
Getting Started: Configure the Odyssey Integration

This guide explains how to integrate Tyler Tech Odyssey with eCourtDate to automate retrieval of the necessary information to send defendants reminders about upcoming hearings.

Before you begin

If you are an Odyssey administrator or IT user with access to the Odyssey instance, verify the following:

- Your organization has the required API Toolkit/Integration Toolkit.
- The TranslationBridge External Service is enabled.
- An HTTPS endpoint is available and reachable from eCourtDate.
- You can create a dedicated Enterprise Justice User.
- You have permission to configure API Message Security.

If you are a non-technical user, we recommend requesting an IT user or your Tyler Account Manager for assistance.

1. Create an Enterprise Justice User

Create a dedicated Enterprise Justice User for eCourtDate. This is the user the integration will rely on. No rights/roles should be defined, as this user only exists for API calls.

Configuration Path: Configure>System>Security>Users>Odyssey Users

Record these values:

- Username
- Password

-
- UserID

The Username and UserID are different:

- The Username and Password authenticate the API request.
- The UserID identifies the user within each Odyssey API transaction.
- Use a dedicated API user instead of a staff member's account. Do not grant broad ordinary user roles unless required by Tyler or your organization's security policy.

2. Configure API Message Security

In Odyssey Administration, authorize the eCourtDate service user for each required message. Menu names and steps may vary by Odyssey/Enterprise Justice release.

Configuration Path:

Configure>Integrations>Codes>TranslationBridge>APIMessageSecurityConfigurations>System

Grant access to the following message types:

- GetOdysseyReleaseLevel
- FindHearings
- LoadCase
- LoadParty
- LoadCourtSession

These messages allow eCourtDate to retrieve hearings, cases, defendants, contact information, and court-session details.

3. Collect the Odyssey environment information

Collect these values separately for Test and Production:

- TranslationBridge External Service endpoint

The standard endpoint format is:

`https://[ClientExternalServer]/ExternalWebService/TranslationBridgeExternalService.asmx`

Enterprise Justice User credentials

Provide:

- ☐ Username
- ☐ Password
- ☐ UserID
- ☐ Endpoint
- ☐ Environment
- ☐ Provide the exact SystemEnvironment value for the environment.
- ☐ (Optional) NodeIDs

Test and Production normally have different System Environment values.

Search NodeIDs

Provide the Odyssey NodeID for every court node whose hearings should be synchronized.

Example:

100, 200, 300

At least one NodeID is required. The integration will not synchronize hearings until one or more valid, authorized NodeIDs are configured.

4. Configuration example

Environment: Test

TranslationBridge server:

<https://odyssey-test.example.gov>

TranslationBridge endpoint:

/ExternalWebService/TranslationBridgeExternalService.asmx

Enterprise Justice Username:

svc_ecourtdate

Enterprise Justice Password:

[provided securely]

Odyssey UserID:

1000

System Environment:

ODYSSEYTEST

Search NodeIDs:

100, 200

5. Validate the integration

After configuration, eCourtDate will:

- Connect to the TranslationBridge External Service.
- Authenticate using the Enterprise Justice User.
- Run *FindHearings* for the configured Search NodeIDs.
- Run *LoadCase* to retrieve case parties.
- Run *LoadParty* to retrieve phone numbers and email addresses.
- Run *LoadCourtSession* to retrieve session details.
- Import the resulting hearings and associated defendants into the Test agency.

Verify that:

- Expected hearings are returned.
- Only the intended NodeIDs are included.
- Case numbers and hearing details are correct.
- Defendant names and contact information are available.
- Cancelled or deleted hearings are handled correctly.
- Virtual session information is interpreted correctly.
- After Test validation is complete, repeat the configuration using the Production endpoint and credentials.

Frequently Asked Questions

Is the Username the same as the UserID?

No. The Username and Password authenticate the request. The UserID is Odyssey's internal identifier and is included in each API transaction.

Should we use an existing Odyssey user?

A dedicated Enterprise Justice User is recommended. This provides cleaner auditing, safer password rotation, and easier troubleshooting.

What is the System Environment?

SystemEnvironment identifies the Odyssey environment receiving the API request. Your Odyssey administrator should provide the exact values.

What is a NodeID?

A NodeID identifies an Odyssey court node. Provide every Search NodeID whose hearings should be synchronized.

If no Search NodeIDs are provided, eCourtDate attempts to request all nodes available to the Enterprise Justice User. If that request fails, the Odyssey administrator must provide at least one valid NodeID.

What happens if no Search NodeIDs are provided?

The integration requests hearings from all nodes available to the Enterprise Justice User. Explicit NodeIDs are recommended to prevent unintended hearings from being imported.

Do Test and Production require separate credentials?

Yes. Each environment should have a different endpoint, Username, Password, UserID, System Environment, and set of NodeIDs.

We recommend configuring the Test credentials with the staging eCourtDate agency.

All configuration and testing should be done in a test environment before configuring and deploying to a production environment.

Which API messages must be authorized?

The standard synchronization requires:

- FindHearings
- LoadCase
- LoadParty
- LoadCourtSession

Why can a connection test succeed while synchronization fails?

A connection test can confirm that the endpoint, Username, and Password work while synchronization still fails because of:

- An incorrect UserID

-
- An incorrect System Environment
 - Missing API Message Security permissions
 - Invalid or unauthorized NodeIDs
 - Network timeouts
 - Odyssey schema or configuration errors

Does the endpoint need to be publicly accessible?

It must be reachable from eCourtDate over HTTPS. If access is restricted by a firewall, VPN, or IP allowlist, coordinate network access with eCourtDate support.

What information does the integration retrieve?

Depending on the available Odyssey data, the integration retrieves:

- Hearings and court sessions
- Cases and case numbers
- Defendant parties
- Phone numbers and email addresses
- Hearing dates and times
- Locations and judges
- Hearing statuses
- Session types and descriptions

Are an API Key, API Secret, or API Version required?

No. Those values are not used by the current integration.

What happens when the Enterprise Justice Password changes?

The credentials stored in eCourtDate must be updated immediately. API requests will fail until the stored Password matches the current Enterprise Justice User Password.

How should credentials be shared?

Use the secure credential-sharing method provided by eCourtDate. Never place Production passwords in support tickets or ordinary email.