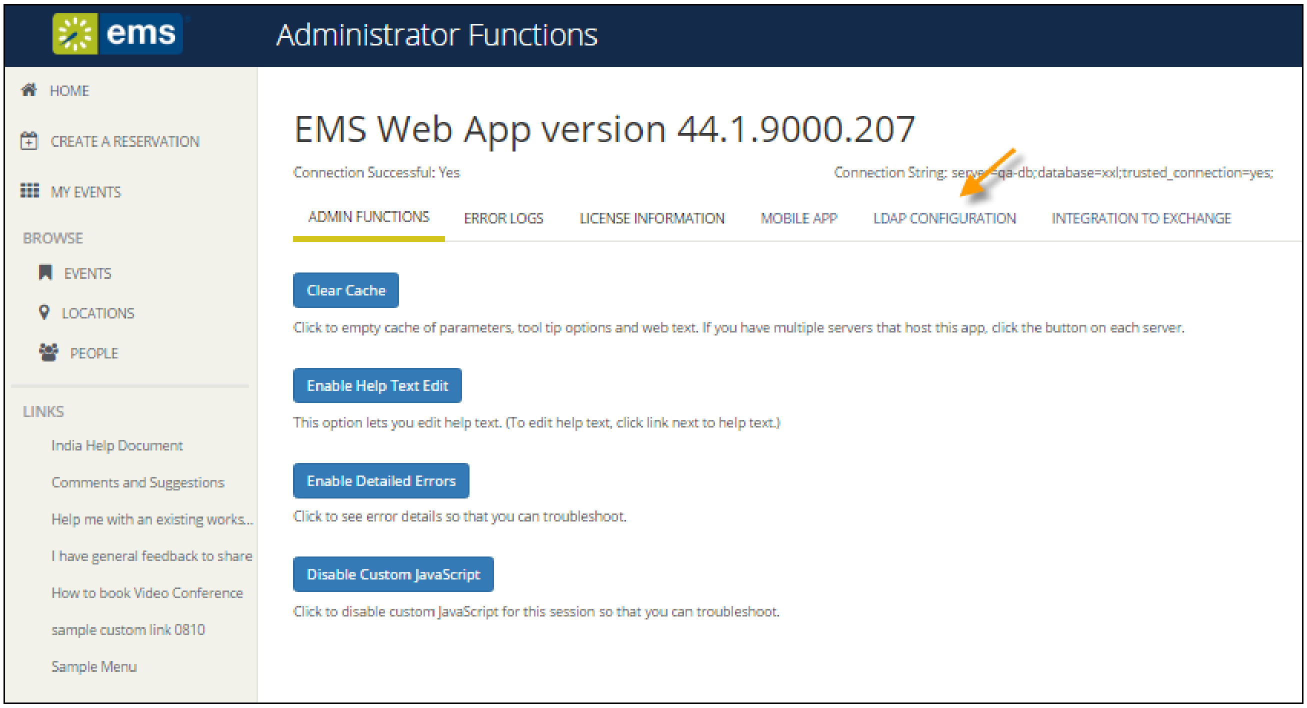
CONFIGURE EMS WEB APP TO USE LDAP AUTHENTICATION

1. Log into EMS Web App with a User that belongs to an Everyday User Security Template containing the Web Administrator role (controlled in the EMS Desktop Client under Configuration > Everyday User Applications > Everyday User Security Templates). See Also: Configuring Security Templates

2. From the User Options, select Admin Functions.



3. Click the LDAP Configuration tab.



EMS Web App version 44.1.9000.207

Connection Successful: Yes

Connection String: server=qa-db;database=xxl;trusted_connection=yes;

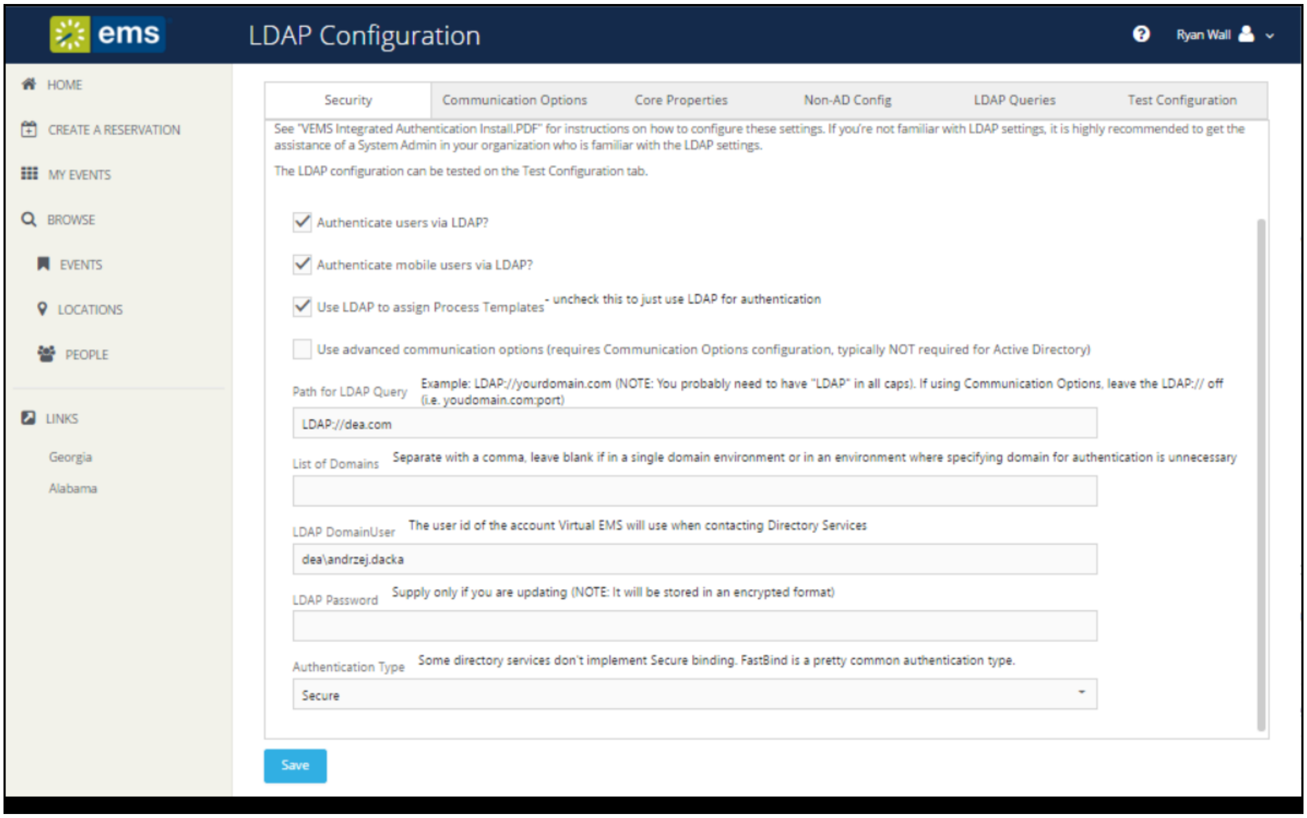
Click to empty cache of parameters, tool tip options and web text. If you have multiple servers that host this app, click the button on each server.

This option lets you edit help text. (To edit help text, click link next to help text.)

Click to see error details so that you can troubleshoot.

Click to disable custom JavaScript for this session so that you can troubleshoot.

4. The LDAP Configuration window appears, presenting multiple tabs for various settings.



See "VEMS Integrated Authentication Install.PDF" for instructions on how to configure these settings. If you're not familiar with LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

The LDAP configuration can be tested on the Test Configuration tab.

☑ Authenticate users via LDAP?

☑ Authenticate mobile users via LDAP?

☑ Use LDAP to assign Process Templates - uncheck this to just use LDAP for authentication

□ Use advanced communication options (requires Communication Options configuration, typically NOT required for Active Directory)

Path for LDAP Query Example: LDAP://yourdomain.com (NOTE: You probably need to have "LDAP" in all caps). If using Communication Options, leave the LDAP:// off (i.e. youdomain.com:port)

LDAP://dea.com

List of Domains Separate with a comma, leave blank if in a single domain environment or in an environment where specifying domain for authentication is unnecessary

LDAP DomainUser The user id of the account Virtual EMS will use when contacting Directory Services

dea\andrzej.dacka

LDAP Password Supply only if you are updating (NOTE: It will be stored in an encrypted format)

Authentication Type Some directory services don't implement Secure binding. FastBind is a pretty common authentication type.

Secure

CONFIGURING EMS WEB APP SECURITY

1. On the Security tab:

    a. Select the Authenticate users via LDAP checkbox to enable LDAP authentication.

b. If LDAP will be used to assign Everyday User Process Templates to your Web Users, select the Use LDAP to assign Process Templates checkbox.

c. Use advanced communication options: Skip this step for Active Directory environments. Enabling this checkbox requires that you complete the settings on the Communication Options tab.

d. In the Path for LDAP Query field, specify a valid LDAP path (example – LDAP://YourCompany.com)

e. List of Domains: Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.

f. In the LDAP Domain\User field, enter a Domain User account that has rights to query LDAP (example – YourDomain\User)

g. In the Password field, enter a valid Password for the User Account entered in the previous step.

h. Specify the appropriate LDAP Authentication Type for your environment.

NOTE: The other tabs (Communication Options, Core Properties, Non-AD Config and LDAP Queries) should only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP.

CONFIGURING COMMUNICATION OPTIONS

> **WARNINGS:** It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you’re not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

The Communication Options tab includes fields that define how to fetch a Group or a User when sending communications from the EMS Desktop Client. You can also set the SSL configurations, including the Security Certificate Path. Checking the Use SSL box will force communication to use SSL.

- **Certificate Path**: If there is a specific certification that you want to use to validate your authentication.
- **Authentication Type**: Type of authentication that your LDAP server will use during the binding process. Basic is the default because it is the most common.
- **Search Root**: The root is the level at which your search will begin.
- **User Search Filter**: Specifies the filter to use when performing the user search.
    - Example: (&(objectClass=Person)(SAMAccountName={0})) or (&(objectClasss=Person)(uid={0}))

- **Group Search Filter**: Specifies the filter to use when performing the group search.
  - Example: (&(objectClass=Person)(objectClass=user))

- **Protocol Version**: Insert the current version number here. The default is 3, as the current version should be 3.

CORE PROPERTIES

> **WARNINGS:** It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

Indicate whether your LDAP implementation is Active Directory. These properties are set to the common defaults, but can be changed here if the LDAP properties differ from the defaults displayed.

- **LDAP Name Property**: The property for user name on the user record in LDAP that will be displayed. Displayname is the default, as it is the most common.
- **LDAP Phone Property**: The property for the phone number on the user record in LDAP that will be displayed. Telephonenumber is the default, as it is the most common.

- **Domain to append to users**: This field is unnecessary unless the domain of your user is different from the domain returned from the query.
- **Field for LDAP Group Lookup**: This identifies the EMS property that should be utilized when performing the search. For example, if you use LDAP solely to assign templates and you want the EMS Web App to look up group membership using a field other than the login name, then you must enter that field's name here.

NON-AD CONFIGURATION

> **WARNING:** It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you’re not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

If your LDAP implementation is not Active Directory, use these fields to redefine the LDAP property names used when searching directory information.

- **LDAP Account/User ID Property**: The property in your LDAP store that contains the user name.
  - Example: If sameaccountname=xxxx, then enter sameaccountname

- **Full LDAP User ID Format**: Leave blank unless authentication requires a full path.
  - Example: cn={0},ou=staff,o=yourdomain

- **LDAP Group Category**: The property in your LDAP store that contains the group category.
  - Example: If filter should be objectClass=groupOfNames, then property should be groupOfNames

- **LDAP Group Name**: The property in your LDAP store that contains the group name.
- **LDAP Group Member Name**: The property in your LDAP store that contains the name of a single member in the group.
  - Example: If member property is member=jdoe, then property should be member

- **LDAP Group Member User Name Attribute**: The property of the user record that corresponds to the group's member property to determine group membership.

LDAP QUERIES

> **WARNING:** It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you’re not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

These are LDAP query overrides to fetch Groups and Users from the domain. These settings rarely need to overridden, but can be used to customize queries.

- **LDAP query for security groups**: Query used to search for security groups in your LDAP store.
- **LDAP query to find users**: Query used to search for users in your LDAP store.
- **LDAP query for find users with space**: Query used to search for users that have spaces surrounding their user names in your LDAP store.

SAVE YOUR CONFIGURATION

1. Click Save.

> **NOTE:** If you want Everyday Users to inherit Everyday User Process Templates based on the LDAP Group(s) with which they belong, see LDAP Groups Tab. Otherwise, you have completed the configuration process.

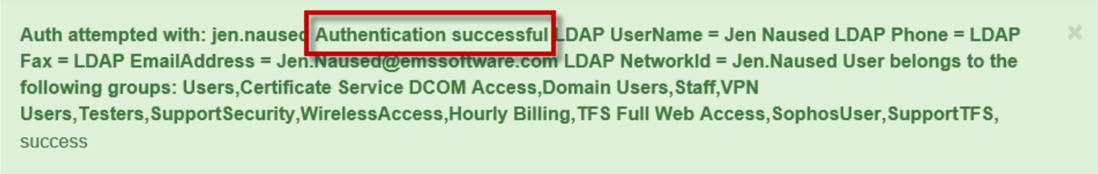
2. Within EMS Desktop Client, go to the Everyday User Process Templates area (Configuration > Web > Everyday User Process Templates).
3. Within an Everyday User Process Template, locate the LDAP Groups tab and select the appropriate LDAP Group(s) to map to that Everyday User Process Tem-

plate.

4. Click OK.

TEST YOUR CONFIGURATION

1. After completing configuration, navigate to the Test Configuration tab in the EMS Web App under LDAP Configuration.
2. Enter your Network UserId Without Domain Name.
3. Enter your Password.
4. Click Test.
   a. If your configuration was successful, you will receive a message in a green box at the top that includes domain information and the words "Authentication successful" (please see example below).



Auth attempted with: jen.naused Authentication successful LDAP UserName = Jen Naused LDAP Phone = LDAP Fax = LDAP EmailAddress = Jen.Naused@emssoftware.com LDAP NetworkId = Jen.Naused User belongs to the following groups: Users,Certificate Service DCOM Access,Domain Users,Staff,VPN Users,Testers,SupportSecurity,WirelessAccess,Hourly Billing,TFS Full Web Access,SophosUser,SupportTFS, success

   b. If the configuration was unsuccessful, you will receive a prompt stating that LDAP could not be accessed. Check your logs to determine the reason for the failure.

CONFIGURING AUTHENTICATION FOR THE EMS MOBILE APP

1. If your organization uses EMS Mobile App, click the Mobile App tab.
2. Choose the LDAP option.

TEST YOUR LDAP CONFIGURATION

Assuming you have installed the EMS Platform Services e.g. https://yourcompany.com/ems-platform-api, then you can test the configuration with a simple curl command:

```
curl -X GET -H 'x-ems-consumer: MobileApp' https://ems.yourcompany.com/endpoint/api/v1/health
```

> **TIP:** You can also use the API's Swagger interface to accomplish this goal.

You should see a portion of the JSON response that looks like this (unrelated details omitted for brevity):

```
{
  ...
  "additionalProperties": {
    "authConfig": {
      "activities":"ldap"  // <-- these are the critical lines
      "ui":"ldap"
    }
  }
}
```

TEST YOUR LDAP AUTHENTICATION

Assuming you have installed the EMS Platform Services API at https://ems.*yourcompany*.com/endpoint, you can test the authentication with a simple curl command:

```
curl -X POST -H 'x-ems-consumer: MobileApp' -H 'Content-Type: application/json' -d '{"username":"your_username", "password":"your_password"}' https://ems.yourcompany.com/endpoint...authentication
```

...where your_*username* and your_*password* are your credentials.

NOTE: api/v1/authentication is the endpoint within the API where your request must be sent.

CHAPTER 5: Open ID Connect Authentication

This section guides you authenticating your users via the Open ID Connect protocol. Authentication with Open ID requires configuration in EMS Mobile App before users can authenticate.

> **NOTE:** For more information about how Open ID can be hosted or pre-configured in the EMS Mobile App, see Open ID Connect Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App.

This topic provides information on the following:

- Register Your EMS Mobile App with idP
  - Customize Your Configuration
  - Create a Configuration File
- Test Your Open ID Connect Configuration
- Test Your Open ID Connect Authentication

OpenID authentication configuration requires two inputs:

1. User Info Endpoint. The EMS Platform Services will send the access_token to this endpoint to retrieve information about the end user.
2. Specify whether the EMS Platform Services should make a GET or POST request to the userinfo endpoint.

REGISTER YOUR EMS MOBILE APP WITH IDP

This is your responsibility. The client_id generated by this registration is required.

CUSTOMIZE YOUR CONFIGURATION

Follow the steps below to customize your Open ID Connect configuration.

CREATE A CONFIGURATION FILE

1. Refer to Customize Your Mobile App Configuration Using config.json (Private Deployment Only) for details on building a configuration file for EMS Mobile App.
2. Once you have created your configuration file, you may proceed with one of the sections below, depending on whether you intend to host the file or pre-configure the application and redistribute it.

USE HOSTED CONFIGURATION

Host your configuration file from a web server an distribute the URL to your end users via the Import SSO Config feature in EMS Mobile App. Users should only have to perform this import one time per installation of the application.

> **WARNING:** It is not recommended to make this configuration file available publicly, since it will likely have URLs and/or other information in it that you do not want made available. Instead, host the file such that it is only available internally to your organization.

PRE-CONFIGURE EMS MOBILE APP

If you wish to pre-configure the mobile app, see Configure and Re-Sign the EMS Mobile App (Private Deployment Only).

TEST YOUR OPEN ID CONNECT CONFIGURATION

Assuming you have installed the EMS Platform Services API at https://ems.yourcompany.com/endpoint, then you can test the configuration with a simple curl command:

```
curl -X GET -H 'x-ems-consumer: MobileApp' https://ems.yourcompany.com/endpoint/api/v1/health
```

TIP: You can also use the API's Swagger interface to accomplish this goal.

You should see a portion of the JSON response that looks like this (unrelated details omitted for brevity):

```
{
  ...
  "additionalProperties": {
    "authConfig": {
      "activities": "openId"  // <-- these are the critical lines
      "ui":"openId"
    }
  }
}
```

TEST YOUR OPEN ID CONNECT AUTHENTICATION

Assuming you have installed the EMS Platform Services API at https://ems.*yourcompany*.com/endpoint, you can test the authentication with a curl command:

```
curl -X POST -H 'x-ems-consumer: MobileApp' -H 'Content-Type: application/json' -d '{"token":"your_access_token"}' https://ems.yourcompany.com/endpoint...authentication
```

...where your_*access_token* is a valid *access_token* retrieved from your IdP.

> **NOTE: api/v1/authentication** is the endpoint within the API where your request must be sent.

CHAPTER 6: Open ID Connect Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App

Hosted Configuration: The configuration can be hosted at a URL available to end users. The user will then enter that URL into the application. EMS Mobile App will download and use that information, and kick off the authentication process. When configured this way, users will launch the EMS Mobile App and see the EMS Server URL screen. Instead of entering an EMS Server URL, the user will tap **About** near the bottom right of the screen and select the option to **Import SSO Configuration**. The user will then tap **Import** Mobile app, which will direct the user to enter the Configuration URL. Then the user will tap **Import**.

Pre-Configured In EMS Mobile App: The configuration can be "baked" into the application. This requires Configure and Re-Sign the EMS Mobile App (Private Deployment Only), hosting, and re-distributing the EMS Mobile App within your organization. With a pre-configured EMS Mobile App, users do not need to import any Open ID configuration details.EMS Mobile App will launch with that configuration and use it directly.

HOW USERS AUTHENTICATE AFTER CONFIGURATION

Assuming successful import of the configuration data, the authentication flow can now begin. EMS Web App will show the user the Open ID authorization web page (this happens in a web view inside the EMS Mobile App, and the user may briefly see a busy indicator while the page loads). The user will authenticate with the Open ID authorization view. The user plays no part in these next steps, which describe the completion of the Open ID flow. The user may simply see the screen change during this process. Successful authentication will redirect the user back to EMS Web App. EMS Web App will resume the Open ID authentication process and retrieve and access_token from the identity provider and will then forward the access_token to the EMS Platform Services API. EMS Platform Services API will verify the access_token by making a userinfo request per the Open ID specification. EMS Platform Services API will authenticate the user by matching the login email field (if provided) to an Everyday User in the EMS database. If there is no email field in the response, the API will try to match the response's sub field to an Everyday User. EMS Platform Services API will respond to EMS Mobile App. Once Open ID workflow above has successfully completed, EMS Web App will direct the user to the Home screen. If the EMS Platform Services API is unable to verify the credentials, EMS Mobile App will inform the user based on that response.

HOW THE IDENTITY PROVIDER (IDP) WORKS

The Identity Provider (IdP) handles the input and verification of end user credentials. It also issues and verifies tokens. The EMS Mobile App must be registered with the IdP. The client_id generated by this registration is required information for the configuration used by the EMS Mobile App and the Open ID flow.

HOW THE EMS PLATFORM SERVICES API WORKS

The EMS Platform Services API receives the access_token from the EMS Mobile App. The token is then sent to the userinfo endpoint for verification. The response from the userinfo endpoint is used to find a user in the EMS database. The API will then respond to the EMS Mobile App based on the results of this process.

CHAPTER 7: Persistent Authentication

Persistent Authentication refers to the ability of the EMS Mobile App to automatically log users in so that they are not required to log into EMS Mobile App every time they need to access it. When using persistent authentication, a user's EMS Mobile App credentials will become invalid after a period of inactivity equal to or greater than the duration defined in settings. If not using persistent authentication, a user will be forced to re-authenticate after the duration defined in settings has elapsed, regardless of activity.

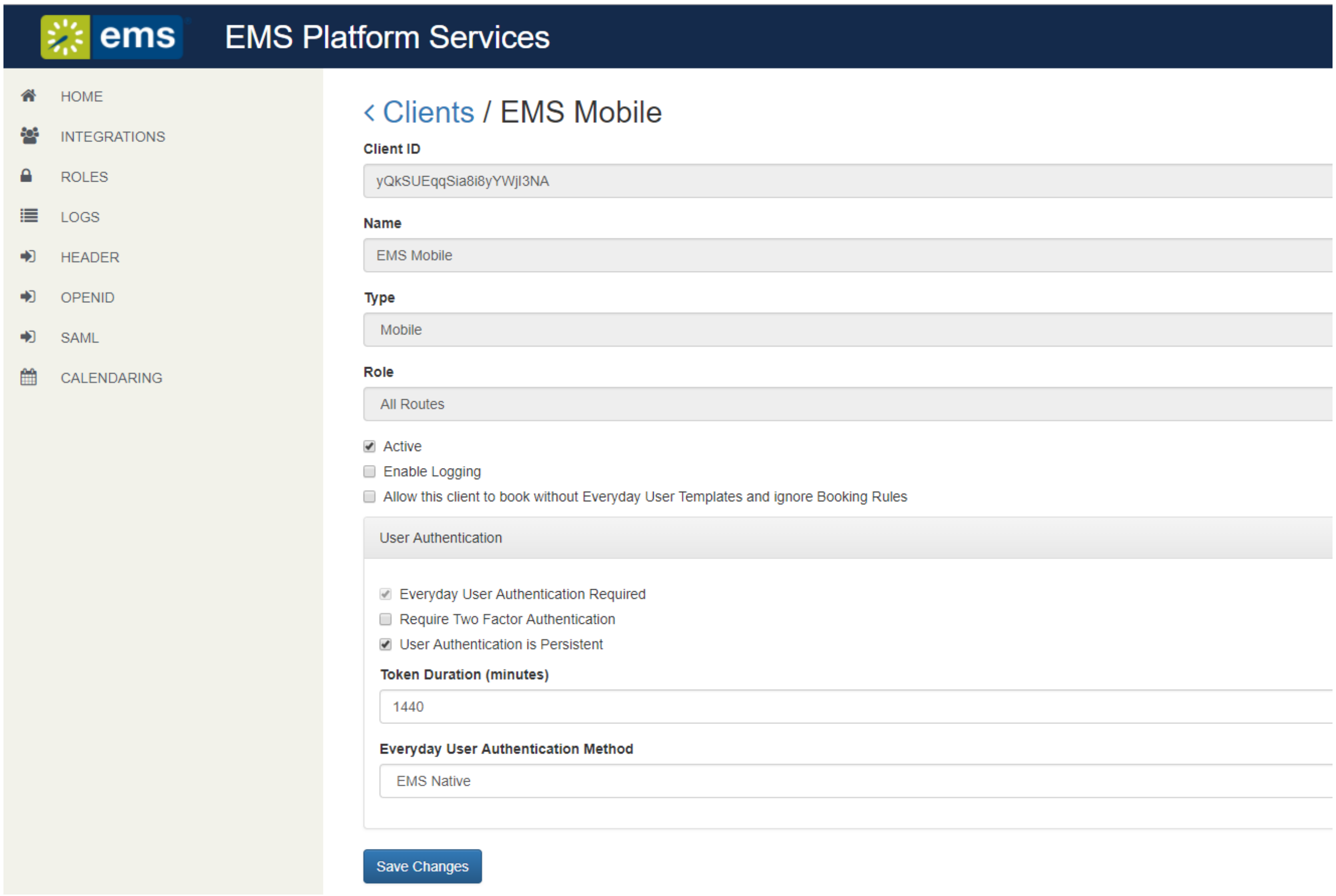
> **TIP:** Users with persistent authentication will be prompted to log back in to EMS Mobile App if anything is changed about their profile in EMS Desktop Client on the Everyday Users tab, such as Email, Password, External Reference, Network ID, and Security Template. If your remove a user's access to a process template, they will also be alerted when they attempt to use it, and then they will be prompted to re-authenticate.

1. Navigate to the EMS Platform Services Admin Page.
2. Click the Integrations tab.

3. Click on EMS Mobile.

4. Select the **User Authentication Is Persistent** checkbox.

5. Set the token duration in minutes.



Client ID

yQkSUEqqSia8i8yYWjI3NA

Name

EMS Mobile

Type

Mobile

Role

All Routes

☑ Active

☐ Enable Logging

☐ Allow this client to book without Everyday User Templates and ignore Booking Rules

User Authentication

☑ Everyday User Authentication Required

☐ Require Two Factor Authentication

☑ User Authentication is Persistent

Token Duration (minutes)

1440

Everyday User Authentication Method

EMS Native

6. Click **Save**.

NOTE: This setting overrides the token duration sent by SSO providers. If a user should leave your organization, you should manually disable his or her profile in EMS, otherwise the employee will have access to EMS Mobile App for the duration defined above. You can also use HR Toolkit to streamline this process.

CHAPTER 8: SAML Authentication

This section guides you authenticating your users with a SAML provider. Authentication with SAML requires configuration prior to beginning the authentication flow.

This topic will give you information on the following:

- Prerequisites for SAML Authentication
- Supported Identity Providers
- Update SAML Configuration
- Configure SAML Authentication for the EMS Mobile App and EMS Web App
- Identify Your Provider in Configuration
- How EMS Platform Services Supports SAML
- Using Hosted Configuration (Public Deployment)
- Pre-Configure EMS Mobile App (Private Deployment)

PREREQUISITES

EMS Platform Services is required for SAML authentication.

EMS WEB APP

The minimum version of EMS Web App and EMS Platform Services for authentication through SAML 2.0 is Update 23.

NOTE: For EMS Web App, Administrators must enable SAML 2.0 authentication by changing the following parameter value to **Yes** in Desktop Client:

1. Navigate to **System Administration** > **Settings** > **Parameters** > **Everyday User Applications** tab > **Authentication** > **Use SAML 2.0 Authentication for User Authentication Web App Only**.
2. Select YES.

If set to **No**, EMS Web App will utilize SAML as configured through Portal Authentication methods.

EMS MOBILE APP

The minimum version of EMS Platform Services for SAML authentication in the EMS Mobile App is Update 9. There are breaking changes in Update 23 and customers will be required to update SAML configuration settings.

SUPPORTED IDENTITY PROVIDERS

- ADFS
- G Suite
- Okta
- Auth0
- Azure AD
- Shibboleth

> **NOTE**: Only Redirect HTTP Binding Type is currently supported.

UPDATE SAML CONFIGURATION

a. Delete existing identity and service provider keys. As of Update 23 (March 2018), SP and IdP certs are stored in the database instead of the file system of EMS Platform Services.

b. Generate encryption key.

c. Update SAML configuration based on these settings.

CONFIGURE SAML AUTHENTICATION FOR EMS MOBILE APP AND EMS WEB APP

PREREQUISITE

Update the Encryption key in default.Json file.

> **NOTE:** The Encryption Key is used for encrypting and decrypting the Service Provider private key when stored in the database via the AuthKey API.

New Customers: The encryption key is already provided in the default.json file.

Existing Customers: The encryption key needs to be generated and added to the default.json file before using the AuthKey API. Run the following command in a terminal, openssl rand -base64 32, to generate a 256-bit key that is Base64 encoded. The encryption key must be 256-bit and must be Base64 encoded. Restart EMS Platform Services after updating default.Json file.

1. Login to EMS Platform Services.
2. Navigate to the Integrations tab.
3. Select EMS Mobile / EMS Web Application.
4. Set Everyday user authentication method to SAML and save changes.

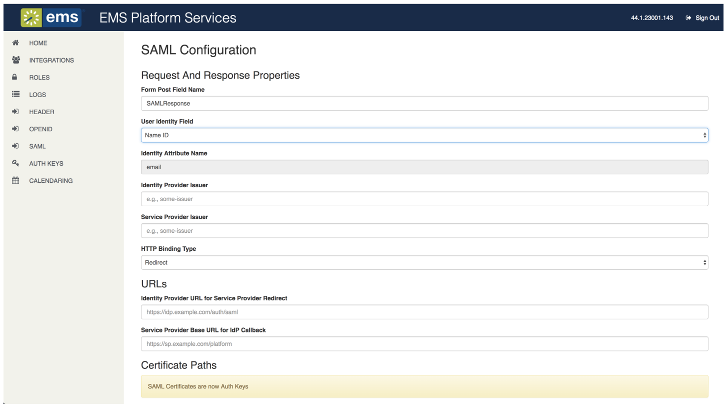
5. Select SAML from the left navigation bar.
6. Configure SAML authentication settings.

> **NOTE:** SAML settings are global and will apply to all integrations utilizing SAML authentication.

IDENTIFY YOUR PROVIDER IN CONFIGURATION

You are responsible for the configuration of your chosen IdP, with information relevant to the EMS Platform Services acting as a Service Provider for SAML Authentication. The following EMS Platform Services related settings may be needed in order to configure your IdP.

The following fields are required to complete SAML authentication configuration:



SAML Configuration

Request And Response Properties

Form Post Field Name
SAMLResponse

User Identity Field
Name ID

Identity Attribute Name
email

Identity Provider Issuer
e.g., some-issuer

Service Provider Issuer
e.g., some-issuer

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
https://sp.example.com/platform

Certificate Paths

SAML Certificates are now Auth Keys

FIELD	DESCRIPTION
REQUEST AND RESPONSE PROPERTIES	
Form Post Field Name	(Optional, default is SamlResponse). Attribute in which assertions are sent, within encoded <samlp:Response> document.
User Identity Field	**REQUIRED**. Dropdown with choice of assertion element containing user identity (Name ID or Attribute). If set to Attribute, then you must set the Identity Attribute Name to the expected assertion attribute name to use for user identity.
Identity Attribute Name	Assertion attribute name containing user identity. Attribute names can be identity provider-specific (i.e., 'uid', 'mail'). This field is ignored when User Identity Field is set to Name ID.
Identity Provider Issuer	**REQUIRED**. Used to verify expected issuer of assertions, including in SAMLResponse as <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion" >http://adfs.mycompany.net/adfs/services/trust</Issuer>.
Service Provider Issuer	**REQUIRED**. Included by EMS Platform Services in AuthnRequest requests sent to Identify Provider. This is included in the SAMLRequest as <saml:Issuer>https://mycompany.com/EmsPlatform</saml:Issuer> EMS Platform Services will autogenerate the values for the Service Provider Issuer and the Service Provider Base URL for IdP Callback.
HTTP Binding Type	Specifies which SAML binding (HTTP Post or HTTP Redirect) EMS Platform Services will use to transmit SAML protocol messages. **Currently only Redirect is supported.**

FIELD	DESCRIPTION
URLS	
Identity Provider URL for Service Provider Redirect	**REQUIRED**. This URL, (e.g., https://idp.example.org/SAML2/SSO/Redirect), includes the authentication request details provided by EMS Platform Services and contains opaque data that it includes in the request. This enables the Identify Provider to include it as Relay State on the SAMLResponse. **NOTE**: If you have the identity provider metadata.xml file, you can upload it through the EMS Platform Services endpoint https://company.platform/api/v1/authentication/saml/metadata/idp. The identity provider certificate will be uploaded for you and Identity Provider Issuer. The Identity Provider URL for Service Provider Redirect fields will be populated for you.
Service Provider Base URL for IdP Callback	**REQUIRED**. Set this URL to the base URL of the EMS Platform Services installation (i.e., https://mycompany.com/EmsPlatform). EMS Platform Services will autogenerate the values for the Service Provider Issuer and the Service Provider Base URL for IdP Callback.
CERTIFICATE PATHS	
IMPORTANT: SAML Certificates are now Auth Keys. These fields are not editable.	
Path to Identity Provider Public Certificate	**REQUIRED**. Uploaded through Auth Keys.
Path to Service Provider Public Certificate	Optional. Uploaded through Auth Keys.

FIELD	DESCRIPTION
Path to Service Provider Private Certificate	Optional. Uploaded through Auth Keys.

HOW EMS PLATFORM SERVICES SUPPORTS SAML

No Two-Factor Authentication (2fa) support is provided with SAML authentication. 2fa is the responsibility of the Identity Provider (3rd-Party or Customer owned) and not the EMS Platform Services. Token expiration is configured and managed the same for SAML as for other authorization types, thus overriding any SAML Assertion Conditions that specify the assertion expiration timestamp.

> **NOTE:** See Also: Persistent Authentication for token expiration configuration details. Refer to Customize Your Mobile App Configuration Using config.json (Private Deployment Only) for details on building a configuration file for EMS Mobile App.

Once you have created your configuration file, you may proceed with one of the sections below, depending on whether you intend to host the file or pre-configure the application and redistribute it.

USING HOSTED CONFIGURATION (PUBLIC DEPLOYMENT)

Host your configuration file from an applicable web server. Distribute the URL to your end users.

> **WARNING:** It is not recommended to make this configuration file publicly available, since it will likely have URLs and/or other information in it that you do not want made available. Instead, host the file in a way such that it is only available internally to your organization. Users should only have to perform this import one time per installation of the application.

PRE-CONFIGURE EMS MOBILE APP (PRIVATE DEPLOYMENT)

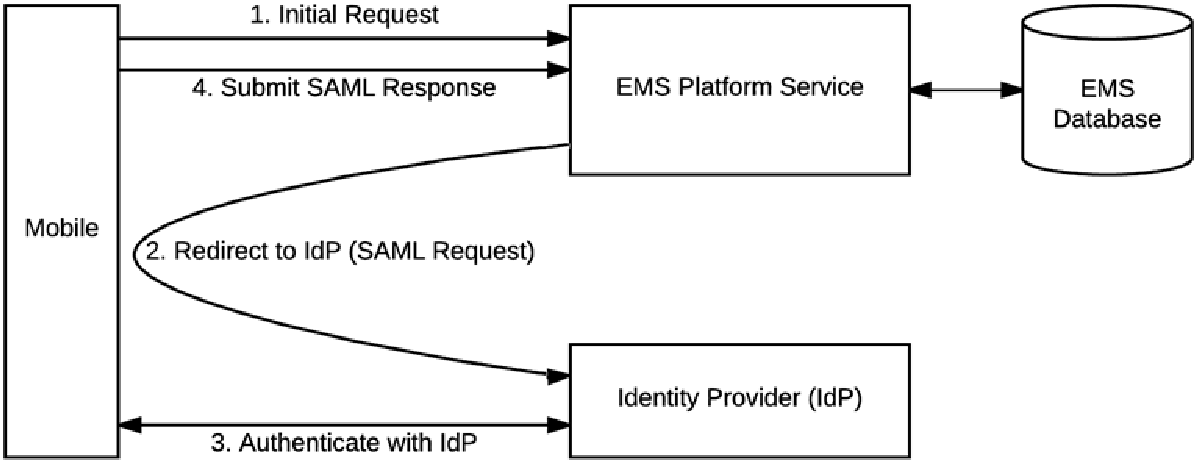
If you wish to pre-configure EMS Mobile App, see Configure and Re-Sign the EMS Mobile App (Private Deployment Only).

CHAPTER 9: SAML Authentication Can Be Hosted or Pre-Configured in the EMS Mobile App

Hosted Configuration: The configuration can be hosted at a URL available to end users. The user will then enter that URL into the application. EMS Mobile App will download and use that information, and kick off the authentication process. When configured this way, users will launch the EMS Mobile App and see the EMS Server URL screen. Instead of entering an EMS Server URL, the user will tap **About** near the bottom right of the screen and select the option to **Import SSO Configuration**. The user will then tap **Import** Mobile app, which will direct the user to enter the **Configuration URL**. Then the user will tap **Import**.

Pre-Configured In EMS Mobile App: The configuration can be "baked" into the application. This requires Configure and Re-Sign the EMS Mobile App (Private Deployment Only), hosting, and re-distributing the EMS Mobile App within your organization. With a pre-configured EMS Mobile App users do not need to import any SAML configuration details. EMS Mobile App will launch with that configuration and use it directly.

HOW USERS AUTHENTICATE AFTER CONFIGURATION



EMS Mobile App makes a request to the configured or default SAML URL

- If the request redirects the user to the SAML authentication web page, then the web user will see the page in a web view inside EMS Mobile App.
- User may briefly see a busy indicator while the page loads.

Users will authenticate using the SAML authorization view. They do not participate in the following steps (which explain the completion of the SAML flow). They may, however, see the screen change during this process. Successful authentication will send an HTML response back to EMS Mobile App, which will silently POST the SAML form and response to the EMS Platform Services API. EMS Platform Services API will then parse the SAML response and find the corresponding user in the EMS database; then it will respond to EMS Mobile App, which will will direct the user to the Home screen. If the EMS Platform Services API is unable to verify the credentials, EMS Mobile App will present an error message informing the user.

HOW THE IDENTITY PROVIDER (IDP) WORKS

The Identity Provider (IdP) handles the input and verification of end user credentials. It also issues and verifies tokens. The EMS Mobile App must be registered with the IdP. The client_id generated by this registration is required information for the configuration used by the EMS Mobile App and the SAML flow.

HOW THE EMS PLATFORM SERVICES API WORKS

The EMS Platform Services API receives the access_token from the EMS Mobile App. The token is then sent to the userinfo endpoint for verification. The response from the userinfoendpoint is used to find a user in the EMS database. The API will then respond to the EMS Mobile App based on the results of this process.

CHAPTER 10: NTLM Windows Authentication

Follow the steps in this section to authenticate your users with Windows Authentication via Microsoft's NTLM challenge-response protocol.

> **TIP:** Windows Authentication requires that you install and use the optional EMS Platform Services API.

USER LOGIN SCENARIO

Once you have established a connection to the EMS Platform Services API, the user log-in process is as follows:

- Users will enter domain credentials to log into their EMS product.
- EMS will send credentials to the EMS Platform Services API.
- IIS will intercept the call and issue a challenge.
  - The EMS access point (e.g., EMS Mobile App, EMS Web App, etc.) will then perform all steps necessary to complete process with the user's provided credentials.

- EMS Platform Services API receives the initial request and extract the authenticated user from the IIS context.
- EMS Platform Services API will verify the authenticated user against the EMS database.
- User will be taken to the **Home** screen.

If the credentials are missing when the user taps **Sign In**, an error message will appear indicating that fields are required. If the EMS Platform Services API is unable to verify the authenticated user, or if IIS rejects the request due to failed authentication, EMS will inform the user.

TEST YOUR WINDOWS AUTHENTICATION

Assuming you have installed the EMS Platform Services API at https://yourcompany.com/ems-platform-api, you can test the authentication with a curl command:

```
curl -X POST -H "x-ems-consumer: MobileApp" -H "Content-Type: application/json" --ntlm  -u your_username:your_password -vvvv -d '{}'
"https://ems.yourcompany.com/endpoint...authentication"
```

...where your_*username* and your_*password* are your credentials.

NOTE: api/v1/authentication is the endpoint within the API where your request must be sent.

CHAPTER 11: Add Mobile Users

EMS Mobile App users are added as "Everyday Users" in EMS Desktop Client. Follow the steps below to create this type of user.

This section guides you in configuring one Everyday User at a time. Once you have configured these users, you may need to assign them to security templates and one or more process templates.

- To assign users to Everyday User process templates, see also: Assign Templates to Everyday Users.
- To assign multiple templates to multiple users in a single step, see also: Assign Security Templates to Multiple Everyday Users.

TIP: You configure EMS Desktop Client user accounts in a different area (under the **System Administration** > **Security** menu). For instructions, see Configure EMS Desktop Client Users.

Additionally, if your organization uses EMS Human Resources Toolkit to manage Everyday User accounts, see also: EMS Human Resources Toolkit.

Lastly, a set of Account Management parameters control account management behavior. To view these parameters, see also: EMS Web App Parameters.

Concept: EMS classifies users into two categories–Guests or Visitors and Everyday Users.

"Guests" or "Visitors" (unauthenticated or anonymous users) can browse events, see details about your organization’s space, and/or submit requests.

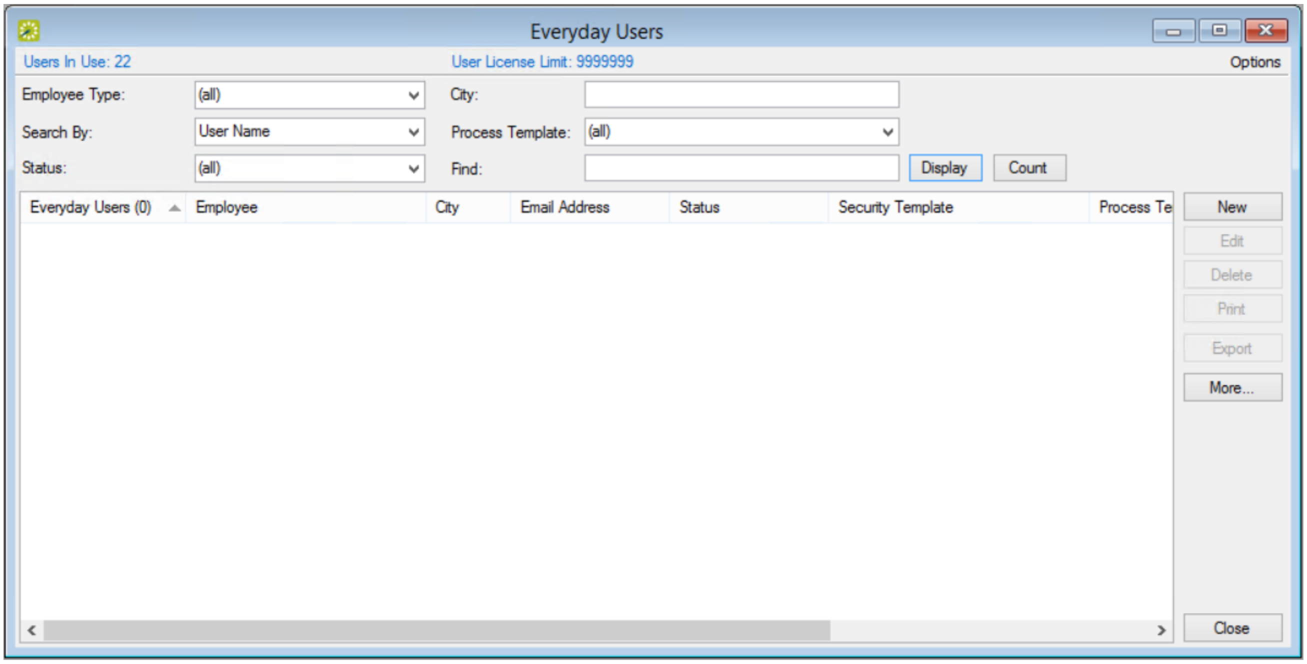
These users can register themselves through the EMS Web App and create a user account. To enable this, you need to set certain account management parameters (see also: EMS Web App System Parameters) and select the Credit\Edit an Account role for the unauthenticated user (see the Roles tab definition in Configuring a Security Template).

"Guests" or "Visitors" (authenticated users) may also submit and manage reservations if you enable them. You can configure these users through the EMS Desktop Client or the optional Integrated Authentication module.

See Also: Configure Additional Information for a Group and Configure Contacts. Before you configure a user, check that the user has not already been created.

Everyday User process templates control access and behavior in EMS Software's Everyday User Applications. If you are upgrading from an older release of EMS, you may recognize Everyday Users as "Web Users" and "Everyday User Process Templates" as "Web Process Templates."

1. On the EMS Desktop Client menu bar, click **Configuration** > **Everyday User Applications** > **Everyday Users**. The Everyday Users window opens. The number of configured users for EMS Web App shows in the upper left corner. The number of users for which your organization is licensed shows in the top center.



Everyday Users

Users In Use: 22

User License Limit: 9999999

Employee Type: (all)

Search By: User Name

Status: (all)

City:

Process Template: (all)

Find:

2. Check that the user you wish to configure does not already exist.

   a. Enter the user name or email address in the **Find** field.

> **TIP:** This search string is not case-sensitive, but your entries must be in the correct order. For example, if searching by Email Address, a search string
>
> of bob returns bobworth@emssoftware.com but
>
> not dbobbett@emssoftware.com.

b. Narrow your search results by:

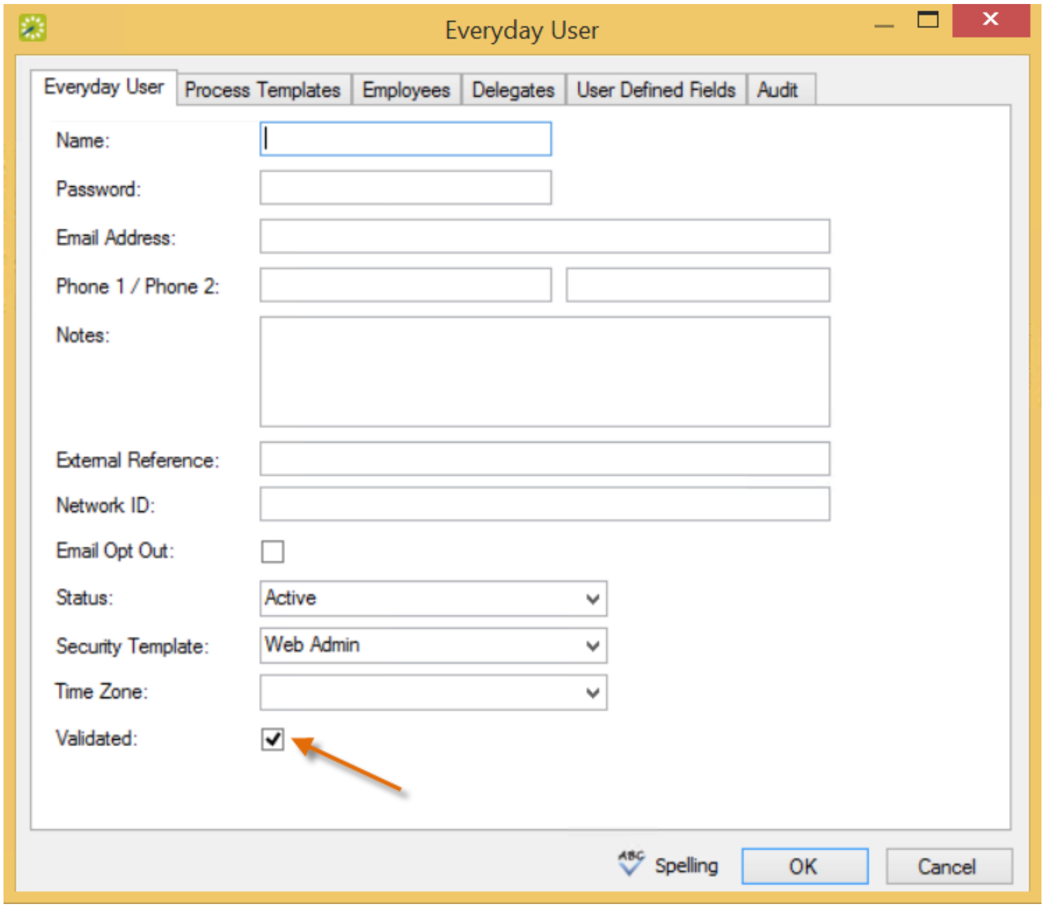
- Group Type
- City
- Status
- Process Template

c. Click **Display**. Search results show in the lower pane of the window. If your user does not already exist in EMS, proceed to the next step.

> **NOTE:** If the EMS system parameter **Users linked to Groups via External Reference** is set to **Yes**, then you will also see a Group column and a City column.

3. Create a new user. Click the **New** button. A dialog box opens.

> **NOTE:** If the user has confirmed membership (by responding to an email containing an activation link), the **Validated** checkbox highlighted below will be selected. If the user had to answer questions when requesting an account, you can view the user's responses on the **User Defined Fields** tab.



Name:

Password:

Email Address:

Phone 1 / Phone 2:

Notes:

External Reference:

Network ID:

Email Opt Out: □

Status: Active

Security Template: Web Admin

Time Zone:

Validated: ☑

TIP: When you configure a user, you can also specify one or more delegates for the user from the Delegates tab. A delegate is a user who can create and view reservations on behalf of another user.

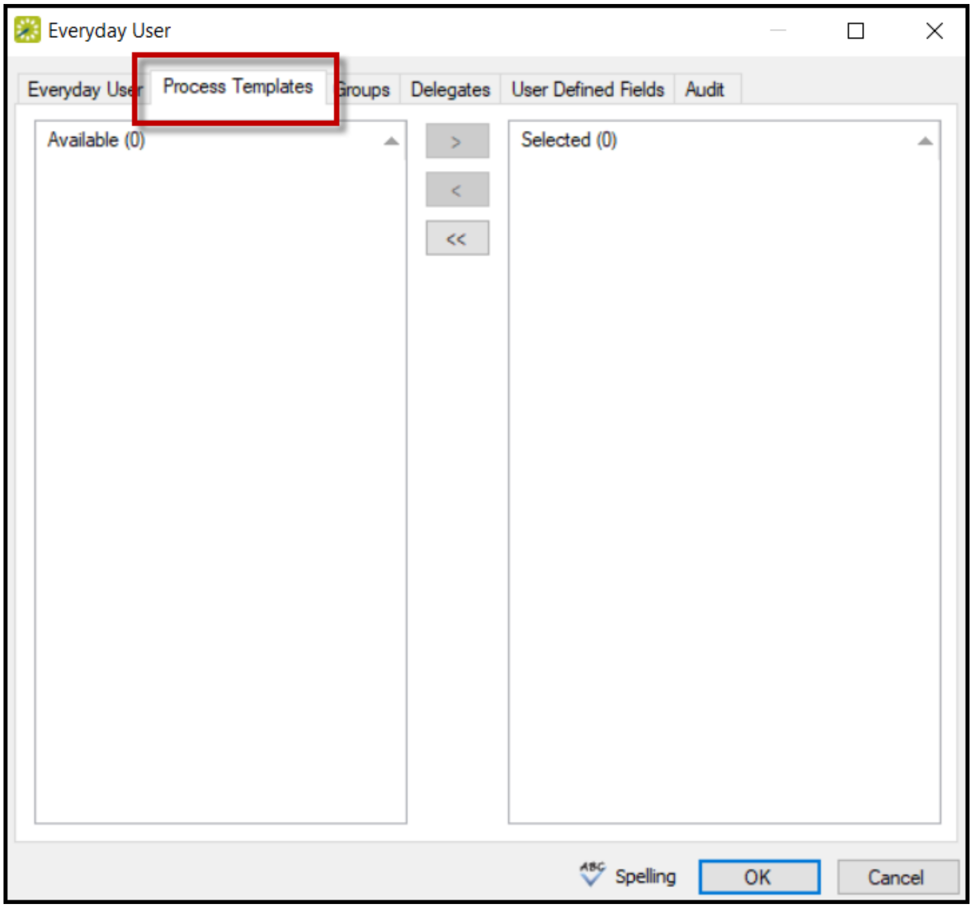
4. Enter information for the new user. User name and email address are required; password is only required if not using the optional Integrated Authentication module. All other information is optional and can be added later as needed.

FIELD	DESCRIPTION
Name	REQUIRED. The name of the user. (Maximum of 30 characters, including spaces.)
Password	The password that the user must enter to log in to the EMS Web App. If using the optional Integrated Authentication module, Password can be left blank since the network password is used instead.
Email Address	REQUIRED. Enter the full email address for the user. Users must enter this email address to log in to the EMS Web App.
Phone 1 /Phone 2	OPTIONAL
Notes	OPTIONAL. Read-only.
External Reference	OPTIONAL. Links the user to an outside program, such as EMS Human Resources Toolkit, if needed.
Network ID	The user’s network ID.
Email Opt Out	OPTIONAL. Select this option if you do not want the user to receive automatic emails (such as reservation summary emails) from the EMS Web App. The user can still receive manually sent emails.

FIELD	DESCRIPTION
Status	REQUIRED. Select the status for the user: » **Active**–The user can log in to EMS Web App, EMS Mobile App, and EMS for Outlook. » **Pending**–The user cannot log in to EMS Web App, EMS Mobile App, and EMS for Outlook and is informed that he/she must check back at a later time. » **Inactive**–The user cannot log in to EMS Web App, EMS Mobile App, and EMS for Outlook and is instructed to contact the EMS administrator.
Security Template	REQUIRED. This determines the user's access to the system (i.e., the menu items the user can see and the event information that the user can view).
Time Zone	OPTIONAL. The time zone in which the user is located. **NOTE**: As of Version 44.1, EMS Software strongly recommends that time zones are assigned to users for an optimal experience on all Everyday User Applications.
Validated	When checked, users who created their own accounts have confirmed membership (by responding to an email containing an activation link). When unchecked, the user will not be able to use the EMS Web App.

5. Open the **Process Templates** tab to assign process templates to the new user. Select one or more Process Templates listed in the Available column (use CTRL-click for multiple groups), and then click **Move** (**>**) to move the selected groups to

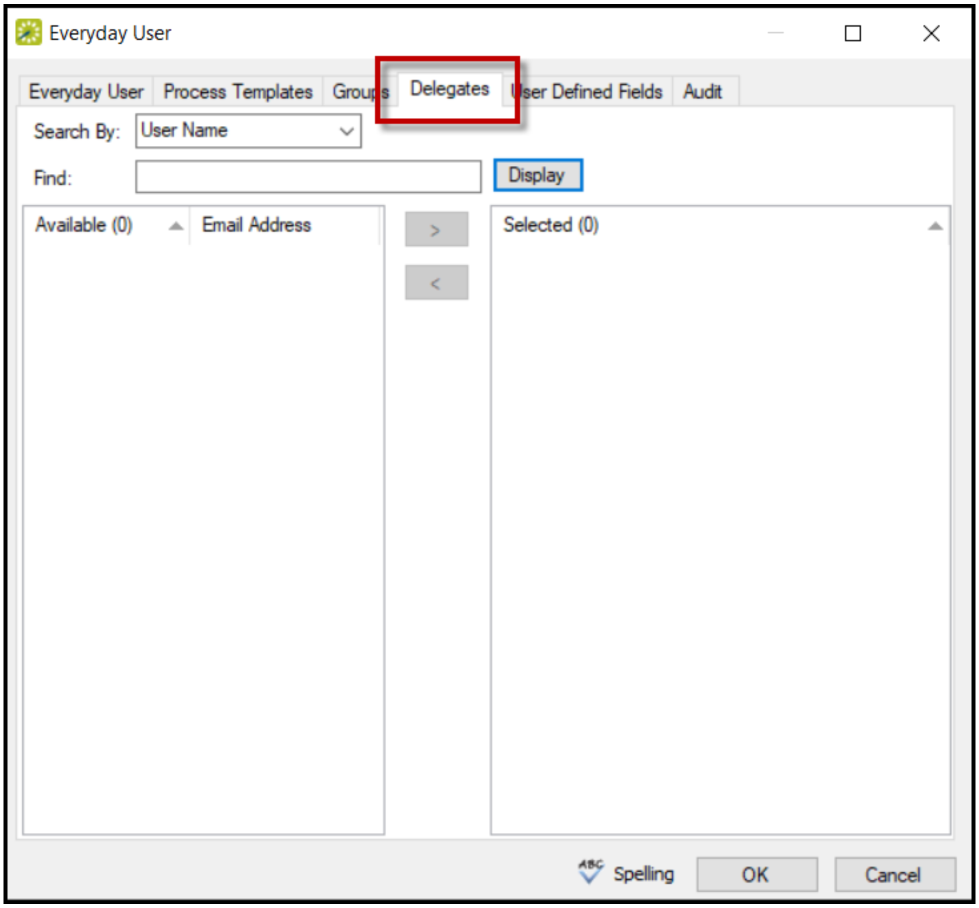
the **Selected** list. The process templates you assign here will appear as menu items to the user in the EMS Web App, EMS Mobile App, and EMS for Outlook.



6. From the **Groups** tab, specify Groups on whose behalf the user can create and manage reservations. To filter the list of active groups displayed, use the **Find** and **Type** fields and then click **Display**. Select one or more Groups (use CTRL-click for multiple groups), and then click **Move** (**>**) to move the selected

groups to the **Selected** list.

7. Specify Delegates the user can impersonate from the **Delegates** tab. To see all available users, click **Display**. To narrow the search results, use the **Search** by dropdown list to search by User Name or Email Address. Select one or more delegates (using CTRL-click for multiple delegates), and then click **Move** (**>**) to move the selected users to the **Selected** list.



TIP: Click the **Spelling** icon to spell-check any information that you manually entered for the user.

8. Click **OK**. The dialog box closes and returns you to the users window with the newly configured user automatically selected.

CHAPTER 12: Deploy EMS Mobile App

There are two ways to deploy the EMS Mobile App for your users:

1. Public Deployment–The standard public app store offered by Apple and Google.
2. Private Deployment–A private enterprise app store. (This approach can also be integrated with your company's Mobile Device Management system.)

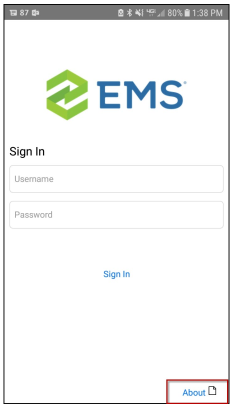
WARNING: It is important to understand the compatibility between the EMS Mobile App and EMS Platform Services. The EMS Mobile App needs to be on the same version or higher as EMS Platform Services. For example, the EMS Mobile App Update 20 version will be compatible with EMS Platform Services Update 19 or older. However, compatibility issues will exist if you try to install EMS Platform Services Update 20 with an older version of the EMS Mobile App (Update 19 or older).

PUBLIC DEPLOYMENT: PUBLIC APP STORE

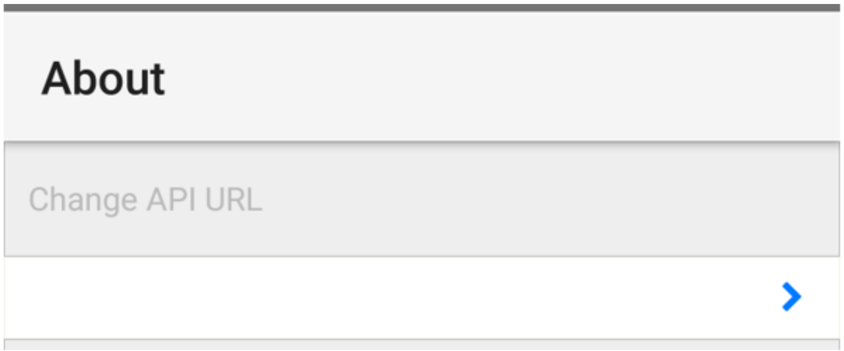
To deploy via the public app store, direct users to the Google Play and Apple app stores on their mobile devices. They will be able to download the EMS Mobile App by clicking on the link. However, they will have to manually input the EMS Mobile API URL. They will receive a prompt to do so the first time they open the EMS Mobile App.

If users need to change the API URL at a later date, they can:

1. Open the EMS Mobile App, and then click **About** in the lower right corner.



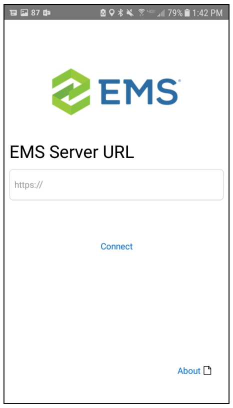
2. Click to change the API URL.



About

Change API URL

3. Enter the API URL you provide and connect.



EMS Server URL

https://

IMPORTANT: While Public Deployment may be easier for your IT staff, please consider the following:

- Users will have to input the EMS Mobile App API URL on their own.
- EMS will frequently deploy EMS Mobile App updates to the app store. Most users will have this app set to automatically update and will receive updates even if you have not yet upgraded your EMS Mobile API.
- While EMS Software aims to make the Mobile API backwards- and forwards-compatible within major updates, we may not do so all the time.
- Deploying via the public app store requires you to make major updates to the EMS Mobile API as soon as they are available.

PRIVATE DEPLOYMENT: PRIVATE APP STORE

To deploy via a private enterprise app store, first download the unsigned apk/ipa files from your EMS Customer Portal. You then have to resign the app and deploy it via your MDM system. This site offers some guidance on how to sign an unsigned ipa file (i.e. for iOS), while this site does the same for Android apk files. Deploying via a private app store allows you to control which version of the EMS Mobile App your users have.

As an example, here are the key steps to resign and deploy the unsigned EMS Mobile App ipa file (following instructions provided here):

1. Download unsigned builds: .ipa and .apk files
   - Optional: Customize Your Mobile App Configuration Using config.json (Private Deployment Only)
2. Configure and Re-Sign the EMS Mobile App (Private Deployment Only)
   - Change the EMS Mobile App Logo (Private Deployment Only) (if using MDM)

CHAPTER 13: Change EMS Mobile App Logo (Private Deployment Only)

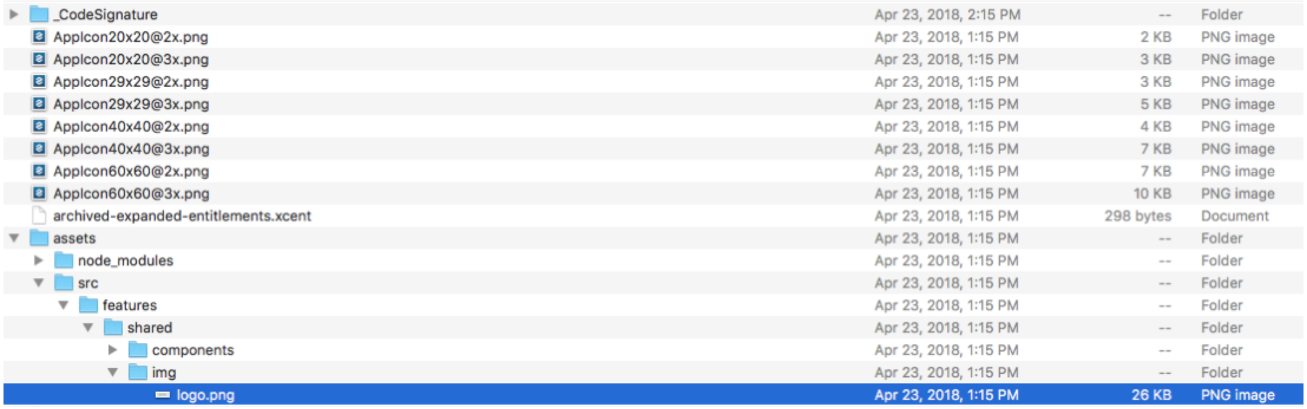
For customers re-signing the application, we provide unsigned builds.

This topic provides information on:

- Changing the EMS Mobile App Logo in iOS
- Changing the EMS Mobile App Logo in Android

CHANGING EMS MOBILE APP LOGO (IOS)

1. Store your unsigned EMS Mobile App in a new or empty directory.
2. Change the extension of the app to .zip. (e.g., IPhone.App-44.1.xxx-unsigned.ipa -> IPhone.App-44.1.xxx-unsigned.zip.)
3. Un-compress/expand the new zip file.
4. To set a custom logo, navigate to **Assets** > **SRC** > **Features** > **Shared** > **IMG.**



▶ _CodeSignature	Apr 23, 2018, 2:15 PM	--	Folder
AppIcon20x20@2x.png	Apr 23, 2018, 1:15 PM	2 KB	PNG image
AppIcon20x20@3x.png	Apr 23, 2018, 1:15 PM	3 KB	PNG image
AppIcon29x29@2x.png	Apr 23, 2018, 1:15 PM	3 KB	PNG image
AppIcon29x29@3x.png	Apr 23, 2018, 1:15 PM	5 KB	PNG image
AppIcon40x40@2x.png	Apr 23, 2018, 1:15 PM	4 KB	PNG image
AppIcon40x40@3x.png	Apr 23, 2018, 1:15 PM	7 KB	PNG image
AppIcon60x60@2x.png	Apr 23, 2018, 1:15 PM	7 KB	PNG image
AppIcon60x60@3x.png	Apr 23, 2018, 1:15 PM	10 KB	PNG image
archived-expanded-entitlements.xcent	Apr 23, 2018, 1:15 PM	298 bytes	Document
▼ assets	Apr 23, 2018, 1:15 PM	--	Folder
▶ node_modules	Apr 23, 2018, 1:15 PM	--	Folder
▼ src	Apr 23, 2018, 1:15 PM	--	Folder
▼ features	Apr 23, 2018, 1:15 PM	--	Folder
▼ shared	Apr 23, 2018, 1:15 PM	--	Folder
▶ components	Apr 23, 2018, 1:15 PM	--	Folder
▼ img	Apr 23, 2018, 1:15 PM	--	Folder
logo.png	Apr 23, 2018, 1:15 PM	26 KB	PNG image

5. Replace the **logo.png** file.

6. Rezip all of the extracted files above.

7. Give the new zip file an ipa extension.

8. Using a Mac computer, install fastlane.

   » sudo gem install fastlane

9. Do the rest of this on your local directory.

10. Login to https://developer.apple.com and switch to team "Your Team Name."

11. Download your teams Distribution provisioning profile.

12. Double click it to install it. This file should exist on your system:

    » ~/Library/MobileDevice/Provisioning Profiles/<a guide for your provisioning profile>.mobileprovision

13. Get your team's existing .p12 file with the cert and private key combined, and then import that into Keychain (by double-clicking it) and then entering the password.

- When the cert is installed successfully you should see iPhone Distribution: <Your Team Name> in your Keychain, with a private key.

14. Assuming you have:
    - fastlane installed on your Mac.
    - the cert & private key installed in Keychain
    - the provisioning profile mentioned above in: ~/Library....mobileprovision

15. Resign your target ipa with this command:

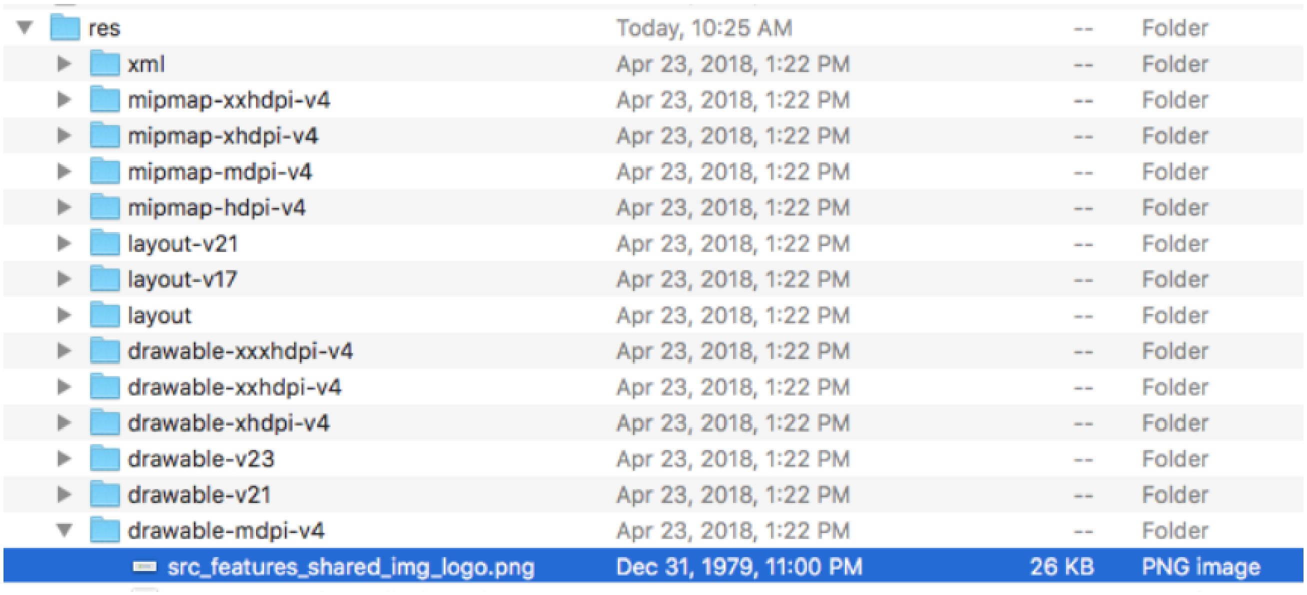
```
fastlane run resign \

ipa:path/to/your/file.ipa \

signing_identity:"iPhone Distribution: <Your Team Name>" \

provisioning_profile:$HOME/Library/MobileDevice/

Provisioning Profiles/<your profile GUID>.mobileprovision \

display_name:EMS-Resigned
```

NOTE: If you want a bash scrip that will do this, copy this into a file (e.g., resign_enterprise.sh):

```
#!/bin/bash
IPA=relative/path/to/file.ipa
IDENTITY="iPhone Distribution: <Your Team Name>"
PROFILE=$HOME/Library/MobileDevice/Provisioning Profiles/
<your profile GUID>.mobileprovision
DISPLAY_NAME=EMS-Resigned
fastlane run resign ipa:"$IPA" signing_identity:
"$IDENTITY" provisioning_profile:"$PROFILE" display_name:
$DISPLAY_NAME
```

CHANGING EMS MOBILE APP LOGO (ANDROID)

1. Store your unsigned EMS Mobile App in a new or empty directory.
2. Change the extension of the app to .zip. (e.g., IPhone.App-44.1.xxx-unsigned.ipa -> IPhone.App-44.1.xxx-unsigned.zip.)
3. Un-compress/expand the new zip file.
4. To set a custom logo, navigate to RES > **Drawable-mdpi-v4**.



▼ res	Today, 10:25 AM	--	Folder
▶ xml	Apr 23, 2018, 1:22 PM	--	Folder
▶ mipmap-xxhdpi-v4	Apr 23, 2018, 1:22 PM	--	Folder
▶ mipmap-xhdpi-v4	Apr 23, 2018, 1:22 PM	--	Folder
▶ mipmap-mdpi-v4	Apr 23, 2018, 1:22 PM	--	Folder
▶ mipmap-hdpi-v4	Apr 23, 2018, 1:22 PM	--	Folder
▶ layout-v21	Apr 23, 2018, 1:22 PM	--	Folder
▶ layout-v17	Apr 23, 2018, 1:22 PM	--	Folder
▶ layout	Apr 23, 2018, 1:22 PM	--	Folder
▶ drawable-xxxhdpi-v4	Apr 23, 2018, 1:22 PM	--	Folder
▶ drawable-xxhdpi-v4	Apr 23, 2018, 1:22 PM	--	Folder
▶ drawable-xhdpi-v4	Apr 23, 2018, 1:22 PM	--	Folder
▶ drawable-v23	Apr 23, 2018, 1:22 PM	--	Folder
▶ drawable-v21	Apr 23, 2018, 1:22 PM	--	Folder
▼ drawable-mdpi-v4	Apr 23, 2018, 1:22 PM	--	Folder
src_features_shared_img_logo.png	Dec 31, 1979, 11:00 PM	26 KB	PNG image

5. Replace the **src_features_shared_img_logo.png** file.

6. Rezip all the extracted files above.

> **IMPORTANT**: Assets, Res, and AndroidManifest.xml are top-level files in an .apk. Please ensure you are zipping the correct files.

» This CLI command will zip all the files in the current directory into a new zip file in the parent directory:

```
zip -qr ../ems-custom-44.1.xxx.zip ./*
```

7. Give the new zip file an apk extension (e.g., myapp.zip -> myapp.apk).
8. Sign the new apk file.
9. The script below is what EMS uses to sign the EMS Mobile App. Please adjust for your needs:

```
#!/bin/bash
APK_TO_SIGN=$1
APK_OUTPUT=$2
EMS_APK_KEYSTORE_PATH=path/to/your/app.keystore

jarsigner -verbose \
-sigalg $EMS_APK_SIG_ALG \
-digestalg $EMS_APK_DIGEST_ALG \
-storepass $EMS_APK_KEYSTORE_PASS \
-keystore $EMS_APK_KEYSTORE_PATH \
$APK_TO_SIGN $EMS_APK_ALIAS_NAME

zipalign 4 $APK_TO_SIGN $APK_OUTPUT
```

NOTE: EMS recommends that you use an image with a 3:1 aspect ratio in order to ensure that the image will be properly rendered by the application.

CHAPTER 14: Configure and Re-Sign the EMS Mobile App (Private Deployment Only)

This topic provides information on the following:

USE UNSIGNED BUILDS

For customers re-signing the application, we provide unsigned builds.

1. Store your unsigned EMS Mobile App in a new or empty directory.
2. Change the extension of the app to .zip. (e.g., IPhone.App-44.1.xxx-unsigned.ipa -> IPhone.App-44.1.xxx-unsigned.zip.)
3. Un-compress/expand the new zip file.

SET CUSTOM CONFIGURATION

1. Refer to Customize Your Mobile App Configuration Using config.json (Private Deployment Only) for details on building a configuration file for the EMS Mobile App.
2. Replace the config.json file with your custom configuration (located as follows):

IOS

- config.json (top-level file)

ANDROID

- assets/config.json

RE-SIGN AND REPACKAGE FOR IOS

Follow the steps below to re-sign and repackage for iOS.

1. INSTALL FASTLANE

Using sudo gem, install fastlane on an administrative Mac computer.

2. INSTALL CERTIFICATE AND PROVISIONING PROFILE

If your Mac computer is already configured with these items, these steps may not be necessary.

PROVISIONING PROFILE

1. Login to https://developer.apple.com.
2. Download your Distribution provisioning profile.
3. Double click it to install it. This file should exist on your system:
   - ~/Library/MobileDevice/Provisioning Profiles/<profile-guid>.mobileprovision

CERTIFICATE

See Apple's documentation for installing and managing certificates and signing identities. When the certificate is installed successfully, you should see iPhone Distribution: Your Company, Inc in your Keychain, with a private key.

3. RE-SIGN

If you have the following, you should be ready to re-sign the EMS Mobile App:

- Fastlane installed on your Apple computer
- the cert and private key installed in Keychain
- the provisioning profile mentioned above in ~/Library/.../<profile-guid>.mobileprovision

Before proceeding, change the following in the command below:

- Replace path/to/your/file.ipa with the real path to the ipa file
- Replace iPhone Distribution: Your Company, Inc with the appropriate signing identity on your machine
- Replace <profile-guid> with the actual GUID or name of the provisioning profile you intend to use
- Replace **EMS-Resigned** with the display name you wish to use, or remove the parameter if you do not wish to rename the application

> **NOTE:** Running these commands will **overwrite** the ipa file you designate. Make a copy first if necessary.

```
fastlane run resign \
    ipa:path/to/your/file.ipa \
    signing_identity:"iPhone Distribution: Your Company, Inc" \
    provisioning_profile:$HOME/Library/MobileDevice/Provisioning
```

```
Profiles/<profile-guid>.mobileprovision \
    display_name:EMS-Resigned
```

(All on one line for copy/paste:)

```
fastlane run resign ipa:path/to/your/file.ipa signing_identity:"iPhone Distribution: Your Company, Inc" provisioning_profile:$HOME/Library/MobileDevice/Provisioning Profiles/<profile-guid>.mobileprovision display_name:EMS-Resigned
```

If you want a bash script that will do this, you can copy this into a file (e.g., resign_enterprise.sh):

```
#!/bin/bash

IPA=relative/path/to/file.ipa
IDENTITY="iPhone Distribution: Your Company, Inc"
PROFILE=$HOME/Library/MobileDevice/Provisioning\ Profiles/<profile-guid>.mobileprovision
DISPLAY_NAME=EMS-Resigned

fastlane run resign ipa:"$IPA" signing_identity:"$IDENTITY"
```

```
provisioning_profile:"$PROFILE" display_name:$DISPLAY_NAME
```

RE-SIGN AND REPACKAGE FOR ANDROID

- Re-zip all the extracted files from earlier
  - Note that assets, res, and AndroidManifest.xml are top-level files in an .apk, so be careful to zip the right files
  - This CLI command will zip all the files in the current directory into a new zip file in the parent directory:
    - zip -qr ../ems-custom-44.1.xxx.zip ./*

- Give the new zip file an .apk extension
  - e.g., myapp.zip -> myapp.apk

- Sign the new .apk file, for example:

```
#!/bin/bash


APK_TO_SIGN=$1

APK_OUTPUT=$2

EMS_APK_KEYSTORE_PATH=path/to/your/app.keystore


jarsigner -verbose \

    -sigalg $EMS_APK_SIG_ALG \
    -digestalg $EMS_APK_DIGEST_ALG \
    -storepass $EMS_APK_KEYSTORE_PASS \
    -keystore $EMS_APK_KEYSTORE_PATH \
    $APK_TO_SIGN $EMS_APK_ALIAS_NAME

zipalign 4 $APK_TO_SIGN $APK_OUTPUT
```

CHAPTER 15: Customize Your Mobile App Configuration Using config.json (Private Deployment Only)

EMS Mobile App ships with a config.json file that you can use to customize before re-signing and distributing in your app store or similar.

This topic provides information that will allow you to:

- Set the API URL so users do not have to type it in on their own.
- Configure authentication
- Find the config.json File
  - For iOS
  - For Android
- Supported Authentication Configurations
  - OpenID
  - SAML
- Change the Logging Location

FIND THE CONFIG.JSON FILE

After unzipping the respective app files, the paths to the file for each OS are:

IOS

- config.json (top-level file)

ANDROID

- assets > config.json

The file looks like the example below (subject to change, per development):

```
{
    "api_doc": [
        "Configure the API here"
    ],
    "api": {

        "url_doc": [
            "The API EMS Mobile App should connect to"
        ],
        "url": ""
    }
}
```

SET THE API URL

1. Open the **config.json** file in a text editor.
2. In the API section, find the URL property.
3. Set the URL property to your desired value (e.g., https://yourcompany.com/ems-platform-api).

CONFIGURE AUTHENTICATION

EMS Mobile App does not ship with an authentication configuration section by default, but you can add it as follows.

> **NOTE:** If you are adding authentication configuration, **it is also necessary to** set the API URL.

Below is an example (the ..._doc entries are omitted for brevity):

```
{
    "api": {
        "url": "https://yourcompany.com/ems-platform-api"
    },
    "authentication": {
        "activities": "openId",
        "openID": {
            "discoveryURL": "https://yourcompany.com/openid",
            "authorizationURL": "",
            "tokenURL": "",
            "clientID": "abcdefxabQijQcJstY4nImWYL5y12345",
            "redirectURL": "emssoftware://oauth-callback/x"
        }
    }
}
```

SUPPORTED AUTHENTICATION CONFIGURATIONS

OPEN ID

```
"authentication": {

    "activities": "openId",

    "openID": {

        "discoveryURL": "https://yourcompany.com/openid",

        "authorizationURL": "",

        "tokenURL": "",

        "clientID": "abcdefxabQijQcJstY4nImWYL5y12345",

        "redirectURL": "emssoftware://oauth-callback/x"

    }

}
```

- Set the **activities** to **openId**
- Add an **openID** section next to **activities**

PROPERTIES FOR THE OPENID SECTION

- **discoveryURL**
  - if your IdP provides it, this is the URL for EMS Mobile App to automatically configure its Open ID settings.

  - if you provide this, leave authorizationURL and tokenURL empty.

- authorizationURL
  - this is the endpoint to send the initial Open ID authorization request

- tokenURL
  - this is the endpoint to request an Open ID access token

- clientID
  - the client ID for the EMS Mobile App as configurd in the IdP

- redirectURL
  - leave this set to emssoftware://oauth-callback/x for EMS Mobile App
  - this is the URL the IdP will redirect to during the Open ID authentication flow

SAML

```
"authentication": {

    "activities": "saml",

    "saml": {

        "url": "https://yourcompany.com/ems-platform...ntication/saml`

    }

}
```

- Set the **activities** to **saml**
- Add a **saml** section next to **activities**

PROPERTIES FOR THE SAML SECTION

- URL
  - this property is optional
  - you can manually specifiy the initial request URL for SAML authentication
  - this URL will be opened in a webview in EMS Mobile App
  - if you do not specify this property, EMS Mobile App will assume the default SAML endpoint for the REST API
    - This is one reason you must specify the URL in the api section for custom authentication configuration (e.g., if you set the custom API URL to https://ems.example.com/api, then EMS Mobile App will use https://ems.example.com/api/api/v1/a...ntication/saml as its initial SAML url)

EXAMPLES

CUSTOM URL ONLY

```
{
    "api": {
        "url": "https://yourcompany.com/ems-platform-api"
    }
}
```

OPEN ID WITH DISCOVERY URL

```
{
    "api": {
        "url": "https://yourcompany.com/ems-platform-api"
    },
    "authentication": {
        "activities": "openId",
        "openID": {
            "discoveryURL": "https://yourcompany.com/openid/discovery",
            "authorizationURL": "",
            "tokenURL": "",
            "clientID": "abcdefxabQijQcJstY4nImWYL5y12345",
            "redirectURL": "emssoftware://oauth-callback/x"
        }
    }
}
```

OPEN ID WITHOUT DISCOVERY URL

```
{
    "api": {
        "url": "https://yourcompany.com/ems-platform-api"
    },
    "authentication": {
        "activities": "openId",
        "openID": {
            "discoveryURL": "",
            "authorizationURL": "https://yourcompany.com/openid/authorize",
            "tokenURL": "https://yourcompany.com/openid/token",
            "clientID": "abcdefxabQijQcJstY4nImWYL5y12345",
            "redirectURL": "emssoftware://oauth-callback/x"
        }
    }
}
```

SAML WITH DEFAULT API SAML ENDPOINT

```
{
    "api": {
        "url": "https://yourcompany.com/ems-platform-api"
    },
    "authentication": {
        "activities": "saml"
    }
}
```

SAML WITH SPECIFIC API SAML ENDPOINT

```
{
    "api": {
        "url": "https://yourcompany.com/ems-platform-api"
    },
    "authentication": {
        "activities": "saml",
        "saml": {
            "url": "https://ems.example.com/saml"
        }
    }
}
```

CHANGE LOGGING LOCATION

1. Modify the logFilePath attribute:

```
"logFilePath": ".\\LogFiles\\api.log"
```

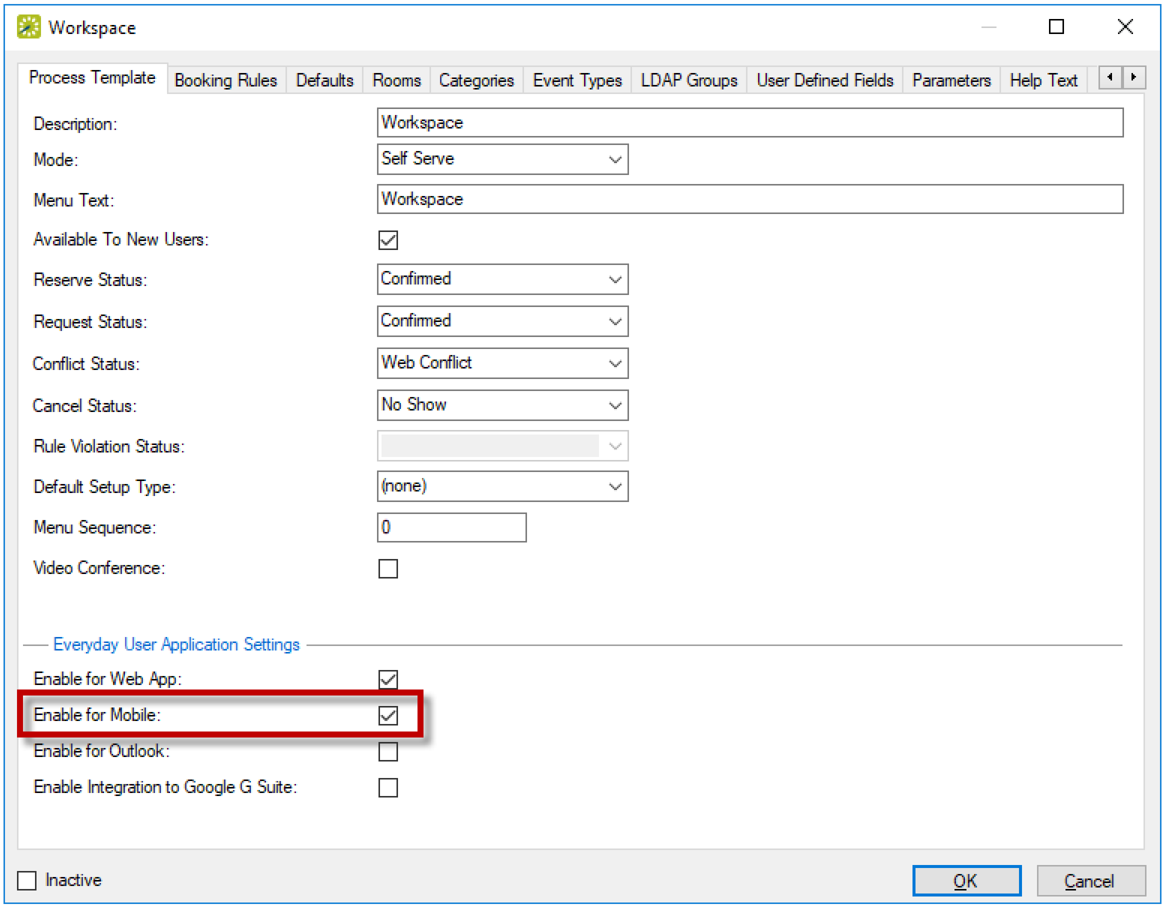
CHAPTER 16: Assign Templates to EMS Mobile App Users

EMS V44.1 allows you to select which Everyday User Process Template (e.g., "web process templates") will be enabled on your users' mobile devices.

1. In the EMS Desktop Client, navigate to **Configuration** > **Everyday User Applications** > **Everyday User Process Templates**.
2. Select the template you want to assign and click **Edit**.

> **NOTE**: If you do not yet have a process template, create one by clicking **New**.
>
> See Also: Configure Everyday User Process Templates.

3. An Everyday User Process Template dialog box will appear. Check the **Enable for Mobile** checkbox on the first tab of the template dialog box:



Description: Workspace

Mode: Self Serve

Menu Text: Workspace

Available To New Users: ☑

Reserve Status: Confirmed

Request Status: Confirmed

Conflict Status: Web Conflict

Cancel Status: No Show

Rule Violation Status:

Default Setup Type: (none)

Menu Sequence: 0

Video Conference: □

Everyday User Application Settings

Enable for Web App: ☑

Enable for Mobile: ☑

Enable for Outlook: □

Enable Integration to Google G Suite: □

□ Inactive

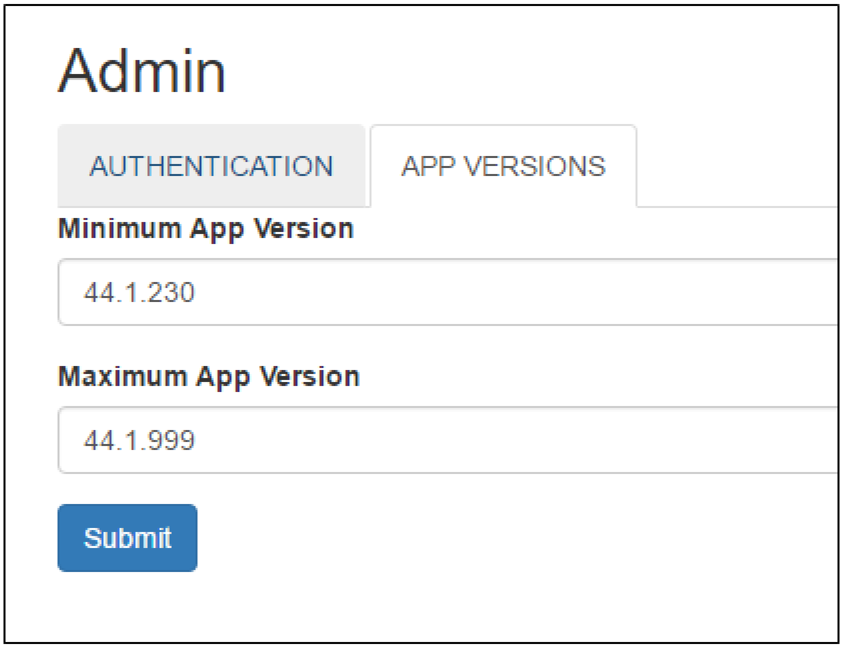
NOTE: EMS Mobile App is designed to make and edit simple reservations for users "on the go." At this time it cannot handle service requests, video conference bookings or complex workflows. Please consider this when you decide which templates should be enabled for the EMS Mobile App. Additionally, you can only change the name and icon of the EMS Mobile App through private deployment via MDM. Please refer to your MDM guide for instructions on how to change the name and icon of the EMS Mobile App.

CHAPTER 17: Restrict Users' EMS Mobile App Versions

Starting with the August 2016 release, EMS will ensure that EMS Mobile App is both forwards- and backwards-compatible, so that the EMS Mobile App will still function even if users update it on their devices. Alternatively, if you update your API but users do not update their app, functionality remains intact.

You may wish to force users to keep their installations up to date. For example, you may want them to upgrade their EMS Mobile App after you upgrade the API, or you may want to prevent them from updating their EMS Mobile App until you upgrade the API. To enforce these restrictions, follow the steps below.

1. Log in to the API admin page (previously configured here).
2. Click on **Admin** tab, and set the minimum and maximum app versions:



Admin

Minimum App Version: 44.1.230

Maximum App Version: 44.1.999

DETERMINE EMS MOBILE API AND VERSION COMPATIBILITY

Use the matrix below to determine how you want to enforce user updates.

EMS RELEASE #	MOBILE APP VERSION SHIPPED	MOBILE API VERSION	MOBILE APP MINIMUM VERSION	MOBILE APP MAXIMUM VERSION
V44.1	44.1.241	44.1.129	44.1.238	44.1.241
V44.1 Update 1	44.1.288	44.1.146	44.1.288	44.1.288
V44.1 Update 2	44.1.319	44.1.158	44.1.288	44.1.319
V44.1 Update 3	44.1.410	44.1.172.0	44.1.288	44.1.410
V44.1 Update 4	44.1.430	44.1.187.0	44.1.288	44.1.430
V44.1 Update 5	NA	NA	NA	NA
V44.1 Update 6	44.1.477	44.1.208.0	44.1.288	44.1.477
V44.1 Update 7	44.1.487	44.1.249.0	44.1.288	44.1.487

TIP: The Minimum App Version means that users running EMS Mobile App below the minimum will not be able to use EMS. Increasing this value essentially forces users on an older version to upgrade. Maximum App Version prevents users from using EMS Mobile App if they run a version above the max.

CHAPTER 18: Change the Help Link Label and URL

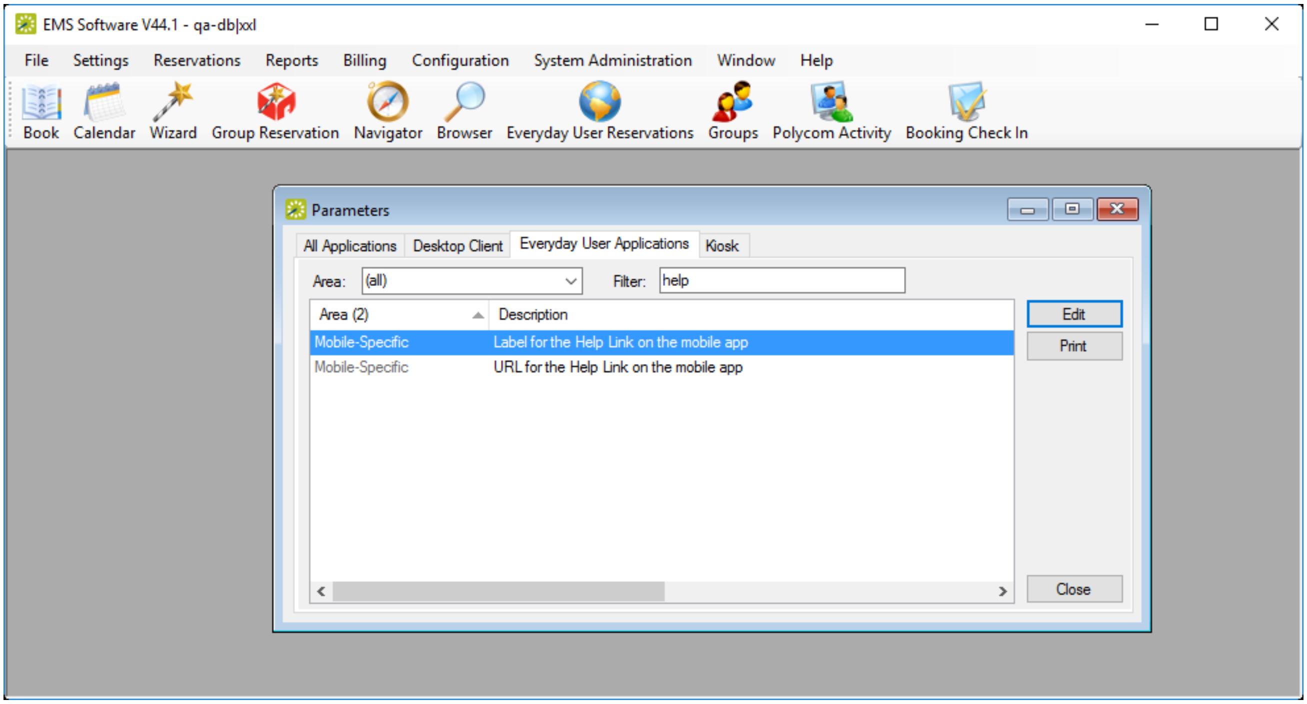
Admins can customize both the Label for the Help Link and the URL for the Help Link on the EMS Mobile App.

This topic will provide information that will allow you to:

- Change the Label for the Help Link on the EMS Mobile App
- Change the URL for the Help Link on the EMS Mobile App

CHANGE THE LABEL FOR THE HELP LINK

1. Locate the Everyday User Applications parameter, **Label for the Help Link on the mobile app.**
2. Enter a new value. See Also: EMS Mobile App Parameters.

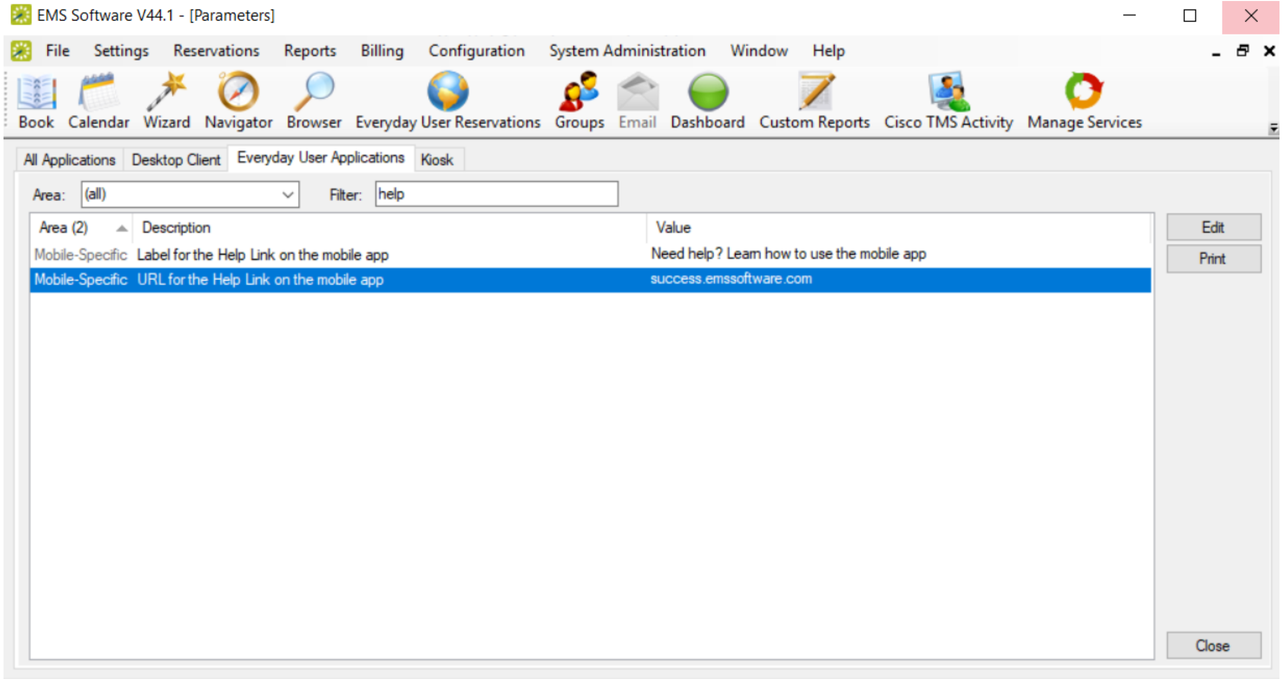


Area: (all) Filter: help

Area (2)	Description
Mobile-Specific	Label for the Help Link on the mobile app
Mobile-Specific	URL for the Help Link on the mobile app

CHANGE THE URL HELP LINK

1. Locate the parameter, **URL for the Help Link on the mobile app**.
2. Enter a new URL.



EMS Software V44.1 - [Parameters]
File Settings Reservations Reports Billing Configuration System Administration Window Help
Book Calendar Wizard Navigator Browser Everyday User Reservations Groups Email Dashboard Custom Reports Cisco TMS Activity Manage Services
All Applications Desktop Client Everyday User Applications Kiosk
Edit
Print
Close

Area: (all) Filter: help

Area (2)	Description	Value
Mobile-Specific	Label for the Help Link on the mobile app	Need help? Learn how to use the mobile app
Mobile-Specific	URL for the Help Link on the mobile app	success.emssoftware.com

CHAPTER 19: Configure EMS Mobile App QR Codes

In order to associate rooms with QR Codes, System Administrators must run and print a Room Card - QR Code report (under Hoteling) in the EMS Desktop Client. This automatically generates the codes and associates them with the designated rooms. See Also: Scan QR Codes in the EMS Mobile App and Configure and Generate Room QR Codes.

CHAPTER 20: How Do I Know When To Upgrade the EMS Mobile App and API?

DETERMINE EMS MOBILE API AND MOBILE APP VERSION COMPATIBILITY

Use the matrix below to determine how you want to enforce user updates.

EMS RELEASE #	MOBILE APP VERSION SHIPPED	MOBILE API VERSION	MOBILE APP MINIMUM VERSION	MOBILE APP MAXIMUM VERSION
V44.1	44.1.241	44.1.129	44.1.238	44.1.241
V44.1 Update 1	44.1.288	44.1.146	44.1.288	44.1.288
V44.1 Update 2	44.1.319	44.1.158	44.1.288	44.1.319
V44.1 Update 3	44.1.410	44.1.172.0	44.1.288	44.1.410

EMS RELEASE #	MOBILE APP VERSION SHIPPED	MOBILE API VERSION	MOBILE APP MINIMUM VERSION	MOBILE APP MAXIMUM VERSION
V44.1 Update 4	44.1.430	44.1.187.0	44.1.288	44.1.430
V44.1 Update 5	NA	NA	NA	NA
V44.1 Update 6	44.1.477	44.1.208.0	44.1.288	44.1.477
V44.1 Update 7	44.1.487	44.1.249.0	44.1.288	44.1.487

TIP: "***Minimum app version***" means that users running EMS Mobile App below the minimum will not be able to use EMS. Increasing this value essentially forces users on an older version to upgrade. "***Maximum app version***" prevents users from using EMS Mobile App if they run a version above the max.

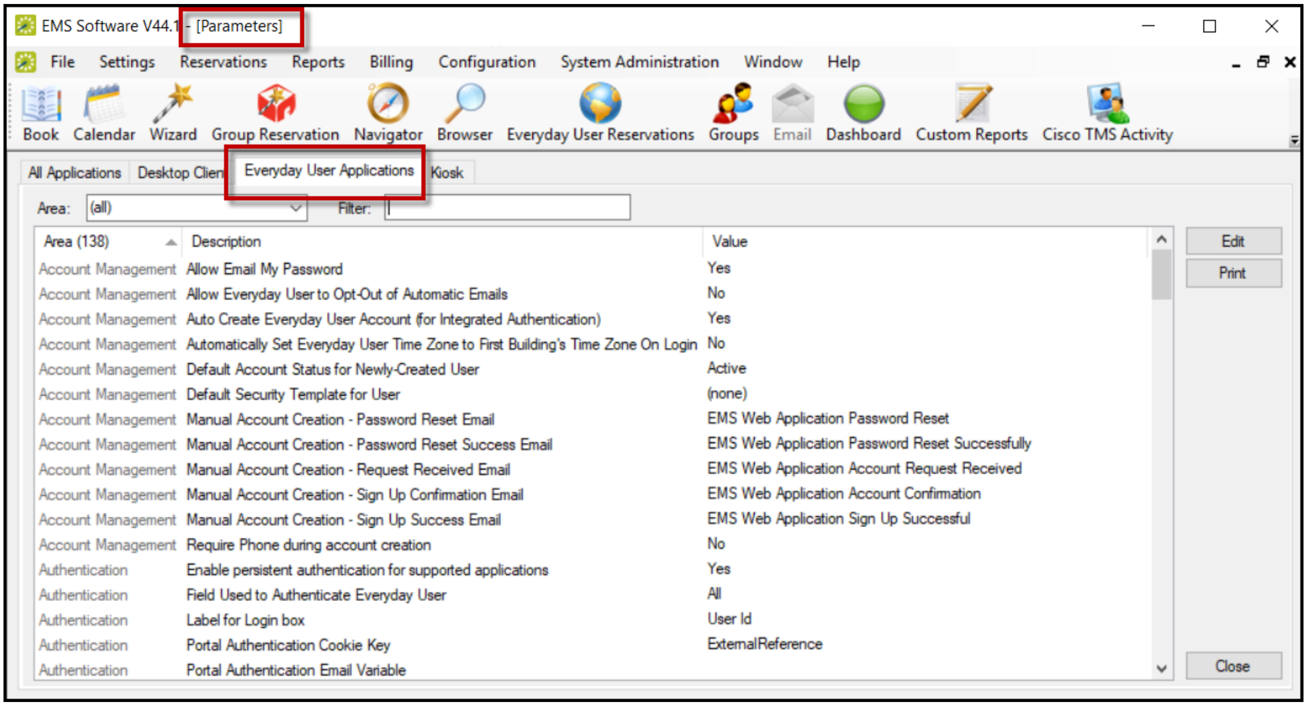
CHAPTER 21: EMS Mobile App System Parameters

Parameters for the EMS Mobile App are configured in the EMS Desktop Client.

1. To access these parameters navigate to **System Administration** > **Settings** > **Parameters** > Everyday User Applications tab.
2. Under the Area dropdown, choose **Mobile Specific**.

> **NOTE:** Parameters for Exchange Integration Web Service and LDAP can be found by navigating to **System Administration** > **Settings** > **Parameters** > Desktop Client tab.

Parameters for the EMS Mobile App



Area (138)	Description	Value
Account Management	Allow Email My Password	Yes
Account Management	Allow Everyday User to Opt-Out of Automatic Emails	No
Account Management	Auto Create Everyday User Account (for Integrated Authentication)	Yes
Account Management	Automatically Set Everyday User Time Zone to First Building's Time Zone On Login	No
Account Management	Default Account Status for Newly-Created User	Active
Account Management	Default Security Template for User	(none)
Account Management	Manual Account Creation - Password Reset Email	EMS Web Application Password Reset
Account Management	Manual Account Creation - Password Reset Success Email	EMS Web Application Password Reset Successfully
Account Management	Manual Account Creation - Request Received Email	EMS Web Application Account Request Received
Account Management	Manual Account Creation - Sign Up Confirmation Email	EMS Web Application Account Confirmation
Account Management	Manual Account Creation - Sign Up Success Email	EMS Web Application Sign Up Successful
Account Management	Require Phone during account creation	No
Authentication	Enable persistent authentication for supported applications	Yes
Authentication	Field Used to Authenticate Everyday User	All
Authentication	Label for Login box	User Id
Authentication	Portal Authentication Cookie Key	ExternalReference
Authentication	Portal Authentication Email Variable	

The table below provides the titles, descriptions, values, and examples for EMS Mobile App parameters.

AREA	TITLE	DESCRIPTION	VALUE	EXAMPLE
Mobile-Specific	Field to find rooms by when scanning QR codes	Indicates the fields you want to match rooms by Room ID, Room Code or External Refer-	Room ID, Room Code, External Reference (on room).	

AREA	TITLE	DESCRIPTION	VALUE	EXAMPLE
		ence.		
Mobile-Specific	Label for the Help Link on the Mobile App	Login to the EMS Mobile App and click on top left navigation bar. On the bottom there is a help URL. This parameter allows you to configure the label for the help link. You can also configure the URL using another parameter - URL for HELP link on the EMS Mobile App.		Login to the EMS Mobile App and click on top left navigation bar. On the bottom there is a help URL.

AREA	TITLE	DESCRIPTION	VALUE	EXAMPLE
Mobile-Specific	Maximum EMS Mobile App version that the API should allow to connect.	Maximum app version that the API will allow to connect.		
Mobile-Specific	Minimum EMS Mobile App version that the API should allow to connect.	Minimum app version that the API will allow to connect.		
Mobile-Specific	Minimum number of minutes to book via QR code or mobile Browse Location			
Mobile-Specific	Mobile check-in proximity distance			

AREA	TITLE	DESCRIPTION	VALUE	EXAMPLE
Mobile-Specific	Mobile proximity unit of measurement			
Mobile-Specific	Scans custom QR codes and interprets them as URLs.	QR Codes when scanned, can be configured to be interpreted as a URL. If the Customer's configuration requires QR codes to be scanned as a URL, this parameter should be set to YES. If set to No, QR Codes will be scanned as plain text.		
Mobile-Specific	Sets the header variable for the	EMS Mobile App supports header		See Also: Portal Authentication Methods.

AREA	TITLE	DESCRIPTION	VALUE	EXAMPLE
	EMS Mobile APIs Header Authentication Method	authentication. The value of the header variable is set on the Platform's Admin page. The same value should also be set for this parameter to make the Header Authentication work.		
Mobile-Specific	The Query String Field in QR Code URLs for looking up Rooms	If you have the parameter SCAN CUSTOM QR CODES and INTERPRETS THEM AS URLS set to YES, then this is what tells the app to look		If set to ROOMID, when it goes to the following URL: http://blah.com?romID=23921, it would use that ROOMID to look up the room based on the parameter: FIELD TO FIND ROOMS BY WHEN SCANNING QR CODES.

AREA	TITLE	DESCRIPTION	VALUE	EXAMPLE
		for in the Query string.		
Mobile-Specific	The subject for the EMS Mobile two-factor setup email	Subject of the email sent to users notifying them to go to the EMS Web App and scan their 2fa barcode.		The first time you configure 2fa (Two-Factor Authentication) you get e-mailed. This is the subject of that e-mail.
Mobile-Specific	URL for the EMS Mobile App in the app store	Setting this parameter to blank prevents the EMS Mobile App popup prompt from appearing.		
Mobile-Specific	URL for the EMS Mobile App in the play store	Setting this parameter to blank prevents the EMS Mobile App popup prompt		

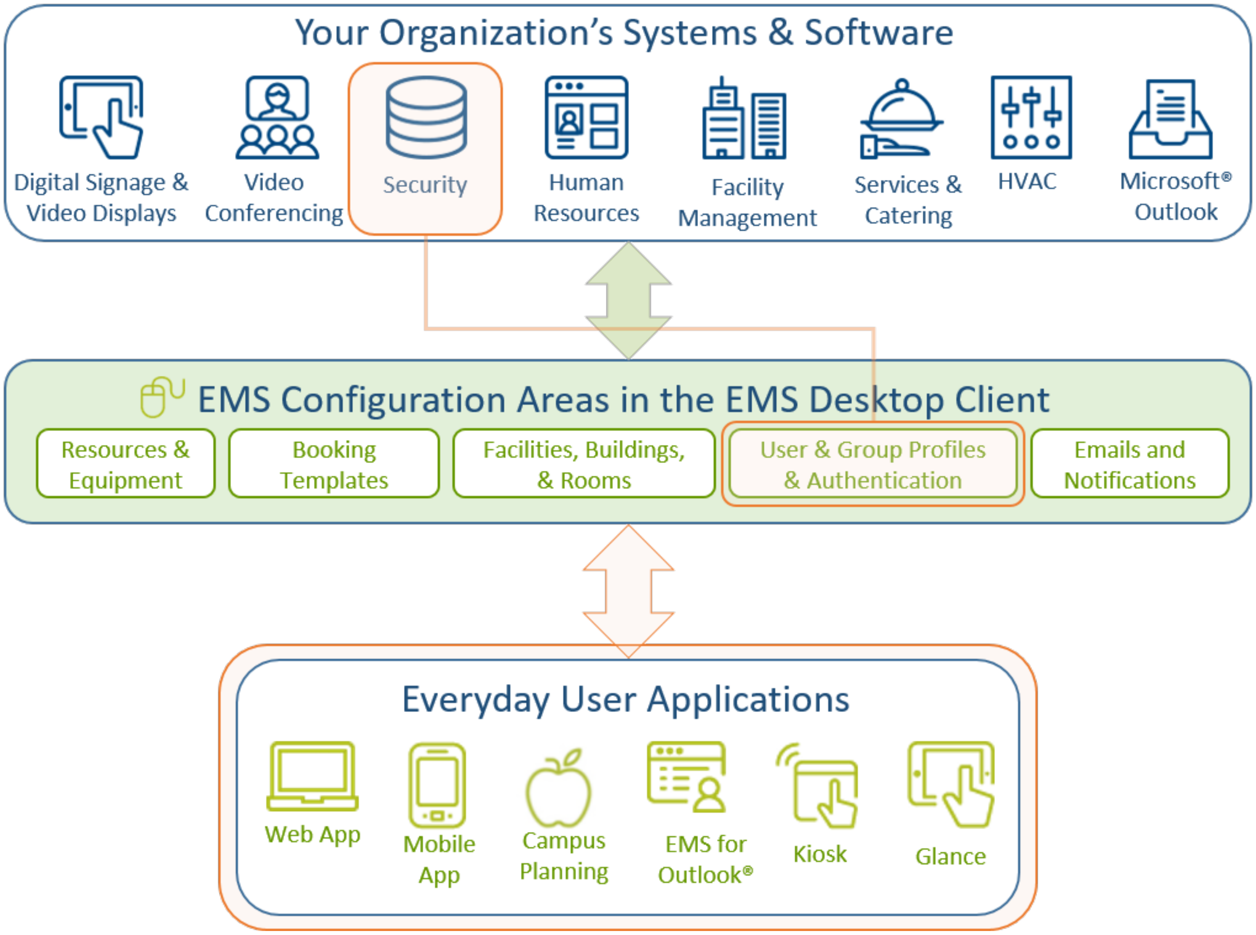
AREA	TITLE	DESCRIPTION	VALUE	EXAMPLE
		from appearing.		
Mobile-Specific	URL for the Help Link on the mobile app	Login to the EMS Mobile App and click on top left navigation bar. On the bottom there is a help URL. The URL you put here, will be the URL for the Help Link. You can also configure the Help Link Label using another parameter - URL for HELP link Label on the EMS Mobile App.		

CHAPTER 22: Introduction to EMS Integrated Authentication

The EMS Integrated Authentication component provides single-sign-on capability using Integrated Windows Authentication, your organization’s portal, or LDAP. The Integrated Authentication Setup Guide lists the steps you must take to configure these Integrated Authentication options. If you are unsure whether your organization is licensed for Integrated Authentication or you would like to learn more about it, please contact your Account Executive.

The diagram below shows how your organizations' existing security software and systems integrate with EMS software applications through configurations you set in EMS Desktop Client.

Integration Diagram



When configuring integrated authentication using this component, you can use the following methods:

- Integrated Windows Authentication
- Portal or Federated Authentication

- LDAP Authentication

WHAT IS INTEGRATED WINDOWS AUTHENTICATION?

Integrated Windows Authentication (IWA) is a built-in Microsoft Internet Information Services (IIS) authentication protocol that can be used to automatically authenticate and sign-in a user to EMS Web App. Integrated Windows Authentication works only with Internet Explorer and is best used on intranets where all clients accessing EMS Web App are within a single domain. When a domain user who is logged on to a networked PC accesses an EMS Everyday User application, such as EMS Web App, EMS Mobile App, or EMS for Outlook, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID information recorded in the **Network ID** and\or **External Reference** fields of your EMS Everyday User records. If a match exists, the Everyday User will be automatically logged in.

For a more detailed explanation of the authentication methods outlined above, see Integrated Windows Authentication.

WHAT IS PORTAL OR FEDERATED AUTHENTICATION?

The Portal Authentication method provides EMS Web App single sign-on capability using your organization’s portal (e.g., CAS, Shibboleth, SiteMinder, Plumtree, uPortal, etc.). When a user logged into your portal accesses EMS Web App, a predefined user-specific variable (e.g., email address, employee/student ID, network ID, etc.) captured by your portal/sign-on page is compared against corresponding information recorded in the **Network ID** and/or **External Reference** fields of your EMS Everyday User records. If a match exists, the Everyday User will be automatically logged-into EMS Web App.

> **NOTE:** The Field Used to Authenticate Everyday User parameter (within **System Administration** > **Settings** > **Parameters** > **Everyday User Applications** tab) is used by EMS Web App to determine which value should be used for authentication.

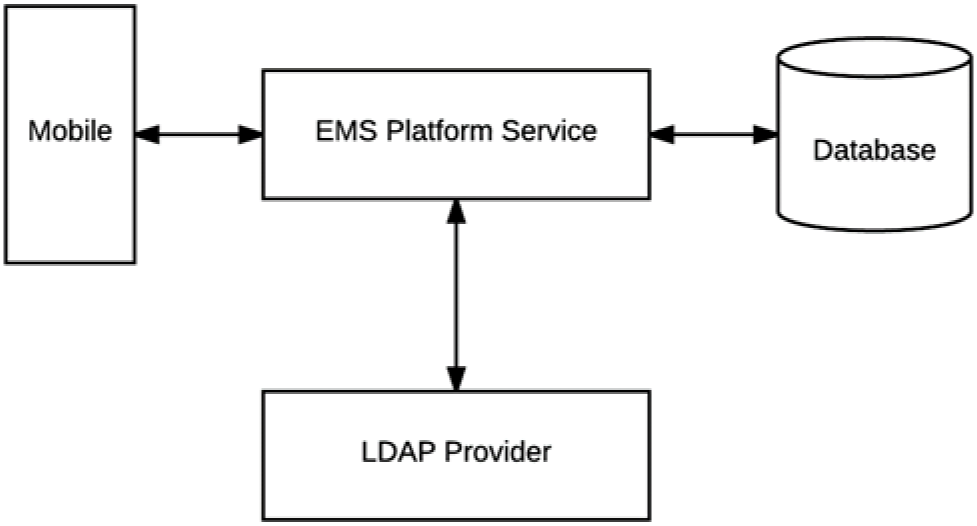
Several built-in authentication methods to pass-in credentials are available including:

- Server Variable (Header Variable)
- Session
- Form
- Cookie
- Query String
- Federated (SAML)

For a more detailed explanation of the authentication methods outlined above, see Portal Authentication Methods.

WHAT IS LDAP AUTHENTICATION?

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory information. 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 Everyday applications such as EMS Web App and EMS Mobile App.



The LDAP Authentication topic covers the following information related to LDAP configuration:

- Configure EMS Web App to Use LDAP Authentication
- Configure EMS Web App Security
- Configure Communication Options
- Core Properties
- Non-AD Config
- LDAP Queries
- Save Your Configuration
- Test Your Configuration
- Configure Authentication for EMS Mobile App

When a user logs into EMS Web App or EMS Mobile App with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the **Network ID** and/or **External Reference** fields of your EMS Everyday User records. If a match exists, the Everyday User will be logged in to the application, inheriting any Everyday User Process Template rights to which their LDAP Group has been assigned.

NOTES:

- The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.
- The Field Used to Authenticate Everyday User parameter (within **System Administration** > **Settings** > **Parameters** > **Everyday User Applications** tab) is used by the applications to determine which value should be used for authentication.

CONTACT CUSTOMER SUPPORT

- **Option 1 (Recommended):** Search the Knowledge Base available in the EMS Customer Portal.
- **Option 2:** Submit a Case directly via the EMS Customer Portal.
- **Option 3:** Email support@emssoftware.com.
- **Option 4 (Recommended for critical issues only):** Phone **(800) 288-4565.**

IMPORTANT: If you do not have a customer login, register here.

CHAPTER 23: Integrated Authentication Considerations

When you purchase the Integrated Authentication Service, you are able to use LDAP Integration, Integrated Authentication (IA), or Portal Authentication. Integrated and Portal Authentications are true Single Sign-On (SSO) solutions; LDAP is not. These methods are not typically used together. This section explains how each one works, along with pros and cons for each method.

LDAP INTEGRATION

LDAP integration allows you to bypass creating individual web users for your organization. By configuring EMS to query your LDAP groups, you can use LDAP groups to assign web template permissions. Your users would just use their windows credentials to login to the site. After creating a web user account (most data is pre-populated from their LDAP account), they receive the template permissions granted to their LDAP group.

PROS

- No need to create/maintain individual accounts for web users. Mass assign process templates.

CONS

- Requires LDAP groups to be precisely defined and maintained to ensure proper access. EMS does not create or update LDAP groups, so product may require assistance from LDAP/Exchange administrators.
- NOT Single Sign-on: users must enter windows credentials on each visit.

INTEGRATED AUTHENTICATION

IA is SSO. For this to work, every user must have a web user account created (manually through client/virtual piece or using our HRToolkit module). In each web account, a network ID is added. When a user visits VEMS or EMS Web App, a call is made to the machine to retrieve the windows account signed in. It compares that value to the network ID field in existing accounts, logging in users automatically. Permissions are assigned to the individual web user accounts.

PROS

- Can be true SSO – the account creation and maintenance can be completely invisible to the end user. Not reliant on Exchange/LDAP administrators.

CONS

- Requires active web user creation and maintenance: manually on the client side, manually through end-user input, or automatically through an HR feed.

PORTAL AUTHENTICATION

With Portal Authentication, user information is passed from your existing portal to records in EMS by cookie, session string or similar. Portal Authentication is true SSO when used with our supported methods.

NOTE: When you implement Integrated Authentication, your consultant will assist you with creating templates and web users during onsite training. If you are adding this module separately and need assistance with virtual configuration contact your account manager about purchasing training. This document is intended to explain the different authentication options available, so you can anticipate any configuration needs. If you choose LDAP Integration, you will need to create an administrator account and admin web template to access the configuration page. See the EMS Setup Guide for questions with creating that template. Using LDAP with IA or Portal Authentication requires each user be responsible for creating/verifying their account on the first visit; SSO isn’t immediate. Portal authentication can be used with LDAP, but this is atypical in most portal environments since other credentialing is available.

CHAPTER 24: Integrated Windows Authentication

Integrated Windows Authentication (IWA) is a built-in Microsoft Internet Information Services (IIS) authentication protocol that can be used to automatically authenticate and sign-in a user to EMS Web App. Integrated Windows Authentication works only with Internet Explorer and is best used on intranets where all clients accessing EMS Web App are within a single domain.

This topic provides information on the following:

- Activate Integrated Windows Authentication for IIS 6.0
- Activate Integrated Windows Authentication for IIS 7.x/8.x

> **NOTE:** Integrated Windows Authentication is supported for EMS Floor Plan (V44.1 Update 11).

See Also:

- Integrated Authentication Overview
- For more information, please review the following Microsoft TechNet articles on IWA for IIS 6.0, 7.0, and 8.0.
- Connect Your Database Using Active Directory

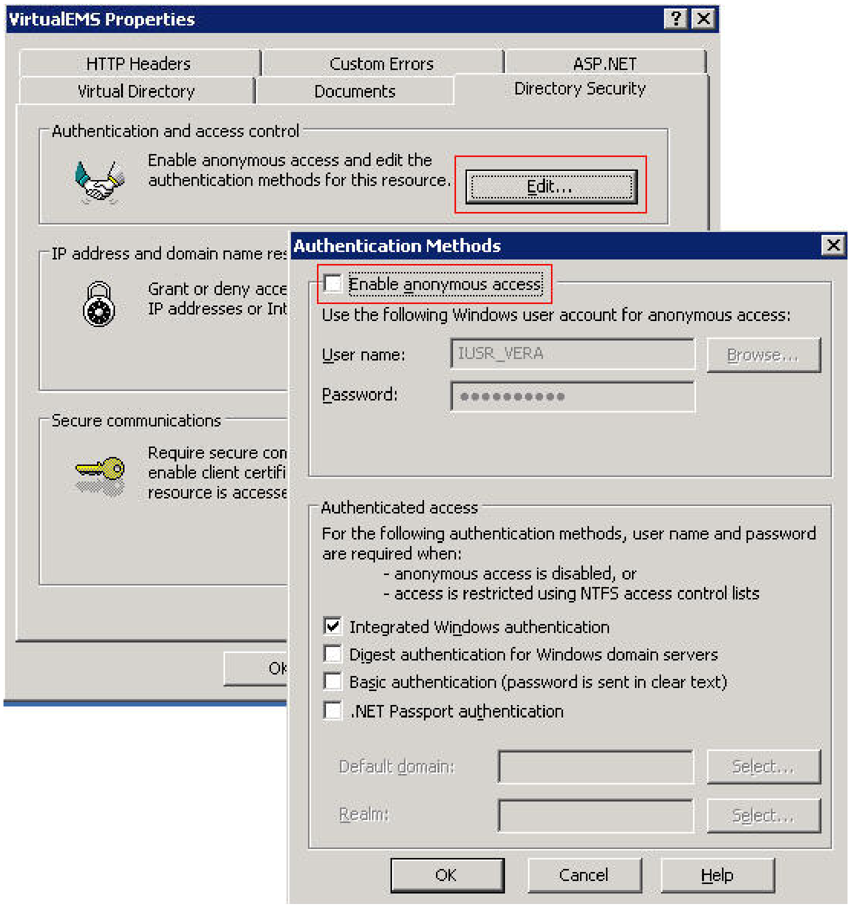
When a domain user who is logged on to a networked PC accesses an EMS Everyday User application, such as EMS Web App, EMS Mobile App, or EMS for Outlook, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID information recorded in the **Network ID** and\or **External Reference** fields of your EMS Everyday User records. If a match exists, the Everyday User will be automatically logged in.

> **NOTE:** The Field Used to Authenticate Web User parameter (within **System Administration** > **Settings** > **Parameters** > **Everyday User Applications** tab is used to determine which value should be used for authentication.

ACTIVATE INTEGRATED WINDOWS AUTHENTICATION FOR IIS 6.0

1. On the web server that hosts your EMS application's site, open **IIS Manager**.
2. Locate your EMS application's site.

3. Right-click your EMS application's site and choose **Properties**. The Properties screen will open.
4. Go to the **Directory Security** tab and click the **Edit** button under the Authentication and access control section. The Authentication Methods screen will open.
5. Uncheck the **Enable anonymous access** option. The **Integrated Windows authentication** option should be the only option checked.



VirtualEMS Properties

Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name res

Grant or deny acce
IP addresses or Int

Secure communications

Require secure con
enable client certifi
resource is accesse

Authentication Methods

□ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_VERA

Password: ●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication
□ Digest authentication for Windows domain servers
□ Basic authentication (password is sent in clear text)
□ .NET Passport authentication

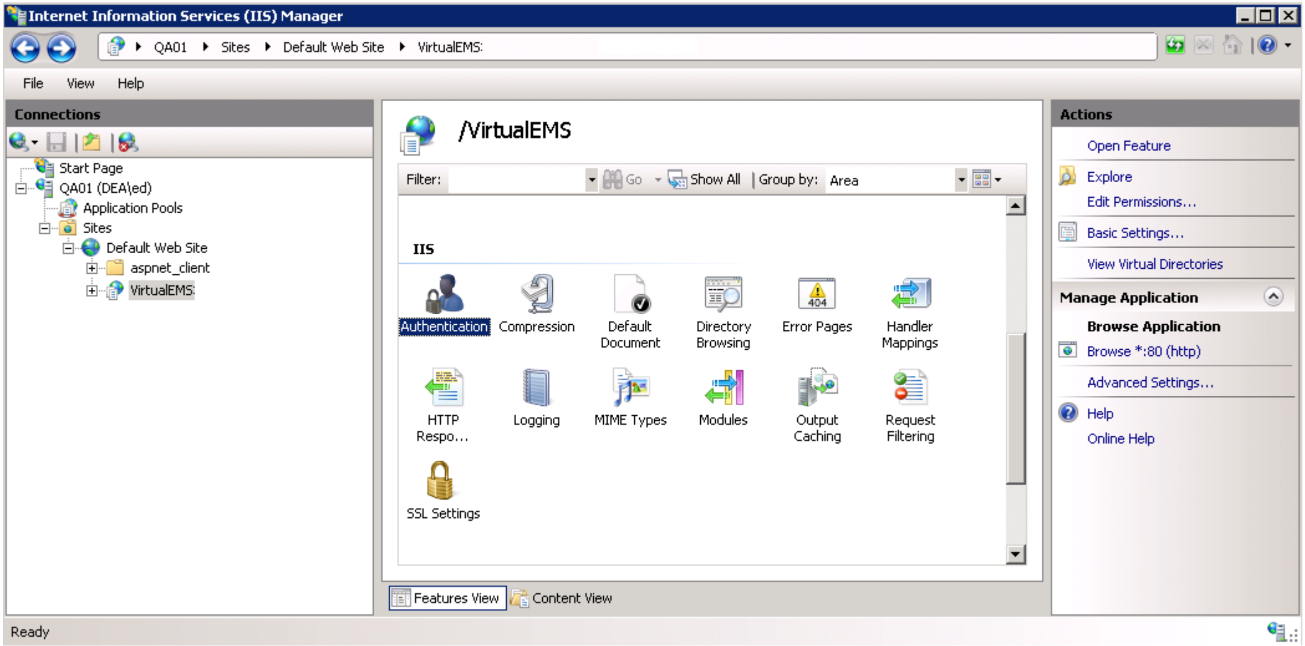
Default domain:

Realm:

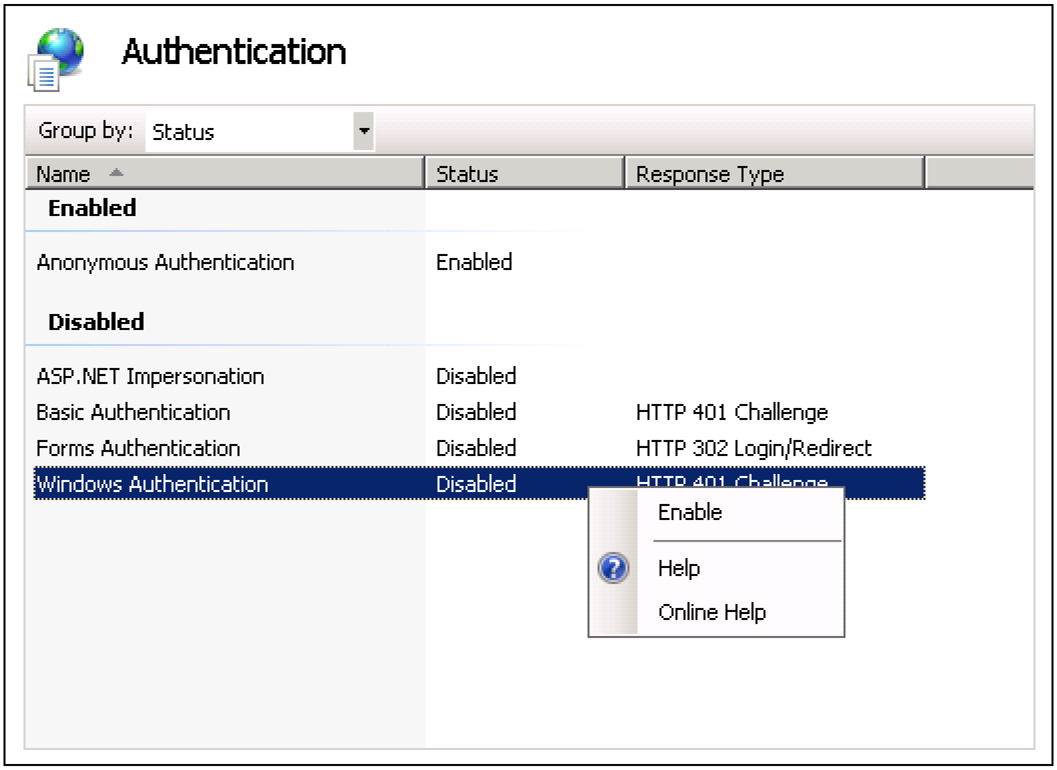
6. Click **OK** to exit the Authentication Methods screen. Click **OK** again to exit the Properties screen. You have completed the necessary IIS configuration steps for IIS 6.0.

ACTIVATE INTEGRATED WINDOWS AUTHENTICATION FOR IIS 7.X/8.X

1. On the web server that hosts your EMS application's site, open **IIS Manager**.
2. Locate and highlight your EMS application's site.



3. Double-click the **Authentication** option in the **IIS** section.



Authentication

Group by: Status

Name	Status	Response Type
Enabled		
Anonymous Authentication	Enabled	
Disabled		
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

4. Right-click the **Windows Authentication** option and select **Enable**.

5. Right-click the **Anonymous Authentication** option and select **Disable**.

6. You have completed the necessary IIS configuration steps for IIS 7.

CHAPTER 25: Manage Everyday Users For Integrated Authentication

In order to make a reservation in EMS Everyday User Applications, such as EMS Web App, EMS Mobile App, and EMS for Outlook, a user must have an active Everyday User account with appropriate security and process templates.

You can create Everyday User accounts within EMS in several ways:

- Manually Create Everyday User Accounts
- Automatically Create Everyday User Accounts
- Modify Existing Everyday User Accounts

MANUAL EVERYDAY USER ACCOUNT CREATION

Everyday User accounts can be created manually by EMS Administrators within EMS Desktop Client or by anonymous Everyday Users on their respective EMS Everyday Applications.

To create Everyday User accounts in the EMS Desktop Client, see Configure Everyday Users.

To configure EMS Web App to allow anonymous Everyday Users to request an account, you adjust parameters. See also: EMS Web App System Parameters.

> **IMPORTANT:** When manually creating an Everyday User account in an Integrated Authentication environment, you must specify a value in the Everyday User Network ID field or the External Reference field. The Field Used to Authenticate Everyday User parameter (within **System Administration** > **Settings** > **Parameters**> **Everyday User Applications** tab) is used to determine which value should be used for authentication.

AUTOMATIC EVERYDAY USER ACCOUNT CREATION

Various configuration settings are available to automatically create Everyday User records (and assign the appropriate Security and Process Template(s) if applicable) when a user accesses an EMS Everyday User Application (such as EMS Web App for the first time.

EMS WEB APP PARAMETERS

Within the Everyday User Applications parameters area of the EMS desktop client (**System Administration** > **Settings** > **Parameters**> **Everyday User**

Applications tab), the following parameters must be set accordingly:

AREA	DESCRIPTION	VALUE
Account Management	Auto Create Everyday User Account (for Integrated Authentication)	Yes
Account Management	Default Security Template for User	*Must be specified*
Account Management	Default Account Status for Newly-Created User	Active

PORTAL/FEDERATED AUTHENTICATION PARAMETERS

For organizations using Portal or Federated authentication, EMS supports a simple account provisioning strategy. When using Auto Create, EMS requires that a Everyday User account is provisioned with a name, an email address and a NetworkId (some authentication key). Otherwise, the user will be redirected to the Account Management page and be asked to manually enter the required information. In addition to the required fields, EMS also supports collecting phone, fax, and an external reference value. The parameters below are meant to help create a more complete Everyday User. The values for each of the parameters are to be determined by the information populated by your portal.

AREA	DESCRIPTION	VALUE
Authentication	Portal Authentication Email Variable	*Must be specified*

AREA	DESCRIPTION	VALUE
Authentication	Portal Authentication External Reference Variable	*Must be specified*
Authentication	Portal Authentication Fax Variable	*Must be specified*
Authentication	Portal Authentication Name Variable	*Must be specified*
Authentication	Portal Authentication Phone Variable	*Must be specified*

HR TOOLKIT (FOR EMS WORKPLACE, EMS CAMPUS, EMS ENTERPRISE, EMS DISTRICT, AND EMS LEGAL ONLY)

The HR Toolkit is an optional component that allows you to automate the creation and maintenance of Everyday User records in EMS using an outside employee data source like your HR system or another data store within your organization. Please refer to the HR Toolkit Installation Instructions for information. If you are not licensed for the HR Toolkit, but would like to learn more about it, please contact your Account Executive.

AUTOMATIC TEMPLATE ASSIGNMENT TO USERS

The Default Security Template for User parameter shown above is used to automatically assign the correct Everyday User Security Template to new Everyday User records.

You can automatically assign default Everyday User Process Templates when a new Everyday User account is created. To automatically assign a Everyday User Process Template to new Everyday Users, select the Available to New Everyday Users option within your Everyday User Process Template(s) (**Configuration** > **Everyday User Applications** > **Everyday User Process Templates** (**Edit** the template > **Process Templates** tab)).

EMS customers using the LDAP Authentication method can use an alternate method to assign a Everyday User Process Template to a Everyday User based on the LDAP Group(s) to which the user belongs. This approach can be used in addition to or in lieu of the Everyday User Process Template assignment approach discussed above. Please see the LDAP Authentication section for configuration instructions.

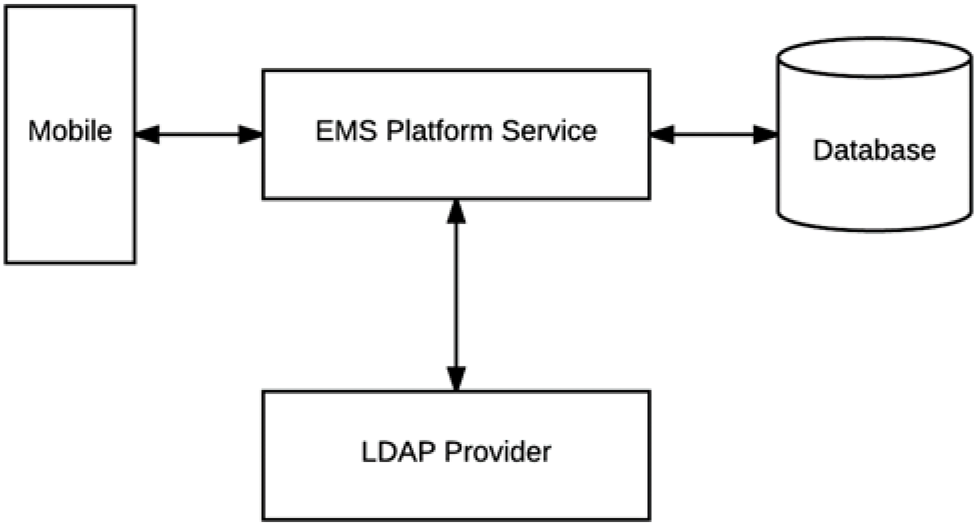
EXISTING EVERYDAY USER ACCOUNTS

> **WARNING FOR EXISTING EMS CUSTOMERS:** Before activating any Integrated Authentication option, the **Network ID** field or **External Reference** field must be populated on all existing Everyday User records. Ignoring this step may result in duplicate Everyday User records.

CHAPTER 26: LDAP Authentication

OVERVIEW

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory information. 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 Everyday applications such as EMS Web App and EMS Mobile App.



This topic provides information on the following:

- Configure EMS Web App to Use LDAP Authentication
- Configure EMS Web App Security
- Configure Communication Options
- Core Properties
- Non-AD Config
- LDAP Queries
- Save Your Configuration
- Test Your Configuration
- Configure Authentication for EMS Mobile App

When a user logs into EMS Web App or EMS Mobile App with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the **Network ID** and/or **External Reference** fields of your EMS Everyday User records. If a match exists, the Everyday User will be logged in to the application, inheriting any Everyday User Process Template rights to which their LDAP Group has been assigned.

NOTES:

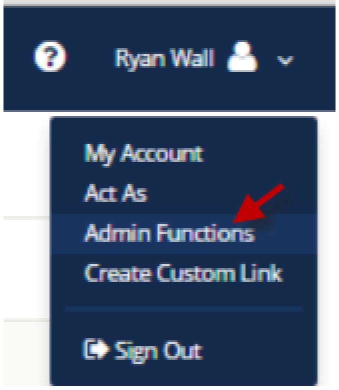
- The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.
- The Field Used to Authenticate Everyday User parameter (within **System Administration** > **Settings** > **Parameters** > **Everyday User Applications** tab) is used by the applications to determine which value should be used for authentication.

CONFIGURE EMS WEB APP TO USE LDAP AUTHENTICATION

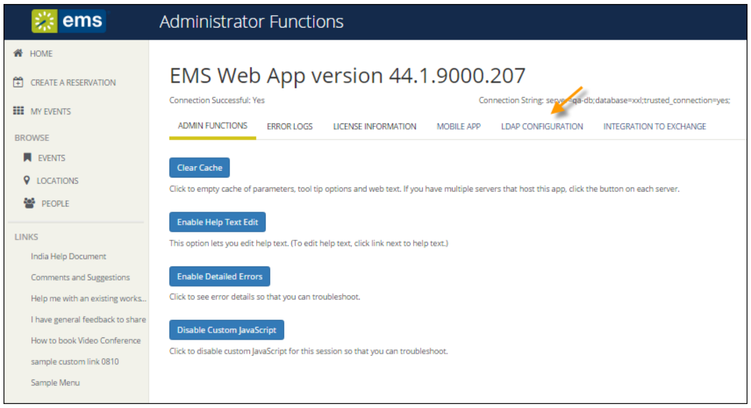
1. Log into EMS Web App with a User that belongs to an Everyday User Security Template containing the **Web Administrator** role (controlled in the EMS Desktop Client under **Configuration** > **Everyday User Applications** > **Everyday User Security Templates**).

   See Also: Configure Security Templates.

2. From the User Options, select **Admin Functions**.



3. Then click the **LDAP Configuration** tab.



Administrator Functions

EMS Web App version 44.1.9000.207

Connection Successful: Yes

Connection String: serve=qa-db;database=xxl;trusted_connection=yes;

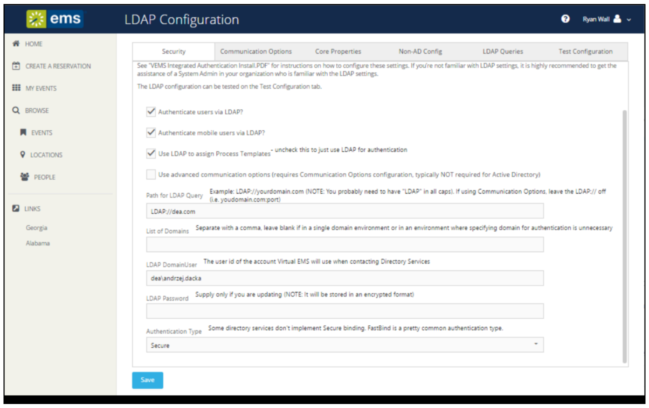
Click to empty cache of parameters, tool tip options and web text. If you have multiple servers that host this app, click the button on each server.

This option lets you edit help text. (To edit help text, click link next to help text.)

Click to see error details so that you can troubleshoot.

Click to disable custom JavaScript for this session so that you can troubleshoot.

4. The LDAP Configuration window appears, presenting multiple tabs for various settings.



See "VEMS Integrated Authentication Install.PDF" for instructions on how to configure these settings. If you're not familiar with LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

The LDAP configuration can be tested on the Test Configuration tab.

☑ Authenticate users via LDAP?

☑ Authenticate mobile users via LDAP?

☑ Use LDAP to assign Process Templates - uncheck this to just use LDAP for authentication

☐ Use advanced communication options (requires Communication Options configuration, typically NOT required for Active Directory)

Path for LDAP Query Example: LDAP://yourdomain.com (NOTE: You probably need to have "LDAP" in all caps). If using Communication Options, leave the LDAP:// off (i.e. youdomain.com:port)

LDAP://dea.com

List of Domains Separate with a comma, leave blank if in a single domain environment or in an environment where specifying domain for authentication is unnecessary

LDAP DomainUser The user id of the account Virtual EMS will use when contacting Directory Services

dea\andrzej.dacka

LDAP Password Supply only if you are updating (NOTE: It will be stored in an encrypted format)

Authentication Type Some directory services don't implement Secure binding. FastBind is a pretty common authentication type.

Secure

CONFIGURE EMS WEB APP SECURITY

1. On the **Security** tab:
    a. Select the **Authenticate users via LDAP** checkbox to enable LDAP authentication.
    b. If LDAP will be used to assign Everyday User Process Templates to your Web Users, select the **Use LDAP to assign Process Templates** checkbox.
    c. **Use advanced communication options:** Skip this step for Active Directory environments. Enabling this checkbox requires that you complete the settings on the **Communication Options** tab.
    d. In the **Path for LDAP Query** field, specify a valid LDAP path (example – LDAP://YourCompany.com)
    e. **List of Domains:** Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.

f. In the **LDAP Domain\User** field, enter a Domain User account that has rights to query LDAP (example – YourDomain\User)

g. In the **Password** field, enter a valid Password for the User Account entered in the previous step.

h. Specify the appropriate LDAP **Authentication Type** for your environment.

NOTE: The other tabs (Communication Options, Core Properties, Non-AD Config and LDAP Queries) should only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP.

CONFIGURE COMMUNICATION OPTIONS

WARNING: It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

The Communication Options tab includes fields that define how to fetch a Group or a User when sending communications from the EMS Desktop Client.

You can also set the SSL configurations, including the Security Certificate Path. Checking the **Use SSL** box will force communication to use SSL.

- **Certificate Path:** If there is a specific certification that you want to use to validate your authentication.
- **Authentication Type:** Type of authentication that your LDAP server will use during the binding process. Basic is the default because it is the most common.
- **Search Root:** The root is the level at which your search will begin.
- **User Search Filter:** Specifies the filter to use when performing the user search.

  Example: (&(objectClass=Person)(SAMAccountName={0})) or (&(objectClass-s=Person)(uid={0}))

- **Group Search Filter:** Specifies the filter to use when performing the group search.

  Example: (&(objectClass=Person)(objectClass=user))

- **Protocol Version:** Insert the current version number here. The default is 3, as the current version should be 3.

CORE PROPERTIES

> **WARNING:** It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

Indicate whether your LDAP implementation is Active Directory. These properties are set to the common defaults, but can be changed here if the LDAP properties differ from the defaults displayed.

- **LDAP Name Property:** The property for user name on the user record in LDAP that will be displayed. Displayname is the default, as it is the most common.
- **LDAP Phone Property:** The property for the phone number on the user record in LDAP that will be displayed. Telephonenumber is the default, as it is the most common.
- **Domain to append to users:** This field is unnecessary unless the domain of your user is different from the domain returned from the query.
- **Field for LDAP Group Lookup:** This identifies the EMS property that should be utilized when performing the search. For example, if you use LDAP solely to assign templates and you want the EMS Web App to look up group membership using a field other than the login name, then you must enter that field's name here.

NON-AD CONFIGURATION

> **WARNING:** It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

If your LDAP implementation is not Active Directory, use these fields to redefine the LDAP property names used when searching directory information.

- **LDAP Account/User ID Property:** The property in your LDAP store that contains the user name.

  Example: If sameaccountname=xxxx, then enter sameaccountname

- **Full LDAP User ID Format:** Leave blank unless authentication requires a full path.

  Example: cn={0},ou=staff,o=yourdomain

- **LDAP Group Category:** The property in your LDAP store that contains the group category.

Example: If filter should be objectClass=groupOfNames, then property should be groupOfNames

- **LDAP Group Name:** The property in your LDAP store that contains the group name.
- **LDAP Group Member Name:** The property in your LDAP store that contains the name of a single member in the group.

  Example: If member property is member=jdoe, then property should be member

- **LDAP Group Member User Name Attribute:** The property of the user record that corresponds to the group's member property to determine group membership.

LDAP QUERIES

> **WARNING:** It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you’re not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

These are LDAP query overrides to fetch Groups and Users from the domain. These settings rarely need to overridden, but can be used to customize queries.

- **LDAP query for security groups:** Query used to search for security groups in your LDAP store.
- **LDAP query to find users:** Query used to search for users in your LDAP store.
- **LDAP query for find users with space:** Query used to search for users that have spaces surrounding their user names in your LDAP store.

SAVE YOUR CONFIGURATION

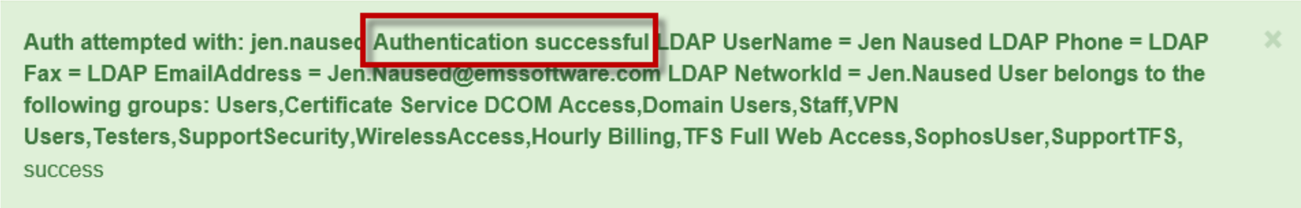
1. Click **Save**.

> **NOTE:** If you want Everyday Users to inherit Everyday User Process Templates based on the LDAP Group(s) with which they belong, see LDAP Groups Tab. Otherwise, you have completed the configuration process.

2. Within EMS Desktop Client, go to the Everyday User Process Templates area (**Configuration** > **Web** > **Everyday User Process Templates**).
3. Within an Everyday User Process Template, locate the LDAP Groups tab and select the appropriate LDAP Group(s) to map to that Everyday User Process Template.
4. Click **OK**.

TEST YOUR CONFIGURATION

1. After completing configuration, navigate to the **Test Configuration** tab in the EMS Web App under LDAP Configuration.
2. Enter your Network UserId Without Domain Name.
3. Enter your Password.
4. Click **Test**.
   a. If your configuration was successful, you will receive a message in a green box at the top that includes domain information and the words "Authentication successful" (please see example below).



```
Auth attempted with: jen.naused Authentication successful LDAP UserName = Jen Naused LDAP Phone = LDAP
Fax = LDAP EmailAddress = Jen.Naused@emssoftware.com LDAP NetworkId = Jen.Naused User belongs to the
following groups: Users,Certificate Service DCOM Access,Domain Users,Staff,VPN
Users,Testers,SupportSecurity,WirelessAccess,Hourly Billing,TFS Full Web Access,SophosUser,SupportTFS,
success
```

   b. If the configuration was unsuccessful, you will receive a prompt stating that LDAP could not be accessed. Check your logs to determine the reason for the failure.

CONFIGURE AUTHENTICATION FOR EMS MOBILE APP

1. If your organization uses EMS Mobile App, click the **Mobile App** tab.
2. Choose the LDAP option.

CHAPTER 27: Portal or Federated Authentication

This topic provides information on the following:

PORTAL AUTHENTICATION OVERVIEW

The Portal Authentication method provides EMS Web App single sign-on capability using your organization’s portal (e.g., CAS, Shibboleth, SiteMinder, Plumtree, uPortal, etc.). When a user who is logged into your portal accesses EMS Web App, a predefined user-specific variable (e.g., email address, employee/student ID, network ID, etc.) captured by your portal/sign-on page is compared against corresponding information recorded in the **Network ID** and/or **External Reference** fields of your EMS Everyday User records. If a match exists, the Everyday User will be automatically logged-into EMS Web App.

NOTE: The Field Used to Authenticate Everyday User parameter (within **System Administration** > **Settings** > **Parameters** > **Everyday User Applications** tab) is used by EMS Web App to determine which value should be used for authentication.

Several built-in authentication methods to pass-in credentials are available including:

- Server Variable (Header Variable)
- Session
- Form
- Cookie
- Query String
- Federated (SAML)

For a more detailed explanation of the authentication methods outlined above, see Portal Authentication Methods.

INSTALLATION/CONFIGURATION

1. Within the Everyday User Applications parameters area of EMS (System Administration > Settings > Parameters (Everyday User Applications tab), the following

parameters must be set accordingly:

AREA	DESCRIPTION	VALUE
Authentication	Portal Authentication Cookie Key	Required if Portal Authentication Method = Cookie
Authentication	Portal Authentication Method	Server Variable Session Form Cookie Query String
Authentication	Portal Authentication Variable	User variable to be compared against the EMS Everyday User External Reference/Network ID field

2. Direct users to the default EMS Web App page. If the default installation settings were used, the default page is:

   (http://[ServerName]/EMSWebApp/Default.aspx)

   (replace [ServerName] with the name of your web server)

REDIRECT USER LOG IN TO YOUR SSO PROVIDER

Administrators can hide the login form on the My Home page and instead, present a single **Sign In** button that links to the override URL. Open the web.-config file and locate the following code to customize the redirect:

```
<!--<add key="loginOverrideUrl" value=""/>-->
```

Additionally, you can do the same for user log out:

```
<!--<add key="logoutOverrideUrl" value=""/>-->
```

Changing the URL in these areas means that when users log in or out, they will pass through your SSO provider.

SPECIFY A DIFFERENT DEFAULT HOME PAGE FOR GUEST USERS

Additionally, you can now specify a different site home page for unauthenticated users.

CHAPTER 28: Portal Authentication Methods

This topic provides information about the following:

NOTE: EMS applications do not natively support SAML. You must use our Portal Authentication to use SAML.

SERVER VARIABLE METHOD (HEADER VARIABLE)

Server Variable/Header Variable is a collection of variables that are set by Internet Information Server (IIS).

Applications like SiteMinder create custom server variables for portal site use.

Set the **Portal Authentication Method** parameter to Server Variable and type the appropriate variable for the **Portal Authentication Variable** parameter. Direct users to your EMS Web App Default.aspx page.

SERVER VARIABLE METHOD - FEDERATED (SAML)

> **NOTE:** As of Update 23 (March 2018), SAML authentication for the EMS Web App is supported through EMS Platform Services. This is now the recommended method for configuring SAML. See Also: SAML Authentication.

SAML can be leveraged for authentication with your EMS applications by leveraging our portal authentication method and a service provider of your choosing.

METHOD 1: LOCALLY INSTALLED SERVICE PROVIDER

Using this method, you install a service provider of choice on the webserver hosting the EMS web applications. All traffic is routed through that service provider (typically via an ISAPI filter). This service provider will manage all of the authentication for the user. Once the user has successfully authenticated, it will pass an identifier for the user to the EMS application using one of our portal methods. In this scenario typically the Server Variable (Header) method is used.

METHOD 1 CONFIGURATION STEPS

1. Install and configure a service provider on the EMS web server
2. Set the service provider to protect the specified EMS web applications
3. Configure the service provider to pass the required user attributes
4. In EMS Desktop Client, configure the EMS Web App parameter "Portal Authentication Method"
5. In EMS Desktop Client configure the applicable Portal Authentication Variables.

METHOD 2

This method can be common if there is already a server configured with a service provider in your environment, handling authentication for other applications. In EMS Desktop Client, you can configure your application to re-direct any login requests to the other server to be authenticated. Once the user is authenticated, the server with your service provider installed sends the user back to the EMS Desktop Client with an identifier for the user in the header, or within a cookie. The EMS application reads this header, or cookie value, and leverages portal authentication to sign the user in with the matched credentials.

METHOD 2 CONFIGURATION STEPS

1. Install and configure a service provider on the EMS web server
2. Set the service provider to protect the specified EMS web applications
3. Configure the service provider to pass the required user attributes
4. In EMS Desktop Client configure the EMS Web App parameter “Portal Authentication Method”
5. In EMS EMS Desktop Client, configure the applicable Portal Authentication Variables.
6. In EMS EMS Desktop Client, change the Login URL under **Configuration** > **Everyday User Applications** > **Web App Menus**.
    a. Select **Login.aspx**and click **Edit**
    b. Enter in the URL to your Remote Service Provider
7. Configure your remote Service provider to send the user back to the default.aspx page of the web application that the request originated from.

EMS DESKTOP CLIENT CONFIGURATION

Please reference our Portal Authentication section for further details around the configuration required within EMS. There are a number of different options available. You will need to know the method that the user identifying value will be passed and the name of that value. Other values can also be passed (ie: email address and phone number) to aid in automatic web user account provisioning as well.

SESSION METHOD

A session is a way to provide/maintain user state information in an inherently stateless environment. It provides access to a session-wide cache you can use to store information.

In order to use the session method, set the Portal Authentication Method parameter to **Session** and type the appropriate variable for the Portal Authentication Variable parameter. Then you must create an asp.net web page and name it with the .aspx extension similar to the example below. The asp.net web page created must be copied into the EMS Web App root web directory. It must be copied there in order for EMS Web App to read the session variable.

You will need to pass through the user’s email address or external reference to your asp.net web page.

Code example in vb.net:

```
<%@ Import Namespace="System" %>

<script runat="server" language="vb">

    Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)

        Session.Item("EMS Web AppSession") = "test@emssoftware.com"

        Response.Redirect("Default.aspx")

    End Sub

</script>
```

FORM METHOD

Forms enable client-side users to submit data to a server in a standardized format via HTML. The creator of a form designs the form to collect the required data using a variety of controls, such as INPUT or SELECT. Users viewing the form fill in the data and then click Submit to send the data to the server.

To use the form method, set the Portal Authentication Method parameter to **Form** and type the appropriate variable for the Portal Authentication Variable parameter. To create portals through a form, create a web page with a form similar to below. Once the user logs on through the portal, the form below can be submitted to log the user on to EMS Web App.

Code example in HTML:

```
        <Form name="form1" method="Post" action=" http://[ServerName]/EMSWebApp/Default.aspx ">

                <input type="hidden" id="EMS Web AppFORM" name="EMS Web AppFORM" value="test@emssoftware.com>

                <input type="submit" value="submit">

</form>
```

COOKIE METHOD

A cookie is a small piece of information stored by the browser. Each cookie is stored in a name/value pair called a crumb–that is, if the cookie name is "id" and you want to save the id's value as "this", the cookie would be saved as id=this.

You can store up to 20 name/value pairs in a cookie, and the cookie is always returned as a string of all the cookies that apply to the page. This means that you must parse the string returned to find the values of individual cookies. Cookies accumulate each time the property is set. If you try to set more than one cookie with a single call to the property, only the first cookie in the list will be retained.

To use the cookie method, set the Portal Authentication Method parameter to **Cookie** and type the appropriate variable for the Portal Authentication Cookie Key parameter. Then create a web page with code similar to below. Once the user logs on through the portal, take their user logon information and create a cookie. After the cookie is created send the user to your EMS Web App Default.aspx page.

Code example in Active Server Pages 2.0:

```
<%@LANGUAGE="VBSCRIPT" %>
```

```
<%

        Response.Expires = -1

        Response.Cookies("EMS Web AppCookie")("CookVal") = "test@ems-software.com"

        Response.Cookies("EMS Web AppCookie").Path = "/"

        Response.Cookies("EMS Web AppCookie").Expires = DateAdd("m", 3, Now)

        Response.Redirect("http://[ServerName]/ EMSWebApp/Default.aspx ")

%>
```

QUERY STRING METHOD

A query string is information appended to the end of a page's URL. An example using portal authentication is below.

Code example:

http://[ServerName]/ EMSWebApp/Default.aspx?MCQS=test@emssoftware.com

To use the query string method, set the Portal Authentication Method parameter to **Query String** and type the appropriate variable for the Portal Authentication Variable parameter.

CHAPTER 29: Authentication Options for EMS Mobile

System Administrators only need to have administrative privileges to EMS Desktop Client (including EMS Web App settings) in order to control setup for the EMS Mobile App. All settings for EMS Web App also control booking behavior and "Everyday User" access and booking templates in EMS Mobile App.

See Also:

- EMS Mobile App System Parameters
- Configuring QR Codes
- Setting Up EMS Web App
- EMS Mobile App Requirements
- Installing EMS Mobile App